

# **Dell Wyse Management Suite**

Version 2.x Quick Start Guide



## Notes, cautions, and warnings

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

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

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

© 2020 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

# Contents

<b>1 Introduction.....</b>	<b>5</b>
<b>2 Getting started with Wyse Management Suite.....</b>	<b>6</b>
Log in to Wyse Management Suite on public cloud.....	6
Prerequisites to deploy Wyse Management Suite on the private cloud.....	7
<b>3 Installing Wyse Management Suite on private cloud.....</b>	<b>8</b>
Logging in to Wyse Management Suite.....	15
Functional areas of management console.....	15
Configuring and managing thin clients.....	15
Creating policy group and updating configuration.....	16
Registering new thin client.....	17
Registering ThinOS device manually.....	17
Registering devices by using DHCP option tags.....	19
Registering devices by using DNS SRV record.....	19
<b>4 Deploying applications to thin clients.....</b>	<b>21</b>
Uploading and deploying ThinOS firmware image inventory.....	21
Creating and deploying standard application policy to thin clients.....	21
<b>5 Uninstalling Wyse Management Suite.....</b>	<b>23</b>
<b>6 Troubleshooting Wyse Management Suite.....</b>	<b>24</b>
<b>7 Wyse Device Agent.....</b>	<b>26</b>
<b>8 Additional resources.....</b>	<b>27</b>
<b>A Remote database.....</b>	<b>28</b>
Configure Mongo database.....	28
Configure Maria database.....	29
<b>B Custom installation.....</b>	<b>30</b>
<b>C Wyse Management Suite feature matrix.....</b>	<b>34</b>
<b>D Access Wyse Management Suite file repository.....</b>	<b>36</b>
<b>E Create and configure DHCP option tags.....</b>	<b>37</b>
<b>F Create and configure DNS SRV records.....</b>	<b>43</b>
<b>G Creating and deploying advanced application policy to thin clients.....</b>	<b>50</b>

<b>H Registering Windows Embedded Standard device manually.....</b>	<b>51</b>
<b>I Register ThinOS 8.x device manually.....</b>	<b>52</b>
<b>J Register ThinOS 9.x device manually.....</b>	<b>53</b>
<b>K Registering Linux device manually.....</b>	<b>54</b>
<b>L Terms and definitions.....</b>	<b>55</b>

# Introduction

Wyse Management Suite is the next generation management solution that lets you centrally configure, monitor, manage, and optimize your Dell Wyse thin clients. The new Suite makes it easier to deploy and manage thin clients with high functionality and performance, and ease of use. It also offers advanced feature options such as cloud versus on-premises deployment, manage-from-anywhere 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, monitoring, alerts, reporting, and troubleshooting of endpoints.

## Editions

Wyse Management Suite is available in the following editions:

- **Standard (Free)**—The standard edition of the Wyse Management Suite is only available for an on-premise deployment. You do not require a license key to use the standard edition. The standard edition is suitable for small and medium businesses.
- **Pro (Paid)**—The pro edition of the Wyse Management Suite is available for both private and public cloud deployment. The pro edition uses subscription-based licensing and requires a license key. With the Pro solution, organizations are able to adopt a hybrid model and float your licenses between on-premises and cloud. The pro on-premise edition is suitable for small, medium, and large businesses. For a cloud deployment, the pro edition can manage your devices on non-corporate networks (home office, third party, partners, mobile thin clients, and so on). The pro edition of the Wyse Management Suite also provides:
  - A mobile application to view critical alerts, notifications, and send commands in real time
  - Enhanced security through two-factor authentication and active directory authentication for role-based administration
  - Advanced app policy and reporting

### NOTE:

- **Cloud services are hosted in the US and Germany. Customers in countries with data residency restrictions may not be able to take advantage of the Wyse management Suite pro cloud based service.**
- **The on-premise version of the Wyse management pro edition is a better solution for customers with data residency restrictions.**

For more information on the features supported in standard and pro editions, see the [Feature matrix](#).

# Getting started with Wyse Management Suite

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

## Topics:

- [Log in to Wyse Management Suite on public cloud](#)
- [Prerequisites to deploy Wyse Management Suite on the private cloud](#)

## Log in to Wyse Management Suite on public cloud

To log in to the Wyse Management Suite console, you must have a supported web browser that is installed on your system. To log in to the Wyse Management Suite console, do the following:

1. Access the public cloud (SaaS) edition of the Wyse Management Suite by using one of the following links:
  - **US data center**—[us1.wysemanagementsuite.com/ccm-web](https://us1.wysemanagementsuite.com/ccm-web)
  - **EU data center**—[eu1.wysemanagementsuite.com/ccm-web](https://eu1.wysemanagementsuite.com/ccm-web)
2. Enter your username and password.
3. Click **Sign In**.

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

**NOTE:** You receive your login credentials when you sign up for the Wyse Management Suite trial on [www.wysemanagementsuite.com](https://www.wysemanagementsuite.com) or when you purchase your subscription. You can purchase the Wyse Management Suite subscription from the Dell Sales team or from your local Dell partner. For more details, see [www.wysemanagementsuite.com](https://www.wysemanagementsuite.com).

**NOTE:** An externally accessible repository must be installed on a server with a DMZ while using the pro edition of Wyse Management Suite on the public cloud. Also, the Fully Qualified Domain Name (FQDN) of the server must be registered in the public DNS.

## Change your password

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

**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.

## Log out of Wyse Management Suite

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

# Prerequisites to deploy Wyse Management Suite on the private cloud

Table 1. Prerequisites

Description	10000 devices or less	50,000 devices or less	120,000 devices or less	Wyse Management Suite – Software repository
Operating system	Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 Supported language pack—English, French, Italian, German, Spanish, Japanese, and Chinese (preview release)			
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	<p>The Wyse Management Suite installer adds Transmission Control Protocol (TCP) ports 443, 8080, and 1883 to the firewall exception list. The ports are added to access the Wyse Management Suite console and to send push notifications to the thin clients.</p> <ul style="list-style-type: none"> <li>TCP 443—HTTPS communication</li> <li>TCP 1883—MQTT communication</li> <li>TCP 3306—MariaDB (optional if remote)</li> <li>TCP 27017—MongoDB (optional if remote)</li> <li>TCP 11211—Memcached</li> <li>TCP 5172, 49159—End-User Management Software Development Kit (EMSDK)—optional and required only to manage Teradici devices</li> </ul> <p>The default ports that are used by the installer may be changed to an alternative port during installation.</p>			The Wyse Management Suite repository installer adds TCP ports 443 and 8080 to the firewall exception list. The ports are added to access the operating system images and application images that are managed by Wyse Management Suite.
Supported browsers	<p>Internet Explorer version 11</p> <p>Google Chrome version 58.0 and later</p> <p>Mozilla Firefox version 52.0 and later</p> <p>Edge browser on Windows—English only</p>			

- 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 will be 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. For more information, see [Accessing file repository](#).

# Installing Wyse Management Suite on private cloud

To set up the Wyse Management Suite on a private cloud, the following requirements must be met:

- Obtain and configure all the required hardware and software. You can download the Wyse Management Suite software from [downloads.dell.com/wyse/wms](https://downloads.dell.com/wyse/wms).
- Install a supported server operating system on one or more server machines.
- Ensure that the systems are up-to-date with current Microsoft service packs, patches, and updates.
- Ensure that the latest version of the supported browser is installed.
- Obtain administrator rights and credentials on all systems that are involved with the installations.
- For the Pro features, obtain a valid Wyse Management Suite license. Standard edition does not require a license.

A simple installation of Wyse Management Suite consists of the following:

- Wyse Management Suite server (includes repository for application and operating system images)
- Optional—Additional Wyse Management Suite repository servers (repositories for additional images, applications, and AD authentication)
- Optional—HTTPS certificate from a Certificate Authority such as [www.geotrust.com/](https://www.geotrust.com/).

To install the Wyse Management Suite on a private cloud, do the following:

1. Double-click the installer package.
2. On the **Welcome** screen, read the license agreement and click **Next**.
3. On the **Setup Type** page, select the components that you want to install, and click **Next**. The available options are:
  - Wyse Management Suite—There are two setup types available for Wyse Management Suite components.
    - Typical—Requires minimum user interaction and installs embedded databases.
    - Custom—Requires maximum user interactions and is recommended for advanced users. For more information, see [Custom installation](#).
  - Teradici EM SDK—Teradici EM SDK components are installed as a service.

**NOTE:** A notification window is displayed, when the Internet Explorer Enhanced Security Configuration feature is enabled. To disable this feature, select the Turn off IE Enhanced Security Configuration check box on the Setup Type page.

If EM SDK is installed on the server along with Wyse Management Suite from a previous installation, the Teradici EM SDK components are updated automatically.

4. Select **Typical** as the **Setup Type**. Enter the new **Database Credentials** for the embedded databases. Also, enter the new **Administrator Credentials** and click **Next**.

**NOTE:** The administrator credentials are required to log in to the Wyse Management Suite web console after the installation.

5. On the **Configuration** page, configure the shared folder and access rights for the CIFS user. The available options are:
  - Use an Existing user—Select this option to validate credentials for the existing user.
  - Create a New user—Select this option and enter the credentials to create a new user.

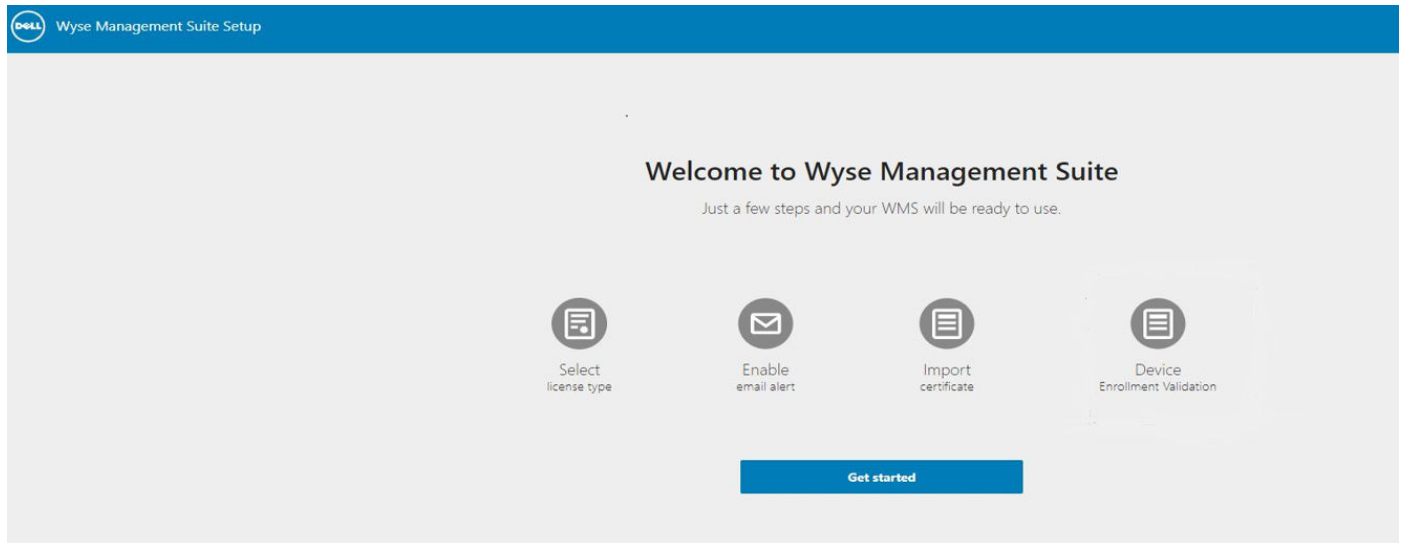
**NOTE:** If the Teradici EM SDK option is enabled on the Setup Type page, you can configure the port for the Teradici server on the Configuration page.

6. Select a path to install the software, and the path to install the local tenant file repository, and then click **Next**.  
The default path of the destination folder to install the software is C:\Program Files\DELL\WMS.
7. Click **Next**.  
The **Pre-Installation Summary** page is displayed.
8. Click **Next** to install the software.



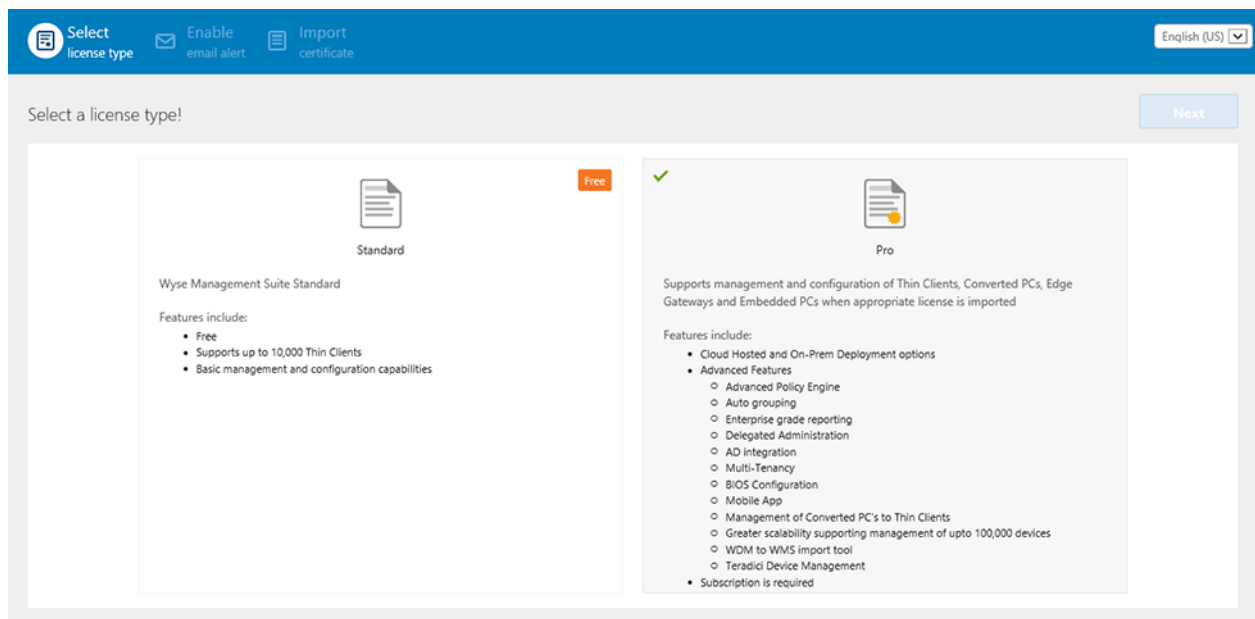
The installer takes approximately 4–5 minutes to complete the installation. However, it may take longer if dependent components such as VC-runtime are not installed on the system.

9. Click **Launch** to open the Wyse Management Suite web console.
10. On the web console, click **Get Started**.



**Figure 1. Welcome page**

11. Select your preferred license.
  - If you select the license type as **Standard**, and then click **Next** to proceed with the standard Wyse Management Suite installation.
  - If you select the license type as **Pro**, you must import a valid Wyse Management Suite license. To import the Wyse Management Suite license, enter the requested information to import license if your server has internet connectivity. Also, you can generate the license key by logging in to Wyse Management Suite public cloud portal and entering the key into the license key field.



**Figure 2. License type**

Enter license information ?

Enter your credentials to import licensing information ?

Username

Password

Data center

Number of TC seats ?

Number of Edge Gateway & Embedded PC seats ?

Number of Wyse Software Thin Client seats ?

Import

OR

Input your WMS Pro license key

License Key ?

Import

**Figure 3. License information**

To export a license key from the Wyse Management Suite cloud portal, do the following:

- a. Log in to the Wyse Management Suite cloud portal by using one of the following links:
  - US data center—[us1.wysemanagementsuite.com/ccm-web](https://us1.wysemanagementsuite.com/ccm-web)
  - EU data center—[eu1.wysemanagementsuite.com/ccm-web](https://eu1.wysemanagementsuite.com/ccm-web)
- b. Go to **Portal Administration > Subscription**.

Console Settings

Active Directory (AD)  
Alert Classification  
Edge Gateway & Embedded PC Registration  
External App Services  
File Repository  
Other Settings  
Thin Clients  
Two-Factor Authentication  
Reports

Account

Custom Branding  
**Subscription**

License Subscription

License Type: Production  
Thin Client (Type/Exp): Production / Jun 1, 2019  
Wyse Software Thin Client (Type/Exp): Production / Jan 1, 2020  
Edge Gateway & Embedded PC (Type/Exp): Production / Dec 1, 2019

License Usage

Registered Thin Client devices

50 Manageable
24 In-Use
45 Used in Public Cloud WMS
5 Used in Private Cloud WMS

Registered Edge Gateways & Embedded PC devices

50 Manageable
0 In-Use
50 Used in Public Cloud WMS
0 Used in Private Cloud WMS

Registered Wyse Software Thin Client devices

50 Manageable
0 In-Use
50 Used in Public Cloud WMS
0 Used in Private Cloud WMS

Server Information:

Version: WMS 1.3.0 40874

Export License For Private Cloud

	Private Cloud	Public Cloud	Manageable
Number of TC seats	<input type="text"/>	45	50
Number of Edge Gateway & Embedded PC seats	<input type="text"/>	50	50
Number of Wyse Software Thin Client seats	<input type="text"/>	50	50

Export
WMS 1.1+

**Figure 4. Portal administration**

- c. Enter the number of thin client seats.
- d. Click **Export**.

**NOTE:** To export the license, select , WMS 1.1 or WMS 1.0 from the drop-down list.

The summary page shows the details of the license after the license is successfully imported.

12. Enter your SMTP server information, and click **Save**.

**NOTE:** You can skip this screen and make changes later in the console.

Figure 5. Email alert

**NOTE:** You must enter valid SMTP server information to receive email notifications from the Wyse Management Suite.

13. Import your SSL certificate to secure communications with the Wyse Management Suite server. Enter the public, private, and apache certificate and click the **Import** button. Importing the certificate takes three minutes to configure and restart Tomcat services. You can skip this screen and complete this setup or make changes later in the console by logging in to the Wyse Management Suite private cloud and importing from the **Portal Administration** page.

**NOTE:** By default, the Wyse Management Suite imports the self-signed SSL certificate that is generated during the installation to secure communication between the client and the Wyse Management Suite server. If you do not import a valid certificate for your Wyse Management Suite server, a security warning message is displayed when you access the Wyse Management Suite from a machine other than the server where it is installed. This warning message is displayed because the self-signed certificate generated during installation is not signed by a Certificate Authority such as [geotrust.com](https://www.geotrust.com). You can either import a .pem or .pfx certificate.

Figure 6. Key or certificate value pair

Import certificate You can complete this setup or make changes later in the console.

[Back](#) [Skip](#) [Next](#)

**PKCS-12 (.pfx or .p12)**

Use this option when you have a .pfx or .p12 file that has the domain certificate, private key, and complete certificate chain (root and potentially intermediate certificates). This is the option you would normally use when using IIS to request the domain certificate.

**Key/Certificate Pair**

Use this option when the domain certificate, private key, and certificate chain (root and potentially intermediate certificates) are separate files. This is the option you would normally use when using a Public CA to request the certificate. When using this method make sure to choose Apache as the certificate type when requesting the certificate. Also note that some Public CA's don't include the intermediate certificate in the chain so you have to download them from the Public CA's website separately.

PKCS-12 (.pfx or .p12)  [Browse](#) \*

Password for PKCS  \*

Intermediate certificate  [Browse](#)

[Import](#)

**Figure 7. PKCS-12**

- In the **Device** page, you can enable **Enrollment Validation** to enable administrators to control the manual and auto registration of thin clients to a group.

[Select device type](#) [Enable email alert](#) [Import certificate](#) **Device Enrollment Validation** English US

Configure Device Enrollment Validation You can complete this setup or make changes later in the console.

[Back](#) [Skip](#) [Next](#)

Enrollment Validation(Unmanaged Group) ☒

[Save](#)

**Figure 8. Enrollment validation**

- Click **Save** and then click **Next**.
- Click **Sign in to WMS**.  
The **Dell Management Portal** login page is displayed.

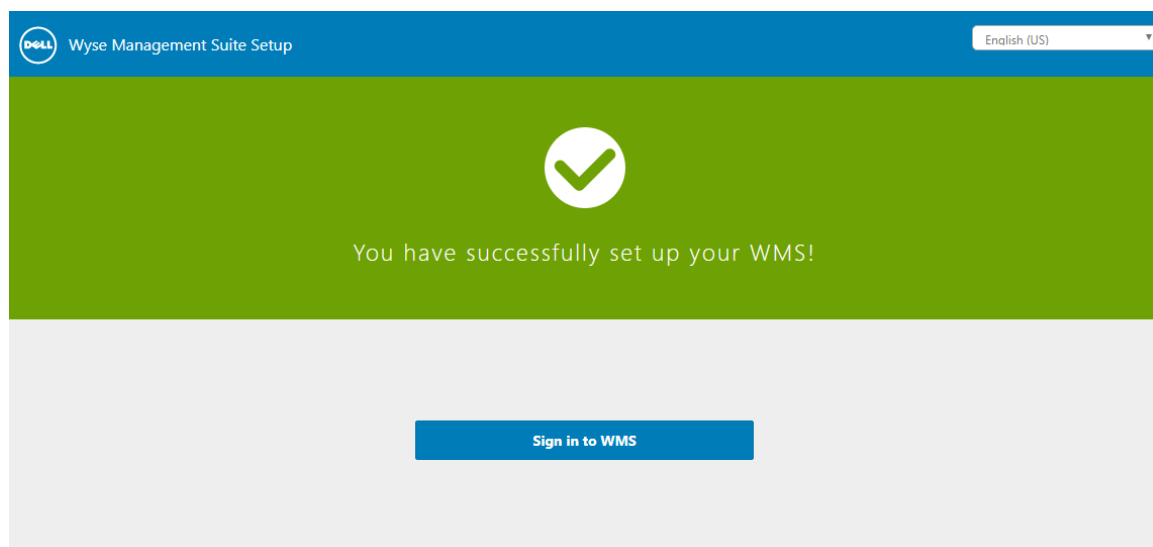


Figure 9. Sign in page

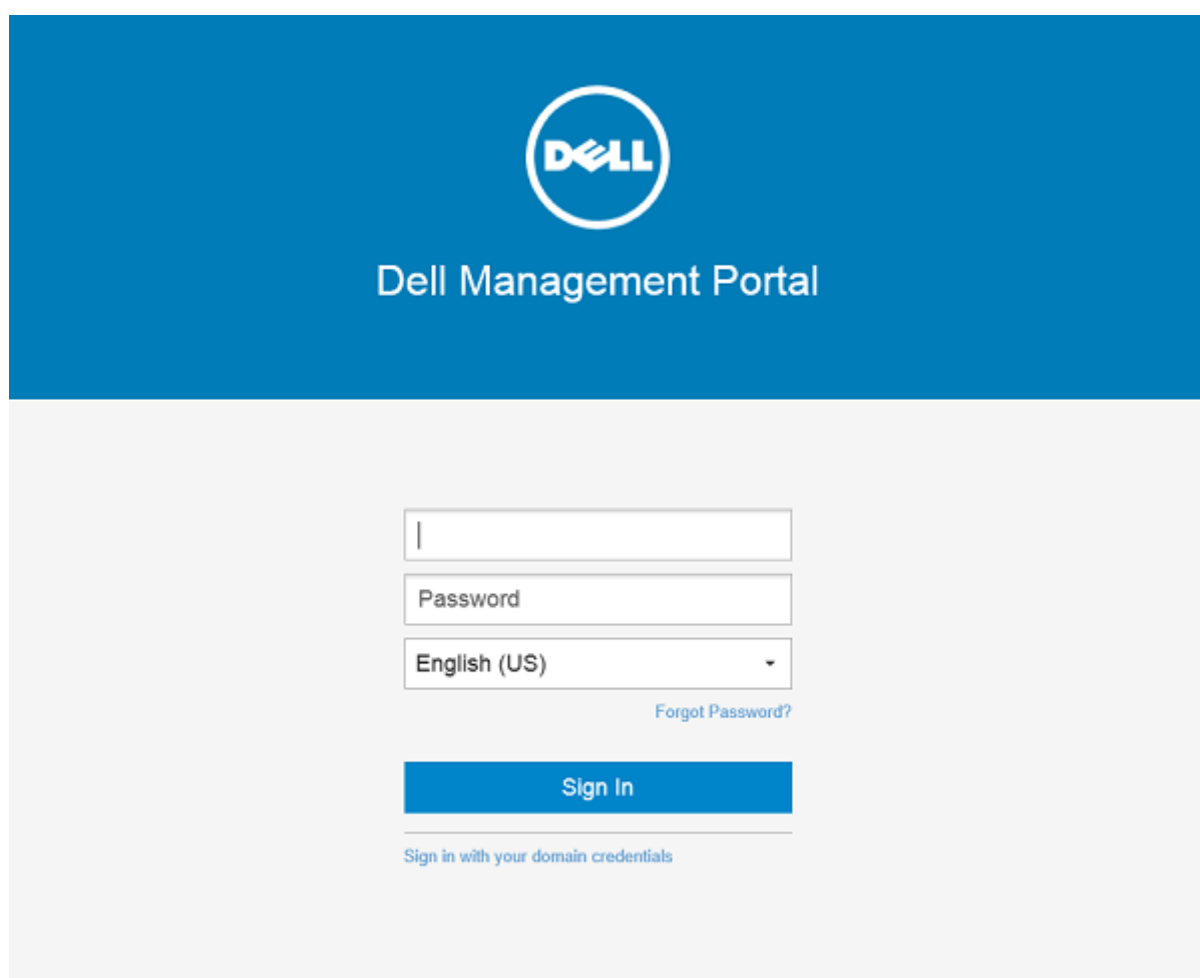


Figure 10. Dell Management Portal

**NOTE:** Licenses can be upgraded or extended at a later point from the Portal Administration page.

#### Topics:

- [Logging in to Wyse Management Suite](#)

- [Functional areas of management console](#)
- [Configuring and managing thin clients](#)
- [Creating policy group and updating configuration](#)
- [Registering new thin client](#)

## Logging in to Wyse Management Suite

To log in to the management console, do the following:

1. If you are using Internet Explorer, disable the **Internet Explorer Enhanced Security** and the **Compatibility View** settings.
2. Use a supported web browser on any machine with access to the internet, and access the private cloud edition of the Wyse Management Suite from <https://<FQDN>/ccm-web>. For example, <https://wmserver.domain.com/ccm-web>, where, [wmserver.domain.com](https://wmserver.domain.com/ccm-web) is the qualified domain name of the server.
3. Enter your user name and password.
4. Click **Sign In**.

## Functional areas of management console

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

- The **Dashboard** page provides information about 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 functions, device type, bring-your-own-device, and so on.
- The **Devices** page enables you to view and manage devices, device types, and device-specific configurations.
- The **Apps & Data** page provides management of device applications, operating system images, policies, certificate files, logos, and wallpaper images.
- The **Rules** page enables you to add, edit, and enable or disable rules such as auto grouping and alert notifications.
- The **Jobs** page enables you to create jobs for tasks such as reboot, WOL, and application or image policy that need to be deployed on registered devices.
- The **Events** page enables you to view and audit system events and alerts.
- The **Users** page enables local users, and users imported from the Active Directory to be assigned global administrator, group administrator, and viewer roles to log in to Wyse Management Suite. Users are given permissions to perform operations based on the roles assigned to them.
- The **Portal Administration** page enables administrators to configure various system settings, such as local repository configuration, license subscription, active directory configuration, and two-factor authentication. For more information, see *Dell Wyse Management Suite Administrator's Guide* at [support.dell.com](http://support.dell.com).

## Configuring and managing thin clients

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

### NOTE:

**In the pro edition, system administrators can add rules to create groups. They 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 or policies that apply to all devices in the tenant account which are set at the Default Policy group. These settings and policies are the global set of parameters that all groups and subgroups inherit from.
- Settings or parameters that are configured at lower-level groups take precedence over the settings that were configured at the parent or higher-level groups.
- Parameters that are specific to a particular device which can be configured from the **Device Details** page. These parameters, like lower-level groups, take precedence over the settings configured in the higher-level groups.

Configuration parameters are deployed to all devices in that group and all the subgroups, when the administrator creates and publishes the policy.

After a configuration is published and propagated to the devices, the settings are not sent again to the devices until the administrator makes 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 inherited from the global group and intermediate level groups.

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

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

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

Wyse Management Suite supports standard and advanced application policies. A standard application policy allows you to install a single application package. You need to reboot the device before and after each application installation. With an advanced application policy, multiple application packages can be installed with only two reboots. This feature is available only in the pro edition. Advanced application policies also support execution of pre and post installation scripts that may be needed to install a particular application.

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

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

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

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

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

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

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

**Mobile application**—Administrator can receive alert notifications and manage devices using mobile application available for the Android devices. To download the mobile application and the quick start guide, click the **Alerts and Classification** tab on the **Portal Administration** page.

## Creating policy group and updating configuration

To create a policy and to update the configuration, do the following:

1. Log in as an administrator.
2. To create a policy group, do the following:
  - a. Select **Groups & Configs**, and click the **+** button on the left pane.
  - b. Enter the group name and description.
  - c. Select the **Enabled** check-box.
  - d. Enter the group token.
  - e. Click **Save**.
3. To update or edit a policy group, do the following:
  - a. Click **Edit Policies**, and select the operating system that the policy is intended to manage.
  - b. Select the policies to be modified, and complete the configuration.
  - c. Click **Save and Publish**.

### **NOTE:**

- For more details on various configuration policies supported by Wyse Management Suite, see *Dell Wyse Management Suite Administrator's Guide* at [support.dell.com](https://support.dell.com).
- You can create a rule to automatically create a group and/or assign a device to a group based on specific attributes such as subnet, time zone, and location.



# Registering new thin client

**NOTE:** For information on customer security environment, see [Wyse Device Agent](#).

A thin client can be registered with Wyse Management Suite manually through the Wyse Device Agent (WDA). You can also register a thin client automatically by configuring appropriate option tags on the DHCP server or configuring appropriate DNS SRV records on the DNS server.

If you want devices in different subnets to automatically check into different Wyse Management Suite groups with multiple subnets, use the DHCP option tags to register a thin client. For example, devices in TimeZone\_A can check into ProfileGroup configured for TimeZoneA.

If you want to enter the Wyse Management Suite server information at TLD, and if you have installed Wyse Management Suite Pro to allow automatic group assignment based on device rules, use the DNS SRV records on the DNS server to register a thin client. For example, if the device checks in from TimeZoneA, assign it to the ProfileGroup configured for TimeZoneA.

For the Wyse Management Suite on a private cloud with self-signed certificates, the thin clients must have the following versions of Wyse Device Agents or firmware installed for secure communication:

- 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 a device with an older version agent using HTTP URL instead of HTTPS. After the agent or firmware is upgraded to the latest version, communication with the Wyse Management Suite will automatically switch to https.
- You can download the latest version WDA at [downloads.dell.com/wyse/wda](https://downloads.dell.com/wyse/wda).
- For Wyse Management Suite installed on a private cloud, go to **Portal Administration > Setup** and select the **Certification Validation** check box, if you have imported certificates from a certificate authority such as [www.geotrust.com](https://www.geotrust.com). This checkbox should not be selected if you have not imported certificates from a well-known certificate authority. This option is not available for Wyse Management Suite on a public cloud as the certificate validation in public cloud is always enabled.

## Registering ThinOS device manually

To register the ThinOS devices manually, do the following:

1. From the desktop menu, go to **System Setup > Central Configuration**. The **Central Configuration** window is displayed.
2. Click the **WDA** tab.

**WMS** is selected by default.

**NOTE:** WDA service automatically runs after the client boot up process is complete.

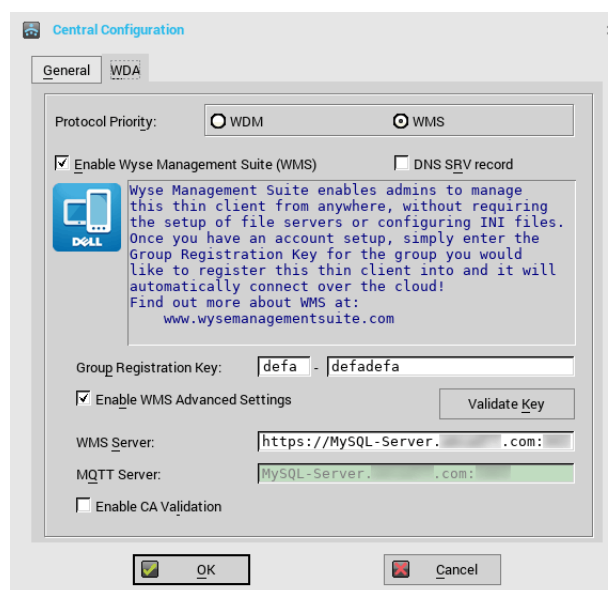


Figure 11. Central Configuration

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

**NOTE:**

**For the pro cloud version of Wyse Management Suite in USA, do not change the default WMS server and MQTT server details. For the pro cloud version of Wyse Management Suite in Europe, use the following:**

- **CCM Server**—[eu1.wysemanagementsuite.com](https://eu1.wysemanagementsuite.com)
- **MQTT Server**—[eu1-pns.wysemanagementsuite.com:1883](https://eu1-pns.wysemanagementsuite.com:1883)

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



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

8. Click **OK**.  
The device is registered to the Wyse Management Suite console.

For information on how to register the Windows Embedded Standard devices and the Linux devices, see [Registering Windows Embedded Device manually](#) and [Registering Linux device manually](#).

## Registering ThinOS devices using INI files

If you want to configure the ThinOS devices using `wnos.ini`, or `xen.ini`, then the additional information can be published in the `.ini` files to inform the devices to check in to a Wyse Management Suite server.

Examples:

- Example for ThinOS 8.5:  

```
WDAService=yes \
Priority=WMS
WMSEnable=yes \
Server=<Server URL> \
CAValidation=no \
Override=yes
```
- Example for ThinOS 8.4:  

```
WDAService=yes \
Priority=CCM
CCMEnable=yes \
CCMServer=<Server URL> \
GroupPrefix=< Prefix > \
GroupKey=< Key > \
MQTTServer=<Server URL> \
Override=yes \
CAValidation=no
```

For more information, see the latest *Dell Wyse ThinOS INI guide* at [support.dell.com](https://support.dell.com).



**NOTE:**

- **For ThinOS 8.3 (ThinOS Lite 2.3) and later versions, a `WDA Service Priority` command allows you to specify the management protocol. This command is used to discover the management server.**

- The CCM tags for ThinOS version 8.3, 8.4, and 8.5 are different.


## Registering devices by using DHCP option tags

### NOTE:

- For detailed instructions on how to add DHCP option tags on the Windows server, see [Creating and configuring DHCP option tags](#). For information about customer security environment, see [Wyse Device Agent](#).

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

**Table 2. Registering device by using DHCP option tags**

Option Tag	Description
<b>Name</b> —WMS <b>Data Type</b> —String <b>Code</b> —165 <b>Description</b> —WMS Server FQDN	<p>This tag points to the Wyse Management Suite server URL. For example, <code>wmsserver.acme.com:443</code>, where <code>wmsserver.acme.com</code> is fully qualified domain name of the server where Wyse Management Suite is installed. For links to register your devices in Wyse Management Suite in public cloud, see <a href="#">Getting started with Wyse Management Suite on public cloud</a>.</p> <p> <b>NOTE:</b> Do not use <code>https://</code> in the server URL, or the thin client will not register under Wyse Management Suite.</p>
<b>Name</b> —MQTT <b>Data Type</b> —String <b>Code</b> —166 <b>Description</b> —MQTT Server	<p>This tag directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, <code>wmsservername.domain.com:1883</code>.</p> <p>To register your devices in Wyse Management Suite public cloud, the device should point to the PNS (MQTT) servers in public cloud. For example,</p> <p>US1:<a href="#">us1-pns.wysemanagementsuite.com</a>          EU1:<a href="#">eu1-pns.wysemanagementsuite.com</a></p>
<b>Name</b> —CA Validation <b>Data Type</b> —String <b>Code</b> —167 <b>Description</b> —Certificate Authority Validation	<p>This tag is required if Wyse Management Suite is installed on your system in your private cloud. Do not add this option tag if you are registering your devices with Wyse Management Suite on public cloud.</p> <p>Enter <b>True</b>, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.</p> <p>Enter <b>False</b>, if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.</p>
<b>Name</b> —GroupToken <b>Data Type</b> —String <b>Code</b> —199 <b>Description</b> —Group Token	<p>This tag is required to register the ThinOS devices with Wyse Management Suite on public or private cloud.</p> <p>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.</p>

## Registering devices by using DNS SRV record

### NOTE: For information on customer security environment, see [Wyse Device Agent](#).

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





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

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

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

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

**Table 3. Configuring device by using DNS SRV record**

URL/Tag	Description
<b>Record Name</b> —_WMS_MGMT <b>Record FQDN</b> —_WMS_MGMT._tcp.<Domainname> <b>Record Type</b> —SRV	<p>This record points to the Wyse Management Suite server URL. For example, <code>wmserver.acme.com:443</code>, where <code>wmserver.acme.com</code> is fully qualified domain name of the server where Wyse Management Suite is installed. For links to register your devices in Wyse Management Suite in public cloud, see <a href="#">Getting started with Wyse Management Suite on public cloud</a>.</p> <p> <b>NOTE:</b> Do not use <code>https://</code> in the server URL, or the thin client will not register under Wyse Management Suite.</p>
<b>Record Name</b> —_WMS_MQTT <b>Record FQDN</b> —_WMS_MQTT._tcp.<Domainname> <b>Record Type</b> —SRV	<p>This record directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, <code>wmservername.domain.com:1883</code>.</p> <p> <b>NOTE:</b> MQTT is optional for the latest version of Wyse Management Suite.</p> <p>To register your devices in Wyse Management Suite public cloud, the device should point to the PNS (MQTT) servers in public cloud. For example,</p> <p>US1—<a href="#">us1-pns.wysemanagementsuite.com</a>          EU1—<a href="#">eu1-pns.wysemanagementsuite.com</a></p>
<b>Record Name</b> —_WMS_GROUPTOKEN <b>Record FQDN</b> —_WMS_GROUPTOKEN.<Domain> <b>Record Type</b> —TEXT	<p>This record is required to register the ThinOS devices with Wyse Management Suite on public or private cloud.</p> <p>This record is optional to register the Windows Embedded Standard or ThinLinux devices with Wyse Management Suite on private cloud. If the record is not available, then the devices are automatically registered to the unmanaged group during on-premise installation.</p> <p> <b>NOTE:</b> Group Token is optional for the latest version of Wyse Management Suite on private cloud.</p>
<b>Record Name</b> —_WMS_CAVVALIDATION <b>Record FQDN</b> —_WMS_CAVVALIDATION.<Domain> <b>Record Type</b> —TEXT	<p>This record is required if Wyse Management Suite is installed on your system in your private cloud. Do not add this optional record if you are registering your devices with Wyse Management Suite on public cloud.</p> <p>Enter <b>True</b>, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.</p> <p>Enter <b>False</b>, if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.</p> <p> <b>NOTE:</b> CA Validation is optional for the latest version of Wyse Management Suite.</p>

# Deploying applications to thin clients

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

## Topics:

- [Uploading and deploying ThinOS firmware image inventory](#)
- [Creating and deploying standard application policy to thin clients](#)

## Uploading and deploying ThinOS firmware image inventory

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

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 navigate to the location where your file is located.
4. Enter the description for your file.
5. Select the check box if you want to override an existing file.
6. Click **Upload**.

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

## Creating and deploying standard application policy to thin clients

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

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

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

3. In **App Policies**, click **Thin Client**.
4. Click **Add Policy**.
5. To create an application policy, enter the appropriate information in the **Add Standard App Policy** window.

- a. Select **Policy Name**, **Group**, **Task**, **Device Type**, and **TC Application**.
- b. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.

Timeout displays a message on the client which gives you time to save your work before the installation begins. Specify the number of minutes the message dialog should be displayed on the client.

- c. To automatically apply this policy to a device that is registered with Wyse Management Suite, select **Apply the policy to new devices** from the **Apply Policy Automatically** drop-down list.

**NOTE:**

- The app policy is applied, when any device is moved to the defined group or registered directly to the group.
- If you select **Apply the policy to devices on check in**, the policy is automatically applied to the device at check-in to the Wyse Management Suite server.

6. To allow a delay in execution of the policy, select the **Allow delay of policy execution** check box. If this option is selected, the following drop-down menus are enabled:
  - From the **Max Hours per Delay** drop-down menu, select the maximum hours (1–24 hours) you can delay execution of the policy.
  - From the **Max delays** drop-down menu, select the number of times (1–3) you can delay the execution of the policy.
7. To stop the installation process after a defined value, specify the number of minutes in the **Application Installation Timeout** field.
8. Click **Save** to create a policy.

A message is displayed to allow the administrator to schedule this policy on devices based on group.
9. Select **Yes** to schedule a job on the same page.

The app/image policy job can run:

  - a. **Immediately**—Server runs the job immediately.
  - b. **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date/time of the device time zone.
  - c. **On selected time zone**—Server creates one job to run at the date/time of the designated time zone.
10. To create the job, click **Preview** and schedules are displayed on the next page.
11. You can check the status of the job by navigating to the **Jobs** page.

# Uninstalling Wyse Management Suite

To uninstall Wyse Management Suite, do the following:

1. Double-click the **WMS** icon.

The uninstaller wizard is initiated, and the **Wyse Management Suite uninstaller** screen is displayed.

2. Click **Next**. By default, the **Remove** radio button is selected that uninstalls all the Wyse Management Suite installer components.

# Troubleshooting Wyse Management Suite

This section provides troubleshooting information for Wyse Management Suite.

## Problems with accessing Wyse Management Suite web console

- Problem: When you attempt to connect to the Wyse Management Suite console, authentication GUI is not displayed and an HTTP Status 404 page is displayed.

Workaround: Stop and start the services in the following order:

1. Dell WMS: MariaDB
2. Dell WMS: memcached
3. Dell WMS: MongoDB
4. Dell WMS: MQTT broker service
5. Dell WMS: Tomcat Service

- Problem: When you attempt to connect to the Wyse Management Suite console, the authentication GUI is not displayed, and the following error message is displayed:

**This page can't be displayed**

Workaround: Restart the Dell WMS: Tomcat Service

- Problem: Wyse Management Suite Web Console does not respond, or the information on the web page is not displayed correctly when using Internet Explorer.

Workaround:

- Ensure that you are using the supported version of Internet Explorer.
- Ensure that the Internet Explorer Enhanced Security is disabled.
- Ensure that the compatibility view settings are disabled.

## Registering devices with Wyse Management Suite

 **NOTE:** For information on customer security environment, see [Wyse Device Agent](#).

- Problem: Unable to register devices with Wyse Management Suite in public cloud

Workaround:

- Ensure that ports 443 and 1883 are open.
- Check your network connectivity, and access to the Wyse Management web application from the browser for public cloud.
- If **Automatic Discovery** is enabled, check if DHCP or DNS SVR records are configured correctly. Also, check the server URL and the group tokens.
- Check if you can register the device manually.

- Problem: Unable to register devices with Wyse Management Suite in private cloud.

Workaround:

- Ensure that the ports 443 and 1883 are open.
- Check the internet connectivity, and if you can access the Wyse Management web application from the browser.
- If automatic discover is enabled, check if DHCP or DNS SRV records are configured correctly. Also, check the server URL and the group tokens.
- Check if you can register the device manually.
- Check if you are using self-signed or well known certificates.



 **NOTE:** By default Wyse Management Suite installs self-signed certificates. CA validation must be disabled for devices to communicate with the Wyse Management Suite server.

## Error while sending commands to the device

Problem: Not able to send commands such as package update, reboot to device and so on.

Workaround:

- Ensure that the Dell WMS: MQTT broker service is running on the Wyse Management Suite server.
- Check if port 1883 is open.
- Ensure that the device is not shutdown or in sleep state before sending a command.

# 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, administrators 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.

## Additional resources

For video tutorials about:

- Installing Wyse management suite, see [Installation of Wyse Management Suite](#).
- Automatic configuration of ThinOS clients using Wyse Management Suite On-Premise with DHCP option tags, see [Configuring ThinOS devices using Wyse Management Suite](#).

## Remote database

A remote or cloud database (DB) is a database that is built for a virtualized environment, such as hybrid cloud, public cloud, or private cloud. In Wyse Management Suite, you can configure either the Mongo database (MongoDB) or the Maria database (MariaDB) or both databases based on your requirement.

### Topics:

- [Configure Mongo database](#)
- [Configure Maria database](#)

## Configure Mongo database

Mongo database (MongoDB) operates on the Transmission Control Protocol (TCP) port number 27017.

 **NOTE:** Replace any value that is boldfaced with your environment variables, as applicable.

To configure MongoDB, do the following:

1. Install the MongoDB version 4.2.1.
2. Copy the MongoDB files to your local system—C:\Mongo.
3. Create the following directories if they do not exist:
  - C:\data
  - C:\data\db
  - C:\data\log
4. Go to the Mongo folder (C:\Mongo), and create a file named `mongod.cfg`.
5. Open the `mongod.cfg` file in a notepad, and add the following script:

```
systemLog:
destination:file
path:c:\data\log\mongod.log
storage:
dbPath:c:\data\db
```

6. Save and close the `mongod.cfg` file.
7. Open command prompt as an administrator, and run the following command:
 

```
mongod.exe --config "C:\Program Files\MongoDB\Server\4.2\mongod.cfg" -install or sc.exe create MongoDB binPath= "\"C:\ProgramFiles\MongoDB\Server\3.2\bin\mongod.exe\" --service --config= \"C:\ProgramFiles\MongoDB\Server\4.2\mongod.cfg\" Display Name= \"Dell WMS: MongoDB\" start=\"auto\"
```

 MongoDB is installed.
8. To start the MongoDB services, run the following command:
 

```
net start mongoDB
```
9. To start the Mongo database, run the following command:
 

```
mongo.exe
```
10. To open the default admin db, run the following command:
 

```
use admin;
```
11. After the MongoDB sheet is displayed, run the following commands:

```
db.createUser(
{
user:"wmsuser",
pwd:"PASSWORD",
roles:[{role:"userAdminAnyDatabase",db:"admin"},
{role:"dbAdminAnyDatabase",db:"admin"},
{role:"readWriteAnyDatabase",db:"admin"}],
```

```
{role:"dbOwner",db:"stratus"}]
}
)
```

12. To switch to the stratus database, run the following command:

```
use stratus;
```

13. To stop the MongoDB services, run the following command:

```
net stop mongodb
```

14. Add an authentication permission to the admin DB. Modify the mongod.cfg file to the following:

```
systemLog:
destination:file
path:c:\data\log\mongod.log
storage:
dbPath:c:\data\db
security:
authorization:enabled
```

15. To restart the MongoDB service, run the following:

```
net Start mongodb;
```

In the Wyse Management Suite installer, the administrator must use the same user name and password that was created to access the stratus databases in MongoDB. For information about setting the MongoDB on the Wyse Management Suite installer, see [Custom installation](#).

## Configure Maria database

Maria database (MariaDB) operates on the Transmission Control Protocol (TCP) port number 3306.

### NOTE:

- **The IP address displayed here belongs to the Wyse Management Suite server that hosts the web components.**
- **Replace any value that is boldfaced with your environment variables, as applicable.**

To configure MariaDB, do the following:

1. Install the MariaDB version 10.2.29.
2. Navigate to the MariaDB installation path—C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p.
3. Provide the root password which was created during installation
4. Create the database stratus—DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8\_unicode\_ci;.
5. Create user 'stratus'@'localhost';
6. Create user 'stratus'@'**IP ADDRESS**' ;
7. Set a password for 'stratus'@'localhost'=password('PASSWORD');
8. Set a password for 'stratus'@'**IP ADDRESS**'=password('PASSWORD');
9. Provide all privileges on \*.\* to 'stratus'@'**IP ADDRESS**' identified by 'PASSWORD' with a grant option.
10. Provide all privileges on \*.\* to 'stratus'@'localhost' identified by 'PASSWORD' with a grant option.

 **NOTE:** To configure custom port for MariaDB, navigate to C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p -P<custom port> in the second step.

In the Wyse Management Suite installer, the administrator must use the same user name and password that was created to access the stratus databases in MariaDB. For information about setting the MariaDB on the Wyse Management Suite installer, see [Custom installation](#).

# Custom installation

In custom installation, you can select a database to set up Wyse Management Suite, and you must know the basic technical working knowledge of Wyse Management Suite. Dell recommends custom installation only for advanced users.

1. Select the **Setup Type** as **Custom**, and click **Next**.

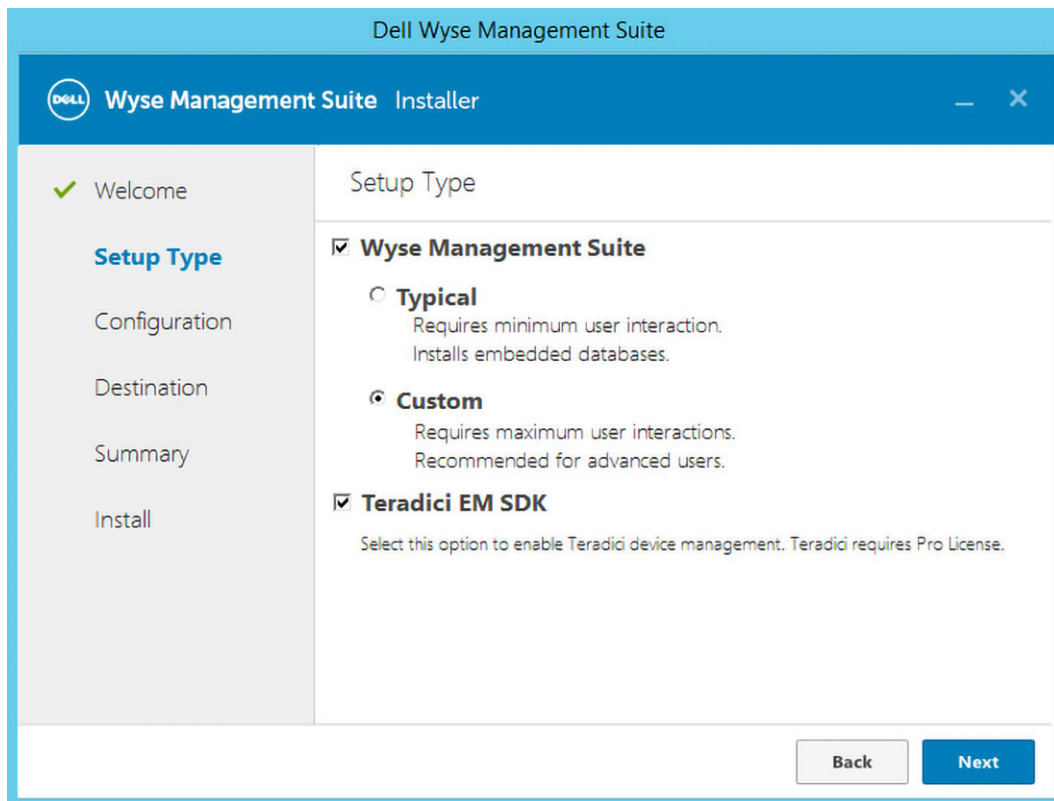


Figure 12. Setup type

The **Mongo Database Server** page is displayed.

2. Select either **Embedded MongoDB** or **External MongoDB** as the Mongo database server.
    - If **Embedded MongoDB** is selected, then provide your password, and click **Next**.
- NOTE:** User name and database server details are not required if the Embedded Mongo database is selected, and the respective fields are grayed out.

The screenshot shows the 'Dell Wyse Management Suite Installer' window. On the left is a sidebar with a progress list: 'Welcome' (checked), 'Setup Type' (checked), 'Configuration' (highlighted), 'Destination', 'Summary', and 'Install'. The main area is titled 'Mongo Database Server'. It has two radio buttons: 'Embedded MongoDB' (selected) and 'External MongoDB'. Below these are four input fields: 'Database Name' (containing 'stratus'), 'Database Server' (containing 'localhost'), 'Username' (containing 'stratus'), and 'Password' (masked with dots). There is also a 'Confirm Password' field (masked with dots). At the bottom right are 'Back' and 'Next' buttons.

**Figure 13. Embedded Mongo Database Server**

- If **External MongoDB** is selected, then provide user name, password, database server details, and the port details, and click **Next**.

**NOTE:** The port field populates the default port which can be changed.

The screenshot shows the 'Dell Wyse Management Suite Installer' window. The sidebar is identical to Figure 13. The main area is titled 'Mongo Database Server'. The 'External MongoDB' radio button is selected. The input fields are: 'Database Name' (containing 'stratus'), 'Database Server' (empty), 'Port' (empty), 'Username' (containing 'stratus'), and 'Password' (masked with dots). The 'Confirm Password' field is not visible. At the bottom right are 'Back' and 'Next' buttons.

**Figure 14. External MongoDB**

The **MariaDB Database Server** page is displayed.

3. Select either **Embedded MariaDB** or **External MariaDB** as the MariaDB database server.

- If **Embedded MariaDB** is selected, provide user name and password, and click **Next**.

The screenshot shows the 'Dell Wyse Management Suite' installer window. The title bar includes the Dell logo and the text 'Wyse Management Suite Installer'. On the left is a sidebar with a progress list: 'Welcome' (checked), 'Setup Type' (checked), 'Configuration' (highlighted), 'Destination', 'Summary', and 'Install'. The main area is titled 'MariaDB Database Server'. It features two radio buttons: 'Embedded MariaDB' (selected) and 'External MariaDB'. Below these are four input fields: 'Database Name' (containing 'stratus'), 'Database Server' (containing 'localhost'), 'Username' (containing 'stratus'), and 'Password' (masked with dots). A 'Confirm Password' field is also present, also masked with dots. At the bottom right are 'Back' and 'Next' buttons.

**Figure 15. Embedded MariaDB**

- If **External MariaDB** is selected, provide user name, password, database server details and the port details, and click **Next**.  
The port field populates the default port which can be changed.

The screenshot shows the 'Dell Wyse Management Suite' installer window, similar to Figure 15 but with 'External MariaDB' selected. The sidebar is identical. The main area shows 'External MariaDB' as the selected option. The input fields are: 'Database Name' (containing 'stratus'), 'Database Server' (empty), 'Port' (empty), 'Username' (containing 'stratus'), and 'Password' (masked with dots). The 'Confirm Password' field is absent. 'Back' and 'Next' buttons are at the bottom right.

**Figure 16. External MariaDB**

4. The **Port** page is displayed which allows you to customize the ports for the following databases:



- Apache Tomcat
- MySQL database
- Mongo database
- MQTT v3.1 Broker
- Memcached

Dell Wyse Management Suite

Wyse Management Suite Installer

✓ Welcome  
 ✓ Setup Type  
**Configuration**  
 Destination  
 Summary  
 Install

Port selection

Please select the port numbers to be used with the following:

Apache Tomcat	<input type="text"/>	<input type="text"/>
MariaDB database	<input type="text"/>	
Mongo database	<input type="text"/>	
MQTT v3.1 Broker	<input type="text"/>	
Memcached	<input type="text"/>	

Back Next

Figure 17. Port selection

- NOTE:** Wyse Management Suite uses the Maria database and Mongo database for the following:
- Maria database**—Relational database for data that requires well-defined structure and normalization
  - Mongo database**—No-SQL database for performance and scalability

To complete the installation, follow the steps in the section [Installing WMS on-premise and initial setup](#).

# Wyse Management Suite feature matrix

The following table provides information about the features supported for each subscription type:

**Table 4. Feature matrix for each subscription type**

Features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Highly scalable solution to manage thin clients	Free up to 10,000 devices	50,000 devices and more	1 million devices and more
License key	Not required	Required	Required
Group based management	Supported	Supported	Supported
Multi-level groups and inheritance	Supported	Supported	Supported
Configuration policy management	Supported	Supported	Supported
Operating system patch and image management	Supported	Supported	Supported
View effective configuration at device level after inheritance	Supported	Supported	Supported
Application policy management	Supported	Supported	Supported
Asset, inventory and systems management	Supported	Supported	Supported
Automatic device discovery	Supported	Supported	Supported
Real-time commands	Supported	Supported	Supported
Smart scheduling	Supported	Supported	Supported
Alerts, events and audit logs	Supported	Supported	Supported
Secure communication (HTTPS)	Supported	Supported	Supported
Manage devices behind firewalls	Limited*	Limited*	Supported
Mobile application	Not supported	Supported	Supported
Alerts using email and mobile application	Not supported	Supported	Supported
Scripting support for customizing application installation	Not supported	Supported	Supported
Bundle applications to simplify deployment and minimize reboots	Not supported	Supported	Supported
Delegated administration	Not supported	Supported	Supported
Dynamic group creation and assignment based on device attributes	Not supported	Supported	Supported

Features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Two-factor authentication	Supported	Supported	Supported
Active directory authentication for role based administration.	Not supported	Supported	Supported
Multi-tenancy	Not supported	Supported	Supported
Enterprise grade reporting	Not supported	Supported	Supported
Multiple repositories	Not supported	Supported	Supported
Enable/disable hardware ports on supported platforms	Not supported	Supported	Supported
BIOS configuration on supported platforms	Not supported	Supported	Supported
Export and import policy configuration	Not supported	Supported	Supported
Repository assignment to application policy	Not supported	Supported	Supported
Shutdown commands for thin clients	Supported	Supported	Supported
Wyse Management Suite console timeout	Not supported	Supported	Supported
Policy order	Not supported	Supported	Supported
Streamlined the application selection as per the operating system	Supported	Supported	Supported
Option to configure alias	Not supported	Supported	Supported

**NOTE:** \*The asterisk indicates that you can manage the devices by using Wyse Management Suite only in a secure firewall work environment. You cannot manage thin clients beyond the purview of the firewall settings.

# 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.

## NOTE:

- **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.

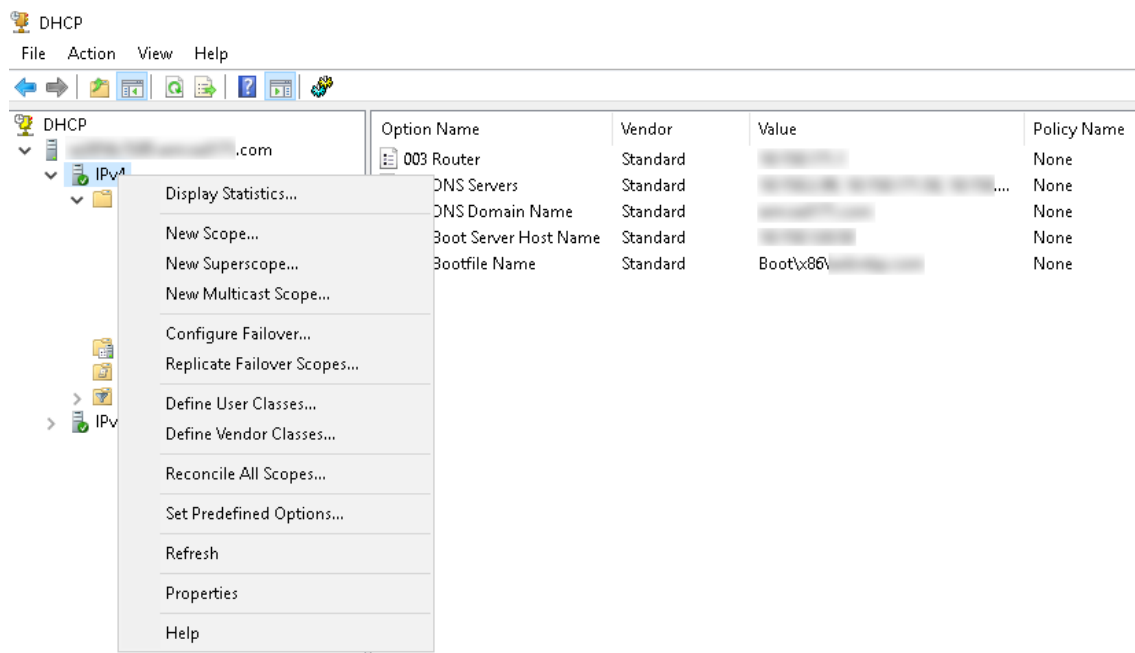
13. Add a note in the provided box.
14. Click **Save Settings**.

# Create and configure DHCP option tags

**NOTE:** For information on customer security environment, see [Wyse Device Agent](#).

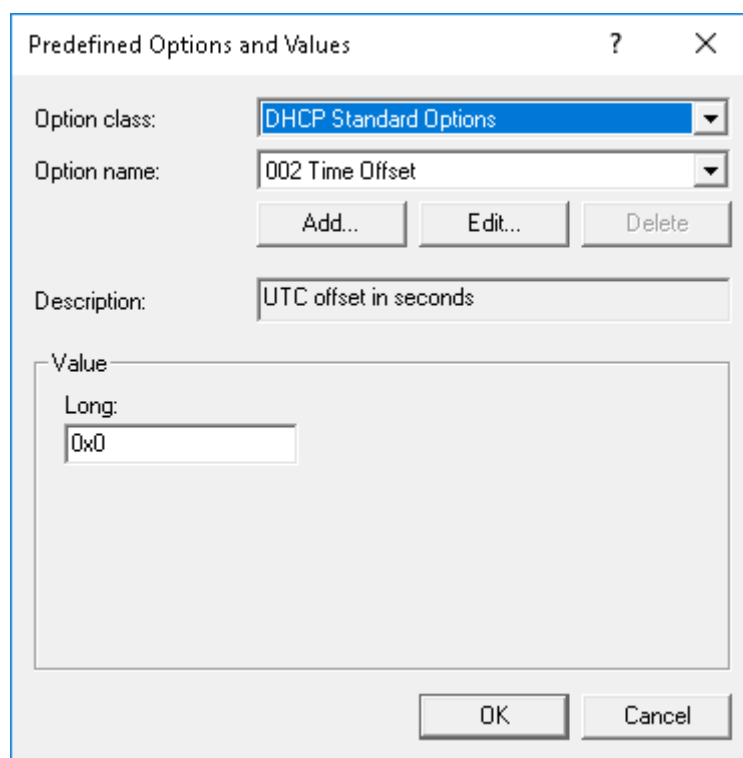
To create a DHCP option tag, do the following:

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



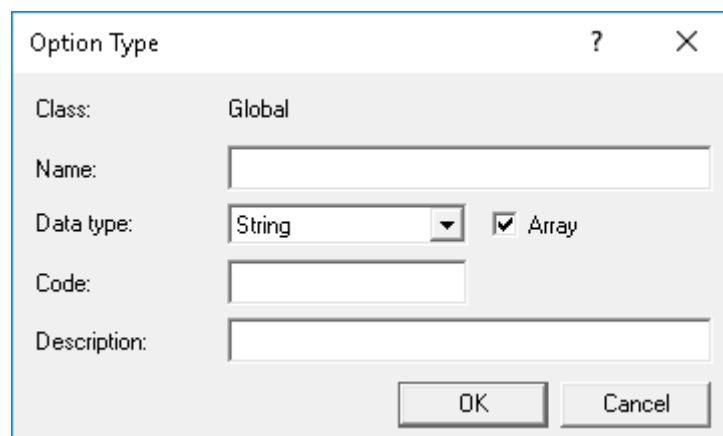
**Figure 18. DHCP**

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



**Figure 19. Predefined Options and Values**

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



**Figure 20. Option Type**

The options must be either added to the server options of the DHCP server or scope options of the DHCP scope.

#### **Configuring the DHCP option tags**

- To create the 165 Wyse Management Suite server URL option tag, do the following:

1. Enter the following values, and click **OK**.

- Name—WMS
- Data type—String
- Code—165
- Description—WMS\_Server

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

String—WMS\_FQDN

For example, WMSServerName.YourDomain.Com:443

Predefined Options and Values

Option class: DHCP Standard Options

Option name: 165 WMS

Add... Edit... Delete

Description: WMS\_Server

Value

String: WMSServerName.YourDomain.Com:443

OK Cancel

**Figure 21. 165 Wyse Management Suite server URL option tag**

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

1. Enter the following values, and click **OK**.

- Name—MQTT
- Data type—String
- Code—166
- Description—MQTT Server

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

String—MQTT FQDN

For example, WMSServerName.YourDomain.Com:1883

Predefined Options and Values

Option class: DHCP Standard Options

Option name: 166 MQTT Server

Add... Edit... Delete

Description: MQTT Server

Value

String: WMSServerName.YourDomain.Com:1883

OK Cancel

**Figure 22. 166 Wyse Management Suite server URL option tag**

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



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 167 CA Validation

Add... Edit... Delete

Description: CA Validation

Value

String: FALSE

OK Cancel

**Figure 23. 167 Wyse Management Suite server URL option tag**

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

Predefined Options and Values ? X

Option class: DHCP Standard Options

Option name: 199 Group token key

Add... Edit... Delete

Description: Group token key

Value

String:

defa-quarantine

OK Cancel

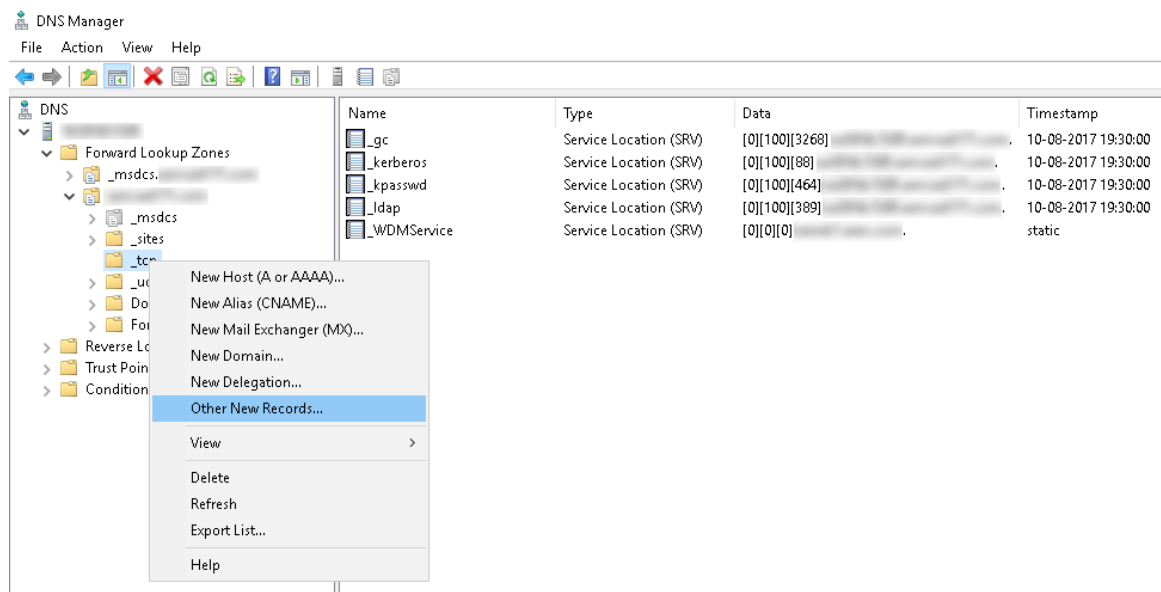
Figure 24. 199 Wyse Management Suite server URL option tag

# Create and configure DNS SRV records

**NOTE:** For information on customer security environment, see [Wyse Device Agent](#).

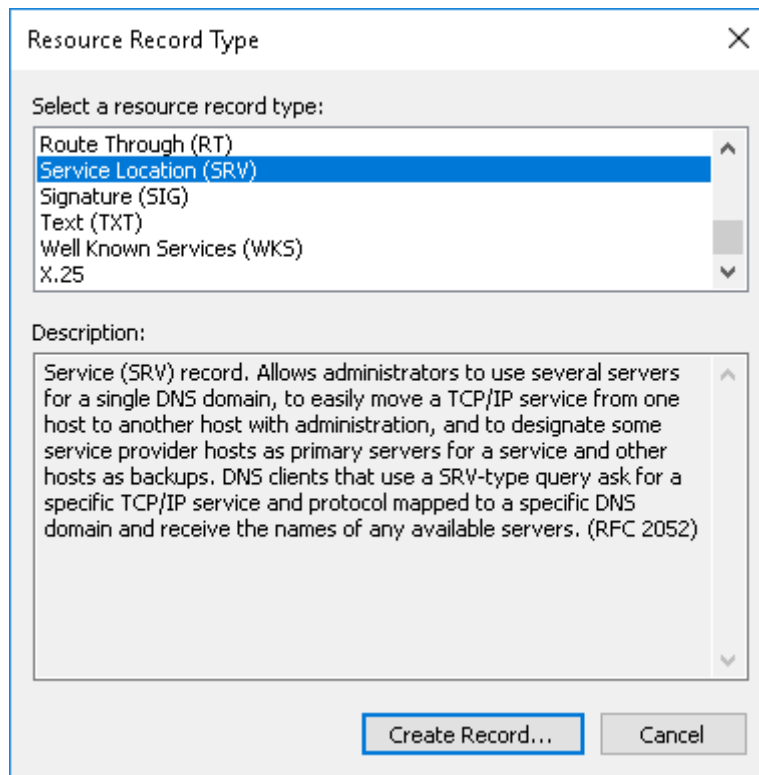
To create a DNS SRV record, do the following:

1. Open the Server Manager.
2. Go to **Tools**, and click **DNS option**.
3. Go to **DNS > DNS Server Host Name > Forward Lookup Zones > Domain > \_tcp** and right-click the **\_tcp** option.



**Figure 25. DNS manager**

4. Click **Other New Records**.  
The **Resource Record Type** window is displayed.
5. Select the **Service Location (SRV)**, click **Create Record**, and do the following:



**Figure 26. Resource Record Type**

- a) To create Wyse Management Suite server record, enter the following details and click **OK**.
- Service—\_WMS\_MGMT
  - Protocol—\_tcp
  - Port number—443
  - Host offering this service—FQDN of WMS server

New Resource Record

Service Location (SRV)

Domain:

Service:

Protocol:

Priority:

Weight:

Port number:

Host offering this service:

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

OK Cancel Help

**Figure 27. \_WMS\_MGMT service**

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

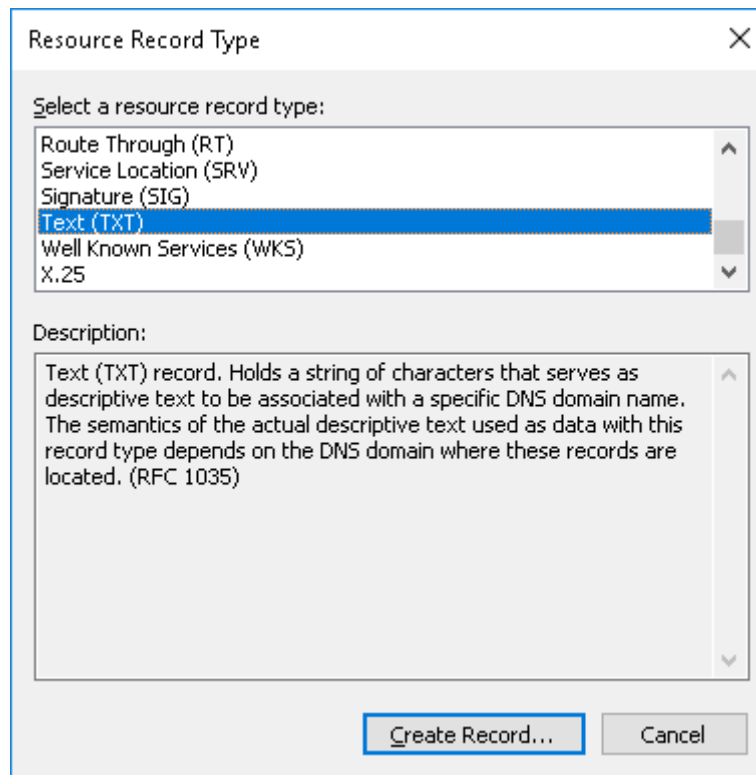
The screenshot shows a 'New Resource Record' dialog box with a close button (X) in the top right corner. The 'Service Location (SRV)' tab is selected. The fields are as follows:

- Domain: [Empty text box]
- Service: [Dropdown menu showing '\_WMS\_MQTT']
- Protocol: [Dropdown menu showing '\_tcp']
- Priority: [Text box containing '0']
- Weight: [Text box containing '0']
- Port number: [Text box containing '1883']
- Host offering this service: [Text box containing 'FQDN of MQTT server']

Below the fields is a checkbox labeled 'Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.' The checkbox is currently unchecked. At the bottom right are three buttons: 'OK' (highlighted with a blue border), 'Cancel', and 'Help'.

**Figure 28. \_WMS\_MQTT service**

6. Go to **DNS > DNS Server Host Name > Forward Lookup Zones > Domain** and right-click the domain.
7. Click **Other New Records**.
8. Select **Text (TXT)**, click **Create Record**, and do the following:



**Figure 29. Resource Record Type**

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

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

**Figure 30. \_WMS\_GROUPTOKEN record name**

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



New Resource Record

Text (TXT)

Record name (uses parent domain if left blank):

\_WMS\_CAVALIDATION

Fully qualified domain name (FQDN):

\_WMS\_CAVALIDATION.\_

Text:


False

OK Cancel

Figure 31. \_WMS\_CAVALIDATION record name

# Creating and deploying advanced application policy to thin clients

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

1. Copy the application and the pre/post install scripts (if necessary) to deploy to the thin clients in the `thinClientApps` folder in the local repository or the Wyse Management Suite repository.
  2. Go to **Apps&Data > AppInventory** and select **Thin Client** to verify if the application is registered.
  3. Click **Thin Client** under **App Policies**.
  4. Click **Add Advanced Policy**.
  5. To create a new application policy, do the following:
    - a. Enter a **Policy Name**, **Group**, **Task**, and **Device Type**.
    - b. Click **Add app**, and select one or more applications under **TC apps**. For each application, you can select a pre and post install script under **Pre-Install**, **Post-Install**, and **Install Parameters**. If you want the system to reboot after the application is successfully installed, select **Reboot**.
    - c. If you want this policy to be applied on all subgroups, select **Include All Subgroups**.
    - d. If you want to deploy this policy to specific operating system or platform, select **OS Subtype Filter** or **Platform Filter**.
    - e. Timeout displays a message on the client which gives you time to save your work before the installation begins. Specify the number of minutes the message dialog should be displayed on the client.
    - f. If you want to automatically apply this policy to a device that is registered with Wyse Management Suite and belongs to a selected group or is moved to a selected group, select **Apply the policy to new devices** from the **Apply Policy Automatically** drop-down list.
-  **NOTE:** If you select **Apply the policy to devices on check in**, the policy is automatically applied to the device at check-in to the Wyse Management Suite server.
- g. To stop the installation process after a defined value, specify the number of minutes in the **Application Installation Timeout** field.
  6. To allow delay in execution of the policy, select the **Allow delay of policy execution** check box. If this option is selected, the following drop-down menus are enabled:
    - From the **Max Hours per Delay** drop-down menu, select the maximum hours (1–24 hours) you can delay the policy execution.
    - From the **Max delays** drop-down menu, select the number of times (1–3) you can delay execution of the policy.
  7. To cancel the application policy at first failure, select **Enable app dependency**. If this option is not selected, failure of an application affects the policy execution.
  8. To create a new policy, click **Save**. A message is displayed to allow administrators to schedule this policy on devices based on the group. Select **Yes** to schedule the application policy for devices immediately or at a scheduled date and time on the **App Policy Job** page.

The app/image policy job can run:

- a. **Immediately**—Server runs the job immediately.
  - b. **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date/time of the device time zone.
  - c. **On selected time zone**—Server creates one job to be run at the date and time of the designated time zone.
9. Click **Preview** and schedule on the next page to create the job.
  10. You can check the status of the job by navigating to the **Jobs** page.

# Registering Windows Embedded Standard device manually

Windows Embedded Standard devices can be registered manually by launching the **WDA UI** icon on the taskbar.

1. Select **Wyse Management Suite-WMS** as the management server.
2. Enter an appropriate tenant and group name. If this field is left blank, devices are registered to an unmanaged group. (Optional)
3. Click **Register**.

The screenshot shows the 'Wyse Device Agent' application window. On the left is a sidebar with three items: 'Registration' (highlighted in blue), 'Support', and 'About'. The main content area is titled 'Device registration'. It features a 'Select management server' section with a dropdown menu currently showing 'Wyse Management Suite - WMS' and a status indicator 'NONE is active'. Below this is the 'Server settings' section, which includes input fields for 'Management Server' (labeled 'Enter server url') and 'Port' (labeled 'Enter Port'). There are also dropdowns for 'Tenant' (labeled 'Tenant') and 'Group' (labeled 'Enter group'). A note below these states: '\*If the tenant and group is empty, the device will get registered to unmanaged group'. At the bottom of the settings is a checkbox for 'Validate Server Certificate CA:' which is currently checked (labeled 'ON'). The bottom status bar shows a red circle with a slash and the text 'Not Registered', along with 'Refresh' and 'Register' buttons.


Figure 32. Device registration

# Register ThinOS 8.x device manually


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.

# Register ThinOS 9.x device manually

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:** 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.

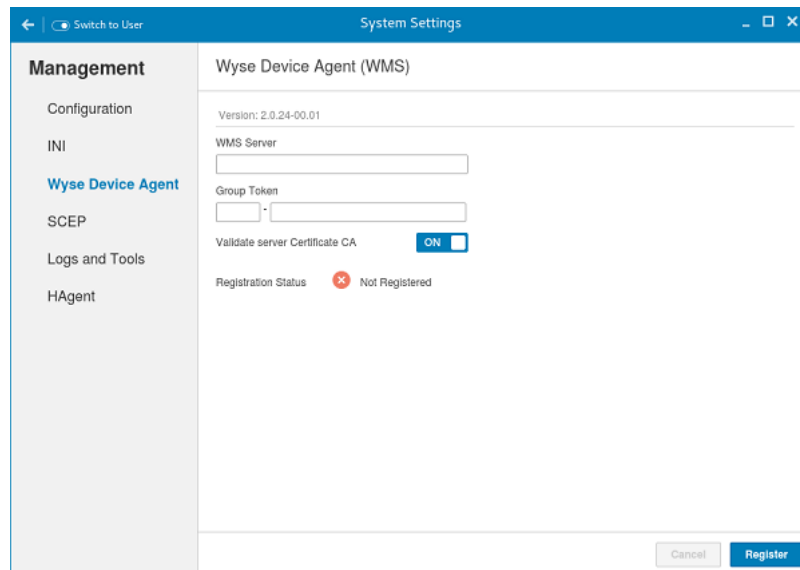
The device is registered to Wyse Management Suite.

# Registering Linux device manually

Linux devices can be registered manually by launching the **WDA UI** icon from **System Settings**.

1. Enter the **WMS Server** details.
2. Enter an appropriate tenant and group name. If this field is left blank, devices are registered to an unmanaged group. (Optional)
3. Click **Register**.

The device is registered to the Wyse Management Suite console.



The screenshot shows a window titled "System Settings" with a sidebar on the left and a main content area. The sidebar has a "Management" section with sub-items: "Configuration", "INI", "Wyse Device Agent" (highlighted in blue), "SCEP", "Logs and Tools", and "HAgent". The main content area is titled "Wyse Device Agent (WMS)" and shows the version "2.0.24-00.01". Below this, there are input fields for "WMS Server" and "Group Token". A "Validate server Certificate CA" toggle is set to "ON". The "Registration Status" is indicated as "Not Registered" with a red 'x' icon. At the bottom right, there are "Cancel" and "Register" buttons.

Figure 33. Device registration

## Terms and definitions

The following table lists the terms used in this document and their definitions:

**Table 5. Terms and definitions**

Terminology	Definition
Private cloud	Wyse Management Suite server installed on the cloud that is private to your organization's datacenter.
WDA	Wyse Device Agent which resides in the device and acts as an agent for communication between server and client.
Local repository	Application, operating system image, and file repository that is installed by default with the Wyse Management Suite server.
Remote repository	Application, operating system image, and file repositories that can be optionally installed for scalability and reliability across geographies to transfer content.
Public cloud	Wyse Management Suite hosted on a public cloud with the convenience and cost savings of not having to set up and maintain the infrastructure and software.
Add-on/App	Any component or package that is not a part of the base build and is provided as an optional component. The component or package can be deployed from the management software. For example — Latest connection brokers from VMware and Citrix
On-premise	Wyse Management Suite server installed on-premise that is private to your organization's datacenter.
Tenant	A group of users who share a common access with specific privileges to the Wyse Management Suite. It is a unique key assigned to specific customers to access the management suite.
Users	Users can be local administrators, global administrators and viewers. Group users and users imported from Active Directory can be assigned global administrator, group administrator, and viewer roles to log in to the Wyse Management Suite. Users are given permissions to perform operations based on roles assigned to them.