Dell Wyse Management Suite

Version 3.x and 4.x Quick Start Guide

February 2024
Rev. A07

Notes, cautions, and warnings

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

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

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

Contents

Introduction to Wyse Management Suite

Wyse Management Suite is the next generation management solution that enables you to centrally configure, monitor, manage, and optimize your Dell 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. This version can only manage Dell Thin Clients. 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.
- **Pro (Paid)**—The Pro edition of the Wyse Management Suite is a more robust solution. It is available for both public and private cloud deployment. A license key is required to use the Pro edition (subscription-based licensing). With the Pro solution, organizations can adopt a hybrid model and float licenses between private and public clouds if required. This version is required to manage any Teradici-based devices, Wyse Covert for PCs-based thin clients, Dell Hybrid Client devices, Embedded PC, and Edge Gateway devices. It also offers more advanced features to manage Dell thin clients. For a public cloud deployment, the Pro edition can be managed on non-corporate networks such as home office, third party, partners, mobile thin clients, and so on.

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

  The Pro edition of the Wyse Management Suite also provides:

  - A mobile application to view critical alerts, notifications, and send commands in real time.
  - Enhanced security through two-factor identification and Active Directory authentication for role-based administration
  - Advanced app policy and reporting

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

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

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

Wyse Management Suite Feature Matrix

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

Table 1. Feature matrix for each subscription type

Features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Highly scalable solution to manage thin clients	Small deployments, single location	Up to 120 thousand devices	Up to 1 million devices
License term	Free download	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	√	√
Wyse thin clients with ThinOS	√	√	√
Wyse thin clients with ThinLinux	√	√	√
Wyse thin clients with Windows 10 IoT Enterprise	√	√	√
Wyse PCoIP zero clients (Teradici firmware)	X	√	√
Software thin clients with Wyse Converter for PCs	X	√	√
Reporting and Monitoring			
Localized management console	X	√	√
Alerts, Events, and Audit log using email and mobile application	X	√	√
Enterprise-Grade Reporting	X	√	√

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 www.dell.com/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	√	√
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	√	√

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
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. Wyse thin clients and zero clients management feature matrix

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

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

Wyse thin clients and zero clients management features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
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	√	√
Configuration			
Wyse ThinOS 8.x and 9.x wizard configuration	√	√	√
Multi-Monitor Support	√	√	√
Wyse Easy Setup and Wyse Overlay Optimizer	√	√	√

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

Wyse thin clients and zero clients management features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
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.

Installing Wyse Management Suite on private cloud

Prerequisites

- Obtain and configure all the required hardware and software. You can download the Wyse Management Suite software from 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 in the installation procedures.
- For the Pro features, obtain a valid Wyse Management Suite license. Standard edition does not require a license.
- Ensure that there is enough space on the drive where Wyse Management Suite is installed and the local repository is configured.
- If you have installed or configured any anti-virus or other monitoring tools on the Wyse Management Suite setup, Dell Technologies recommends that you disable the tools temporarily till the upgrade is complete. You can also add appropriate exclusion to Wyse Management Suite install directory, temporary directory, and local repository directory.

About this task

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/

Steps

1. Double-click the installer package.
2. On the **Welcome** screen, click **Next**.
   The **EULA** details are displayed.
   > **NOTE:** This screen is displayed only on Wyse Management Suite version 3.1 or later.
3. Read the license agreement.
4. Select the **I accept the terms in the license agreement** check box and click **Next**.
5. 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.
6. Select **Typical** as the **Setup Type**.
7. Enter the new **Database Credentials** for the embedded databases and 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.
8. On the **Configuration** page, do the following:

a. 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.

     The password must be more than eight characters.

     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.

b. Click **Next**.

   The **Service Account Credentials** screen is displayed with the following options:
   - **Create a New Local User**—Select this option to enter credentials and create a new local user with least privileges. The new user is added to the **Users** group, but the user will not have administrator rights.

     NOTE: The username that you enter in the **Service Account Credentials** screen must not be the same as your Teradici username. The username must be 2 to 20 characters. Your password must be 9 to 127 characters with at least one upper case, one lower case, one number, and one special character. Spaces are not allowed in the password.
   - **Use an Existing Local User**—Select this option to enter the credentials of an existing local user. A message is displayed when you select this option. Ensure that the user already exists, has service logon rights (**SeServiceLogonRight**), and has successfully logged in at least once to the system. Dell Technologies recommends ensuring that the user does not carry administrative rights.

     NOTE: If you select this option, the complexity of the password is not verified and the username that you enter must be 2 to 20 characters.
   - **Use an Existing Domain User**—Select this option to enter the credentials of an existing domain user. A message is displayed when you select this option. Ensure that the user already exists in the domain, has service logon rights (**SeServiceLogonRight**), and has successfully logged in at least once to the system. Dell Technologies recommends ensuring that the user does not carry administrative rights.

     NOTE: If you select this option, the complexity of the password is not verified.

c. Click **Next** after you enter the credentials.
   The **Software Vault Credentials** screen is displayed. Software vault is used to store sensitive data required by the Dell Wyse Management Suite application.

d. Enter the password for software vault.
   The password must be more than eight characters.

e. Click **Next**.

9. Ensure that you select all the appropriate versions of TLS, based on the support criteria of the devices being managed.

   NOTE: The WDA version lower than WDA_14.4.0.135_Unified, Import tool, and the 32-bit Merlin image are not compatible with TLSv1.1 and later. Select TLSv1.0 if the Wyse Management Suite environment has devices with older version of WDA, Import tool, or devices installed with 32-bit Merlin image.

10. Browse to the location where you want to install the software and 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`.

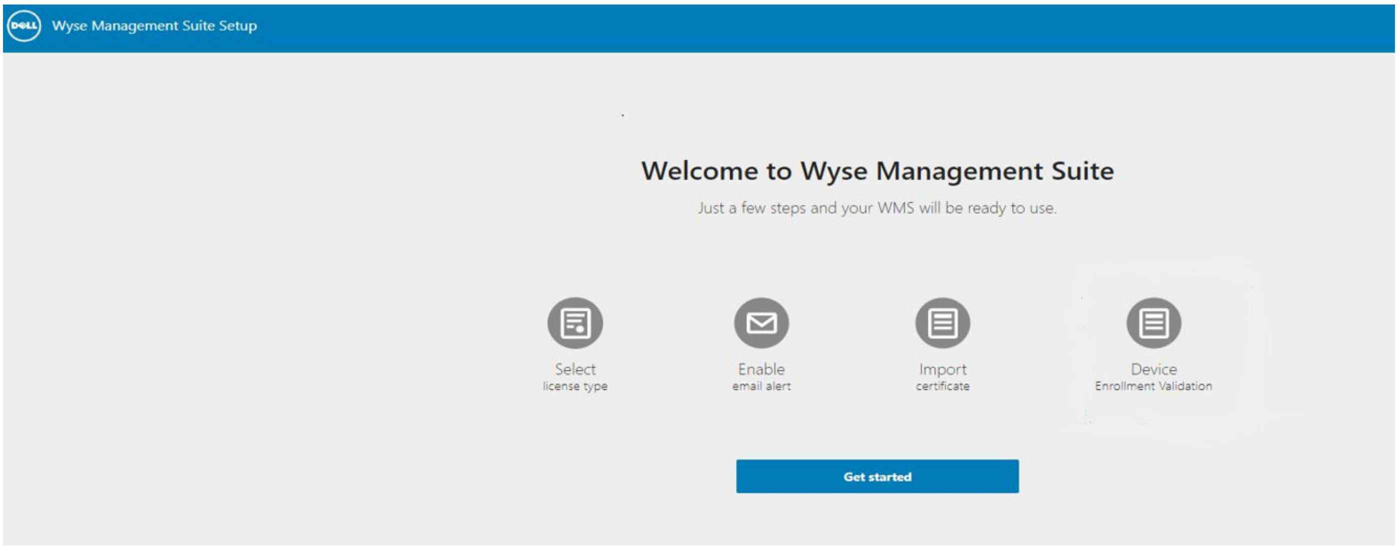
11. Click **Next**.
    The **Pre-Installation Summary** page is displayed.

12. Click **Next** to install the software.

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

13. Click **Launch** to open the Wyse Management Suite web console.

14. On the web console, click **Get Started**.

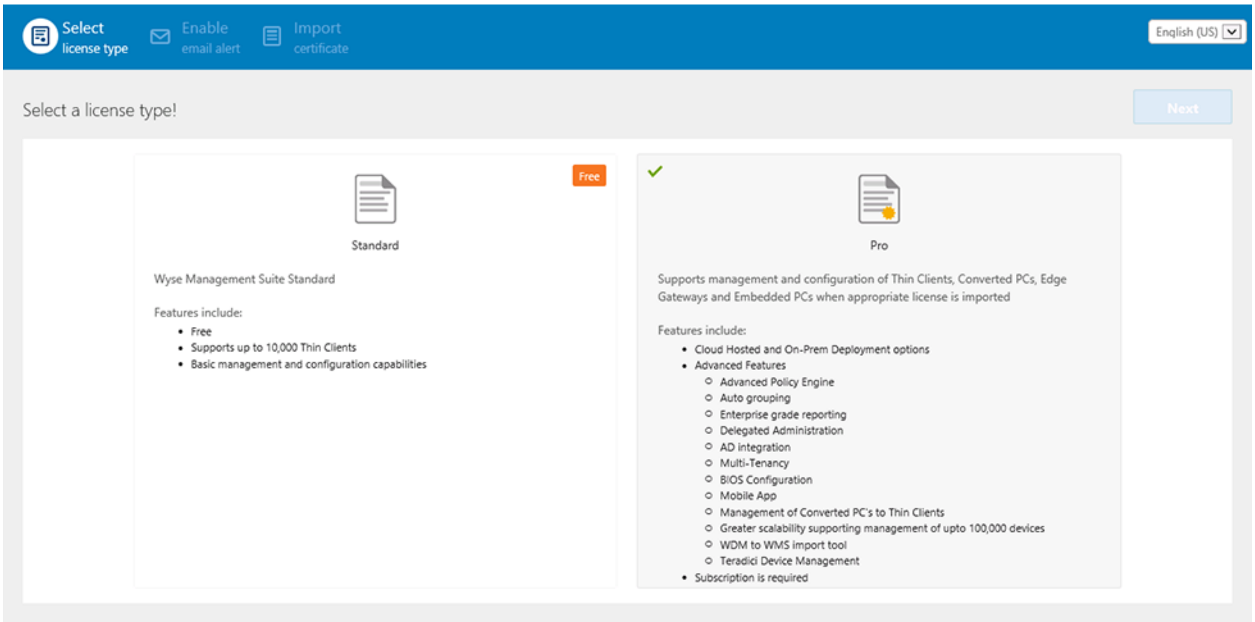


Welcome to Wyse Management Suite

Just a few steps and your WMS will be ready to use.

Figure 1. Welcome page

15. Select your preferred license.
    - If you select the license type as **Standard**, you can 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.



Select a license type!

Wyse management Suite Standard

Features include:

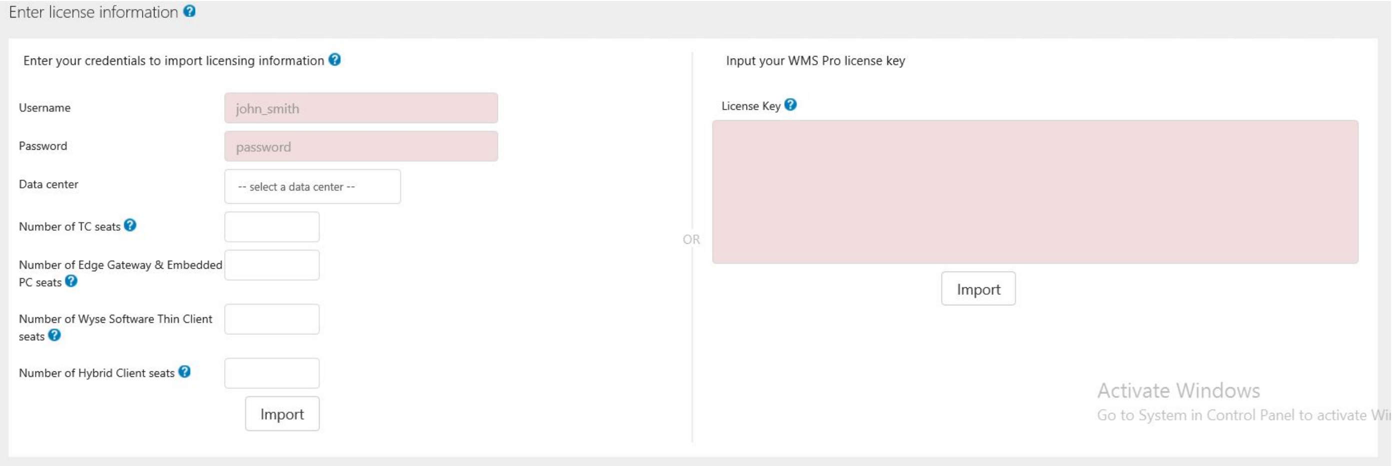
- Free
- Supports up to 10,000 Thin Clients
- Basic management and configuration capabilities

Supports management and configuration of Thin Clients, Converted PCs, Edge Gateways and Embedded PCs when appropriate license is imported

Features include:

- Cloud Hosted and On-Prem Deployment options
- Advanced Features
  - Advanced Policy Engine
  - Auto grouping
  - Enterprise grade reporting
  - Delegated Administration
  - AD integration
  - Multi-Tenancy
  - BIOS Configuration
  - Mobile App
  - Management of Converted PC's to Thin Clients
  - Greater scalability supporting management of upto 100,000 devices
  - WDM to WMS import tool
  - Teradici Device Management
- Subscription is required

Figure 2. License type



Enter license information

Enter your credentials to import licensing information

Username: john_smith

Password: password

Data center: -- select a data center --

Number of TC seats

Number of Edge Gateway & Embedded PC seats

Number of Wyse Software Thin Client seats

Number of Hybrid Client seats

Input your WMS Pro license key

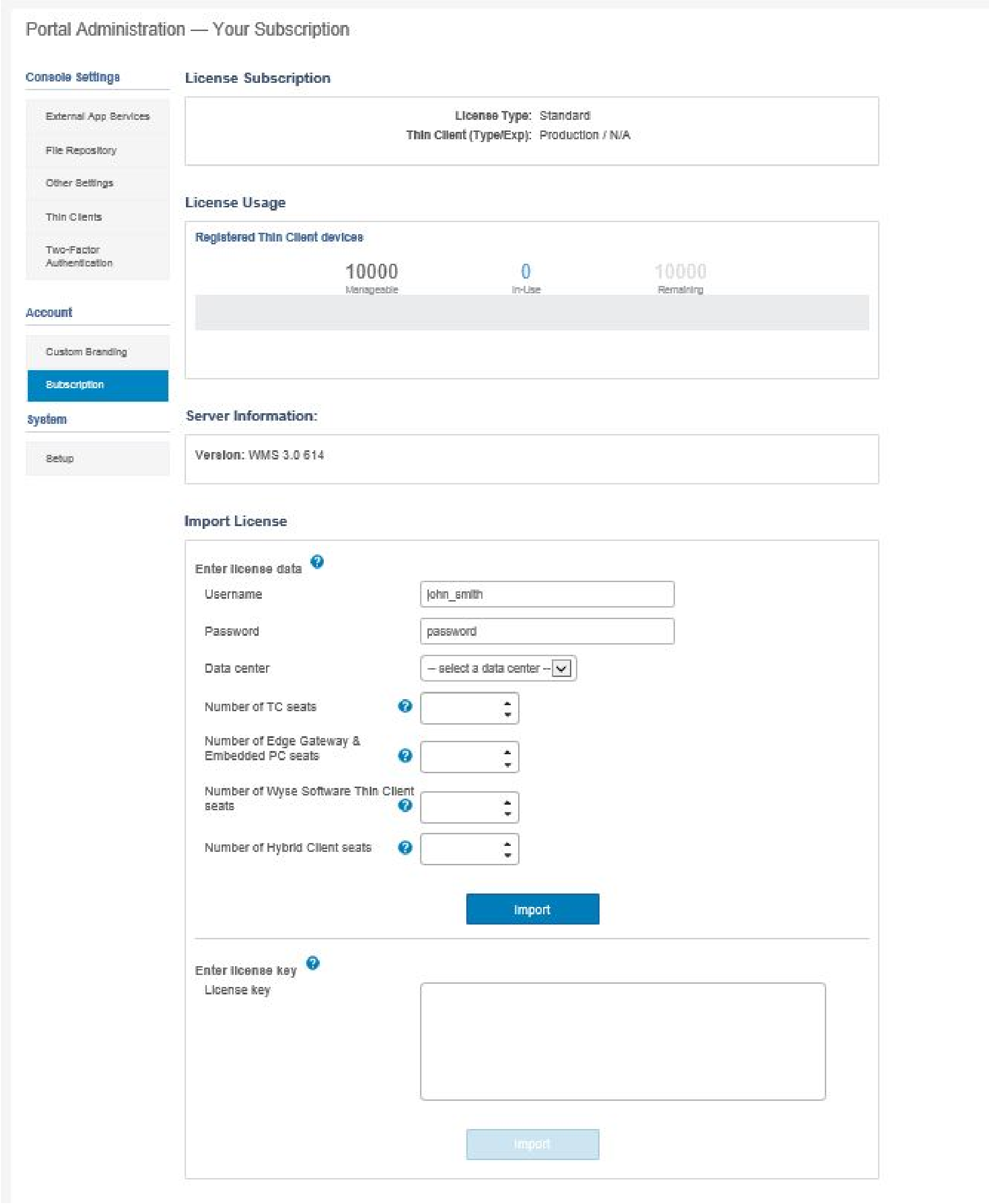
License Key

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
   - EU data center—eu1.wysemanagementsuite.com/ccm-web

b. Go to **Portal Administration** > **Subscription**.



Portal Administration — Your Subscription

Console Settings

- External App Services
- File Repository
- Other Settings
- Thin Clients
- Two-Factor Authentication

Account

- Custom Branding
- Subscription

System

- Setup

License Subscription

License Type: Standard
Thin Client (Type/Exp): Production / N/A

License Usage

Registered Thin Client devices

10000	0	10000
Manageable	In-Use	Remaining

Server Information:

Version: WMS 3.0 614

Import License

Enter license data

Username	john_smith
Password	password
Data center	-- select a data center --
Number of TC seats	
Number of Edge Gateway & Embedded PC seats	
Number of Wyse Software Thin Client seats	
Number of Hybrid Client seats	

Import

Enter license key

License key

Import

Figure 4. Portal administration

c. Enter the number of thin client seats.

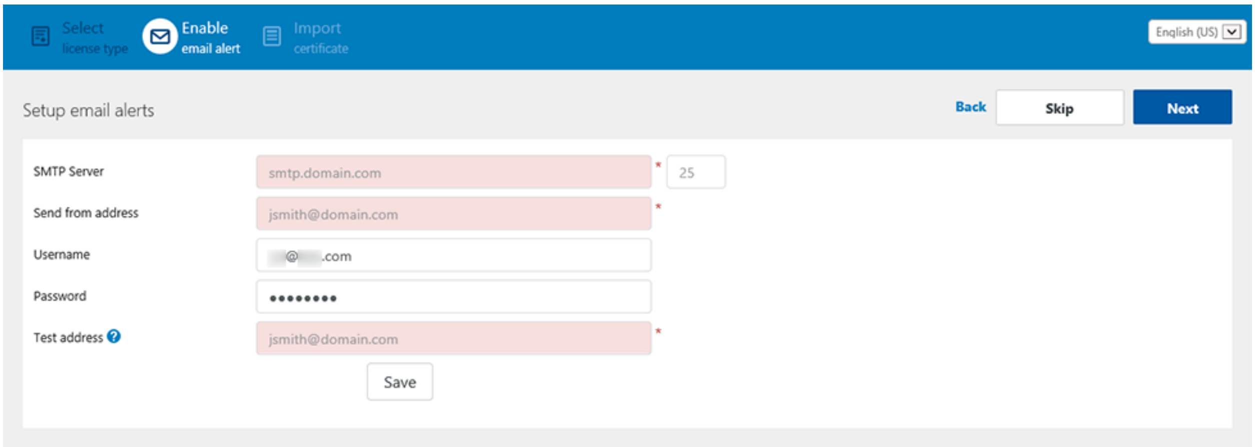
d. Click **Export**.

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.

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

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



Setup email alerts

SMTP Server	smtp.domain.com * 25
Send from address	jsmith@domain.com *
Username	[redacted]@[redacted].com
Password	••••••••
Test address	jsmith@domain.com *

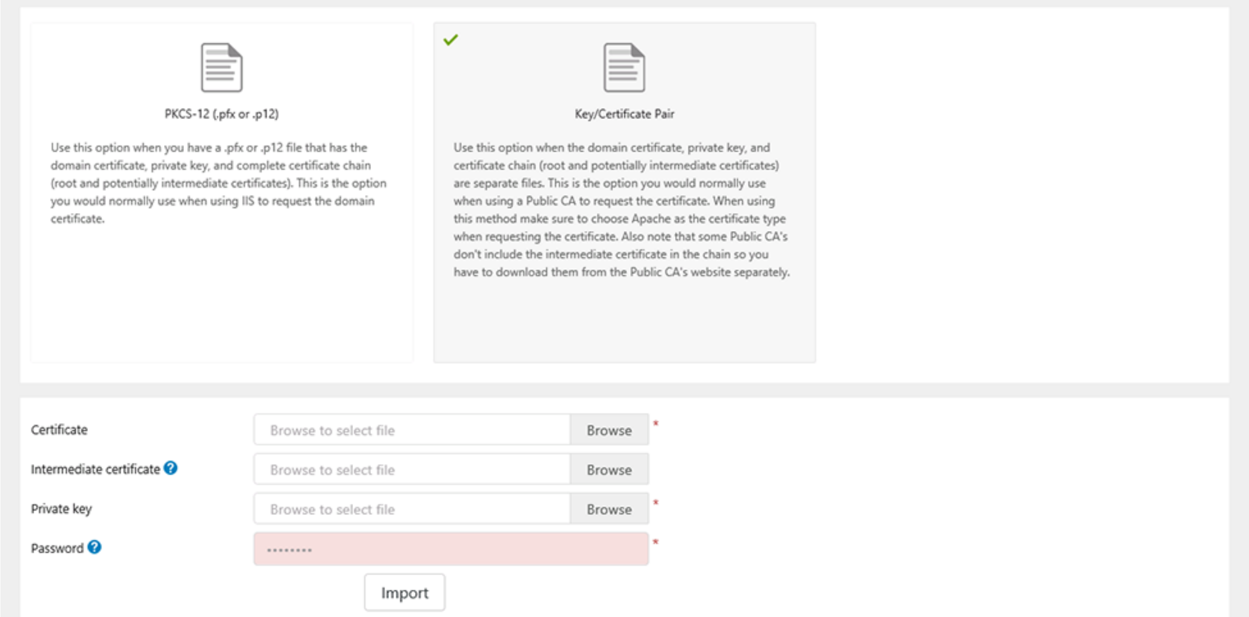
Figure 5. Email alert

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

17. 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 that is generated during installation is not signed by a Certificate Authority such as geotrust.com. You can either import a .pem or .pfx certificate.



PKCS-12 (.pfx or .p12)

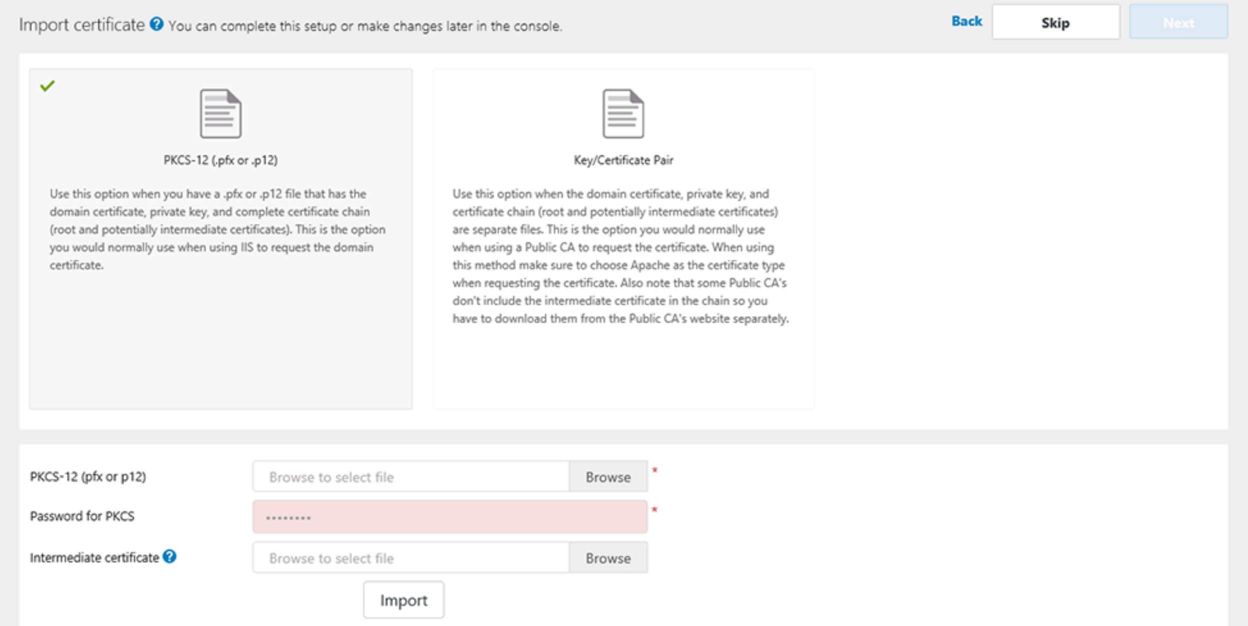
Use this option when you have a .pfx or .p12 file that has the domain certificate, private key, and complete certificate chain (root and potentially intermediate certificates). This is the option you would normally use when using IIS to request the domain certificate.

✓ 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.

Certificate	Browse to select file *
Intermediate certificate	Browse to select file
Private key	Browse to select file *
Password	•••••••• *

Figure 6. Key or certificate value pair



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

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.

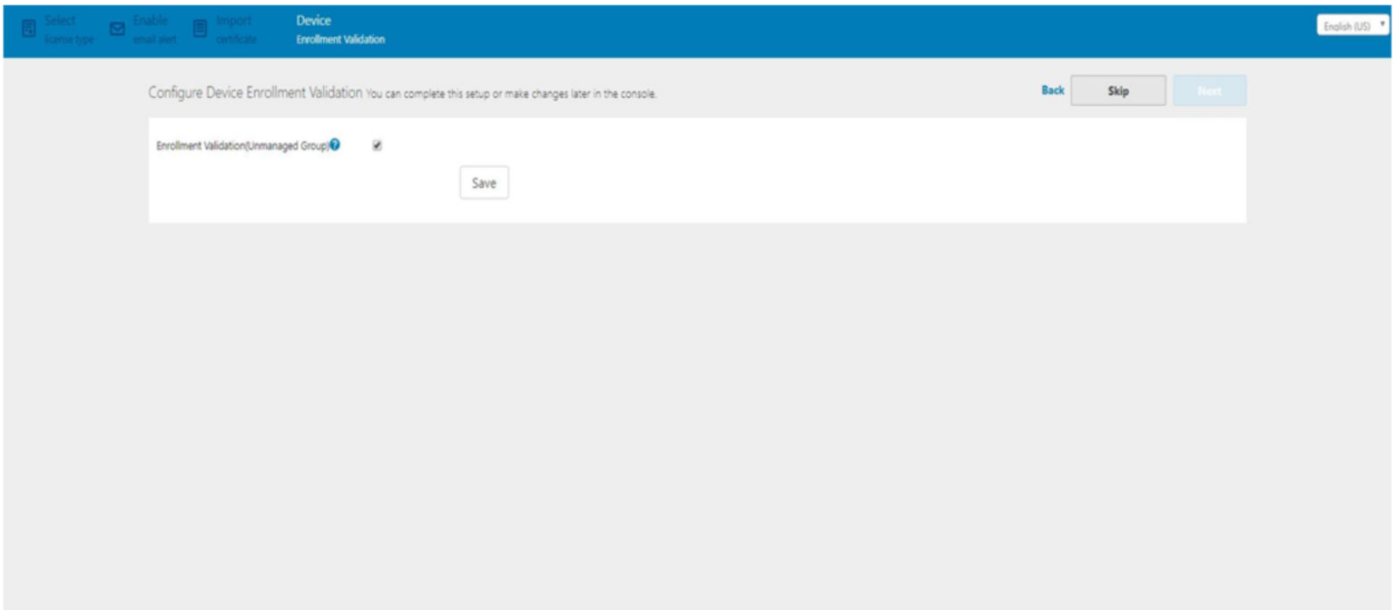
Key/Certificate Pair

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 to select file Browse *
Password for PKCS	•••••••• *
Intermediate certificate	Browse to select file Browse

Figure 7. PKCS-12

18. 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.



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

Enrollment Validation(Unmanaged Group) ☑

Figure 8. Enrollment validation

19. Click **Save** and then click **Next**.
20. Click **Sign in to WMS**.

    The **Dell Management Portal** login page is displayed.

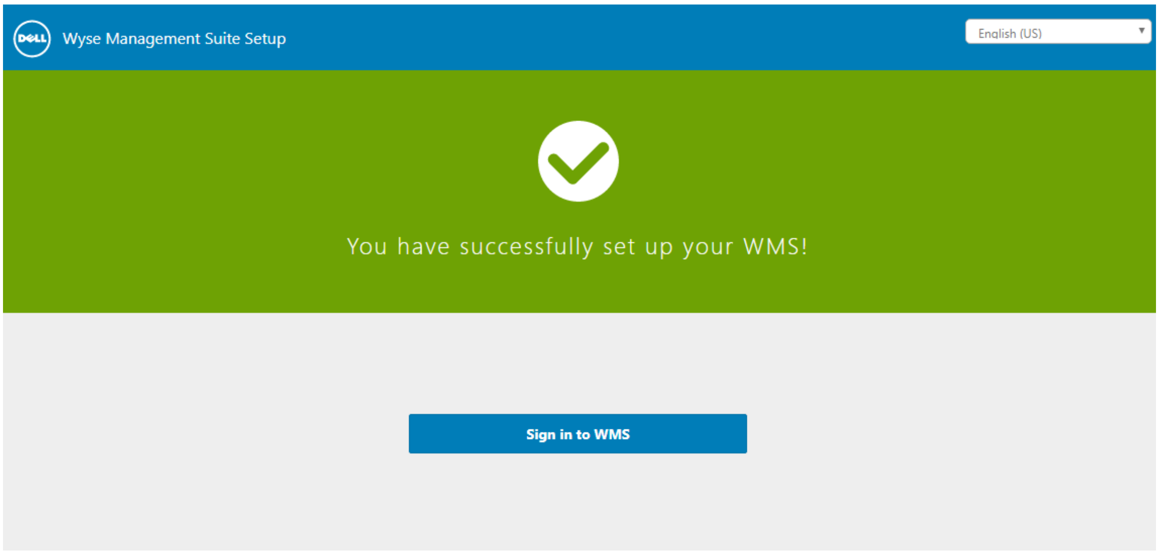

Wyse Management Suite Setup
English (US)
You have successfully set up your WMS!
Sign in to WMS

Figure 9. Sign in page

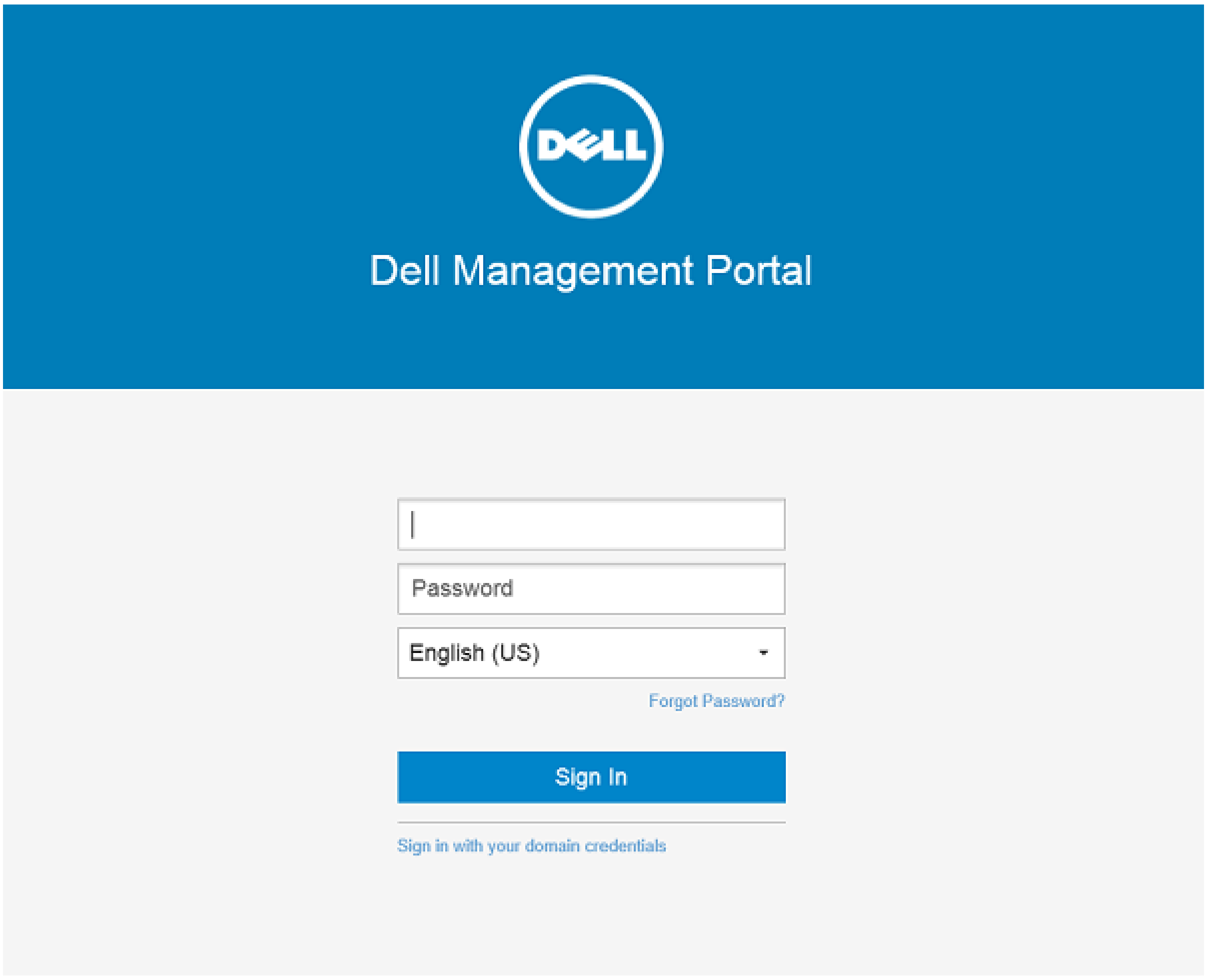


Figure 10. Dell Management Portal

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

Topics:

Logging in to Wyse Management Suite

About this task

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

Steps

1. If you are using Internet Explorer, disable the **Internet Explorer Enhanced Security** and the **Compatibility View** setting
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://wmsserver.domain.com/ccm-web, where, wmsserver.domain.com 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:

About this task

- 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.

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.
   - 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.
- For Wyse Management Suite installed on a private cloud, go to **Portal Adminstration** > **Setup** and select the **Certification Validation** check box, if you have imported certificates from a certificate authority such as 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

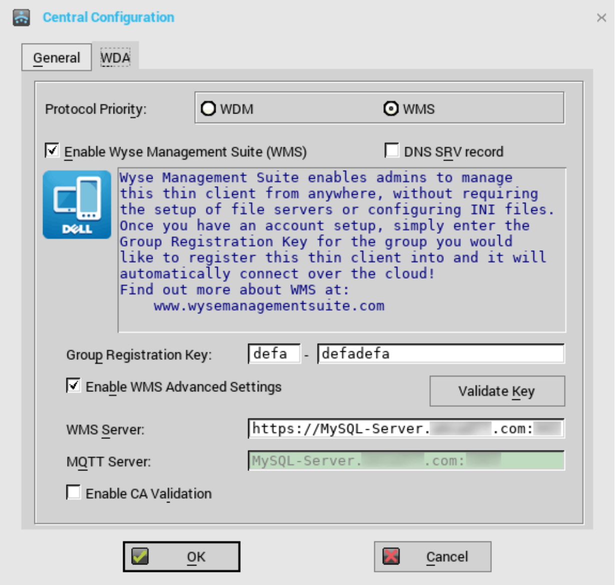
To register the ThinOS devices manually, do the following:

Steps

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.



Central Configuration

General | WDA

Protocol Priority: ○ WDM ● WMS

☑ Enable Wyse Management Suite (WMS) □ DNS SRV record

```
Wyse Management Suite enables admins to manage
this thin client from anywhere, without requiring
the setup of file servers or configuring INI files.
Once you have an account setup, simply enter the
Group Registration Key for the group you would
like to register this thin client into and it will
automatically connect over the cloud!
Find out more about WMS at:
    www.wysemanagementsuite.com
```

Group Registration Key: defa - defadefa

☑ Enable WMS Advanced Settings

Validate Key

WMS Server: https://MySQL-Server.[redacted].com:[redacted]

MQTT Server: MySQL-Server.[redacted].com:[redacted]

□ Enable CA Validation

OK Cancel

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
   - MQTT Server—*eu1-pns.wysemanagementsuite.com:1883*
7. To verify the setup, click **Validate Key**. The device automatically restarts after the key is validated.

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

Next steps

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.

ⓘ **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 4. Registering device by using DHCP option tags

Option Tag	Description
Name—WMS **Data Type**—String **Code**—165 **Description**—WMS Server FQDN	This tag points to the Wyse Management Suite server URL. For example, `wmsserver.acme.com:443`, where wmsserver.acme.com is fully qualified domain name of the server where Wyse Management Suite is installed. For links to register your devices in Wyse Management Suite in public cloud, see Getting started with Wyse Management Suite on public cloud. ⓘ **NOTE:** Do not use https:// in the server URL, or the thin client will not register under Wyse Management Suite. Use https:// if you cannot register the ThinOS 9.x device 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 4. Registering device by using 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	This tag is required if Wyse Management Suite is installed on your system in your private cloud. Do not add this option tag if you are registering your devices with Wyse Management Suite on public cloud. Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. Enter **False** , if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.
Name—GroupToken **Data Type**—String **Code**—199 **Description**—Group Token	This tag is required to register the ThinOS devices with Wyse Management Suite on public or private cloud. This tag is optional to register the Windows Embedded Standard or ThinLinux devices with Wyse Management Suite on private cloud. If the tag is not available, then the devices are automatically registered to the unmanaged group during on-site installation.

Registering devices by using DNS SRV record

ⓘ **NOTE:** For information about 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 the 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 5. 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 hovers over the Wyse Management Suite server URL. For example, `wmsserver.acme.com:443`, where wmsserver.acme.com is fully qualified domain name of the server where Wyse Management Suite is installed. For links to register your devices in Wyse Management Suite in public cloud, see Getting started with Wyse Management Suite on public cloud. ⓘ **NOTE:** Do not use https:// in the server URL, or the thin client will not register under Wyse Management Suite. Use

Table 5. Configuring device by using DNS SRV record (continued)

URL/Tag	Description
	https:// if you cannot register the ThinOS 9.x device 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 hover over 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.<Domain> **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-premises 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.<Domain> **Record Type**—TEXT	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. 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.

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.

3

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

To log in to the Wyse Management Suite console, you must have a supported web browser that is installed on your computer. 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 the 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 on www.wysemanagementsuite.com or when you purchase your subscription. You can purchase the Wyse Management Suite subscription from the Dell Sales team or from your local Dell partner. For more details, see www.wysemanagementsuite.com.

NOTE: An externally accessible repository must be installed on a server with a DMZ while using the pro edition of Wyse Management Suite on the public cloud if you are using thin clients that do not support cloud applications such as Windows Embedded computers. 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.

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 computer 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 an 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 6. 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 ● TCP 5172, 49159—End-User Management Software Development Kit (EMSDK)—optional and required only to manage Teradici devices ● TLS 443—Secure MQTT communication			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 6. Prerequisites (continued)

Description	10,000 devices or less	50,000 devices or less	120,000 devices or less	Wyse Management Suite – Software repository
	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.

4

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:

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 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.

5

Upgrade Wyse Management Suite version 2.x to 3.x

Prerequisites

- Ensure that there is enough space on the drive where Wyse Management Suite is installed and the local repository is configured.
- If you have installed or configured an antivirus or other monitoring tools on the Wyse Management Suite setup, Dell Technologies recommends that you disable the tools temporarily till the upgrade is complete. You can also add an appropriate exclusion to the Wyse Management Suite install directory, temporary directory and local repository directory.

Steps

1. Double-click the Wyse Management Suite 3.x installer package.
2. On the **Welcome** screen, click **Next**.
   The EULA details are displayed.

   NOTE: This screen is displayed when you upgrade from Wyse Management Suite 3.0 to 3.x.
3. Read the License Agreement.
4. Select the **I accept the terms in the license agreement** and click **Next**.
5. On the **Upgrade** 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 EM SDK is installed on the server during the previous Wyse Management Suite installation, the Teradici EM SDK components are updated automatically. If EM SDK is not installed on the device during the previous installation, select the Teradici EM SDK checkbox to install and configure the Teradici EM SDK components.

   NOTE: You can also install and update Teradici EM SDK using the Wyse Management Suite installer.
6. Select the **Bind Memcached to 127.0.0.1** check box to bind the memcache to local server—127.0.0.1. If this check box is not selected, the memcache is **binded** to FQDN.
7. Select all the appropriate versions of TLS based on the support criteria of the devices being managed.

   NOTE: The WDA version lower than WDA_14.4.0.135_Unified, Import tool, and the 32-bit Merlin image are not compatible with TLSv1.1 and later. Select TLSv1.0 if the Wyse Management Suite environment has devices with older version of WDA, Import tool, or devices installed with 32-bit Merlin image.
8. Click **Launch** to open the Wyse Management Suite web console.

6

Upgrade Wyse Management Suite version 3.x to 3.3

Prerequisites

- Ensure that there is enough space on the drive where Wyse Management Suite is installed and the local repository is configured.
- If you have installed or configured an antivirus or other monitoring tools on the Wyse Management Suite setup, Dell Technologies recommends that you disable the tools temporarily until the upgrade is complete. You can also add an appropriate exclusion to the Wyse Management Suite install directory, temporary directory, and local repository directory.

Steps

1. Double-click the Wyse Management Suite 3.2 installer package.
2. On the **Welcome** screen, click **Next**.
   The EULA details are displayed.

   ⓘ **NOTE:** This screen is displayed when you upgrade from Wyse Management Suite 3.0 to 3.x.
3. Read the License Agreement.
4. Select the **I accept the terms in the license agreement** and click **Next**.
5. On the **Upgrade** 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 user.

   ⓘ **NOTE:** If EM SDK is installed on the server during the previous Wyse Management Suite installation, the Teradici EM SDK components are updated automatically. If EM SDK is not installed on the device during the previous installation, select the Teradici EM SDK checkbox to install and configure the Teradici EM SDK components.

   ⓘ **NOTE:** You can also install and update Teradici EM SDK using the Wyse Management Suite installer.
6. Select the **Bind Memcached to 127.0.0.1** check box to bind the memcache to local server—127.0.0.1. If this check box is not selected, the memcache is **binded** to FQDN.
7. Select a port for secure MQTT communication. The default port is 8443.

   ⓘ **NOTE:** The port number for secure MQTT communication should not be 0. The port selection option is displayed when you are upgrading Wyse Management Suite from version 3.1 and 3.1.1 to version 3.3.

   Update MQTT Config window is displayed when there is a Hostname mismatch between MQTT URLs in the database.
8. Select the **Apply recommended changes** check box if you want to change the URLs.

   ⓘ **NOTE: Update MQTT Config** window is displayed when you are upgrading Wyse Management Suite from version 3.2 and 3.2.1 to version 3.3.
9. Click **Next**.
10. Click **Launch** to open the Wyse Management Suite web console.

7

Upgrade Wyse Management Suite version 3.x to 3.5

Prerequisites

- Ensure that there is enough space on the drive where Wyse Management Suite is installed and the local repository is configured.
- If you have installed or configured an antivirus or other monitoring tools on the Wyse Management Suite setup, Dell Technologies recommends that you disable the tools temporarily until the upgrade is complete. You can also add an appropriate exclusion to the Wyse Management Suite install directory, temporary directory, and local repository directory.

Steps

1. Double-click the Wyse Management Suite 3.5 installer package.
2. On the **Welcome** screen, click **Next**.
   The EULA details are displayed.

   ⓘ **NOTE:** This screen is displayed when you upgrade from Wyse Management Suite 3.0 to 3.x.
3. Read the License Agreement.
4. Select the **I accept the terms in the license agreement** and click **Next**.
5. On the **Upgrade** page, do the following:
   a. 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.

      The password must be more than 8 characters.

   b. Click **Next**.
   c. The **Service Account Credentials** screen is displayed. A local user with least privileges is created with the credentials that are entered in this screen. The Dell Wyse Management Suite services run on this user account.
   d. Enter the service account credentials.

      The password must be 9 to 127 characters.

   e. Click **Next**.
      The **Software Vault Credentials** screen is displayed. Software vault is used to store sensitive data required by the Dell Wyse Management Suite application.
   f. Enter the password for software vault.

      The password must be more than 8 characters.

   g. Click **Next**.

   ⓘ **NOTE:** If EM SDK is installed on the server during the previous Wyse Management Suite installation, the Teradici EM SDK components are updated automatically. If EM SDK is not installed on the device during the previous installation, select the **Teradici EM SDK** checkbox to install and configure the Teradici EM SDK components.

   ⓘ **NOTE:** You can also install and update Teradici EM SDK using the Wyse Management Suite installer.
6. Select a port for secure MQTT communication. The default port is 8443.

   ⓘ **NOTE:** The port number for secure MQTT communication should not be 0. The port selection option is displayed when you are upgrading Wyse Management Suite from version 3.1 and 3.1.1 to version 3.5.
7. Select the **Apply recommended changes** check box if you want to change the URLs.

   ⓘ **NOTE:** **Update MQTT Config** window is displayed when you are upgrading Wyse Management Suite from version 3.2 and 3.2.1 to version 3.5.
8. Click **Next**.
9. Click **Launch** to open the Wyse Management Suite web console.

8

Upgrade Wyse Management Suite version 3.x to 3.6

Prerequisites

- Ensure that there is enough space on the drive where Wyse Management Suite is installed and the local repository is configured.
- If you have installed or configured an anti-virus or other monitoring tools on the Wyse Management Suite setup, Dell Technologies recommends that you disable the tools temporarily until the upgrade is complete. You can also add an appropriate exclusion to the Wyse Management Suite install directory, temporary directory, and local repository directory.

Steps

1. Double-click the Wyse Management Suite 3.6 installer package.
2. On the **Welcome** screen, click **Next**.
   The EULA details are displayed.

   ⓘ **NOTE:** This screen is displayed when you upgrade from Wyse Management Suite 3.0 to 3.x.
3. Read the License Agreement.
4. Select the **I accept the terms in the license agreement** and click **Next**.
5. On the **Upgrade** page, do the following:
   a. 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 user.

      The password must be more than eight characters.

   b. Click **Next**.

      The **Service Account Credentials** screen is displayed. Select the options based on your existing Wyse Management Suite version.

      - If you are upgrading from Wyse Management Suite version 3.3 or 3.3.1 to 3.6, the following options are displayed:
        - **Create a New Local User**—Select this option to enter credentials and create a new local user with least privileges. The new user is added to the **Users** group, but the user will not have administrator rights.

          ⓘ **NOTE:** The username that you enter in the **Service Account Credentials** screen must not be the same as your Teradici username. The username must be 2 to 20 characters. Your password must be 9 to 127 characters with at least one upper case, one lower case, one number, and one special character. Spaces are not allowed in the password.
        - **Use an Existing Local User**—Select this option to enter the credentials of an existing local user. A message is displayed when you select this option. Ensure that the user already exists, has service logon rights (**SeServiceLogonRight**), and has successfully logged in at least once to the system. Dell Technologies recommends ensuring that the user does not carry administrative rights.

          ⓘ **NOTE:** If you select this option, the complexity of the password is not verified and the username that you enter must be 2 to 20 characters.
        - **Use an Existing Domain User**—Select this option to enter the credentials of an existing domain user. A message is displayed when you select this option. Ensure that the user already exists in the domain, has service logon rights (**SeServiceLogonRight**), and has successfully logged in at least once to the system. Dell Technologies recommends ensuring that the user does not carry administrative rights.

          ⓘ **NOTE:** If you select this option, the complexity of the password is not verified.

          ⓘ **NOTE:** Ensure that the LDAP port 389 is open to communicate from Wyse Management Suite on-premise server to AD domain server.
      - If you are upgrading from Wyse Management Suite version 3.5 to 3.6, enter the credentials to create a local user with least privileges. The Dell Wyse Management Suite services run on this user account.

   c. Click **Next** after you enter the credentials.

The **Software Vault Credentials** screen is displayed. Software vault is used to store sensitive data required by the Dell Wyse Management Suite application.

d. Enter the password for software vault.

   The password must be more than eight characters.

e. Click **Next**.

ⓘ **NOTE:** If EM SDK is installed on the server during the previous Wyse Management Suite installation, the Teradici EM SDK components are updated automatically. If EM SDK is not installed on the device during the previous installation, select the **Teradici EM SDK** checkbox to install and configure the Teradici EM SDK components.

ⓘ **NOTE:** You can also install and update Teradici EM SDK using the Wyse Management Suite installer.

6. Select a port for secure MQTT communication. The default port is 8443.

   ⓘ **NOTE:** The port number for secure MQTT communication should not be 0. The port selection option is displayed when you are upgrading Wyse Management Suite from version 3.1 and 3.1.1 to version 3.6.

7. Select the **Apply recommended changes** check box if you want to change the URLs.

   ⓘ **NOTE:** **Update MQTT Config** window is displayed when you are upgrading Wyse Management Suite from version 3.2 and 3.2.1 to version 3.6.

8. Click **Next**.
9. Click **Launch** to open the Wyse Management Suite web console.

9

Upgrade Wyse Management Suite version 3.x to 4.0

Prerequisites

- Ensure that there is enough space on the drive where Wyse Management Suite is installed and the local repository is configured.
- If you have installed or configured an anti-virus or other monitoring tools on the Wyse Management Suite setup, Dell Technologies recommends that you disable the tools temporarily until the upgrade is complete. You can also add an appropriate exclusion to the Wyse Management Suite install directory, temporary directory, and local repository directory.

Steps

1. Double-click the Wyse Management Suite 4.0 installer package.
2. On the **Welcome** screen, click **Next**.
   The EULA details are displayed.

   ⓘ **NOTE:** This screen is displayed when you upgrade from Wyse Management Suite 3.0 to 3.x and 4.0.
3. Read the License Agreement.
4. Select the **I accept the terms in the license agreement** and click **Next**.
5. On the **Upgrade** page, do the following:
   a. 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 user.

      The password must be more than eight characters.

   b. Click **Next**.

      The **Service Account Credentials** screen is displayed. Select the options based on your existing Wyse Management Suite version.
      - If you are upgrading from Wyse Management Suite version 3.3 or 3.3.1 to 4.0, the following options are displayed:
        - **Create a New Local User**—Select this option to enter credentials and create a new local user with least privileges. The new user is added to the **Users** group, but the user will not have administrator rights.

          ⓘ **NOTE:** The username that you enter in the **Service Account Credentials** screen must not be the same as your Teradici username. The username must be 2 to 20 characters. Your password must be 9 to 127 characters with at least one upper case, one lower case, one number, and one special character. Spaces are not allowed in the password.
        - **Use an Existing Local User**—Select this option to enter the credentials of an existing local user. A message is displayed when you select this option. Ensure that the user already exists, has service logon rights (**SeServiceLogonRight**), and has successfully logged in at least once to the system. Dell Technologies recommends ensuring that the user does not carry administrative rights.

          ⓘ **NOTE:** If you select this option, the complexity of the password is not verified and the username that you enter must be 2 to 20 characters.
        - **Use an Existing Domain User**—Select this option to enter the credentials of an existing domain user. A message is displayed when you select this option. Ensure that the user already exists in the domain, has service logon rights (**SeServiceLogonRight**), and has successfully logged in at least once to the system. Dell Technologies recommends ensuring that the user does not carry administrative rights.

          ⓘ **NOTE:** If you select this option, the complexity of the password is not verified.

          ⓘ **NOTE:** Ensure that the LDAP port 389 is open to communicate from Wyse Management Suite on-premise server to AD domain server.
      - If you are upgrading from Wyse Management Suite version 3.5 to 4.0, enter the credentials to create a local user with least privileges. The Dell Wyse Management Suite services run on this user account.

   c. Click **Next** after you enter the credentials.

The **Software Vault Credentials** screen is displayed. Software vault is used to store sensitive data required by the Dell Wyse Management Suite application.

d. Enter the password for software vault.

   The password must be more than eight characters.

e. Click **Next**.

ⓘ **NOTE:** If EM SDK is installed on the server during the previous Wyse Management Suite installation, the Teradici EM SDK components are updated automatically. If EM SDK is not installed on the device during the previous installation, select the **Teradici EM SDK** checkbox to install and configure the Teradici EM SDK components.

ⓘ **NOTE:** You can also install and update Teradici EM SDK using the Wyse Management Suite installer.

6. Select a port for secure MQTT communication. The default port is 8443.

   ⓘ **NOTE:** The port number for secure MQTT communication should not be 0. The port selection option is displayed when you are upgrading Wyse Management Suite from version 3.1 and 3.1.1 to version 4.0.

7. Select the **Apply recommended changes** check box if you want to change the URLs.

   ⓘ **NOTE:** **Update MQTT Config** window is displayed when you are upgrading Wyse Management Suite from version 3.2 and 3.2.1 to version 4.0.

8. Click **Next**.
9. Click **Launch** to open the Wyse Management Suite web console.

10

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.

11

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.

12

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.

13

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.

A

User creation for on-premise installation

This section describes the best practices for user creation and how to use the same username for on-premise installation and repository installation.

-

Topics:

Installation using an existing local user

Steps

1. Log in to the Windows server as an administrator where Wyse Management Suite should be installed.
2. Go to **Computer Management** > **Local users and groups** > **Users**.
3. Right-click the right window pane and click **New User**.
   The **New User** window is displayed.
4. Enter the details in the **User name**, **Full name**, **Description**, **Password**, and **Confirm Password** field.
5. Click **Create**.
   The new user is created.
6. Right-click the created user and click **Properties**.
7. Click the **Member** tab and add the user group, if required. By default, the created user is part of the local user's group.
8. Go to **Local Security Policy** > **Local Policies** > **User Right Assignment**.
9. In the right pane, select the following policies and add the created user:
   - **Log on as a service**
   - **Access this computer from the network**
   - **Allow log on locally**
   - **Allow log on through Remote Desktop Services**

   NOTE: Ensure that the user or the user group is not part of the following **Deny Policies**:
   - **Deny access to this computer from the network**
   - **Deny log on locally**
   - **Deny log on through Remote Desktop Services**

Results

During the installation, use the credentials that are created from the above steps when you select the **Use an Existing Local User** option.

NOTE:
- The selected user must exist and successfully log in to the device once.
- Dell Technologies recommends that this user does not have administrative rights.
- The installer does not perform any password complexity checks for this user.
- Run `gpupdate /force` after creating user rights on the server where Wyse Management Suite is installed.

Installation using an existing domain user

Steps

1. Log in to the Active Directory Domain server as an administrator.
2. Go to **Active Directory Users** > **Computers** > **Users**.
3. Right-click the right window pane and click **New User**.
   The **New User** window is displayed.
4. Enter the details in the **First name**, **Last name**, **Full name**, and **User logon name** fields.
5. Click **Next** and enter the password details.
6. Save the new user details.
7. Right-click the created user and click **Properties**.
8. Click the **Member** tab and add the user group, if required. By default, the created user is part of the local user's group.
9. Log in to the Windows server as an administrator where Wyse Management Suite should be installed.
10. Go to **Local Security Policy** > **Local Policies** > **User Right Assignment**.
11. In the right pane, select the following policies and add the created domain user:
    - **Log on as a service**
    - **Access this computer from the network**
    - **Allow log on locally**
    - **Allow log on through Remote Desktop Services**

    NOTE: Ensure that the domain user is not part of the following **Deny Policies**:
    - **Deny access to this computer from the network**
    - **Deny log on locally**
    - **Deny log on through Remote Desktop Services**

Results

During the installation, use the credentials that are created from the above steps when you select the **Use an Existing Domain User** option.

NOTE:
- The selected user must exist and successfully log in to the device once.
- Dell Technologies recommends that this user does not have administrative rights.
- The installer does not perform any password complexity checks for this user.
- Run `gpupdate /force` after creating user rights on the server where Wyse Management Suite is installed.

Alternate way to identify allow or deny Policy for a user or user group

You can identify whether a user or a user group belongs to the **Allow Policy** or **Deny Policy** by running the command `secedit /export /areas USER_RIGHTS /cfg C:\Policy.txt` in **Command Prompt** as an administrator.

You can open the `Policy.txt` file and check the **Allow Policy** or **Deny Policy** assignments about the Wyse Management Suite user.

B

Remote database

A remote or cloud database 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. The functionality of Wyse Management Suite does not change if the database is installed using Wyse Management Suite or externally.

For information about update, backup, restore, rollback, or vulnerability update, go to https://docs.mongodb.com/ and https://mariadb.org/documentation/.

Topics:

Configure Mongo database

Prerequisites

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.

Steps

1. Install the MongoDB version 4.2.16.
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\"" DisplayName= "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;`

Next steps

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.

About this task

ⓘ **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:

Steps

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.

Next steps

ⓘ **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.

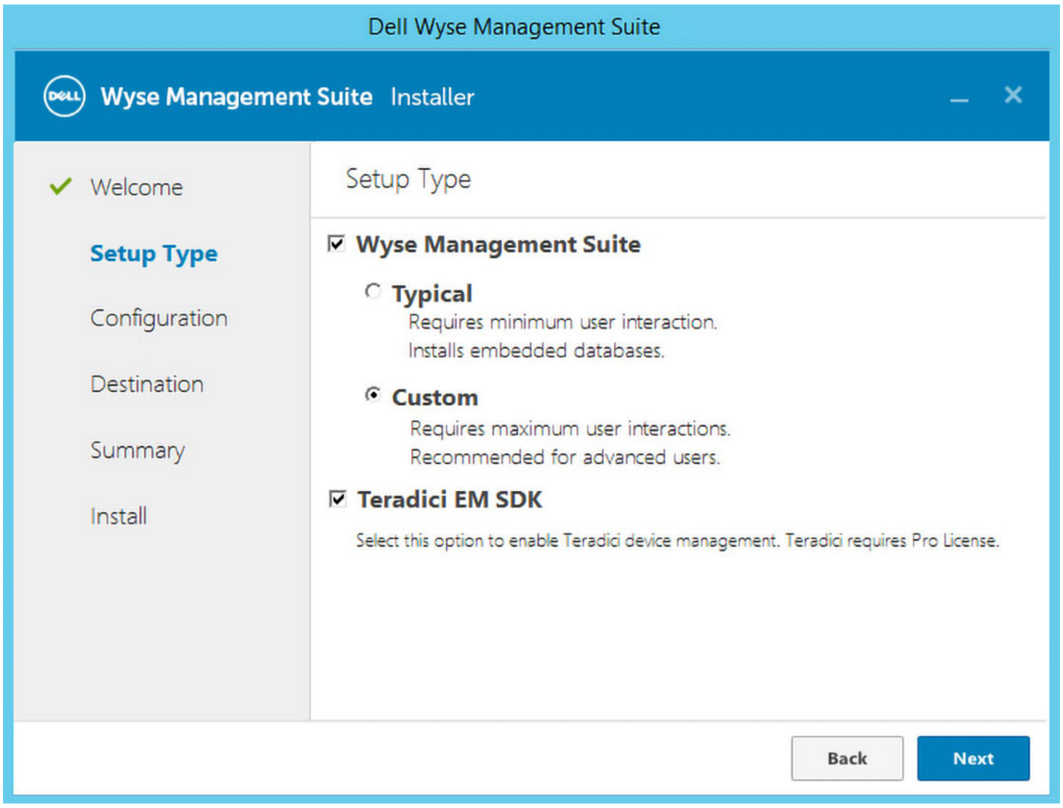
In the Wyse Management Suite installer, the administrator must use the same user name and password that was created to access the stratus databases in MariaDB. For information about setting the MariaDB on the Wyse Management Suite installer, see Custom installation.

C

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**.



Setup Type

☑ **Wyse Management Suite**

○ **Typical**
Requires minimum user interaction.
Installs embedded databases.

● **Custom**
Requires maximum user interactions.
Recommended for advanced users.

☑ **Teradici EM SDK**
Select this option to enable Teradici device management. Teradici requires Pro License.

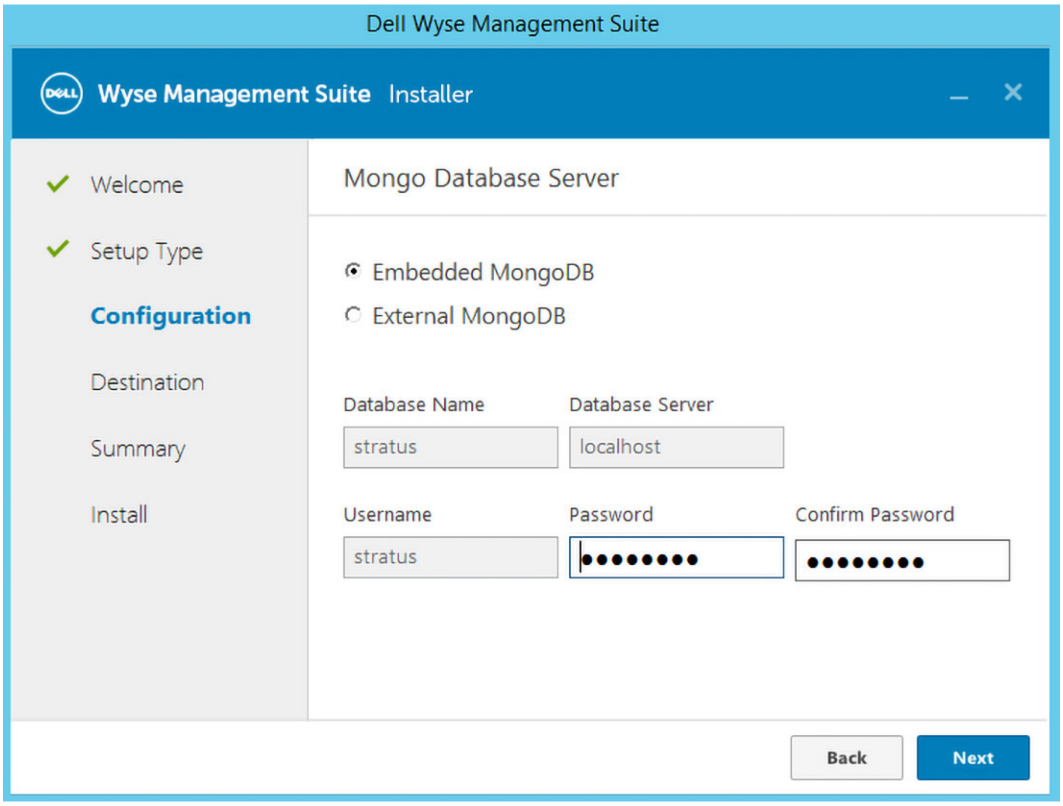
Figure 12. Setup type

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:** The password must be 9 to 31 characters long.

     ⓘ **NOTE:** User name and database server details are not required if the Embedded Mongo database is selected, and the respective fields are grayed out.



Mongo Database Server

● Embedded MongoDB

○ External MongoDB

Database Name: stratus

Database Server: localhost

Username: stratus

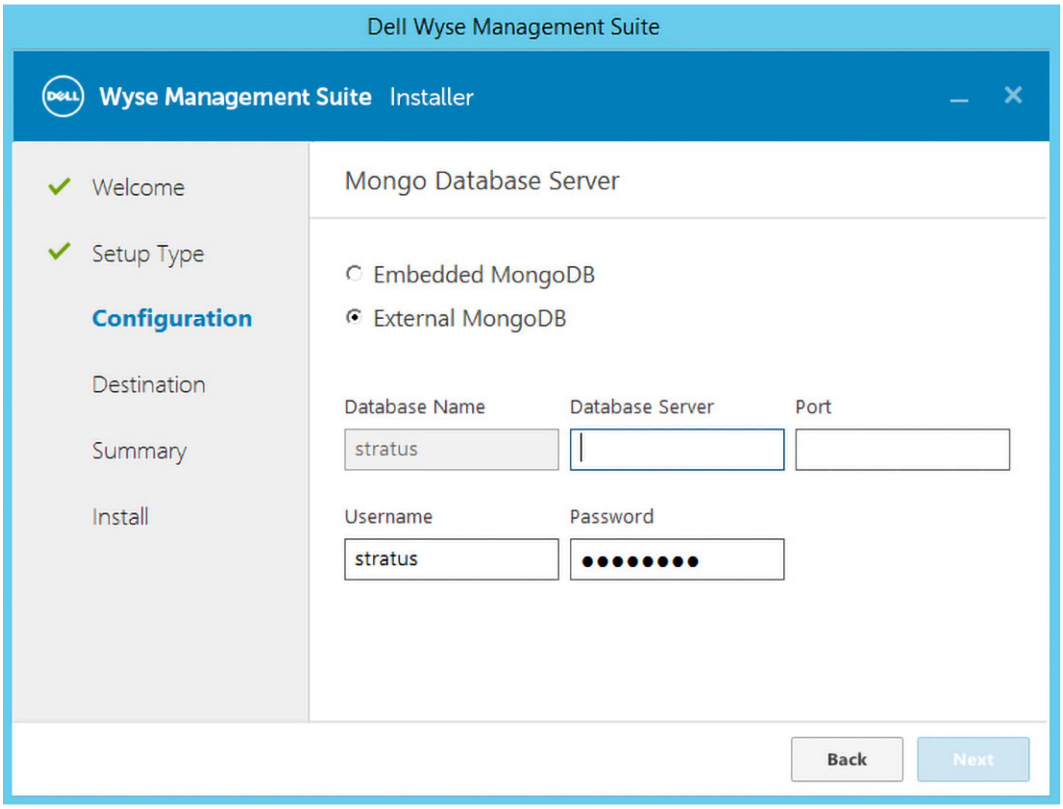
Password: ••••••••

Confirm Password: ••••••••

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.



Mongo Database Server

○ Embedded MongoDB

● External MongoDB

Database Name: stratus

Database Server:

Port:

Username: stratus

Password: ••••••••

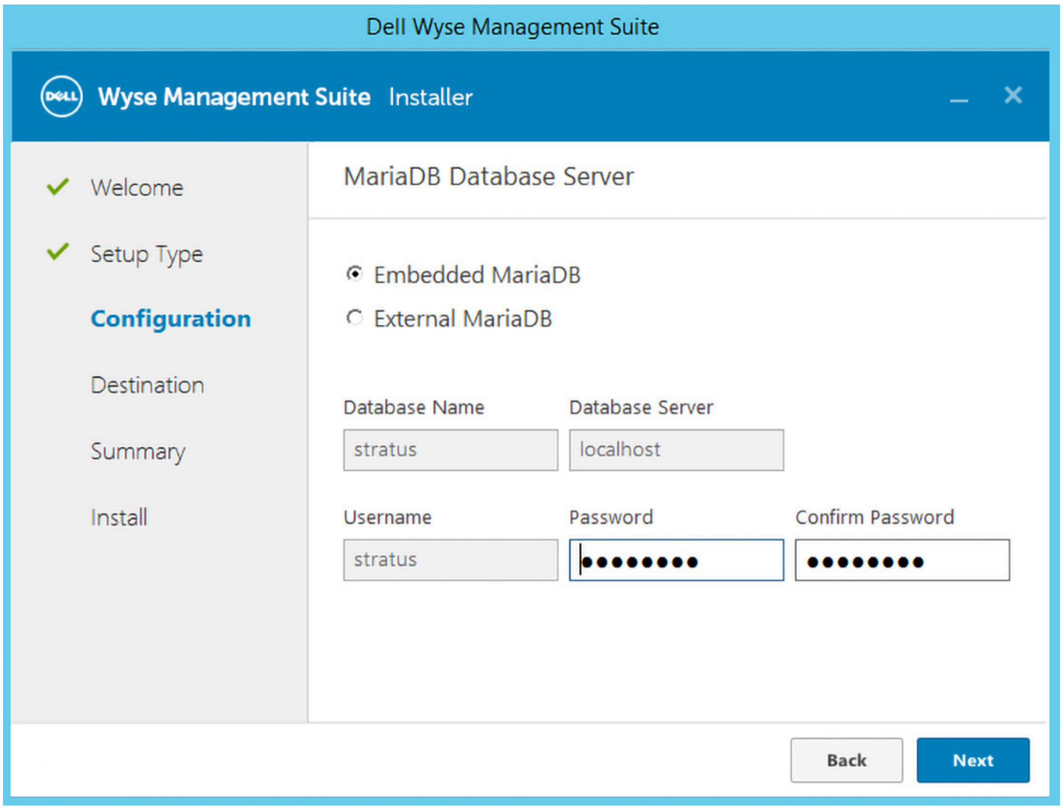
Figure 14. External MongoDB

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**.

     ⓘ **NOTE:** The password must be 9 to 31 characters long.



Dell Wyse Management Suite

Wyse Management Suite Installer

MariaDB Database Server

● Embedded MariaDB

○ External MariaDB

Database Name: stratus

Database Server: localhost

Username: stratus

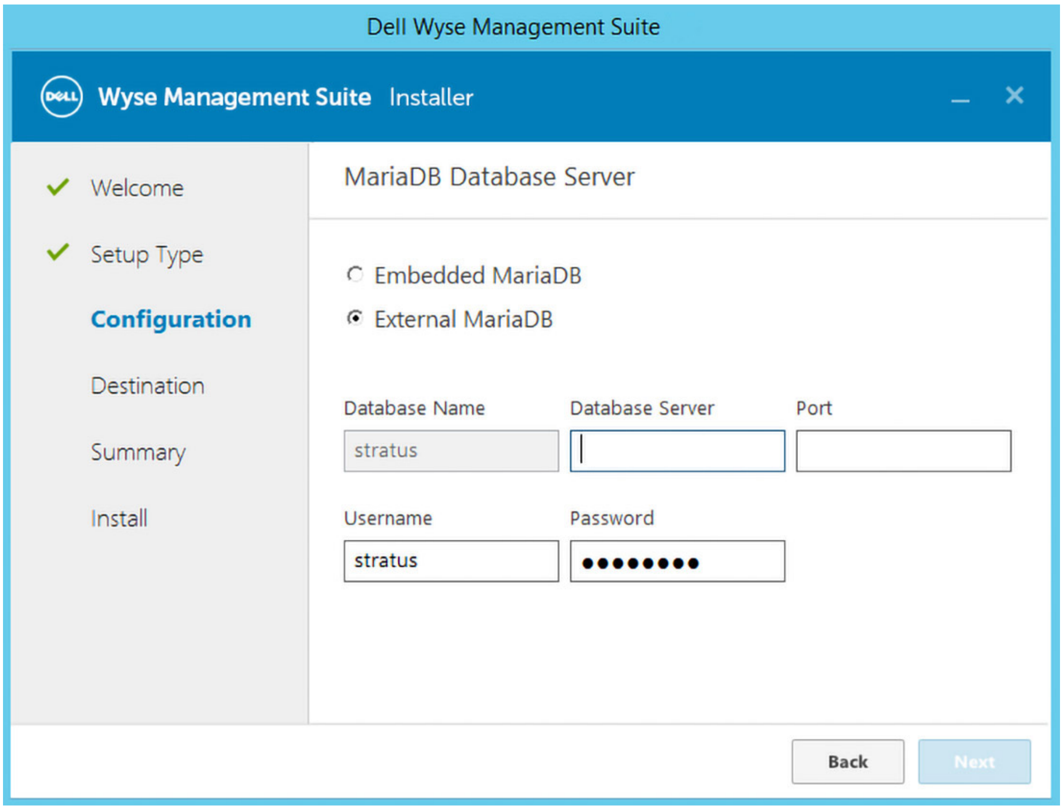
Password: ••••••••

Confirm Password: ••••••••

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.



MariaDB Database Server

○ Embedded MariaDB

● External MariaDB

Database Name: stratus

Database Server:

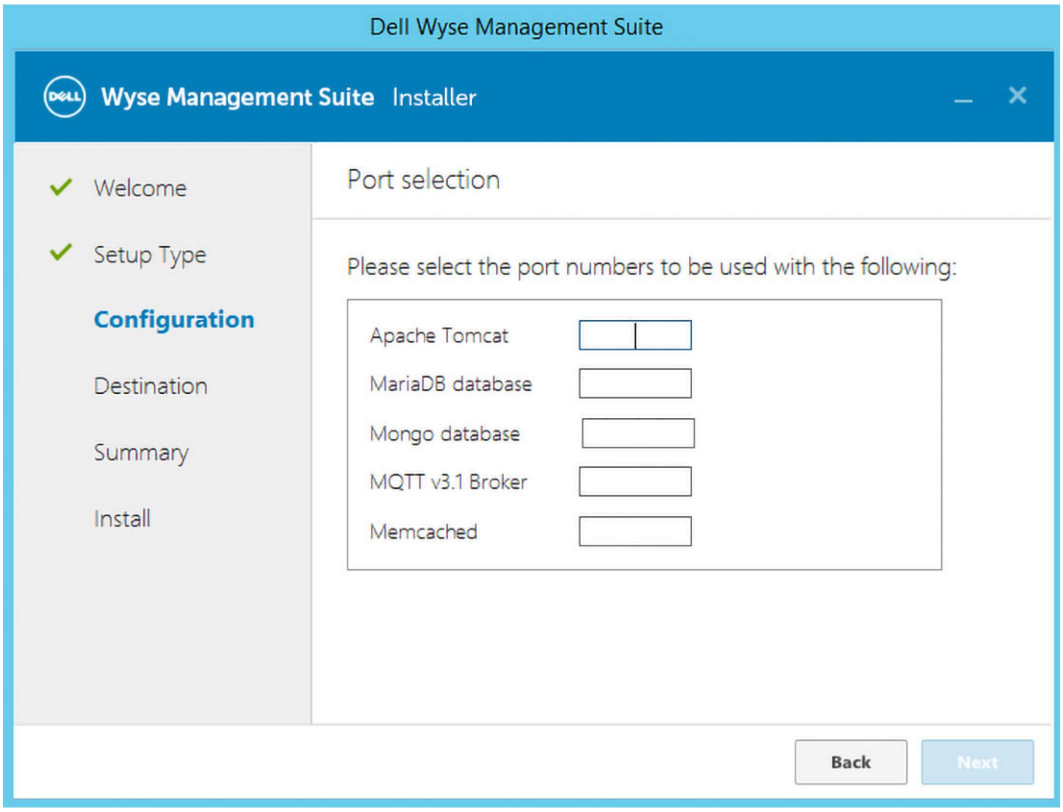
Port:

Username: stratus

Password: ●●●●●●●●

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



Port selection

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

Apache Tomcat	
MariaDB database	
Mongo database	
MQTT v3.1 Broker	
Memcached	

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.

D

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.

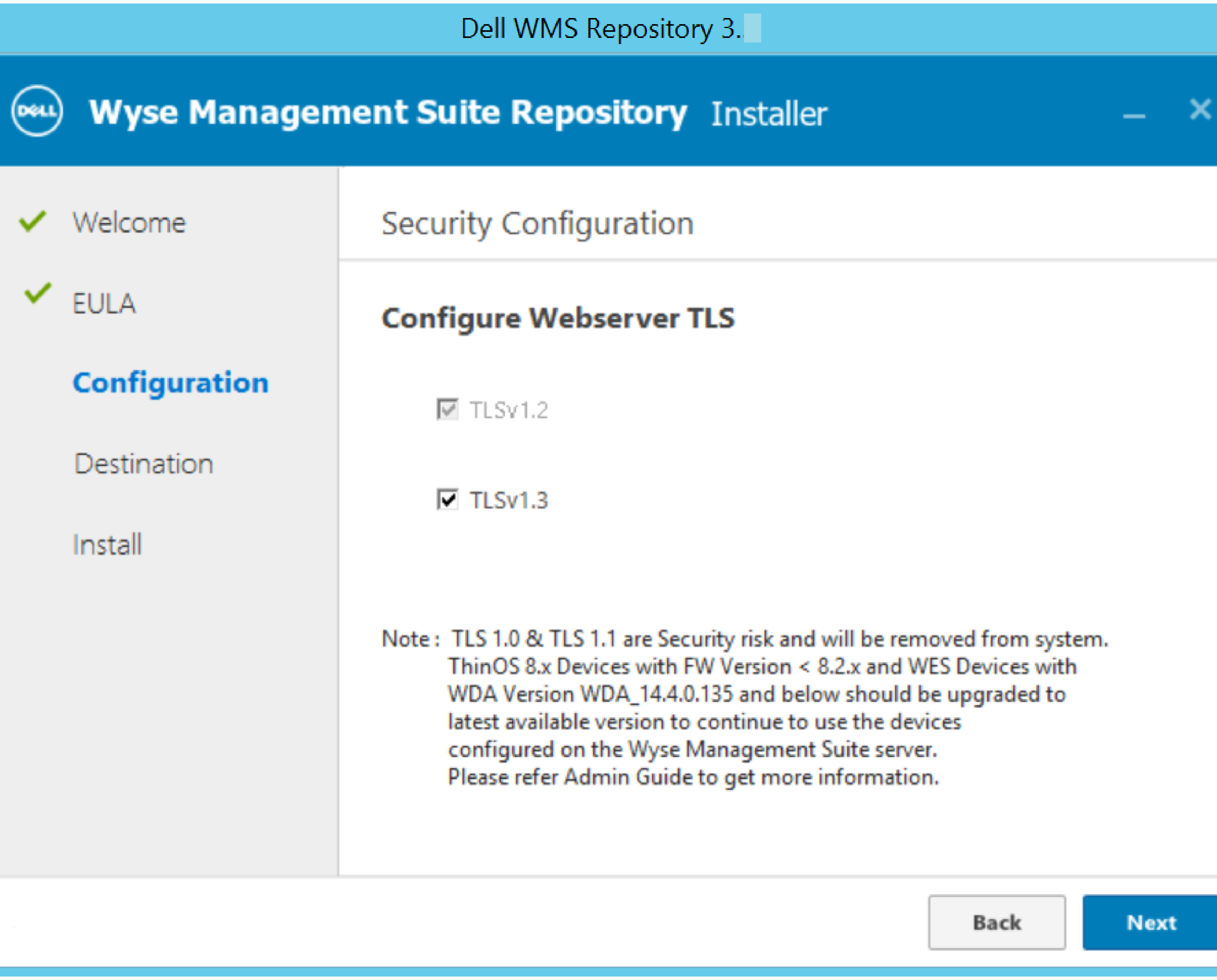
Replicate existing file option is applicable if the repository is already registered. When a new repository is registered, then all the files are copied to the new repository. You can view the file replication status in the **Events** page.

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.

The selected TLS version must be same or higher than the TLS version configured on the Wyse Management Suite server. Make sure to select all the appropriate versions of TLS based on the support criteria of the devices being managed.



Dell WMS Repository 3.

Wyse Management Suite Repository Installer

Security Configuration

Configure Webserver TLS

☑ TLSv1.2

☑ TLSv1.3

Note : TLS 1.0 & TLS 1.1 are Security risk and will be removed from system. ThinOS 8.x Devices with FW Version < 8.2.x and WES Devices with WDA Version WDA_14.4.0.135 and below should be upgraded to latest available version to continue to use the devices configured on the Wyse Management Suite server. Please refer Admin Guide to get more information.

Figure 18. Wyse Management Suite Repository Installer

NOTE: Do not select TLSv1.1 and later if the WDA version in the Windows Embedded Device is lower than 14.4.0.153_Unified, and if you are using Merlin Imaging agent. The TLSv1.1 and later should not be selected if you are using the import tool to migrate from Wyse Device Manager to Wyse Management Suite.

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

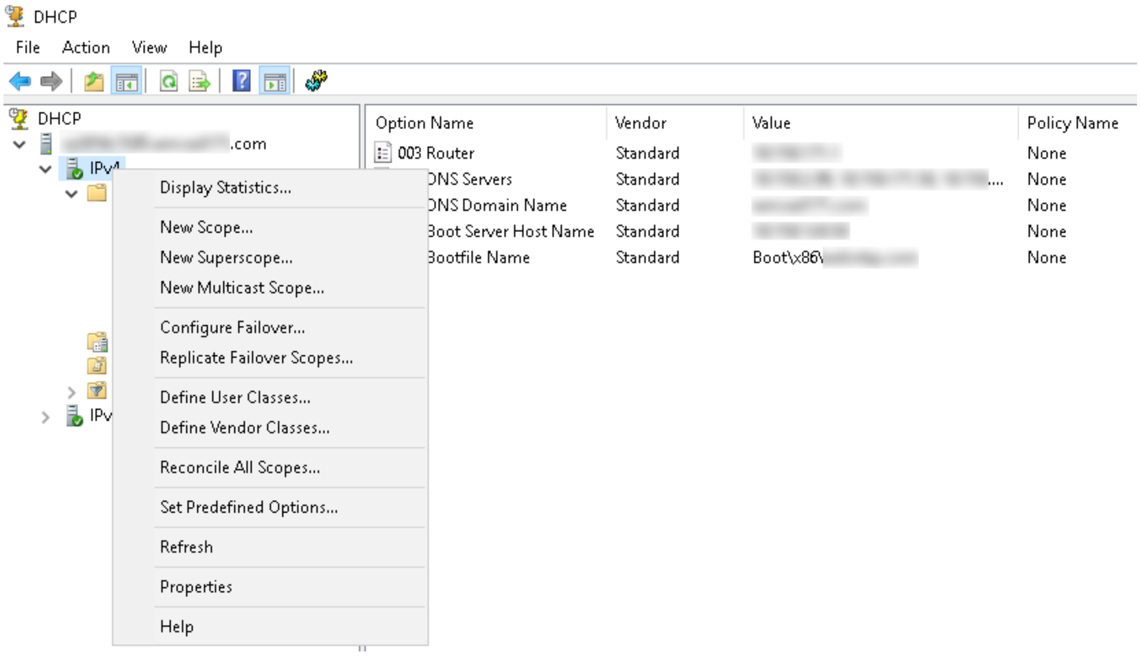
About this task

NOTE: For information on customer security environment, see Wyse Device Agent.

To create a DHCP option tag, do the following:

Steps

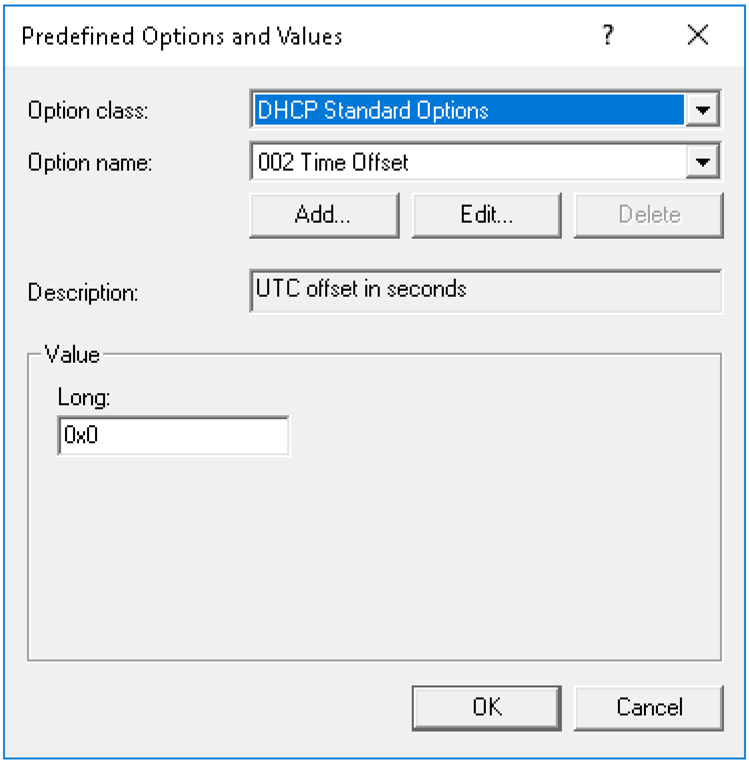
1. Open the Server Manager.
2. Go to **Tools**, and click **DHCP option**.
3. Go to **FQDN** > **IPv4** and right-click **IPv4**.



Option Name	Vendor	Value	Policy Name
003 Router	Standard	[redacted]	None
DNS Servers	Standard	[redacted]...	None
DNS Domain Name	Standard	[redacted]	None
Boot Server Host Name	Standard	[redacted]	None
Bootfile Name	Standard	Boot\x86\[redacted]	None

Figure 19. 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.



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 002 Time Offset

Description: UTC offset in seconds

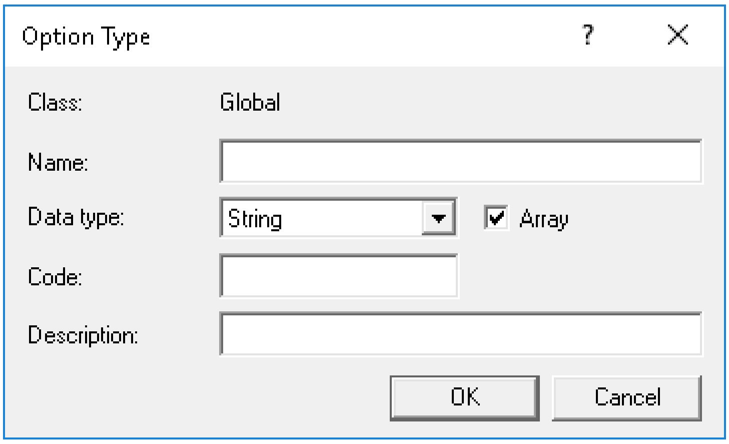
Value

Long:

0x0

Figure 20. Predefined Options and Values

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



Option Type

Class: Global

Name:

Data type: String ☑ Array

Code:

Description:

Figure 21. Option Type

Example

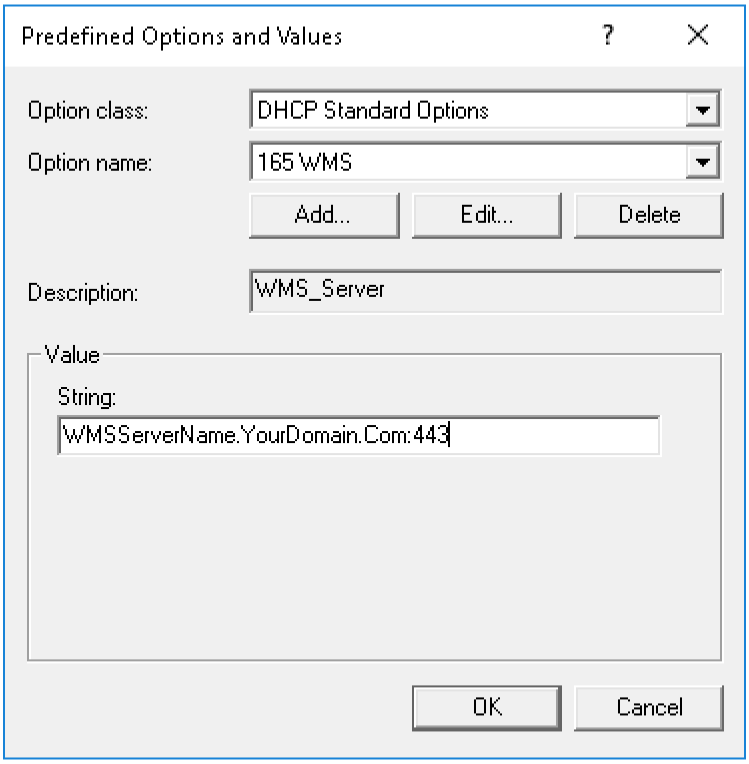
The options must be either added to the server options of the DHCP server or scope options of the DHCP scope.

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

Description: WMS_Server

Value

String: WMSServerName.YourDomain.Com:443

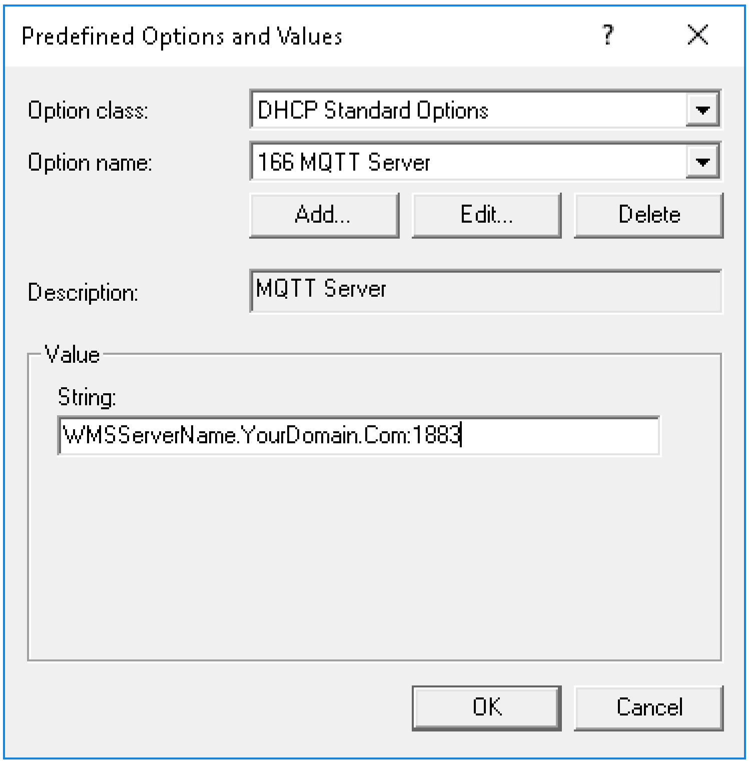
Figure 22. 165 Wyse Management Suite server URL option tag

- 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

Description: MQTT Server

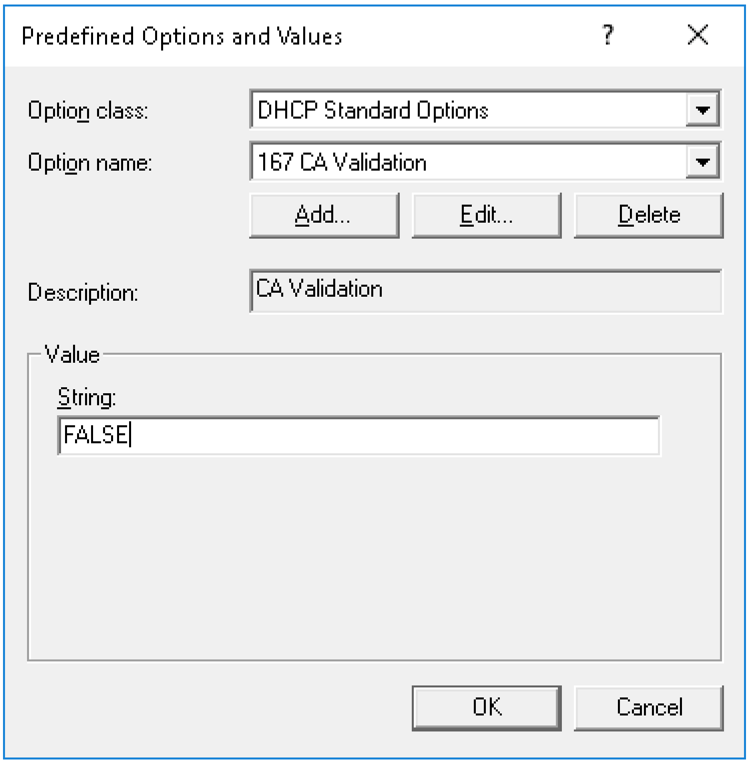
Value

String: WMSServerName.YourDomain.Com:1883

Figure 23. 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



Option class: DHCP Standard Options

Option name: 167 CA Validation

Description: CA Validation

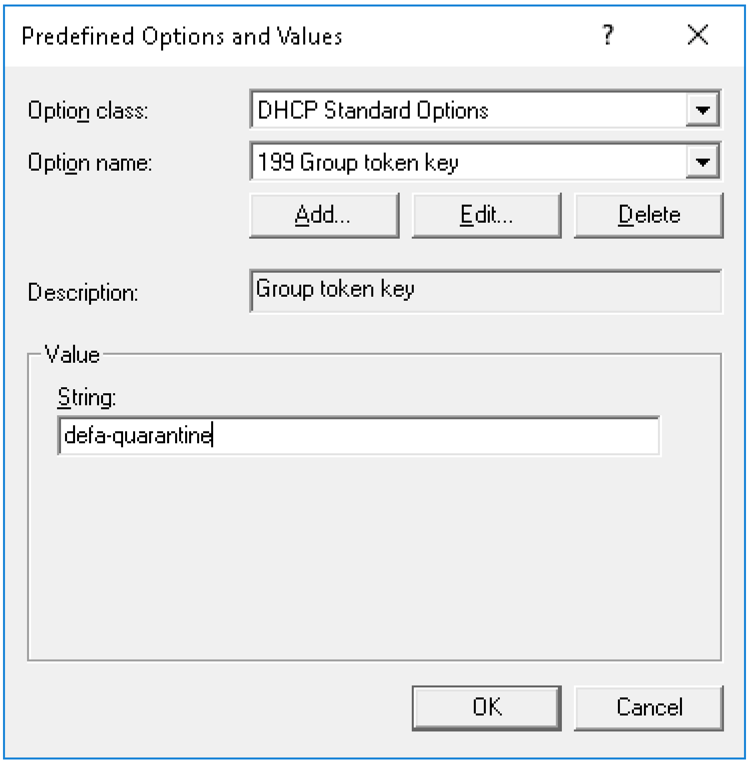
Value

String: FALSE

Figure 24. 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



Option class: DHCP Standard Options

Option name: 199 Group token key

Description: Group token key

Value

String: defa-quarantine

Figure 25. 199 Wyse Management Suite server URL option tag

Create and configure DNS SRV records

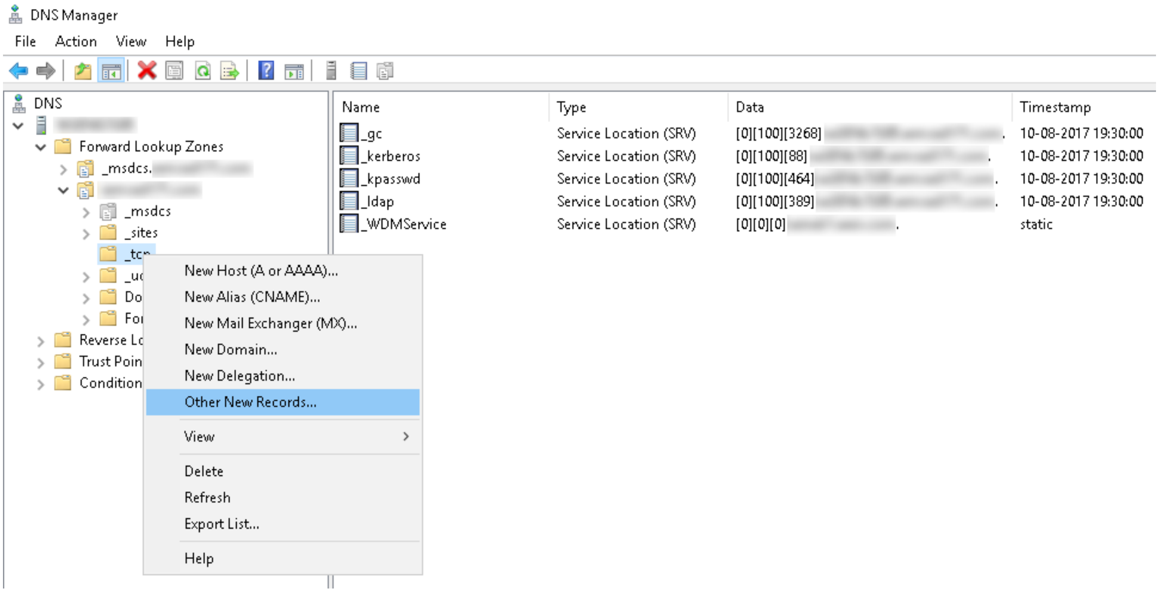
About this task

ⓘ **NOTE:** For information on customer security environment, see Wyse Device Agent.

To create a DNS SRV record, do the following:

Steps

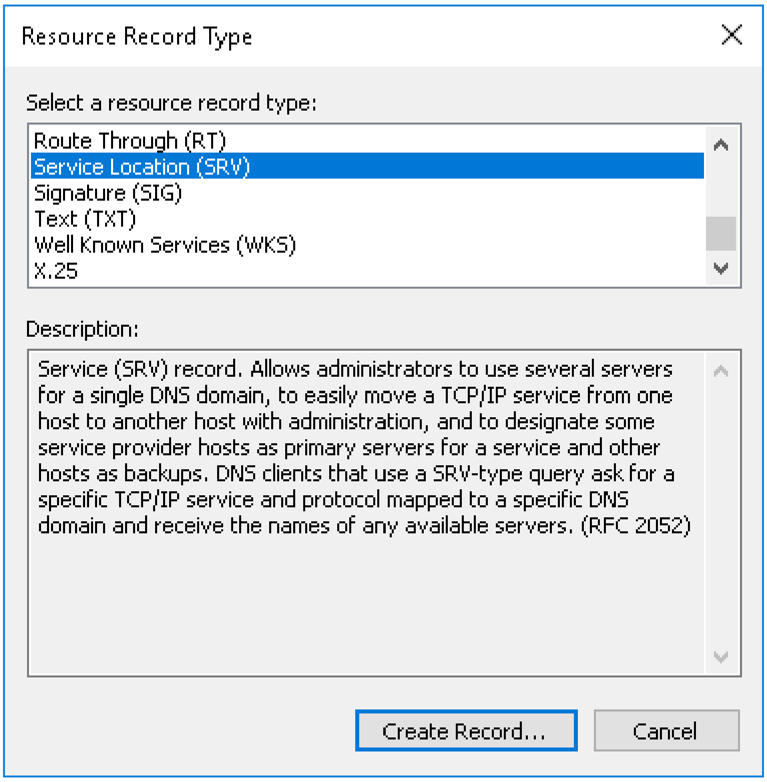
1. Open the Server Manager.
2. Go to **Tools**, and click **DNS option**.
3. Go to **DNS** > **DNS Server Host Name** > **Forward Lookup Zones** > **Domain** > **_tcp** and right-click the **_tcp option**.



Name	Type	Data	Timestamp
_gc	Service Location (SRV)	[0][100][3268] [redacted].	10-08-2017 19:30:00
_kerberos	Service Location (SRV)	[0][100][88] [redacted].	10-08-2017 19:30:00
_kpasswd	Service Location (SRV)	[0][100][464] [redacted].	10-08-2017 19:30:00
_ldap	Service Location (SRV)	[0][100][389] [redacted].	10-08-2017 19:30:00
_WDMService	Service Location (SRV)	[0][0][0] [redacted].	static

Figure 26. DNS manager

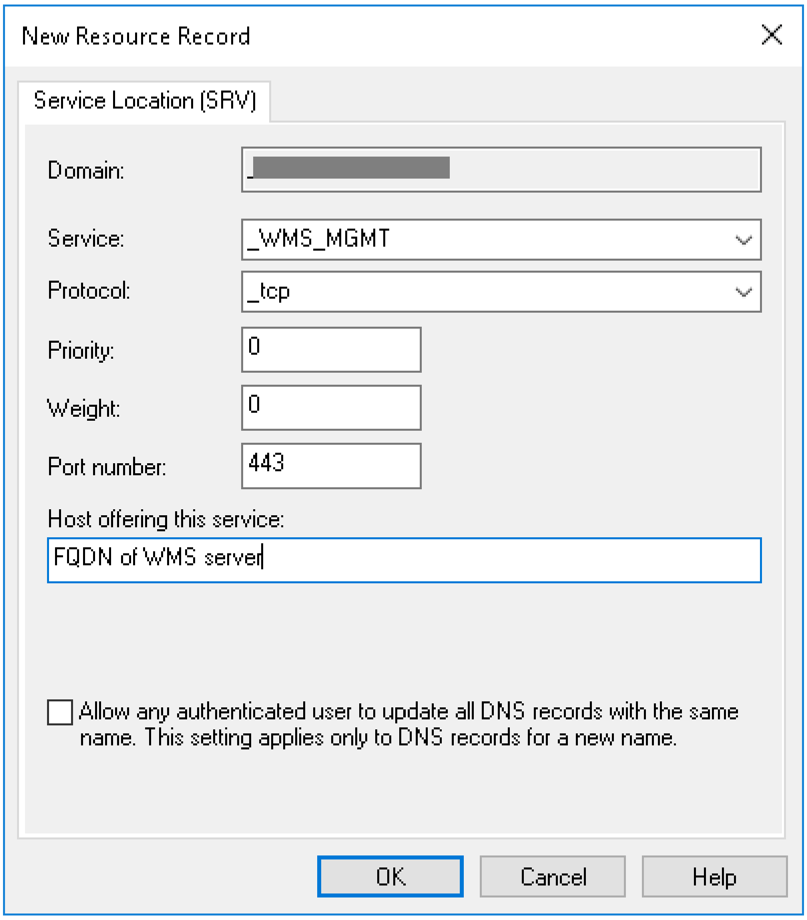
4. Click **Other New Records**.
   The **Resource Record Type** window is displayed.
5. Select the **Service Location (SRV)**, click **Create Record**, and do the following:



Service (SRV) record. Allows administrators to use several servers for a single DNS domain, to easily move a TCP/IP service from one host to another host with administration, and to designate some service provider hosts as primary servers for a service and other hosts as backups. DNS clients that use a SRV-type query ask for a specific TCP/IP service and protocol mapped to a specific DNS domain and receive the names of any available servers. (RFC 2052)

Figure 27. 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: _[redacted]

Service: _WMS_MGMT

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 443

Host offering this service:

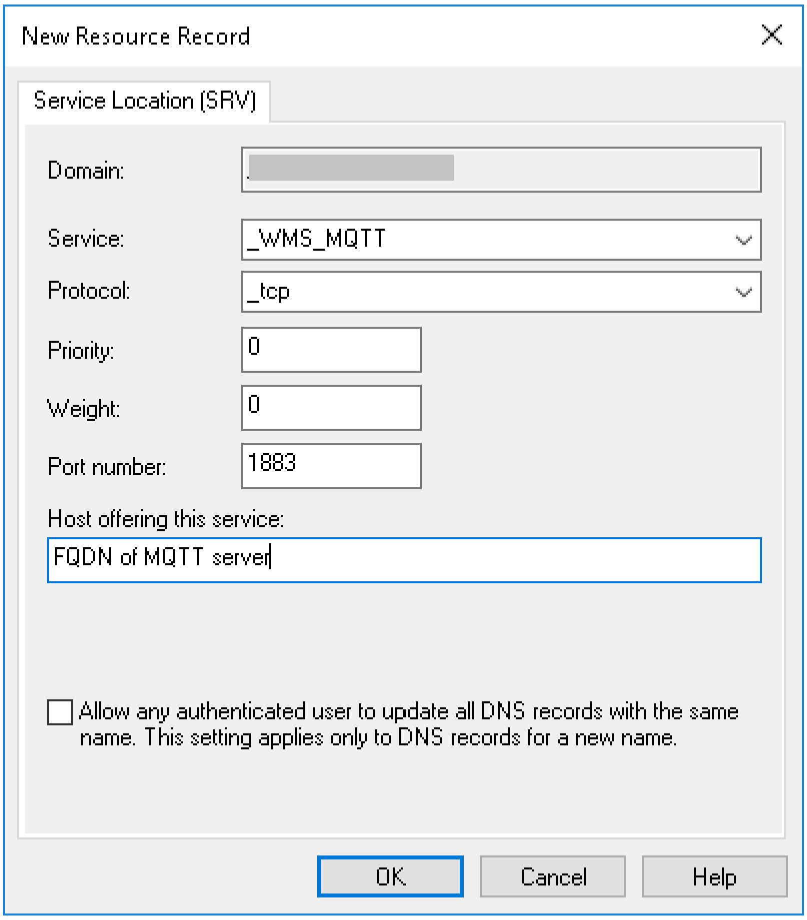
FQDN of WMS server

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

Figure 28. _WMS_MGMT service

b. To create MQTT server record, enter the following values, and then click **ÓK**.

- Service—_WMS_MQTT
- Protocol—_tcp
- Port number—1883
- Host offering this service—FQDN of MQTT server



Domain: .[redacted]

Service: _WMS_MQTT

Protocol: _tcp

Priority: 0

Weight: 0

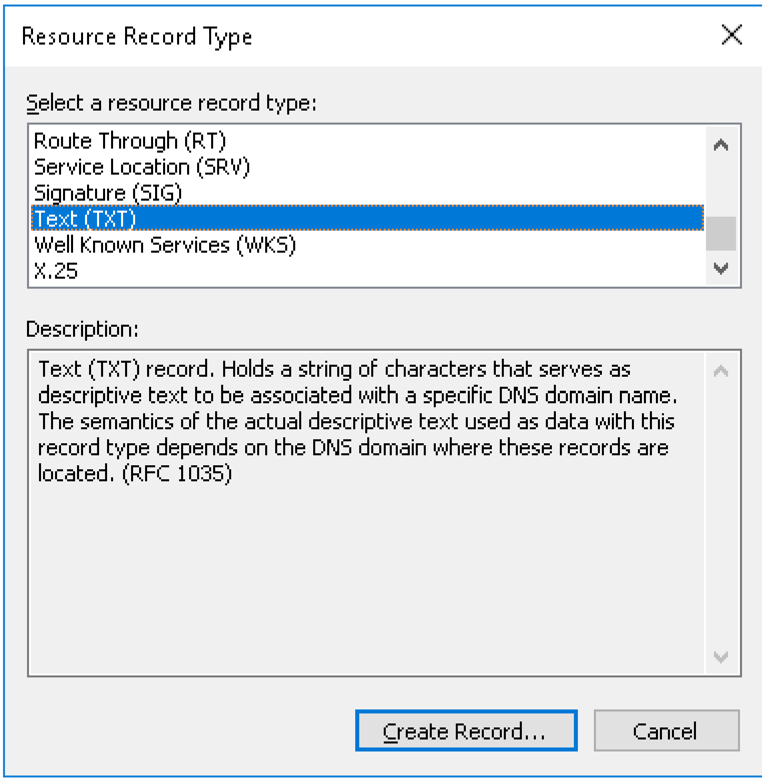
Port number: 1883

Host offering this service:
FQDN of MQTT server

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

Figure 29. _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:



Resource Record Type

Select a resource record type:

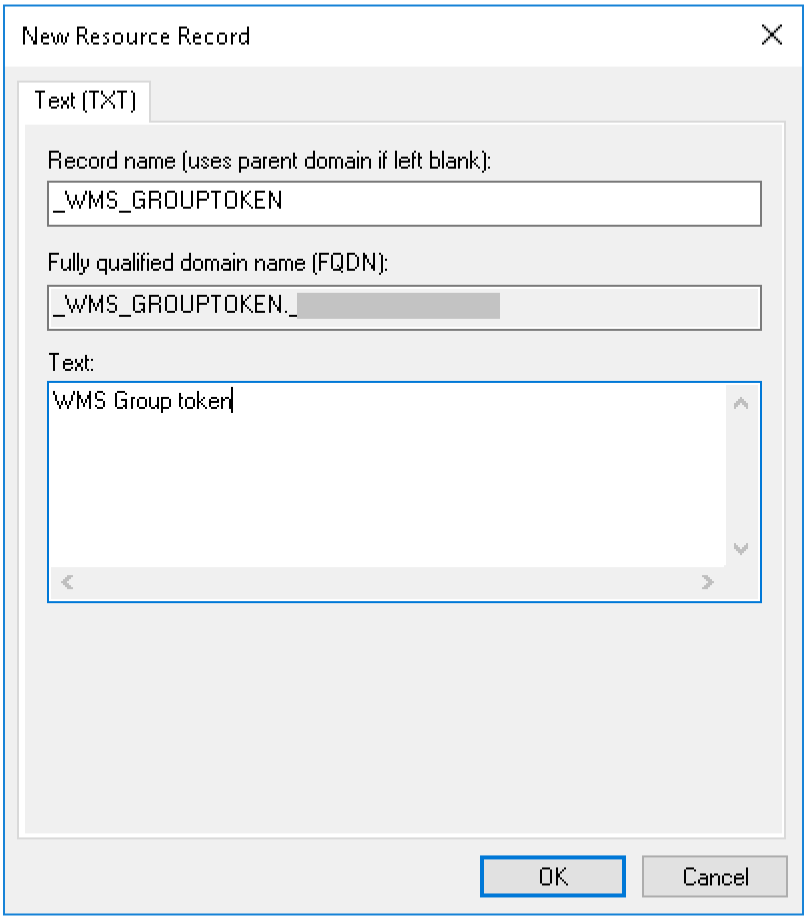
Route Through (RT)
Service Location (SRV)
Signature (SIG)
Text (TXT)
Well Known Services (WKS)
X.25

Description:

Text (TXT) record. Holds a string of characters that serves as descriptive text to be associated with a specific DNS domain name. The semantics of the actual descriptive text used as data with this record type depends on the DNS domain where these records are located. (RFC 1035)

Figure 30. 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



New Resource Record

Text (TXT)

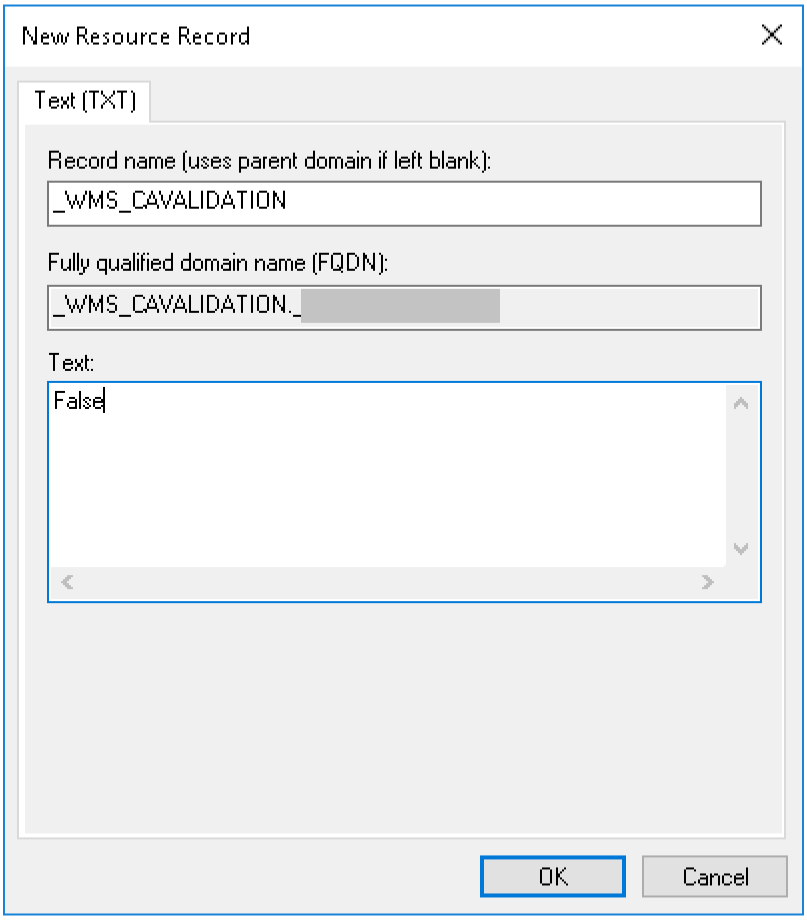
Record name (uses parent domain if left blank):
_WMS_GROUPTOKEN

Fully qualified domain name (FQDN):
_WMS_GROUPTOKEN._[redacted]

Text:
WMS Group token

Figure 31. _WMS_GROUPTOKEN record name

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



New Resource Record

Text (TXT)

Record name (uses parent domain if left blank):
_WMS_CAVALIDATION

Fully qualified domain name (FQDN):
_WMS_CAVALIDATION._[redacted]

Text:
False

Figure 32. _WMS_CAVALIDATION record name

G

Creating and deploying standard application policy to thin clients

About this task

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

Steps

1. In the local repository, go to **thinClientApps**, and copy the application to the folder.
2. Ensure that the application is registered by going 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.
   - Select **Policy Name**, **Group**, **Task**, **Device Type**, and **TC Application**.
   - To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter**, **Platform Filter** or **Manufacturer 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.
   - 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:
   - **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/time of the device time zone.
   - **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 going to the **Jobs** page.

H

Register Dell Hybrid Client manually

Prerequisites

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

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

Steps

1. Log in to the hybrid client as a guest user.
2. On the top bar, click the **Dell Client Agent** icon.

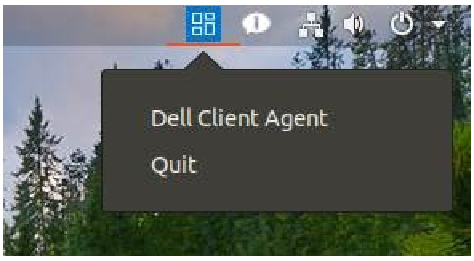


Figure 33. DCA icon

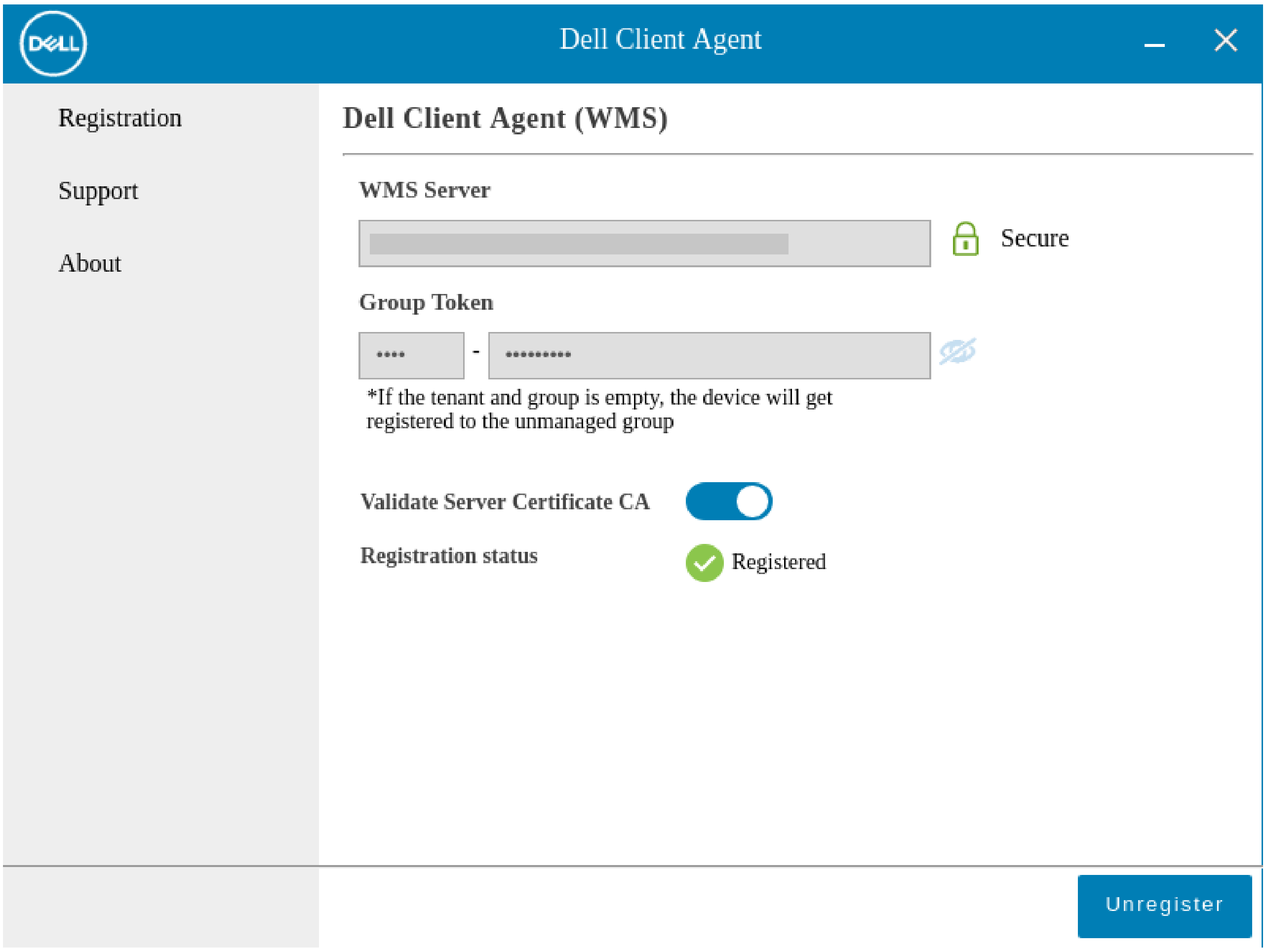
3. Click **Dell Client Agent**.
   The **Dell Client Agent** dialog box is displayed.
4. Click **Registration**.
   The default status is displayed as **Discovery In Progress**.
5. To register manually, click the **Cancel** button.
6. In the **WMS Server** field, enter the URL of the Wyse Management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

   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

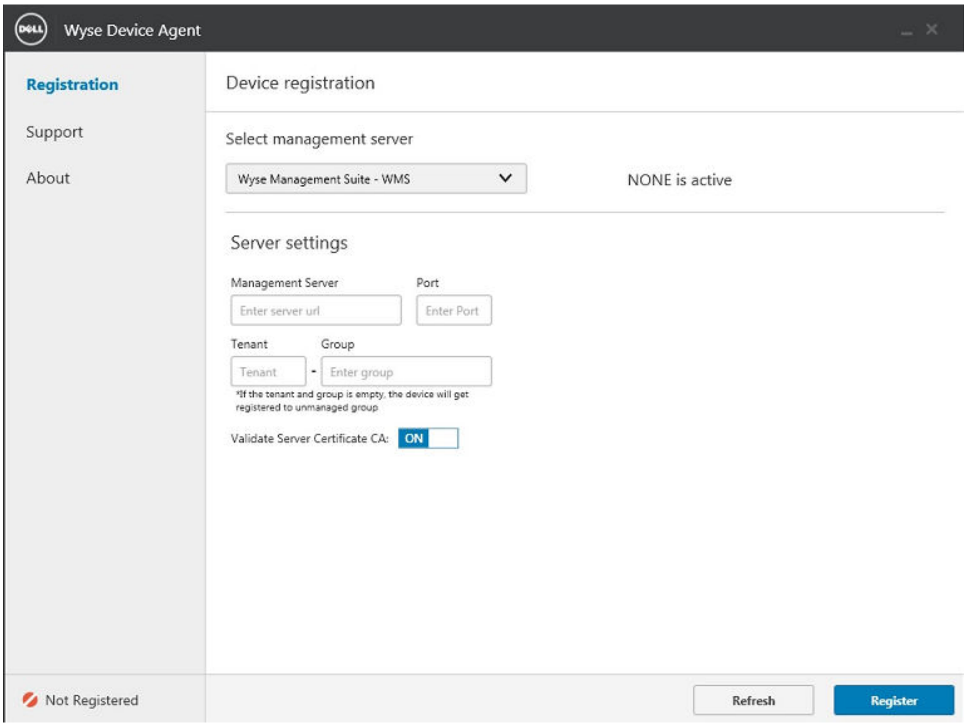
Figure 34. Dell Client Agent

I

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**.



Select management server: Wyse Management Suite - WMS

NONE is active

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

Validate Server Certificate CA: ON

Not Registered

Figure 35. Device registration

Register ThinOS 8.x device manually

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.

K

Register ThinOS 9.x device manually

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: 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.

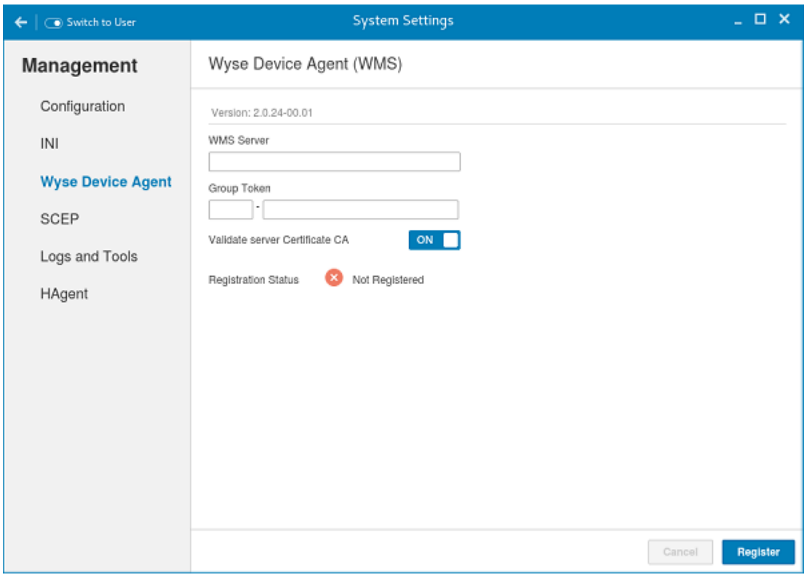


Figure 36. Device registration

M

Terms and definitions

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

Table 7. Terms and definitions

Terminology	Definition
Private cloud	Wyse Management Suite server installed on the cloud that is private to your parent data center.
WDA	Wyse Device Agent which resides in the device and acts as an agent for communication between server and client.
Local repository	Wyse Device Agent which resides in the device and acts as an agent for communication between server and client.
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-premises that is private to your organization's data center.
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 that are assigned to them.