Edge Device Manager

Version R16 Quick Start Guide

February 2021
Rev. A01

Notes, cautions, and warnings

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

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

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

Contents

1

Introduction

Edge Device Manager is the next generation management solution that lets you centrally configure, monitor, manage, and optimize your Edge Gateway devices. It offers advanced feature options such as cloud versus on-premises deployment, manage-from-anywhere using a mobile application, enhanced security such as BIOS configuration and port lockdown. Other features include device discovery and registration, asset and inventory management, configuration management, applications deployment, real-time commands, monitoring, alerts, reporting, and troubleshooting of endpoints.

ⓘ **NOTE:** Wyse Management Suite user interface is re-branded to Edge Device Manager (EDM).

You must consider the following information when selecting the EDM public versus private cloud editions:

Private cloud

This edition is suited for users with the following requirements:

- Small, medium, or large deployments
- Delegated administration, reports, and two factor authentication
- Monitor and manage from anywhere through mobile app
- Install and maintain software and infrastructure on-site

ⓘ **NOTE:** Devices must be isolated from the internet (no communication through a forward-proxy service)

Public cloud

This edition is suited for users with the following requirements:

- Small, medium, or large deployments
- Cost-effective set up and maintenance of infrastructure and software
- Delegated administration, reports, and two factor authentication
- Monitor and manage from anywhere through mobile app
- Configure devices to communicate with external server directly or through a forward-proxy service
- Manage devices on non-corporate networks

Topics:

Getting started with Edge Device Manager on public cloud

This section provides information about the general features that help you to get started as an administrator.

Logging in

ⓘ **NOTE:** You receive your credentials when you sign up for Edge Device Manager trial on www.wysemanagementsuite.com or when you purchase your subscription. You can purchase the Edge Device Manager subscription at the Dell sales or your local Dell partner. For more details, see www.wysemanagementsuite.com.

To log into the management console, do the following:

1. Start a supported web browser on any machine with access to the internet .
2. To access Public Cloud (SaaS) edition of Edge Device Manager use the following links:
   - US Datacenter: us1.wysemanagementsuite.com
   - EU Datacenter: eu1.dellmobilitymanager.com

3. Enter your user name and password.

   NOTE: The default user name and password are provided by the account representative.

4. Click **Sign In**.

NOTE: Dell recommends you to change your password after logging in for the first time.

Changing your password

To change the login password, do the following:

1. On the upper-right corner of the management console, click **Account**, and then click **Change Password**.
2. Enter your current password.
3. Enter a new password.
4. Enter your new password in the **Confirm New Password** field.
5. Click **Change Password**.

Logging out

To log out from the management console, click **Account**, and then click **Sign out**.

Getting started with Edge Device Manager on private cloud

The following table lists the prerequisites to deploy Edge Device Manager on a private cloud:

Table 1. Prerequisites

	Edge Device Manager server		Edge Device Manager software repository
	For 10,000 or less devices	For 50,000 or less devices	
Operating system	Windows Server 2012 R2 or Windows Server 2016 Supported language pack—English, French, Italian, German, and Spanish		Windows Server 2012 R2 or Windows Server 2016
Minimum disk space	40 GB	120 GB	120 GB
Minimum memory (RAM)	8 GB	16 GB	16 GB
Minimum CPU requirements	4	4	4
Network communication ports	The EDM installer adds Transfer Control Protocol (TCP) ports 443, 8080, and 1883 to the firewall exception list. The ports are added to access the EDM console and to send the push notifications to the thin clients. ● TCP 443—HTTPS communication ● TCP 8080—HTTP communication (optional) ● TCP 1883—MQTT communication ● TCP 3306—MariaDB (optional if remote) ● TCP 27017—MongoDB (optional if remote) ● TCP 11211—Memcache		The EDM 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 EDM.
Supported browsers	● Microsoft Internet Explorer version 11 ● Google Chrome 58.0 and later versions ● Mozilla Firefox 52.0 and later versions ● Microsoft Edge browser on Windows—English only		

NOTE:

- `WMS.exe` and `WMS_Repo.exe` must be installed on two different servers.
- The software can be installed on a physical or a virtual machine.
- It is not necessary that the software repository and the Edge Device Manager server run on the same operating system.

For installation procedure, see support.dell.com/manuals.

2

Installing Edge Device Manager on private cloud

A simple installation of Edge Device Manager consists of the following:

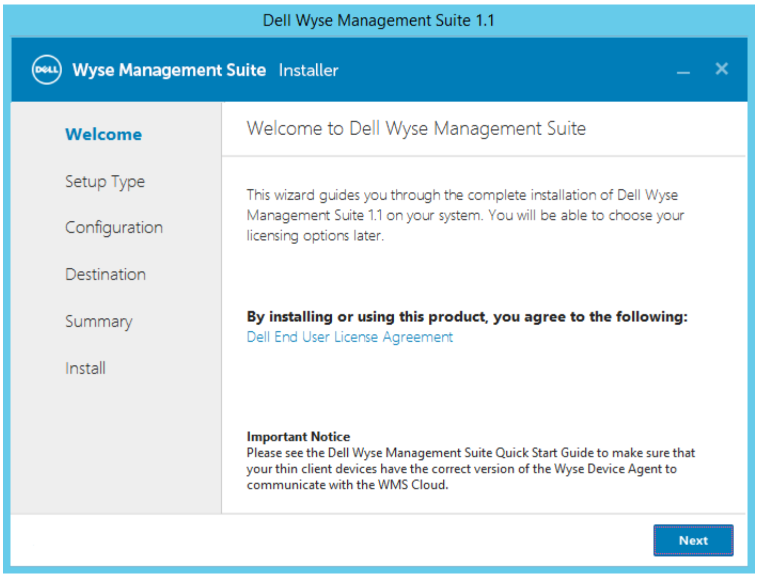
- Edge Device Manager server that includes repository for application and operating system images
- Additional Edge Device Manager repository servers for image and applications and active directory authentication—Optional
- HTTPS certificate from a certificate authority. For example, certificate issued by Geotrust, www.geotrust.com/—Optional

Ensure that you meet the following requirements:

- Obtain and configure all the required hardware and software. You can download the Edge Device Manager software at 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.
- Install the latest version of the supported browser.
- Obtain administrator rights and credentials on all systems involved with installations.
- Obtain a valid Edge Device Manager license.

To install the Edge Device Manager on a private cloud, do the following:

1. Double-click the installer package.
2. On the **Welcome** screen, read the license agreement and click **Next**.



Dell Wyse Management Suite 1.1

Welcome to Dell Wyse Management Suite

This wizard guides you through the complete installation of Dell Wyse Management Suite 1.1 on your system. You will be able to choose your licensing options later.

By installing or using this product, you agree to the following:
Dell End User License Agreement

Important Notice
Please see the Dell Wyse Management Suite Quick Start Guide to make sure that your thin client devices have the correct version of the Wyse Device Agent to communicate with the WMS Cloud.

Figure 1. Welcome screen

3. Select the **Setup Type** you want to install, and click **Next**. The available options are:
   - 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.

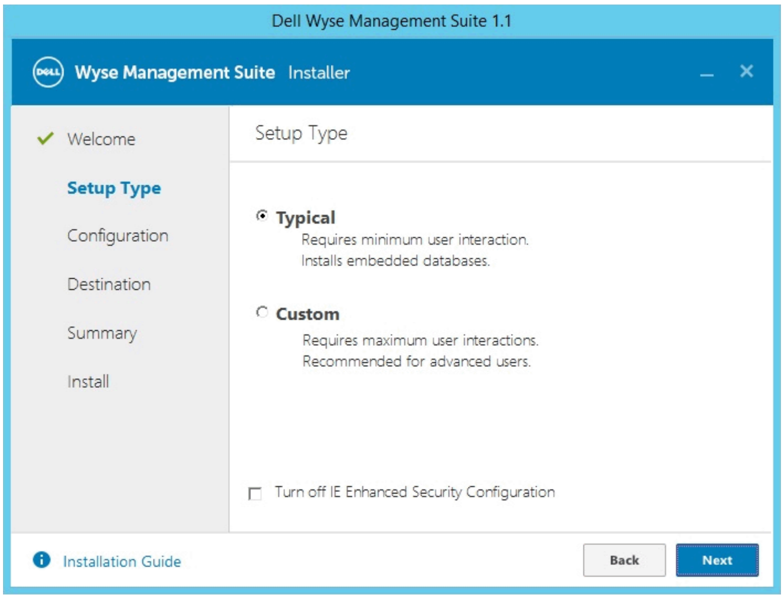
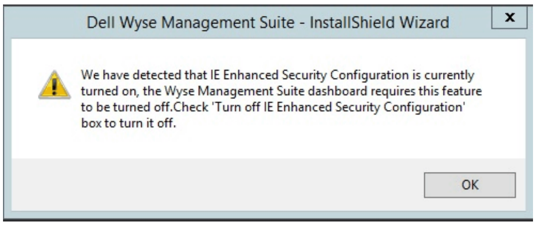

Dell Wyse Management Suite 1.1
Wyse Management Suite Installer
✓ Welcome
Setup Type
Configuration
Destination
Summary
Install
Setup Type
● Typical
Requires minimum user interaction.
Installs embedded databases.
○ Custom
Requires maximum user interactions.
Recommended for advanced users.
□ Turn off IE Enhanced Security Configuration
Installation Guide
Back
Next

Figure 2. Setup type

NOTE: A notification window is displayed, when the Internet Explorer Enhanced Security Configuration feature is enabled. Select the **Turn off IE Enhanced Security Configuration** check box to turn off the Internet Explorer enhanced security configuration.

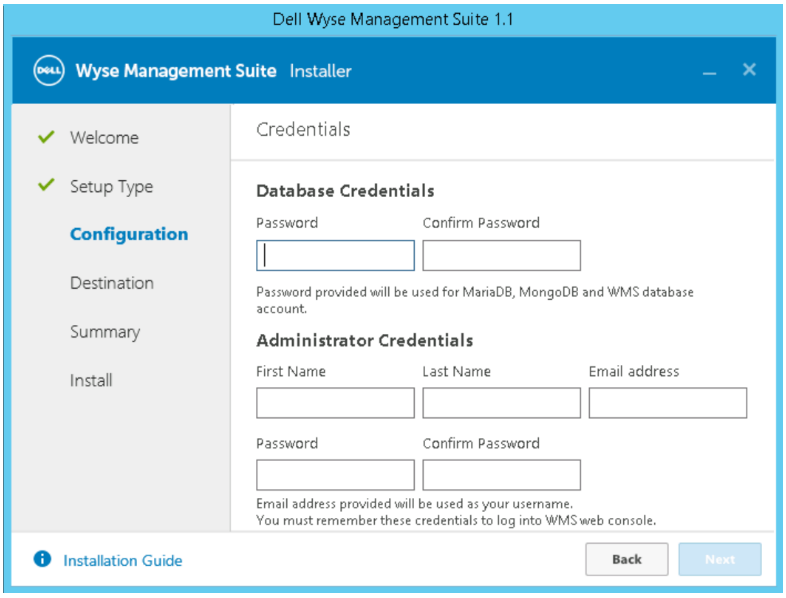


We have detected that IE Enhanced Security Configuration is currently turned on, the Wyse Management Suite dashboard requires this feature to be turned off.Check 'Turn off IE Enhanced Security Configuration' box to turn it off.

Figure 3. IE Enhanced Security Configuration

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

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



Credentials

Database Credentials

Password □ Confirm Password □

Password provided will be used for MariaDB, MongoDB and WMS database account.

Administrator Credentials

First Name □ Last Name □ Email address □

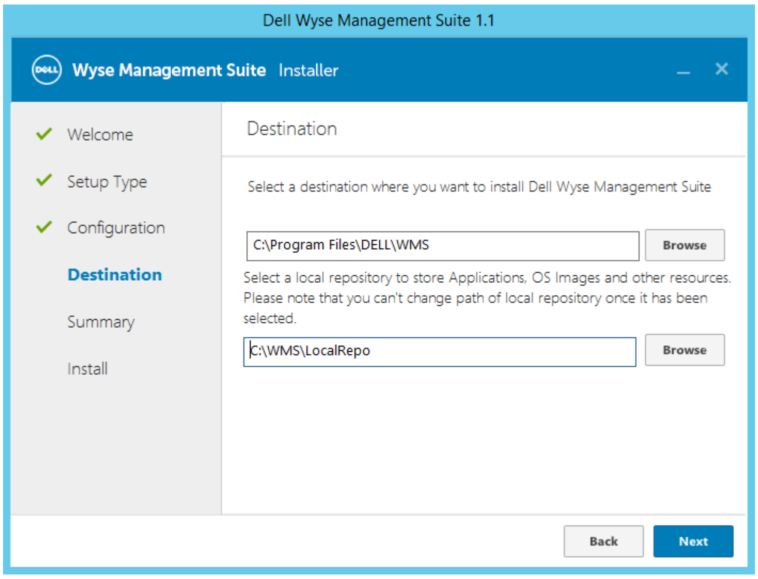
Password □ Confirm Password □

Email address provided will be used as your username.
You must remember these credentials to log into WMS web console.

Figure 4. Credentials

5. Select a path where you want to install the software, and the path to install the local tenant file repository.

   The default path of the destination folder to install the software is `C:\Program Files\DELL\WMS`.



Destination

Select a destination where you want to install Dell Wyse Management Suite

C:\Program Files\DELL\WMS

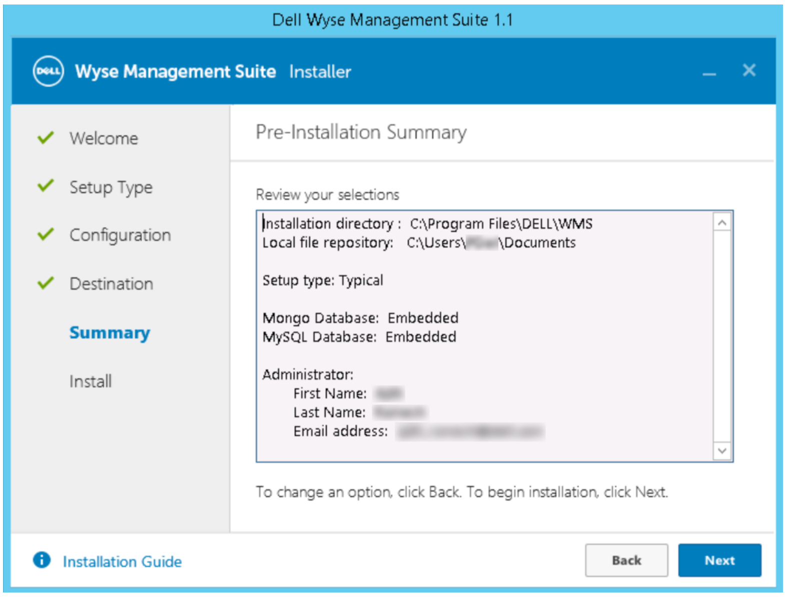
Select a local repository to store Applications, OS Images and other resources. Please note that you can't change path of local repository once it has been selected.

C:\WMS\LocalRepo

Figure 5. Destination

6. Click **Next**.

   The **Pre-Installation Summary** page is displayed. You can review your selections.



Pre-Installation Summary

Review your selections

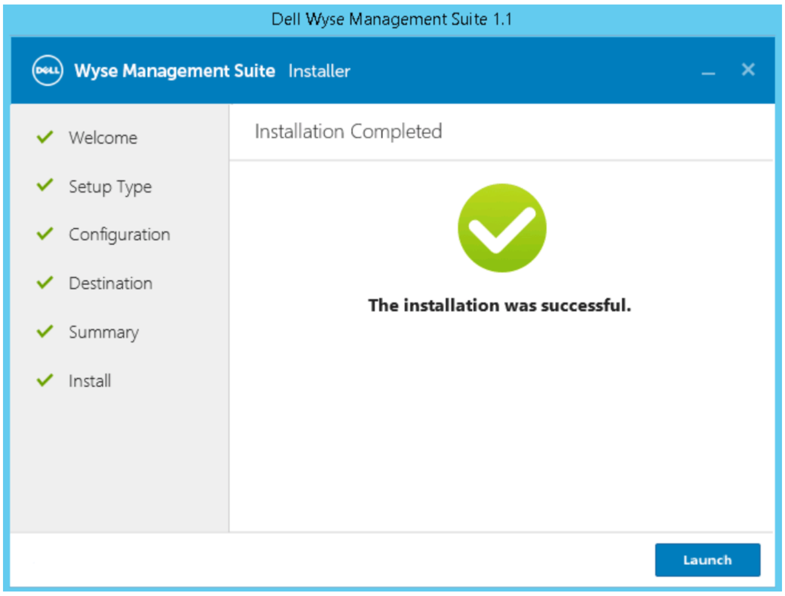
```
Installation directory :  C:\Program Files\DELL\WMS
Local file repository:   C:\Users\[redacted]\Documents

Setup type: Typical

Mongo Database:  Embedded
MySQL Database:  Embedded

Administrator:
     First Name:  [redacted]
     Last Name:  [redacted]
     Email address:  [redacted]
```

To change an option, click Back. To begin installation, click Next.

Figure 6. Summary

7. Click **Next**.

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

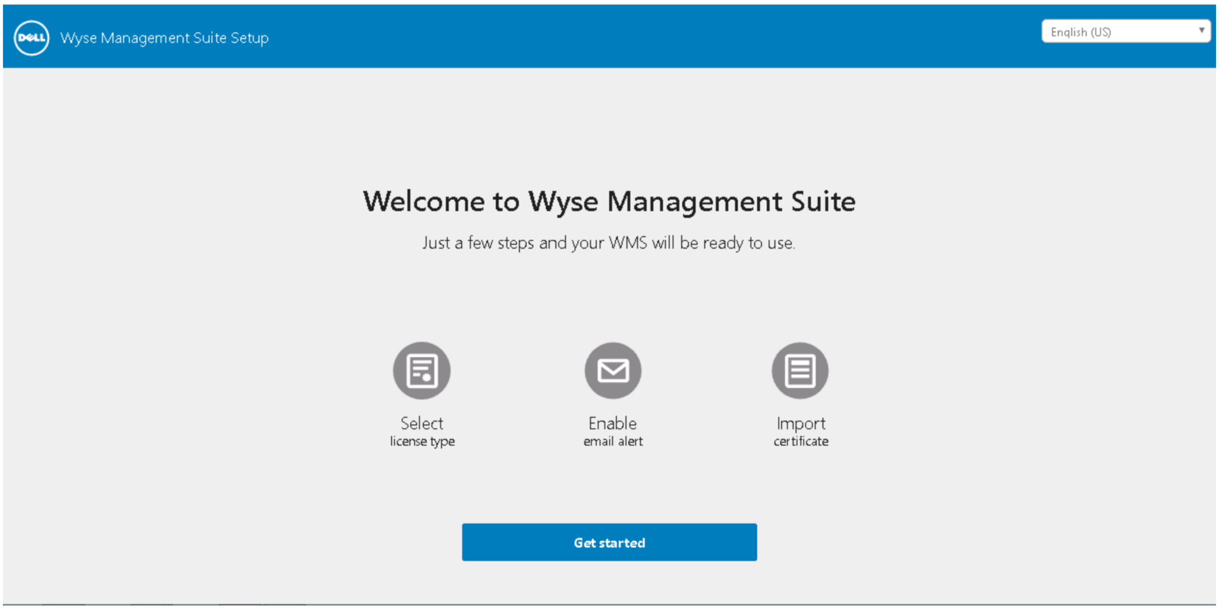

Dell Wyse Management Suite 1.1
Wyse Management Suite Installer
Welcome
Setup Type
Configuration
Destination
Summary
Install
Launch

Installation Completed

The installation was successful.

Figure 7. Installation complete status

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

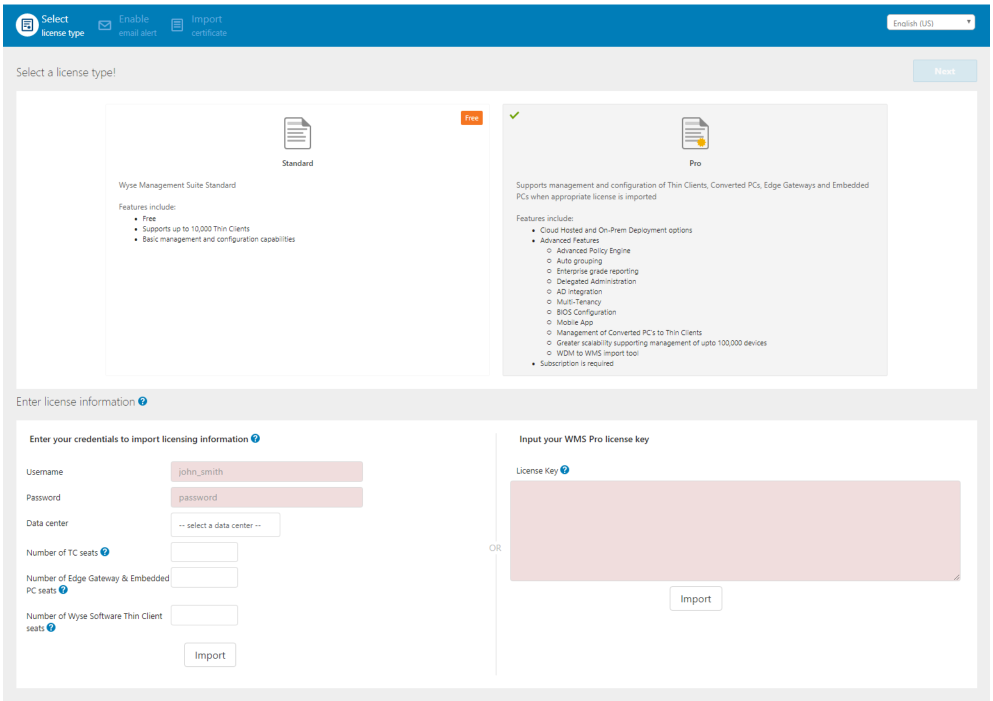


Welcome to Wyse Management Suite

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

Figure 8. Welcome page

10. To enable Edge Device Manager on-premise and cloud, select the license type as **Pro**. You must import a valid Edge Device Manager license. If the server has internet connection you can import the Edge Device Manager license. To import the license key, log in to Edge Device Manager public cloud portal and enter the key into the license key field.



Select a license type!

Standard

Wyse Management Suite Standard

Features include:

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

Pro

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
- Subscription is required

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	

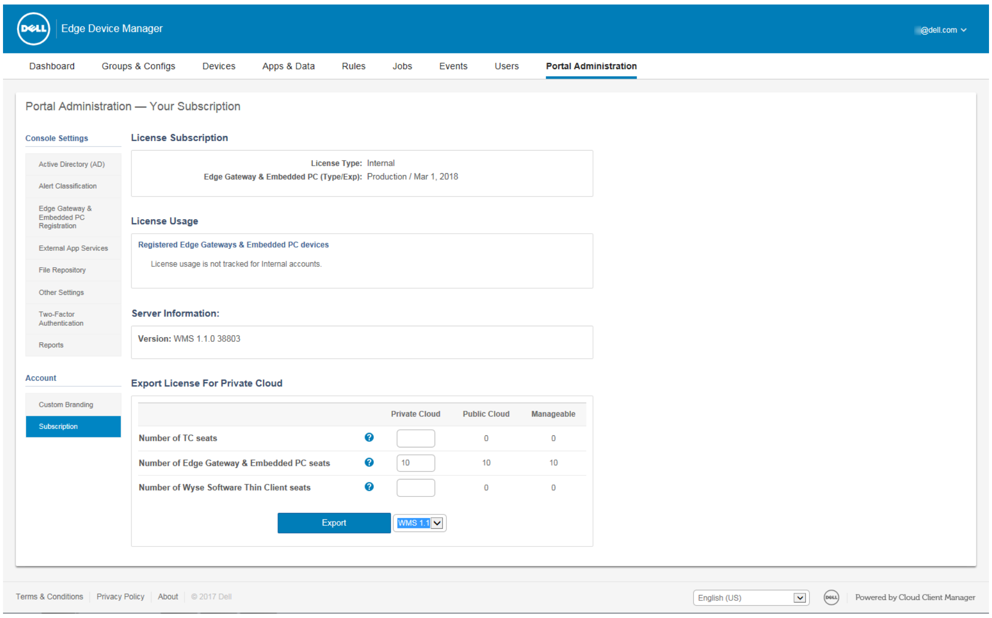
Input your WMS Pro license key

License Key

Figure 9. License type

To export a license key from the Edge Device Manager cloud portal, do the following:

a. Log in to the Edge Device Manager cloud portal.
b. Go to **Portal Administration** > **Subscription**.



Portal Administration — Your Subscription

License Subscription

License Type: Internal
Edge Gateway & Embedded PC (Type/Exp): Production / Mar 1, 2018

License Usage

Registered Edge Gateways & Embedded PC devices

License usage is not tracked for Internal accounts.

Server Information:

Version: WMS 1.1.0 38803

Export License For Private Cloud

	Private Cloud	Public Cloud	Manageable
Number of TC seats		0	0
Number of Edge Gateway & Embedded PC seats	10	10	10
Number of Wyse Software Thin Client seats		0	0

Figure 10. Portal administration

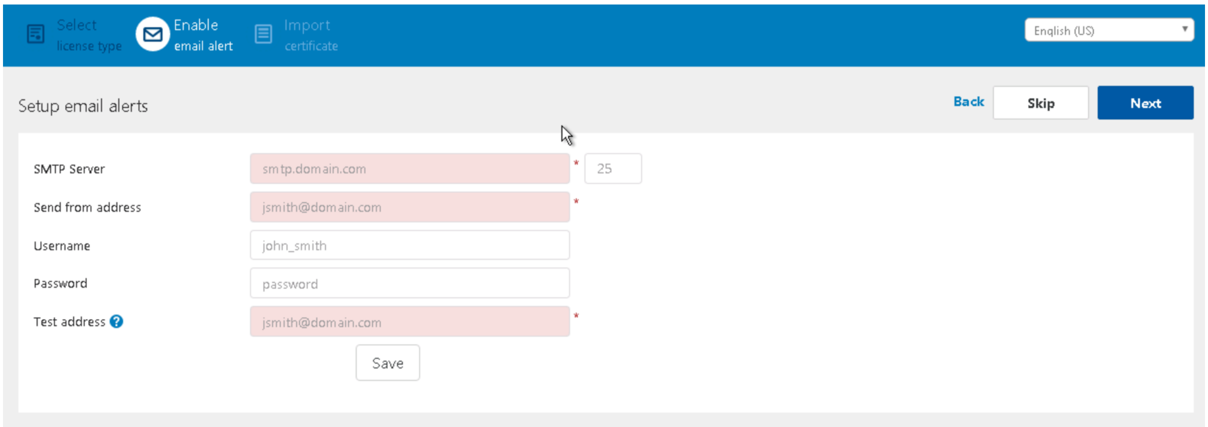
c. Enter the number of seats.
d. Click **Export**.

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

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

11. Enter your Simple Mail Transfer Protocol (SMTP) server information, and click **Save**.

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



Setup email alerts

SMTP Server	smtp.domain.com * 25
Send from address	jsmith@domain.com *
Username	john_smith
Password	password
Test address	jsmith@domain.com *

Figure 11. Email alert

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

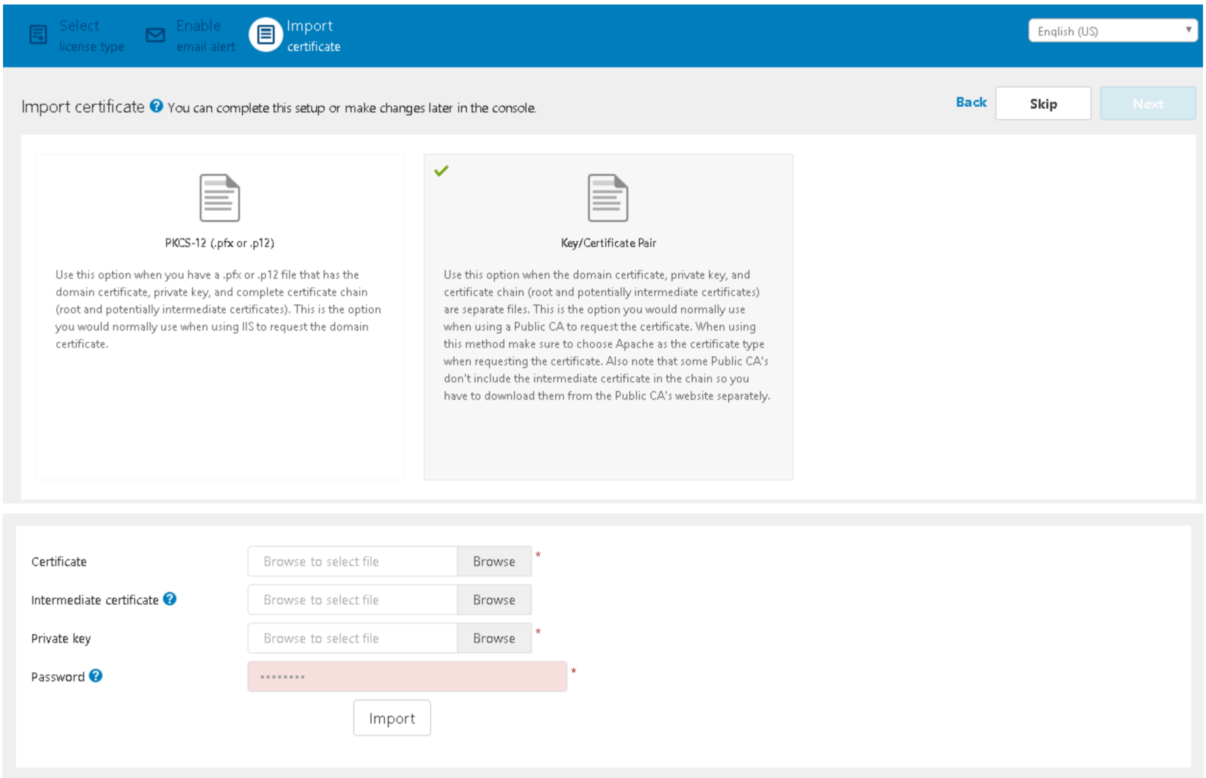
12. Import your Secure Sockets Layer (SSL) certificate to secure communications with the Wyse Management Suite server. Enter the public, private, and apache certificate and click the **Import** button. Importing the certificate takes three minutes to configure and restart Apache tomcat services.

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 appears because the self-signed certificate generated during installation is not signed by a certificate authority.

- You can either import a .pem or .pfx certificate.

You can skip this screen and complete this setup or make changes later in the console by logging in to the Edge Device Manager private cloud and importing the license from the **Portal Administration** page.



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.

Figure 12. Key or certificate value pair

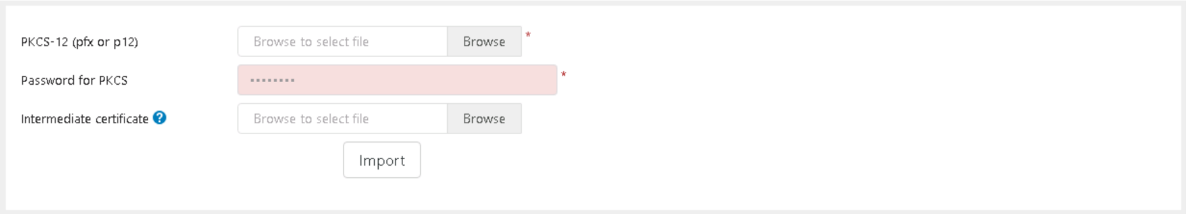
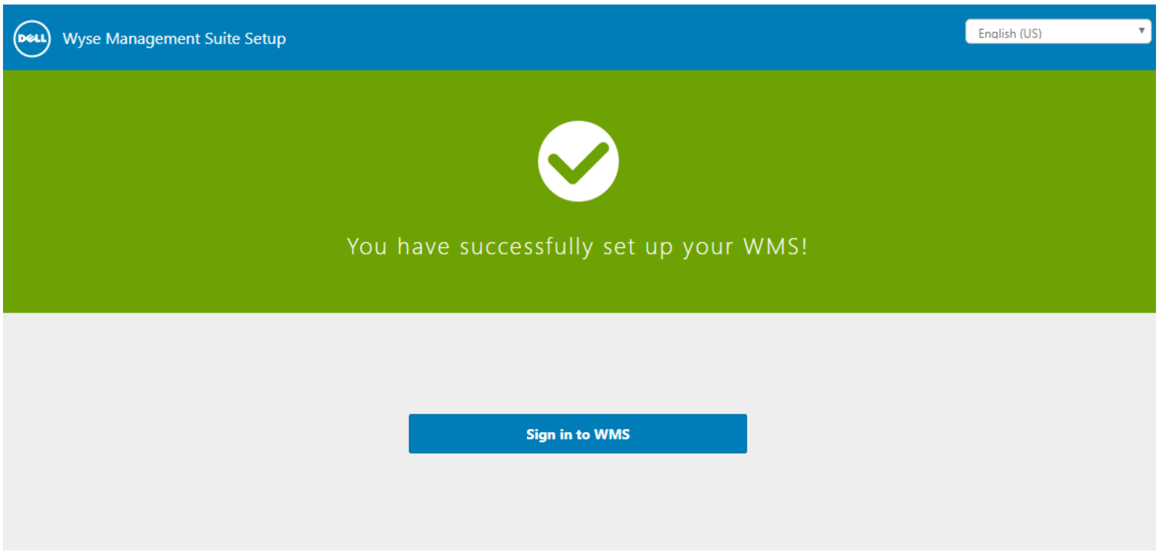


Figure 13. PKCS-12

13. Click **Next**.
14. Click **Sign in to WMS**.

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

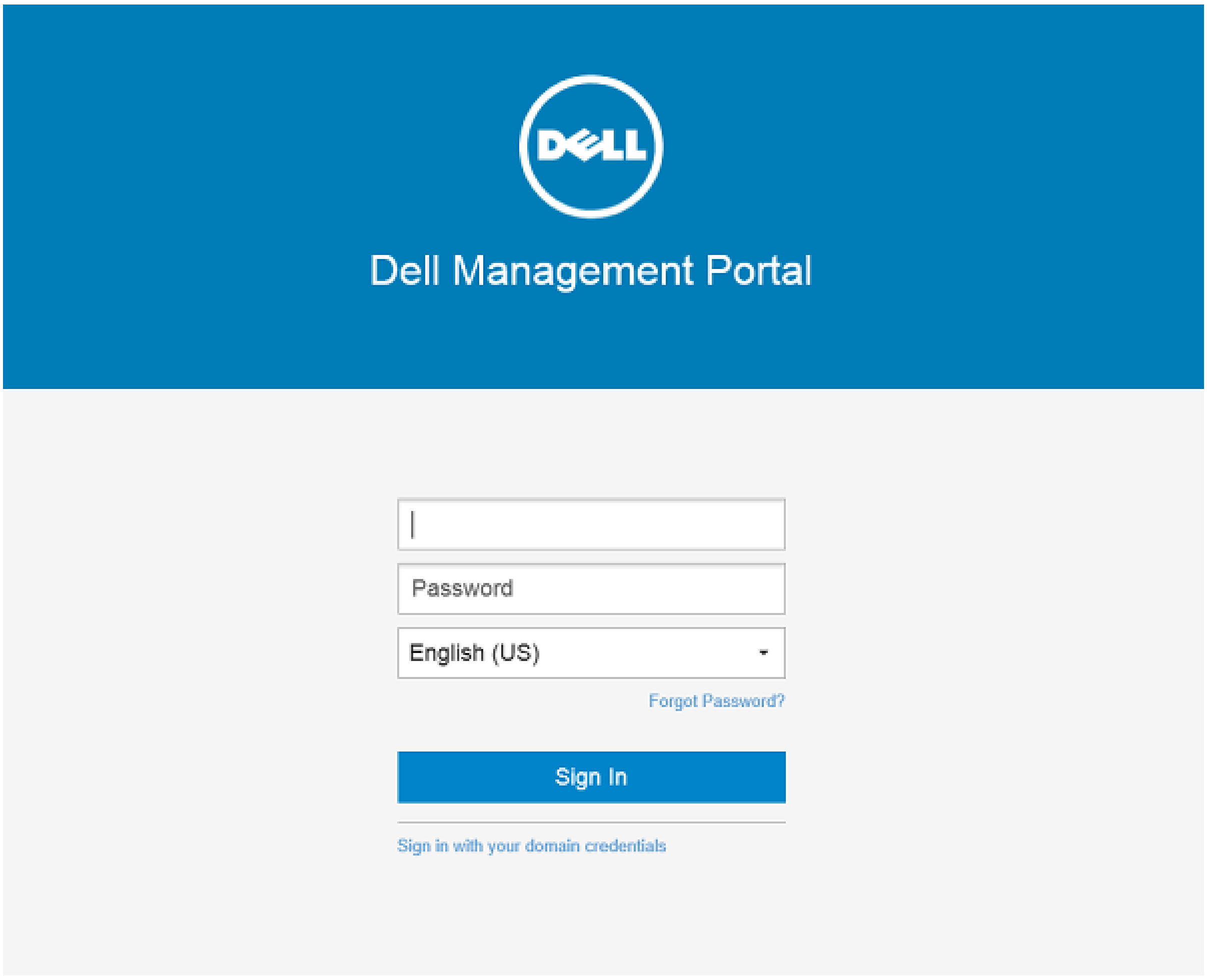


Wyse Management Suite Setup

English (US)

You have successfully set up your WMS!

Figure 14. Sign in page



Dell Management Portal

Password

English (US)

Figure 15. Dell Management Portal

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

Topics:

Logging in to Edge Device Manager

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

1. If you are using Internet Explorer, disable the **Internet Explorer Enhanced Security** and the **Compatibility View** settings.
2. Use a supported web browser on any machine with access to the internet, and access the private cloud edition of the Wyse Management Suite from https://<FQDN>/ccm-web. For example, https://wmsserver.domainname.com/ccm-web, where, wmsserver.domainname.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:

- 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 Edge Device Manager R16 Administrator's Guide* at support.dell.com.

Configuring and managing Edge Gateway devices

Configuration management—Edge Device Manager 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:

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—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.

Edge Device Manager supports standard and advanced application policies. A standard application policy allows you to install a single application package. 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 Edge Device Manager 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 a policy group and updating configuration

1. Log in as the administrator and enter the credentials.
2. To create a policy group, do the following:
   a. Select **Groups and Configs** and click the **+** button on the left pane.
   b. Enter the group name and description.
   c. Enter group token.
   d. Click **Save**.
3. Select a policy group, do the following:

a. Click **Edit Policies** and select **Ubuntu Core**.

b. Select **System Personalization** and click **Configure this item**.

c. Set up the required configuration parameters.

d. Click the **Save and Publish** button to save the configuration.

NOTE:

For more details on various configuration policies supported by Edge Device Manager, see *Edge Device Manager R16 Administrator's Guide*.

Registering devices to Edge Device Manager

Devices can be registered with EDM using the following methods:

- Configuring appropriate option tags on DHCP server
- Configuring appropriate DNS SRV records on DNS server
- USB based registration
- File based registration

NOTE:

- For public cloud you must register your thin clients by providing Wyse Management Suite URL and the group token for the group to which you want to register this device.
- For private cloud you must register your thin clients by providing Wyse Management Suite URL and optionally the group token for the group to which you want to register this device. Devices are registered to the unmanaged group if the group token is not provided.

Registering devices by using DHCP option tags

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

NOTE:

For detailed instructions on how to add DHCP option tags on the Windows server, see Creating and configuring DHCP option tags.

Table 2. Registering device by using DHCP option tags (continued)

Option Tag	Description
Name—WMS **Data Type**—String **Code**—165 **Description**—CCMServer	This tag points to the Edge Device Manager server URL. For example, `edmserver.acme.com:443`, where edmserver.acme.com is fully qualified domain name of the server where Edge Device Manager is installed. For links to register your devices in Edge Device Manager in public cloud, see Getting started with EDM on public cloud. **NOTE:** Do not use https:// in the server URL, or the device will not register in Edge Device Manager.
Name—MQTT **Data Type**—String **Code**—166 **Description**—MQTTServer	This tag directs the device to the Edge Device Manager Push Notification server (PNS). To register your devices in Edge Device Manager public cloud, the device must point to the PNS (MQTT) servers in public cloud. For example, US1: us1-pns.wysemanagementsuite.com EU1: eu1-pns.wysemanagementsuite.com
Name—CA Validation **Data Type**—String	Do not add this option tag if the devices are registered with Edge Device Manager on public cloud.

Table 2. Registering device by using DHCP option tags

Option Tag	Description
Code—167 **Description**—CAValidation	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**—GroupKey	This tag is required to register the devices with Edge Device Manager on public cloud. This tag is optional to register the devices with Edge Device Manager in private cloud. If the tag is not available, then the devices are automatically registered to the unmanaged group during on-premise installation.

Registering devices by using DNS SRV record

Domain Name System based device registration is supported with the following versions of Wyse Device Agent:

- Windows Embedded Systems—14.0 or later versions
- Ubuntu Core—16

You can register devices with the Edge Device Manager server if DNS SRV record fields are set with valid values.

ⓘ **NOTE:** For detailed instructions on how to add DNS SRV records on the Windows server, see Creating and configuring using DNS SRV records.

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

Table 3. Configuring device by using DNS SRV record

URL/Tag	Description
Record Name—_WMS_MGMT **Record FQDN**—_WMS_MGMT._tcp.<Domainname> **Record Type**— SRV	This record points to the Edge Device Manager server URL. For example, `edmserver.acme.com:443`, where edmserver.acme.com is fully qualified domain name of the server where Edge Device Manager is installed. For links to register your devices in Edge Device Manager in public cloud, see Getting started with EDM on public cloud. ⓘ **NOTE:** Do not use https:// in the server URL, or the device will not register in Edge Device Manager.
Record Name—_WMS_MQTT **Record FQDN**—_WMS_MQTT._tcp.<Domainname> **Record Type**—SRV	This record directs the device to the Edge Device Manager Push Notification server (PNS). To register your devices in Edge Device Manager public cloud, the device must point to the PNS (MQTT) servers in public cloud. For example, US1—us1-pns.wysemanagementsuite.com EU1—eu1-pns.wysemanagementsuite.com
Record Name—_WMS_GROUPTOKEN **Record FQDN**—_WMS_GROUPTOKEN._tcp.<Domainname> **Record Type**— TEXT	This record is required to register the devices with Edge Device Manager on public cloud. This record is optional to register the Windows or Ubuntu Core devices with Edge Device Manager on private cloud. If the record is not available, then the devices are automatically registered to the unmanaged group during on-premise installation.

Table 3. Configuring device by using DNS SRV record

URL/Tag	Description
Record Name—_WMS_CAVALIDATION **Record FQDN**—_WMS_CAVALIDATION._tcp.<Domainname> **Record Type**—TEXT	Do not add this option tag if the devices are registered with Edge Device Manager 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.

Edge Gateway and Embedded PC registration from USB device

Follow these steps to register Edge Gateway and Embedded PC from a USB device:

1. Insert a USB drive into the laptop with which you are logged in to EDM.
2. Create a folder named **config** at the root level of the USB drive.
3. Within the **config** folder, create another folder named **ccm-wda**.
4. Download the bootstrap file for the group to which you want to register the Edge Gateway/Embedded PC.
5. Rename the file to `reg.json` and place the file in the **ccm-wda** folder on the USB drive.
6. Eject the USB drive and plug the USB drive in to the Edge Gateway/Embedded PC device and restart the device.

File based registration for Edge Gateway and Embedded PC

Follow these steps to do a file based registration for Edge Gateway and Embedded PCs:

1. Log in to the EDM server.
2. Navigate to **Portal administration** > **Edge gateway and embedded PC registration**.
3. Download the bootstrap file for the group to which you want to register.
4. Copy the file to a valid location on your device:
   - Ubuntu Core/Ubuntu Desktop Devices—`\root\config\ccm-wda\`
   - Windows Devices—`C:\config\ccm-wda`
5. Restart the device.

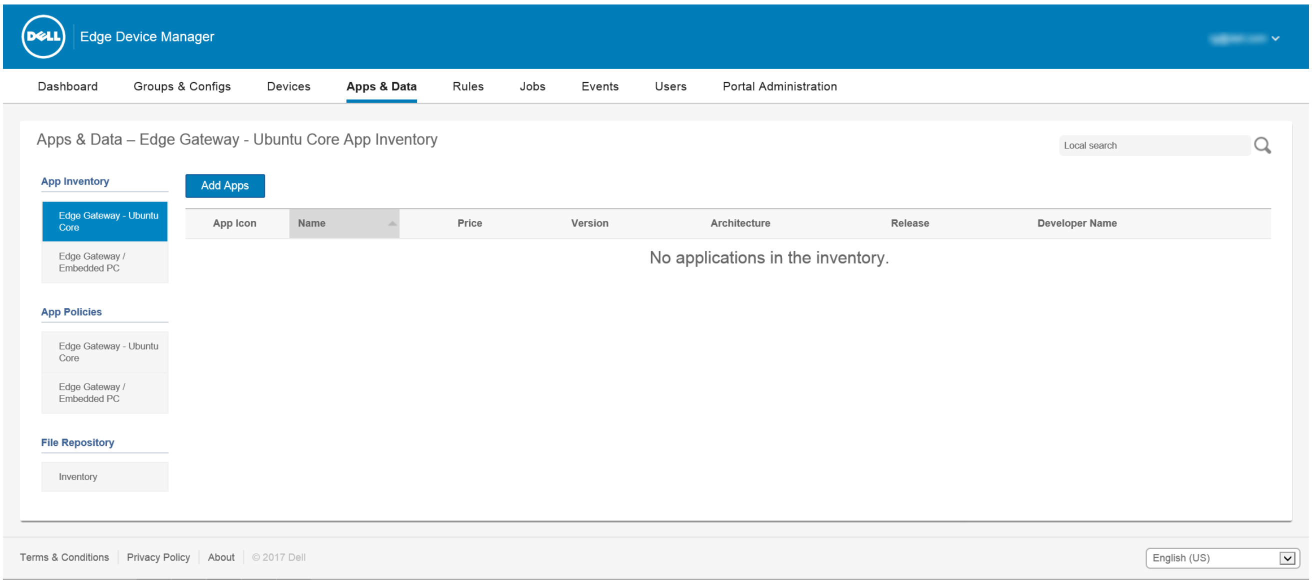
Edge Device Manager Jobs

Edge Device Manager creates job for any task such as reboot, Wake On LAN, and application policy that need to be deployed to the registered devices. Administrator can track the status of job by navigating to the **Jobs** tab in the Edge Device Manager web console. For more information, see *Edge Device Manager R16 Administrator's guide.*

Publishing application to Edge Gateway devices

To publish standard application policy to devices, do the following:

1. Select **Edge Gateway - Ubuntu Core** in **App Inventory** and click **Add App**.



Edge Device Manager

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

Apps & Data – Edge Gateway - Ubuntu Core App Inventory

Local search

App Inventory
- Edge Gateway - Ubuntu Core
- Edge Gateway / Embedded PC

App Policies
- Edge Gateway - Ubuntu Core
- Edge Gateway / Embedded PC

File Repository
- Inventory

Add Apps

App Icon	Name	Price	Version	Architecture	Release	Developer Name

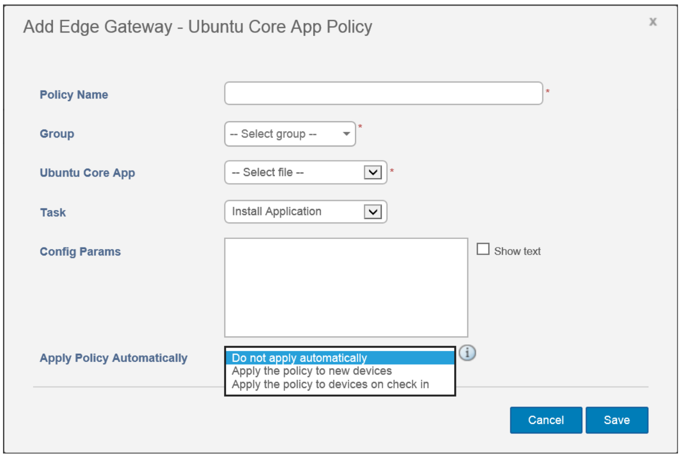
No applications in the inventory.

Terms & Conditions | Privacy Policy | About | © 2017 Dell

English (US)

Figure 16. Apps and Data

2. Click **Edge Gateway – Ubuntu Core** in **App Policies**.
3. Click **Add Policy**.
4. Enter the appropriate information to create a new application policy.



Add Edge Gateway - Ubuntu Core App Policy

Policy Name	*
Group	-- Select group -- *
Ubuntu Core App	-- Select file -- *
Task	Install Application
Config Params	□ Show text
Apply Policy Automatically	Do not apply automatically Apply the policy to new devices Apply the policy to devices on check in

Cancel | Save

Figure 17. Ubuntu Core App Policy

a. Enter the policy name.
b. From the drop-down menus, select the group, Ubuntu Core App, and task.
c. Enter the configuration parameters in **Config Params**.
d. From the **Apply Policy Automatically** drop-down list, select **Apply the policy to new devices**, to automatically apply this policy to a device that is registered with Edge Device Manager and belongs to a specified group or is moved to a specified group.

> **NOTE:** If you select **Apply the policy to devices on check in**, the policy is automatically applied to the device at check-in to the Wyse Management Suite server.

5. Click **Save**.

   A window is displayed to allow the administrator to schedule this policy on devices based on group.
6. Select **Yes** to push application policy to devices.
7. The app policy job can be run using the following options:

   a. Immediately—Server runs the job right away

   b. On device time zone— Server creates a job for each device time zone and schedule the job to the selected date/time of the device time zone.

    c. On selected time zone—Server will create a job to be run at the date and time of the designated time zone.

8. You may check the status of job by navigating to **Jobs** page at any time.

3

Uninstalling Edge Device Manager

To uninstall Edge Device Manager, do the following:

1. Go to **Add/Remove Programs** and select **Wyse Management Suite**.

   The uninstaller wizard is initiated, and the **Edge Device Manager uninstaller** screen is displayed.

2. Click **Next**. By default, the **Remove** radio button is selected that uninstalls all the Edge Device Manager installer components.

4

Troubleshooting Edge Device Manager

This section provides troubleshooting information for Wyse Management Suite.

Problems with accessing Edge Device Manager web console

- Problem: When you attempt to connect to the Edge Device Manager 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: Mosquitto
  5. Dell WMS: Tomcat Service

- Problem: When you attempt to connect to the Edge Device Manager 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: Edge Device Manager 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 Edge Device Manager

- Problem: Unable to register devices with Edge Device Manager in public cloud.

  Workaround:

  - Ensure that ports 443 and 1883 are open.
  - Check your internet connectivity, and access to the Wyse Management web application from the browser.
  - 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 Edge Device Manager in private cloud.

  Workaround:

  - Ensure that the ports 443 and 1883 are open.
  - Check the network, 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 Edge Device Manager 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: Mosquitto service is running on the Edge Device Manager server.
- Check if port 1883 is open.
- Ensure that the device is not in a sleep or shutdown state before sending a command.

A

Introduction to remote database

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

Topics:

Configuring Mongo database

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

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

To configure MongoDB, do the following:

1. Install the MongoDB version 3.2.9.
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\3.2\mongod.cfg" -install` or `sc.exe create MongoDB binPath= "\"C:\ProgramFiles\MongoDB\Server\3.2\bin\mongod.exe\"--service --config=\"C:\ProgramFiles\MongoDB\Server\3.2\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;`

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.

Configuring Maria database

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

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

To configure MariaDB, do the following:

1. Install the MariaDB version 10.0.26.
2. Navigate to the MariaDB installation path—`C:\Program Files\MariaDB 10.0\bin>mysql.exe -u root -p`.
3. Provide the root password which was created during installation
4. Create the database stratus—`DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_unicode_ci;`.
5. Create user `'stratus'@'localhost';`
6. Create user `'stratus'@'`**IP ADDRESS**`';`
7. Set a password for `'stratus'@'localhost'=password('`**PASSWORD**`');`
8. Set a password for `'stratus'@'IP ADDRESS'=password('`**PASSWORD**`');`
9. Provide all privileges on `*.* to 'stratus'@'`**IP ADDRESS**`'` identified by `'`**PASSWORD**`'` with a grant option.
10. Provide all privileges on `*.* to 'stratus'@'localhost'` identified by `'`**PASSWORD**`'` with a grant option.

NOTE: To configure custom port for Maria DB navigate to `C:\Program Files\MariaDB 10.0\bin>mysql.exe -u root -p -P<custom port>` in the second step.

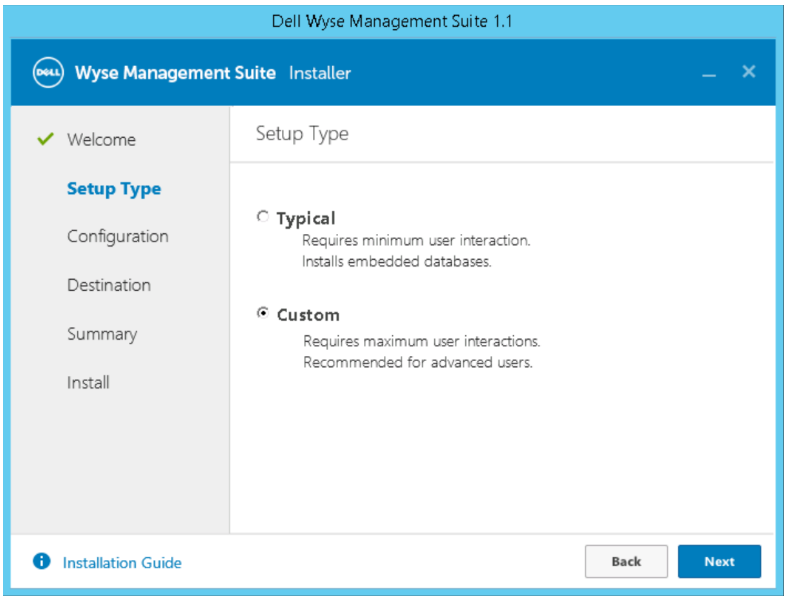
In the Wyse Management Suite installer, the administrator must use the same user name and password that was created to access the stratus databases in MariaDB. For information about setting the MariaDB on the Wyse Management Suite installer, see Custom installation.

B

Custom installation

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

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



Setup Type

○ Typical
Requires minimum user interaction.
Installs embedded databases.

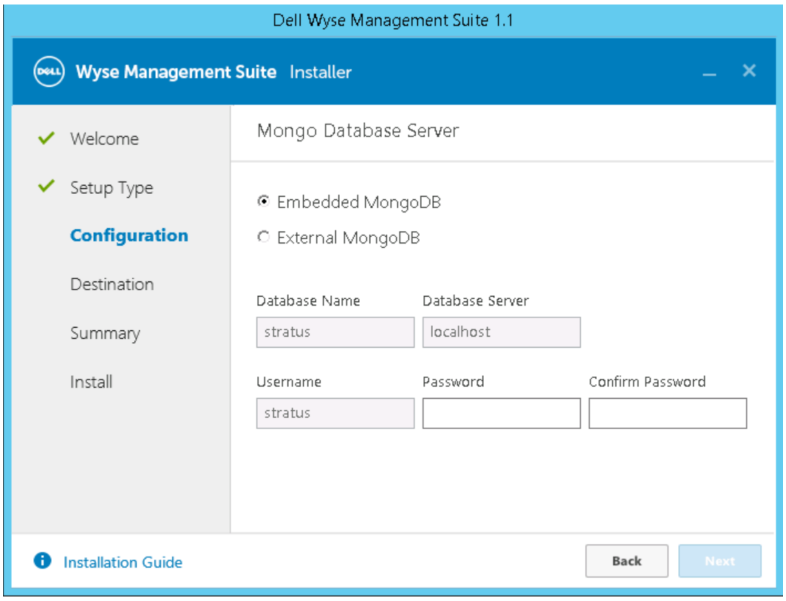
● Custom
Requires maximum user interactions.
Recommended for advanced users.

Figure 18. Setup type

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

2. Select either **Embedded MongoDB** or **External MongoDB** as the Mongo database server.
   - If **Embedded MongoDB** is selected, then provide your password, and click **Next**.

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



Dell Wyse Management Suite 1.1

Wyse Management Suite Installer

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

Mongo Database Server

● Embedded MongoDB

○ External MongoDB

Database Name: stratus

Database Server: localhost

Username: stratus

Password:

Confirm Password:

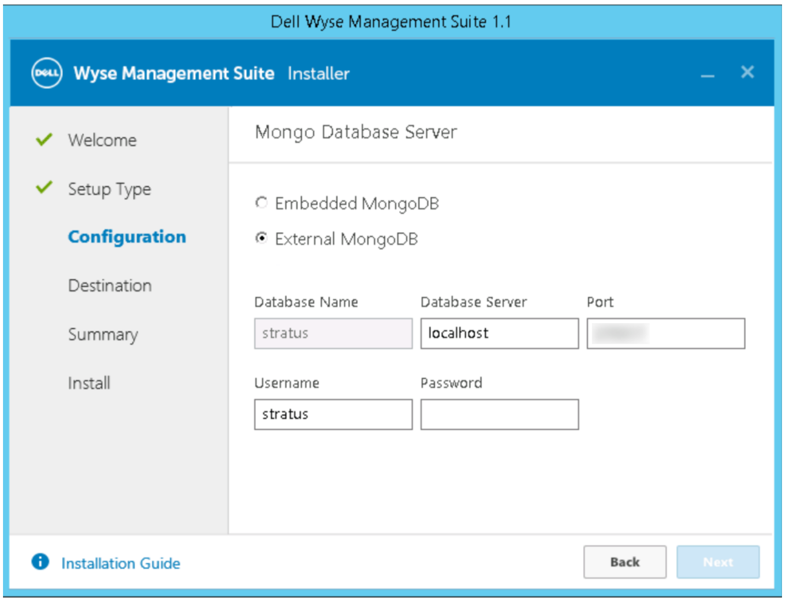
Installation Guide

Back | Next

Figure 19. 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.



Dell Wyse Management Suite 1.1

Wyse Management Suite Installer

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

Mongo Database Server

○ Embedded MongoDB

● External MongoDB

Database Name: stratus

Database Server: localhost

Port: [redacted]

Username: stratus

Password:

Installation Guide

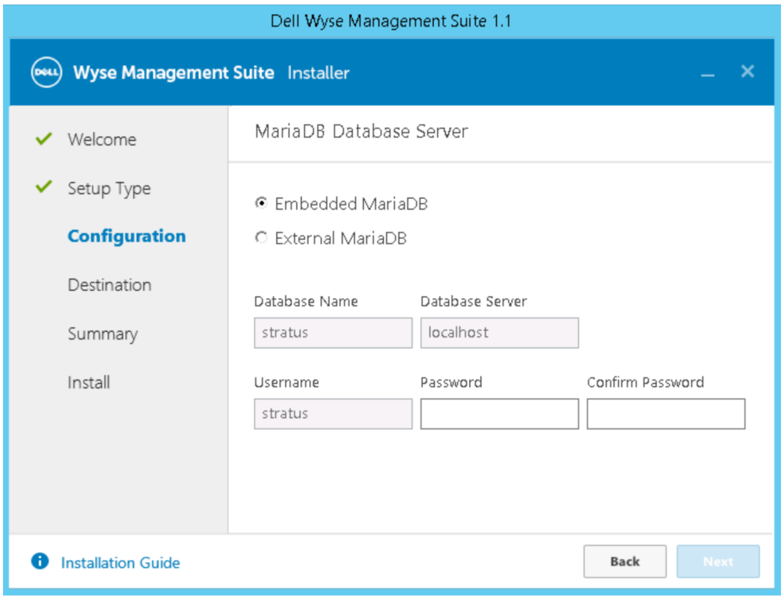
Back | Next

Figure 20. Mongo Database Server

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**.



Dell Wyse Management Suite 1.1

Wyse Management Suite Installer

MariaDB Database Server

● Embedded MariaDB

○ External MariaDB

Database Name: stratus

Database Server: localhost

Username: stratus

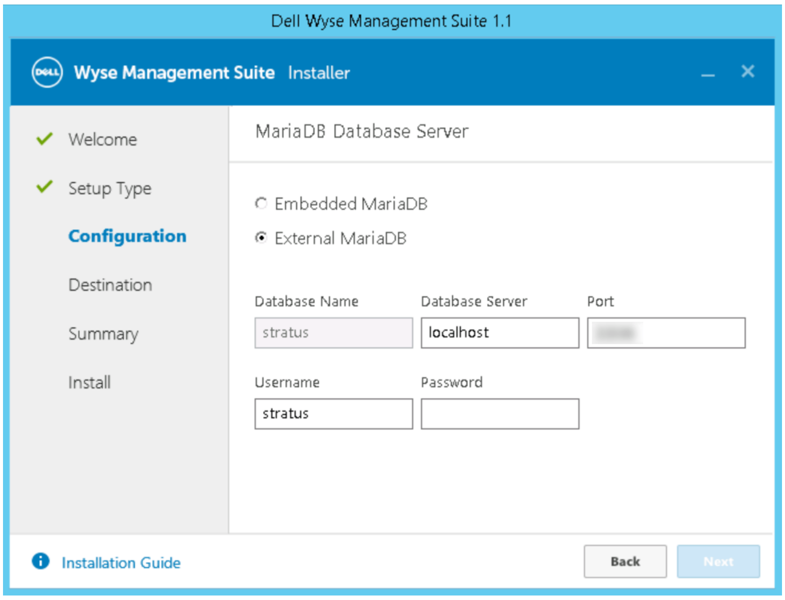
Password:

Confirm Password:

Figure 21. MariaDB Database server

- 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.



Dell Wyse Management Suite 1.1

Wyse Management Suite Installer

MariaDB Database Server

○ Embedded MariaDB

● External MariaDB

Database Name: stratus

Database Server: localhost

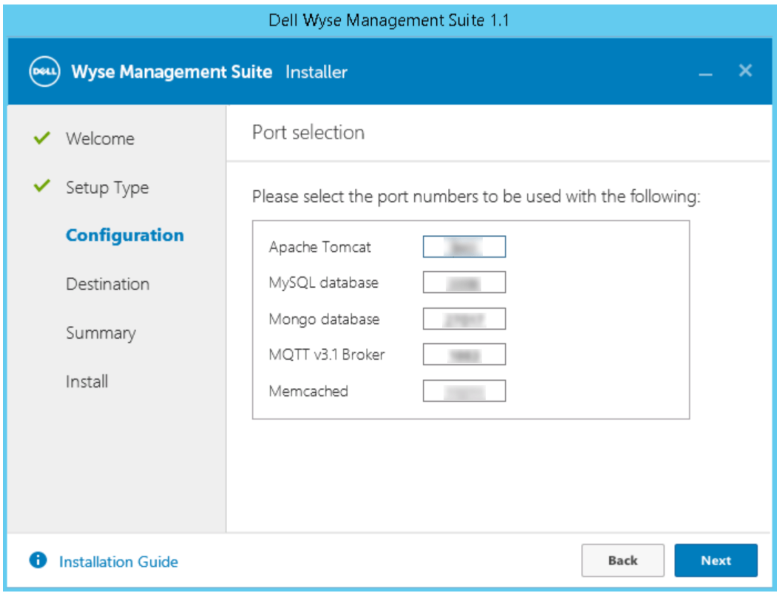
Port: [redacted]

Username: stratus

Password:

Figure 22. MariaDB Database server

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 [redacted]

MySQL database [redacted]

Mongo database [redacted]

MQTT v3.1 Broker [redacted]

Memcached [redacted]

Figure 23. Port Selection

NOTE: Edge Device Manager 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 Edge Device Manager on private cloud.

C

Feature list

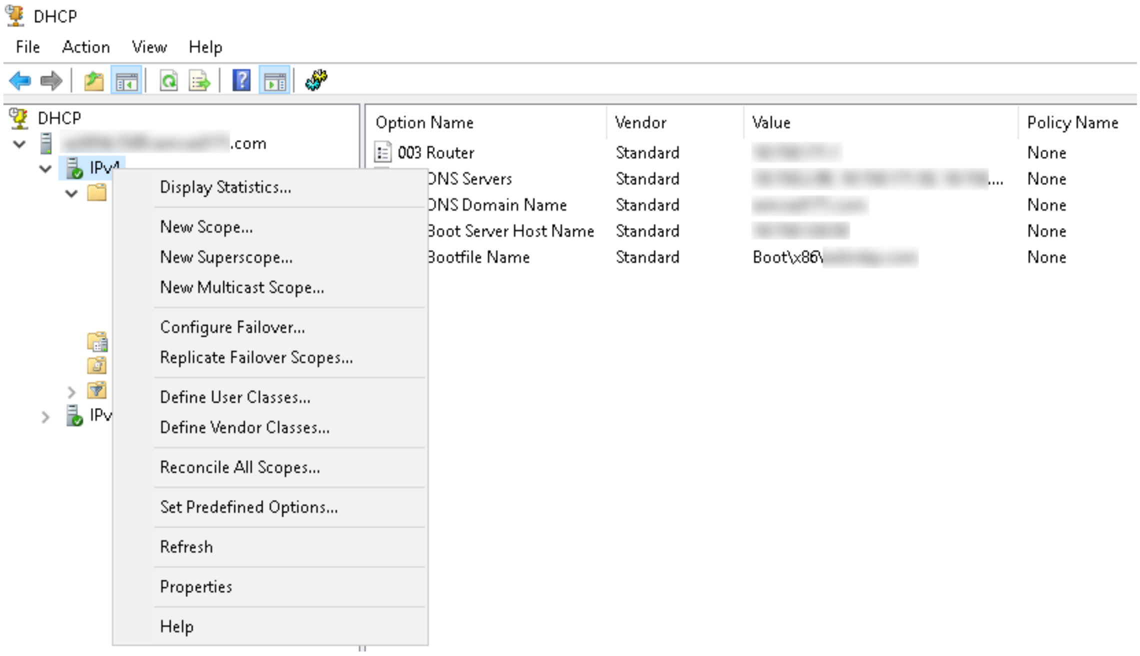
- Highly scalable solution to manage Edge Gateway devices
- Group based management
- Multi Level Groups and Inheritance
- Configuration Policy management
- View effective configuration at device level after inheritance
- Application policy management
- Asset, Inventory and Systems management
- Automatic device discovery
- Real-time commands
- Smart Scheduling
- Alerts, Events and Audit logs Secure communication (HTTPS)
- Manage devices behind firewalls
- Mobile app
- Alerts through Email and mobile app
- Delegated administration
- Dynamic group creation and assignment based on device attributes
- Two-factor authentication
- Active directory authentication for role based administration
- Multi-tenancy
- Enterprise Grade Reporting
- Multiple repositories
- Enable/Disable hardware ports
- BIOS configuration

D

Creating and configuring DHCP option tags

To create a DHCP option tag, do the following:

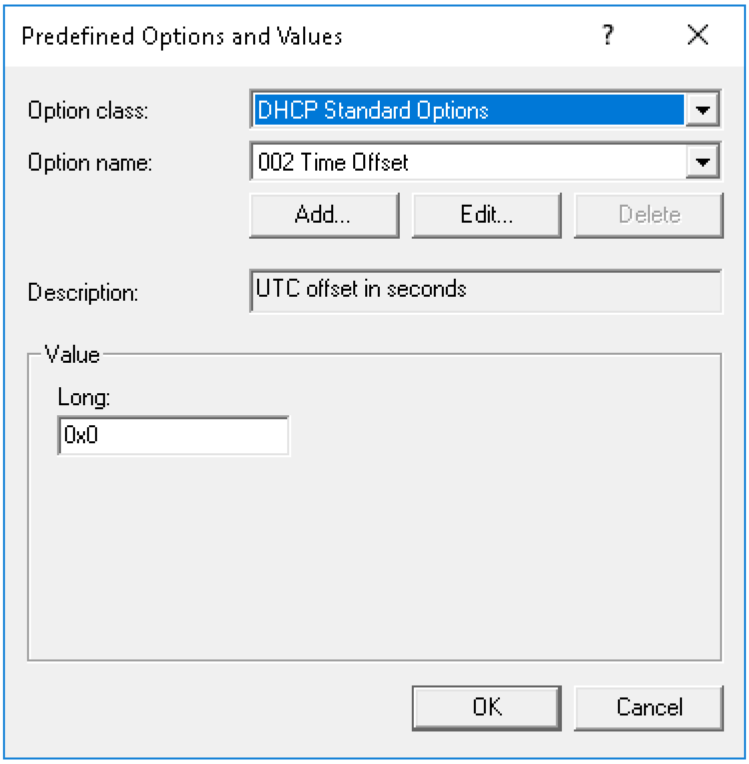
1. Open the Server Manager.
2. Go to **Tools** and click **DHCP option**.
3. Go to **FQDN** > **IPv4** and right-click **IPv4**.



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 24. DHCP

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



Option class: DHCP Standard Options

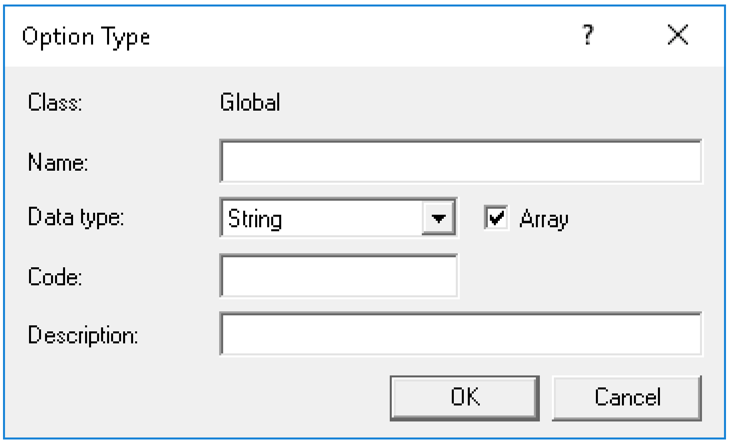
Option name: 002 Time Offset

Description: UTC offset in seconds

Long: 0x0

Figure 25. Predefined Options and Values

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



Class: Global

Name:

Data type: String ☑ Array

Code:

Description:

Figure 26. Option Type

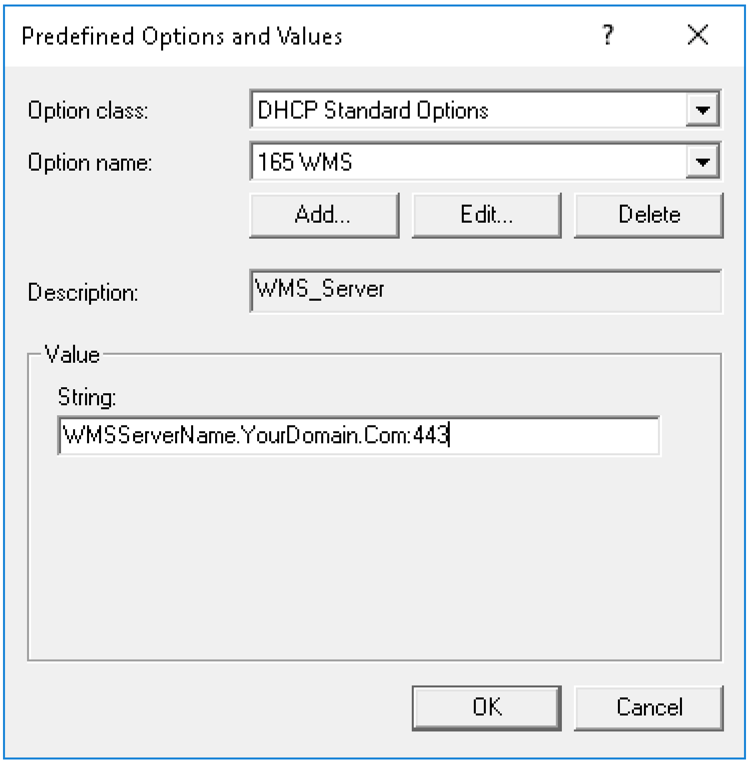
The options need to be either added to the server options of the DHCP server or scope options of the DHCP scope.

Configuring the DHCP option tags

- To create the 165 Wyse Management Suite server URL option tag, do the following:
  1. Enter the following values and click **OK**.
     - Name—WMS
     - Data type—String
     - Code—165
     - Description—WMS_Server
  2. Enter the following value and then click **OK**.

     String—`WMS FQDN`

For example, WMSServerName.YourDomain.Com:443.



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 165 WMS

Description: WMS_Server

Value

String: WMSServerName.YourDomain.Com:443

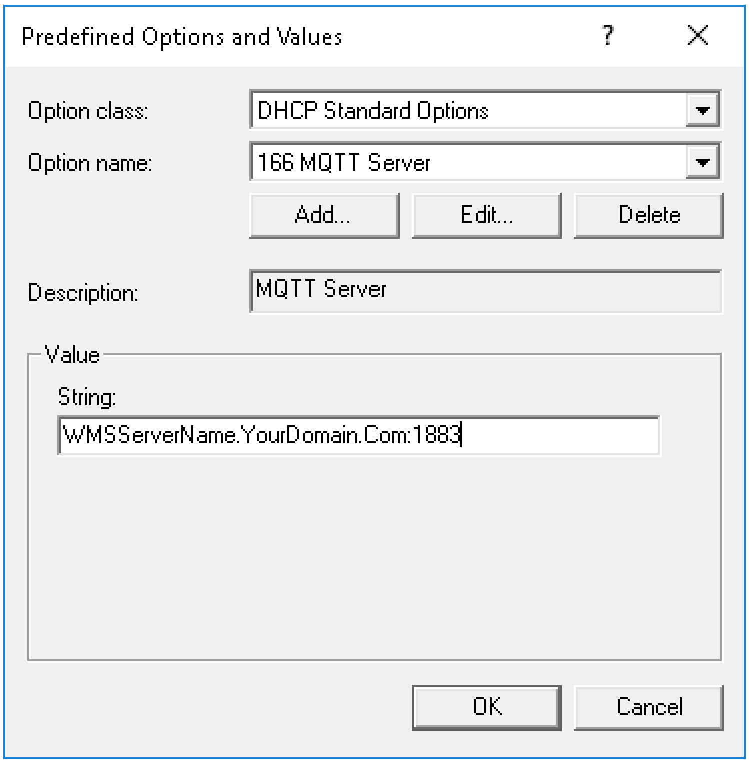
Figure 27. 165 Wyse Management Suite server URL option tag

- 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



Option class: DHCP Standard Options

Option name: 166 MQTT Server

Description: MQTT Server

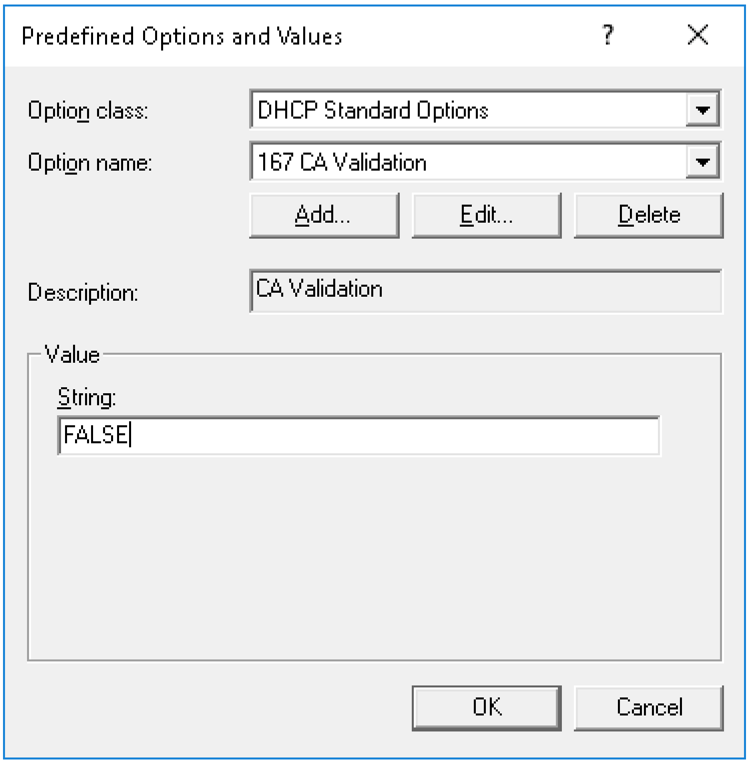
Value

String: WMSServerName.YourDomain.Com:1883

Figure 28. 166 Wyse Management Suite server URL option tag

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

     String—TRUE/FALSE



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 167 CA Validation

Description: CA Validation

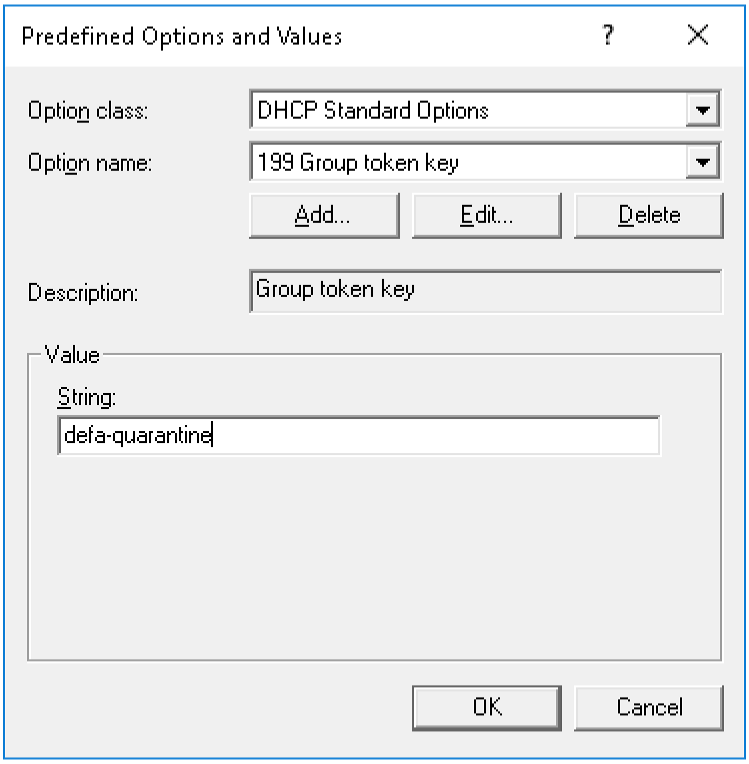
Value

String: FALSE

Figure 29. 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

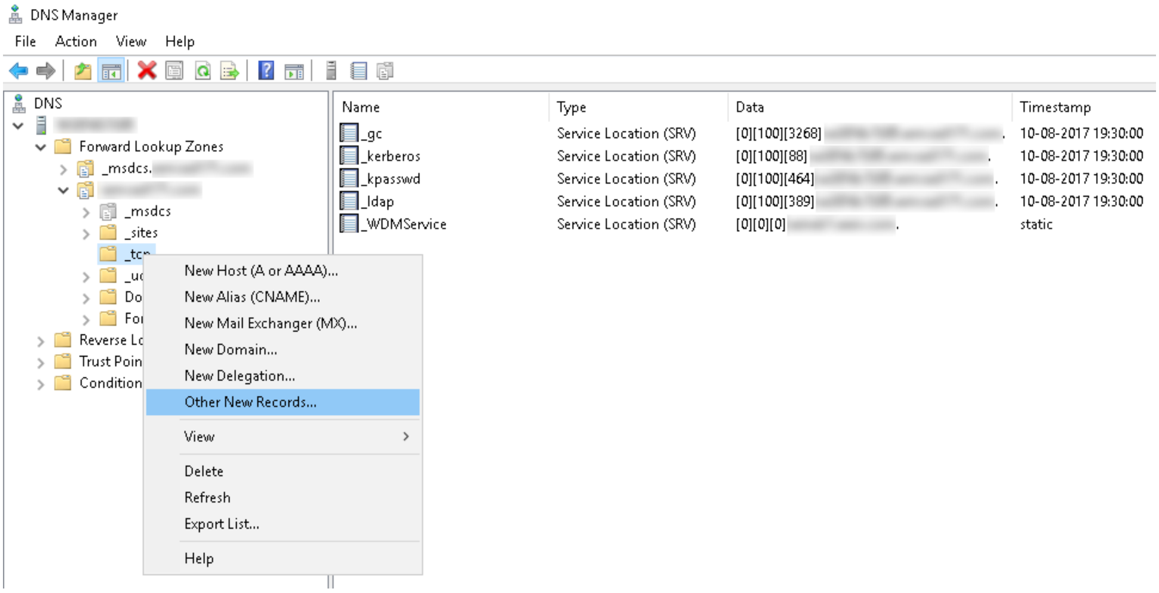
Figure 30. 199 Wyse Management Suite server URL option tag

E

Creating and configuring DNS SRV records

To create a DNS SRV record, do the following:

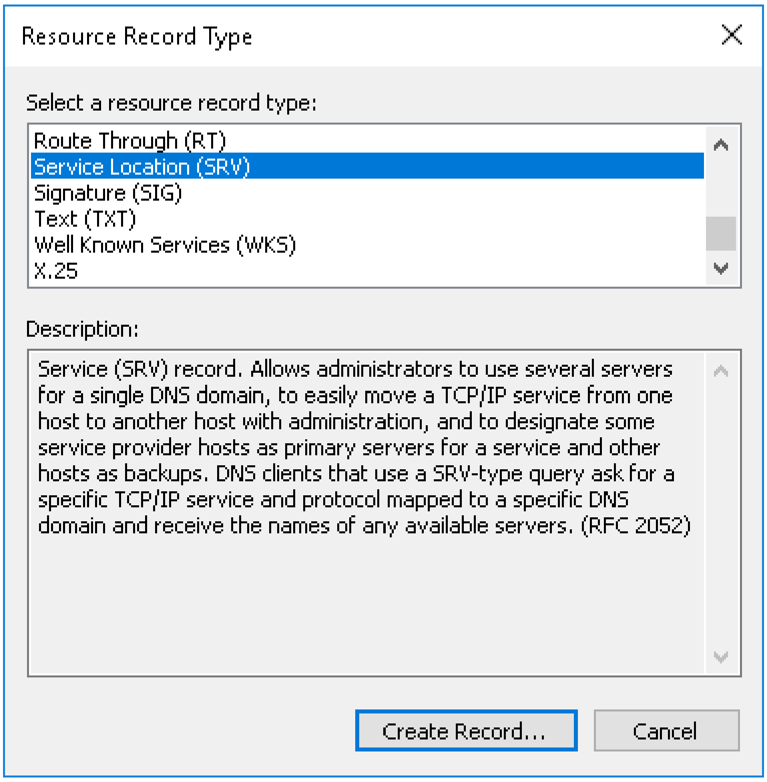
1. Open the Server Manager.
2. Go to **Tools** and click **DNS option**.
3. Go to **DNS** > **DNS Server Host Name** > **Forward Lookup Zones** > **Domain** > **_tcp** and right-click the **_tcp option**.



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 31. DNS Manager

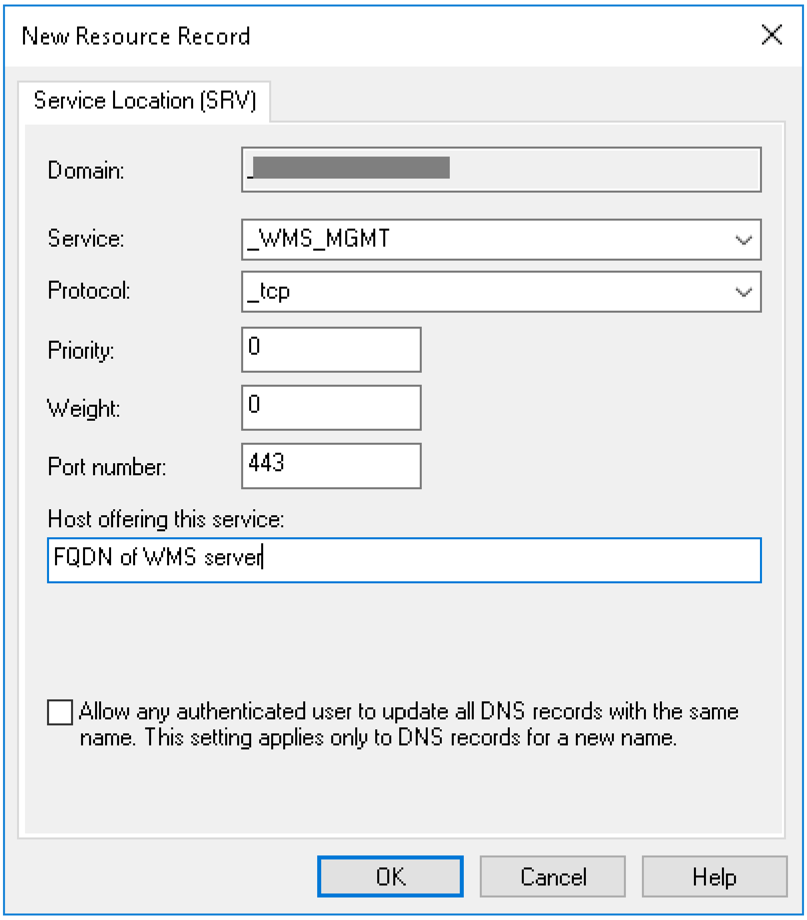
4. Click **Other New Records**.
   The **Resource Record Type** window is displayed.
5. Select the **Service Location (SRV)**, click **Create Record**, and do the following:



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 32. 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



Domain: [redacted]

Service: _WMS_MGMT

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 443

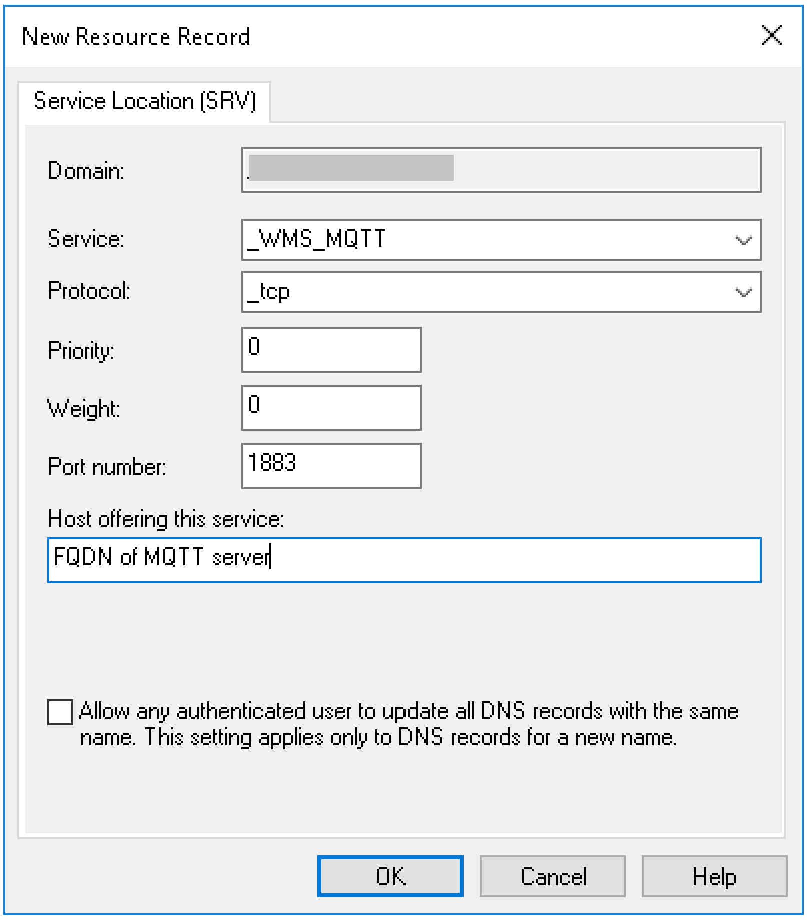
Host offering this service: FQDN of WMS server

☐ 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 33. _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

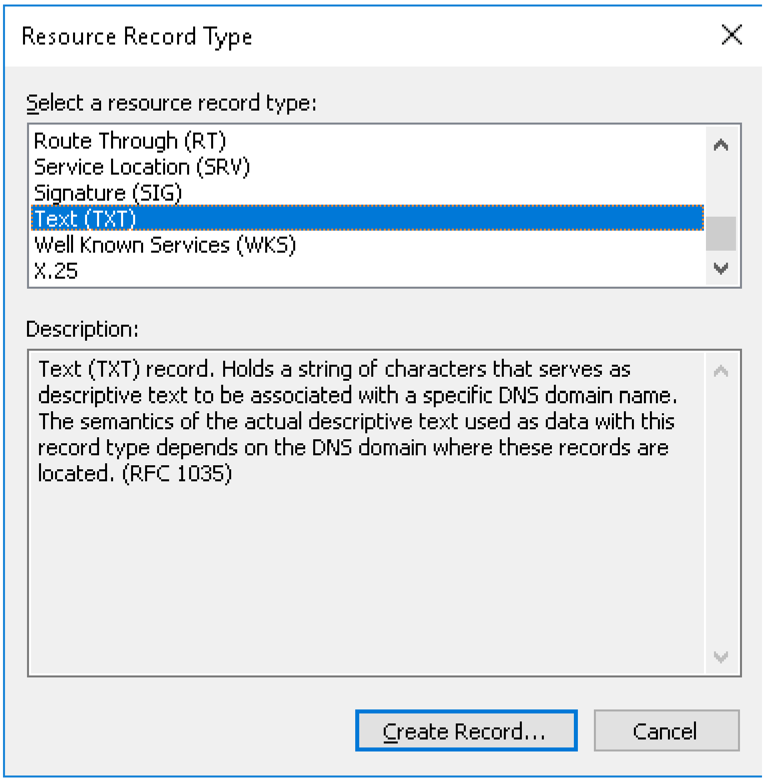
Port number: 1883

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 34. _WMS_MQTT service

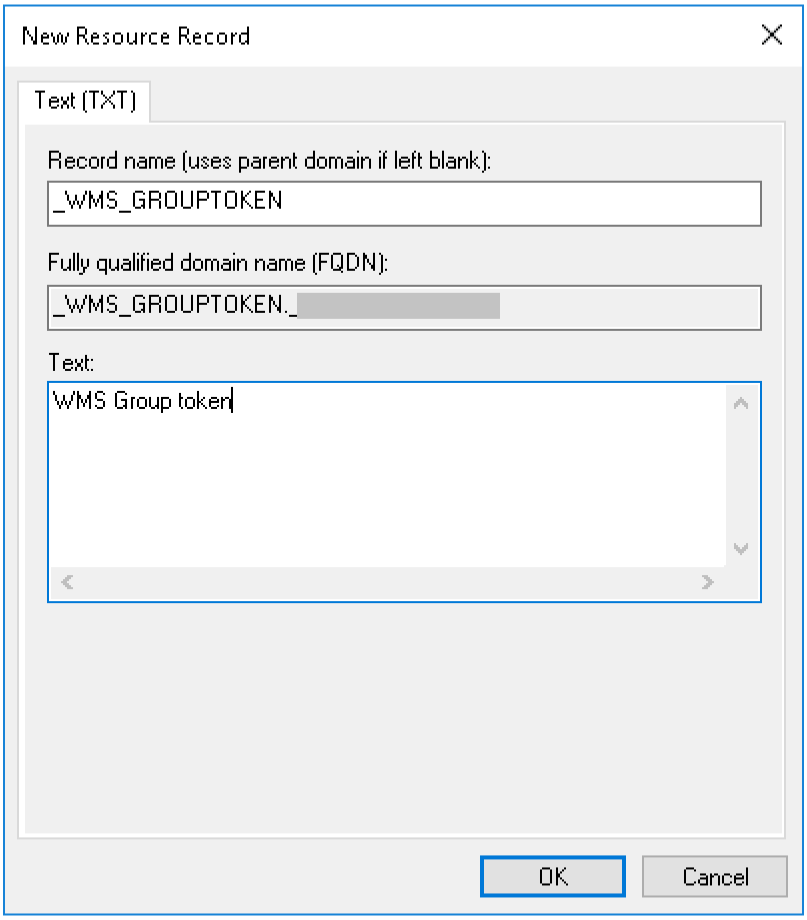
6. Go to **DNS** > **DNS Server Host Name** > **Forward Lookup Zones** > **Domain** and right-click the domain.
7. Click **Other New Records**.
8. Select **Text (TXT)**, click **Create Record**, and do the following:



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 35. 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



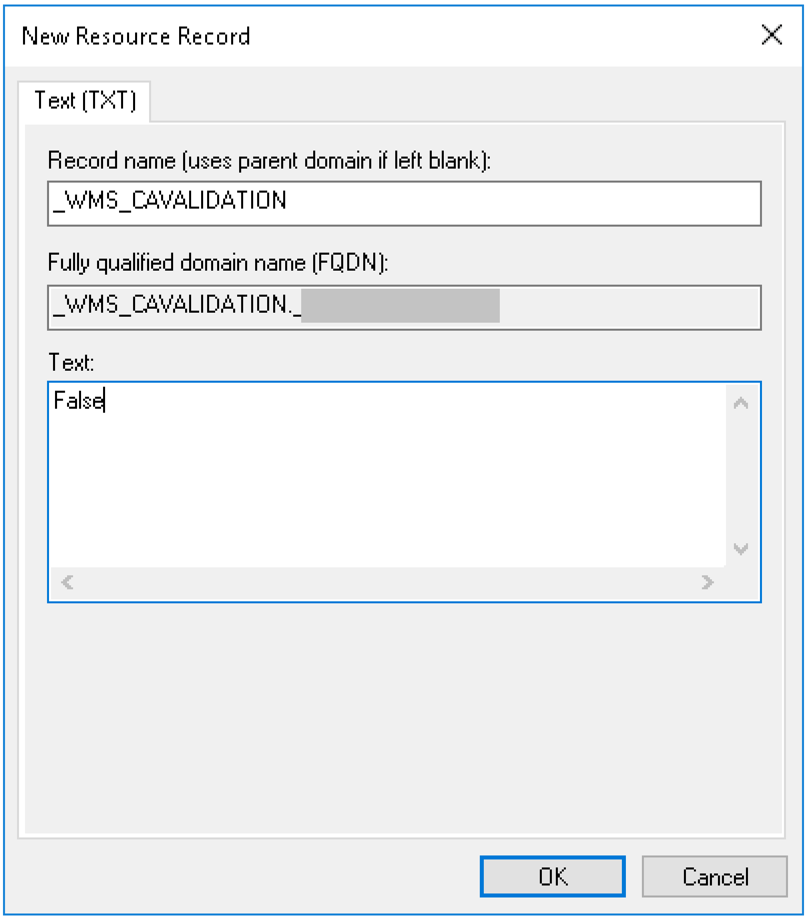
Record name (uses parent domain if left blank): _WMS_GROUPTOKEN

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

Text: WMS Group token

Figure 36. _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 37. _WMS_CAVALIDATION record name

F

Supported devices

- Edge gateway 5000 running Windows 10 LTSB 15
- Edge gateway 3000 running Ubuntu Core 16
- Edge gateway 3000 running Windows 10 IoT LTSB 2016
- Edge gateway 5000 running Ubuntu Core 16
- Edge gateway 5000 running Windows 10 IoT LTSB 2016
- Embedded PC 3000 running Windows 7 Pro
- Embedded PC 3000 running Windows 7 Pro for FES
- Embedded PC 3000 running Windows Embedded Standard 7P
- Embedded PC 3000 running Windows Embedded Standard 7E
- Embedded PC 3000 running Windows 10 IoT LTSB 15
- Embedded PC 3000 running Windows 10 Pro
- Embedded PC 5000 running Windows 7 Pro
- Embedded PC 5000 running Windows 7 Pro for FES
- Embedded PC 5000 running Windows Embedded Standard 7P
- Embedded PC 5000 running Windows Embedded Standard 7E
- Embedded PC 5000 running Windows 10 IoT LTSB 15
- Embedded PC 5000 running Windows 10 Pro
- Embedded PC 3000 running Ubuntu Core 16
- Embedded PC 5000 running Ubuntu Core 16

G

Support matrix

Supported operating system

The following are the supported operating systems for Edge Gateway and Embedded PC:

Edge Gateway—3000 series

- Ubuntu Core 16
- Windows 10 IoT Enterprise 2016 LTSB

Edge Gateway—5000 series

- Ubuntu Core 16
- Windows 10 IoT Enterprise 2015 LTSB
- Windows 10 IoT Enterprise 2016 LTSB

Embedded PC

- Ubuntu Desktop 16.04
- Windows 10 IoT Enterprise 2015 LTSB
- Windows 10 IoT Enterprise 2016 LTSB
- Windows 7 Pro
- Windows 10 Pro
- Windows 7 Pro for Embedded Systems—FES7
- Windows Embedded Standard 7P
- Windows Embedded Standard 7E

Supported operating system language pack for EDM web console

The following are supported operating system language pack:

1. English
2. French
3. Italian
4. German
5. Spanish
6. Simplified Chinese
7. Japanese

Supported browsers

The following are the supported browsers:

1. Internet Explorer 11.0 and later
2. Google Chrome 62.0 and later
3. Firefox 56 and later

H

Terms and definitions

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

Table 4. Terms and definitions

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