

Dell Wyse Management Suite

Version 3.x and 4.x Deployment Guide



Notes, cautions, and warnings

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

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

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

Contents

Chapter 1: Introduction.....	4
Chapter 2: Hardware requirements.....	5
Chapter 3: Wyse Management Suite deployment architecture.....	7
Chapter 4: Deployment details.....	8
Chapter 5: Custom port configurations.....	14
Change the Tomcat service port	14
Change the MQTT port.....	15
Change the MariaDB port	15
Change the MongoDB database port.....	16
Remote repository.....	16
Manage Wyse Management Suite repository service.....	20
Chapter 6: Upgrade Wyse Management Suite version 2.x to 3.x.....	21
Chapter 7: Upgrade Wyse Management Suite version 3.x to 3.3.....	22
Chapter 8: Upgrade Wyse Management Suite version 3.x to 3.5.....	23
Chapter 9: Upgrade Wyse Management Suite version 3.x to 3.6.....	24
Chapter 10: Upgrade Wyse Management Suite version 3.x to 4.0.....	26
Chapter 11: Software Vault Utility.....	28
Back up your database.....	28
Restore your database.....	28
Export the Software Vault key.....	29
Import the Software Vault key.....	29

Introduction

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.

This document provides a deployment strategy of Wyse Management Suite in a single virtual machine or server on a private cloud to support the management of up to 120,000 devices.

Hardware requirements

The following table lists the hardware requirements:

Table 1. Hardware requirements

Description	10,000 devices or less	50,000 devices or less	120,000 devices or less	Wyse Management Suite – Software repository
Operating system	Windows Server 2012 R2, Windows Server 2016 or Windows Server 2019 Standard. The Wyse Management Suite web server has an inbuilt Apache Tomcat web server. Ensure that you do not install Microsoft IIS, Apache Tomcat web servers separately. Supported language pack—English, French, Italian, German, Spanish, Japanese, and Traditional Chinese			
Minimum disk space	40 GB	120 GB	200 GB	120 GB
Minimum memory (RAM)	8 GB	16 GB	32 GB	16 GB
Minimum CPU requirements	4	4	16	4
Network communication ports	The Wyse Management Suite installer adds TCP ports 443 and 1883 to the firewall exception list. The ports are added to access the Wyse Management Suite console, and to send the 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 8443—On premise secure MQTT communication • TLS 9443—Software vault service The default ports that are used by the installer may be changed to an alternative port during installation.			The Wyse Management Suite repository installer adds TCP port 443 and 8080 to the firewall exception list. The ports are added to access the operating system images and application images that are managed by Wyse Management Suite.
Supported browsers	Internet Explorer version 11.0 and later 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)			

NOTE: Wyse Management Suite can be installed on a physical or a virtual machine.

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 3.5, you must use MongoDB version 4.2.16 for distributed setups. You can not install or upgrade Wyse Management Suite 3.5 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.

Wyse Management Suite deployment architecture

The following are the Wyse Management Suite installer components to deploy at the work place:

- WMS Web Application—Application Server that hosts Wyse Management Suite.
- Memcached—Used to Cache data for performance and scalability.
- MQTT—Used to push notifications to thin clients.
- MongoDB—No SQL database for performance and scalability.
- MariaDB—Relational database for structured data and normalization.
- EMSDK—SDK to manage Teradici devices.

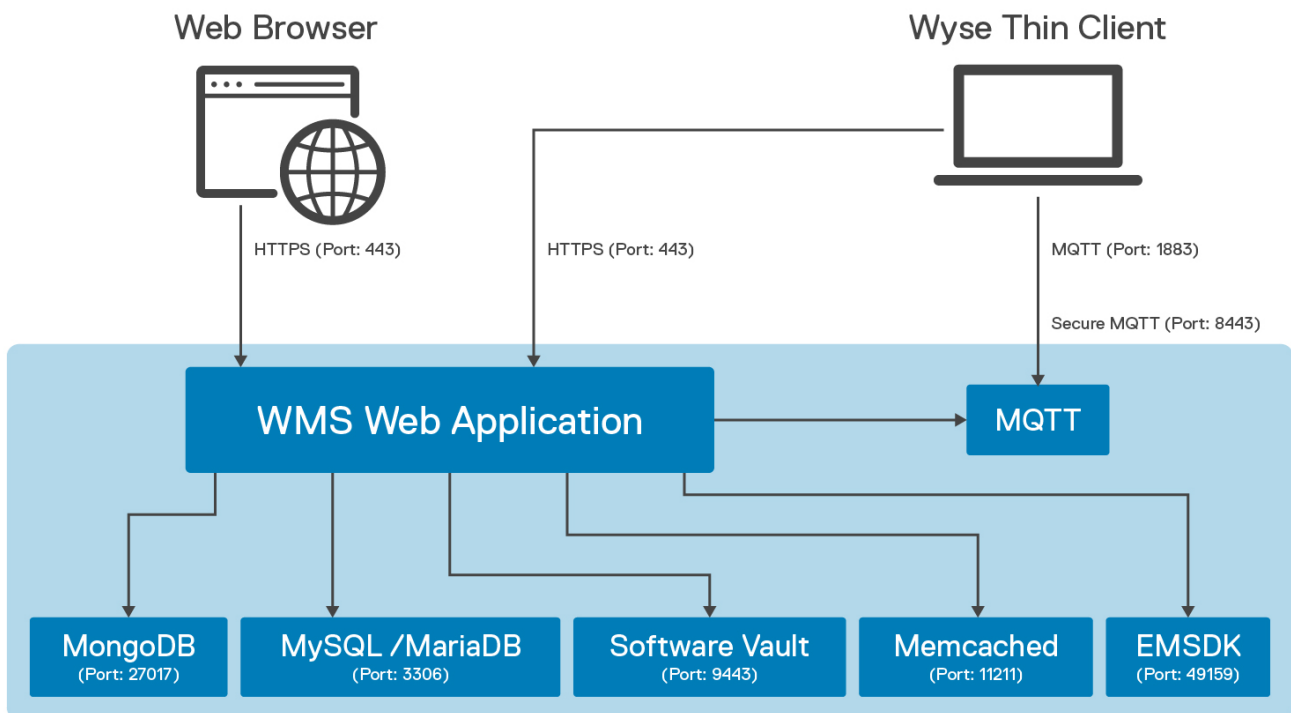


Figure 1. Wyse Management Suite architecture

Deployment details

This chapter contains the deployment architecture details for Wyse Management Suite.

The Wyse Management Suite supports up to 120,000 connected devices.

Single server deployment is easier to maintain, however, you have an option to deploy Wyse Management Suite on multiple servers as per your preference.

Deployment on a single server to support 50,000 thin client devices

The minimum hardware requirement on a single server for 50,000 devices is:

Table 2. Hardware specification

Application	Hardware specification
Wyse Management Suite	• 4 CPUs • 16 GB RAM • 120 GB HDD

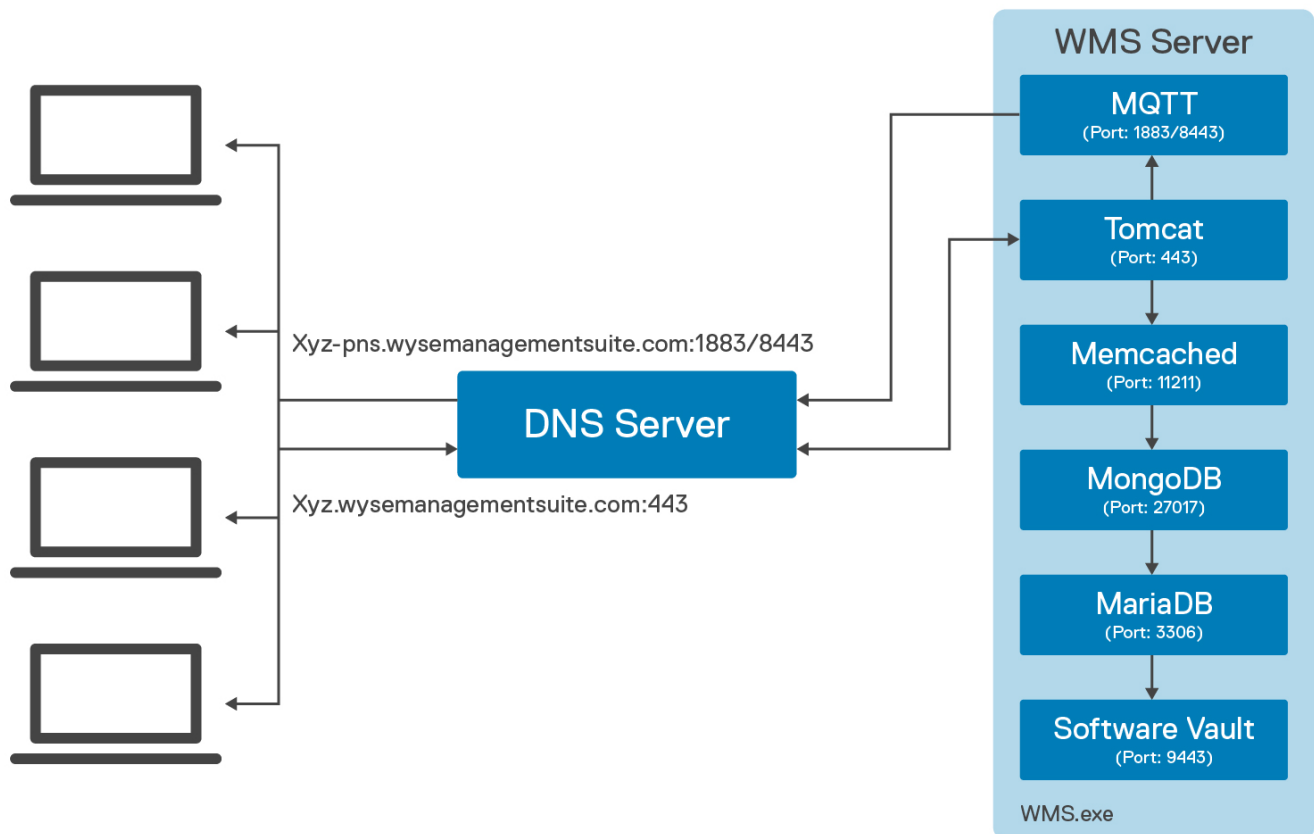
Deployment on a single server to support 120,000 thin client devices

The minimum hardware requirement on a single server for 120,000 devices is:

Table 3. Hardware specification

Application	Hardware specification
Wyse Management Suite	• 16 CPUs • 32 GB RAM • 200 GB HDD

The following diagram explains deployment of Wyse Management Suite on a single server:



Deployment Architecture of Wyse Management Suite on a single VM

Figure 2. Wyse Management Suite on a single server

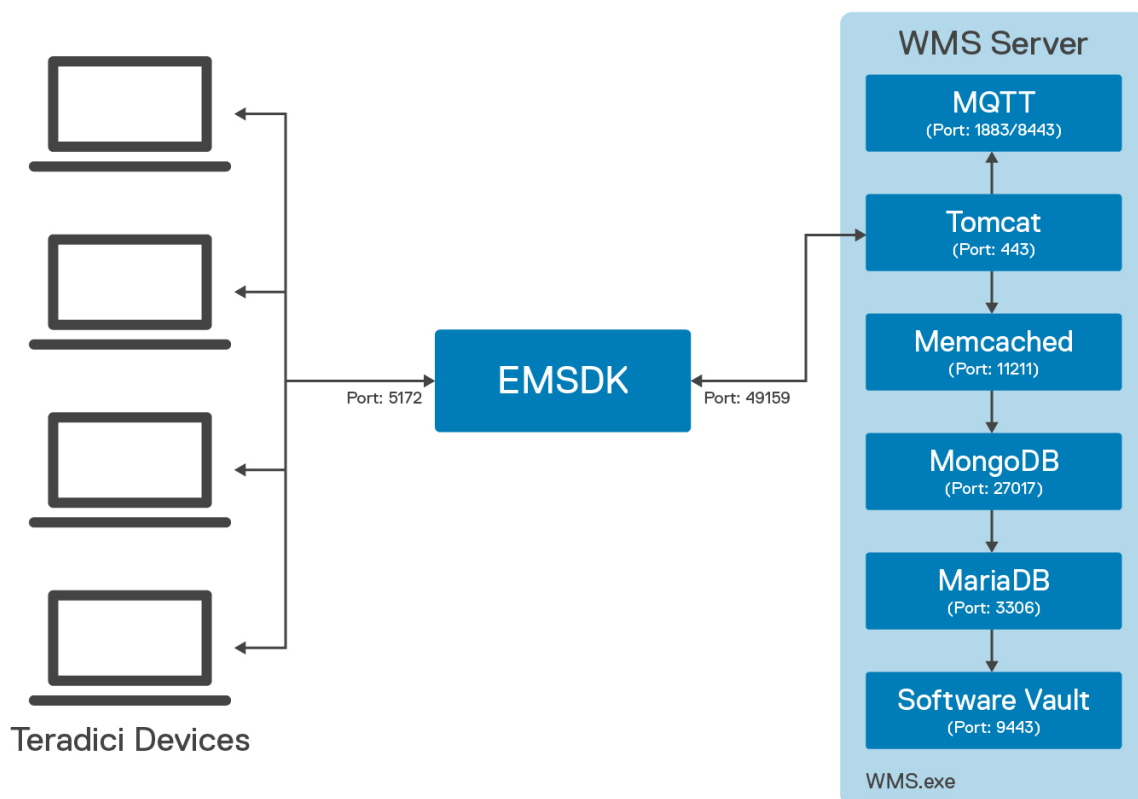
Deployment details to support Teradici devices

EMSDK software component must be installed with Wyse Management Suite, to support Teradici devices. EMSDK components are included in WMS .exe installer, however the installation is optional.

EMSDK can be installed locally on Wyse Management Suite server or on a separate VM or server. Wyse Management Suite deployment can have multiple instances of EMSDK, however each instance must run on a separate server, and each instance can support up to 5,000 Teradici devices.

Deployment on a single server to support 5,000 Teradici devices

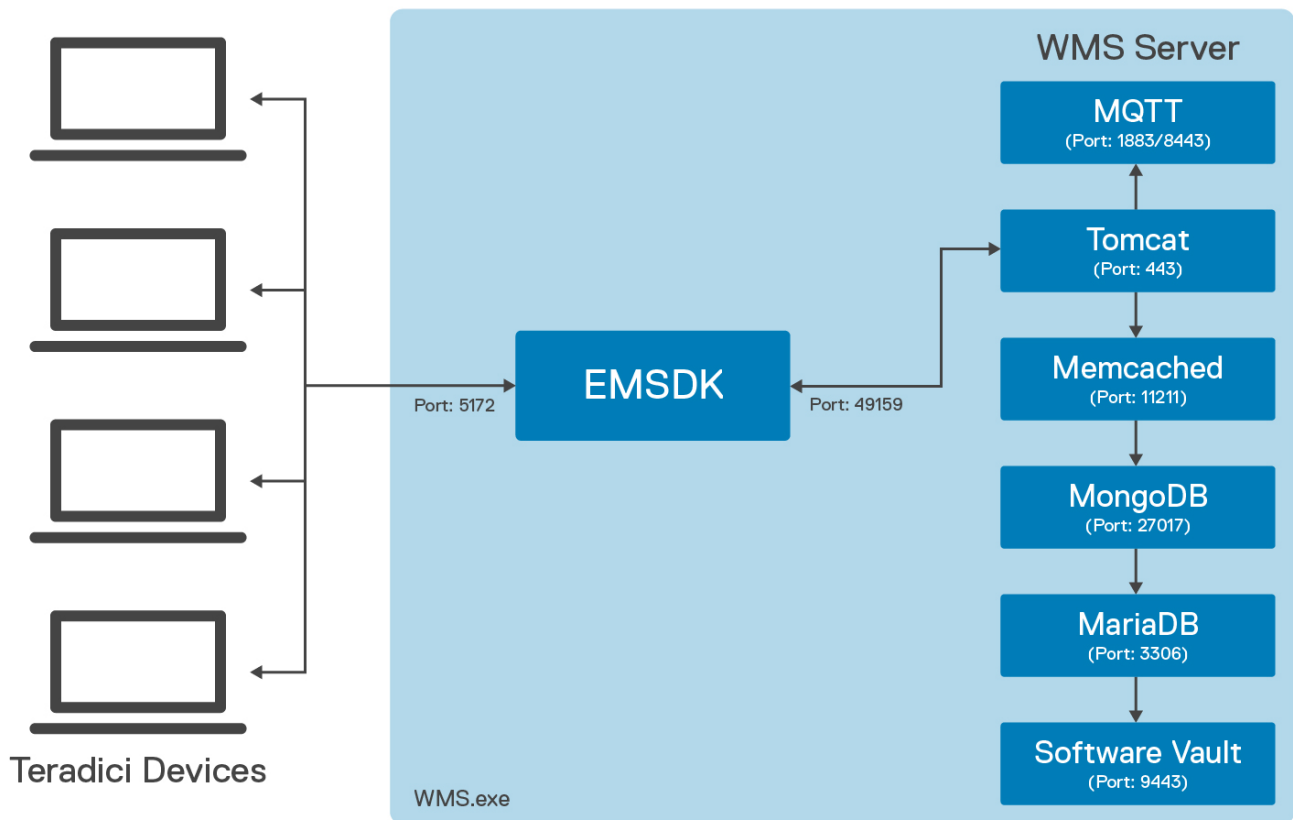
The following diagram explains deployment architecture of Wyse Management Suite on a single VM with remote EMSDK:



Deployment Architecture of Wyse Management Suite on a single VM with remote EMSDK (supports up to 5000 Teradici devices)

Figure 3. Wyse Management Suite on a single VM with remote EMSDK

The following diagram explains deployment architecture of Wyse Management Suite with EMSDK on a single VM :

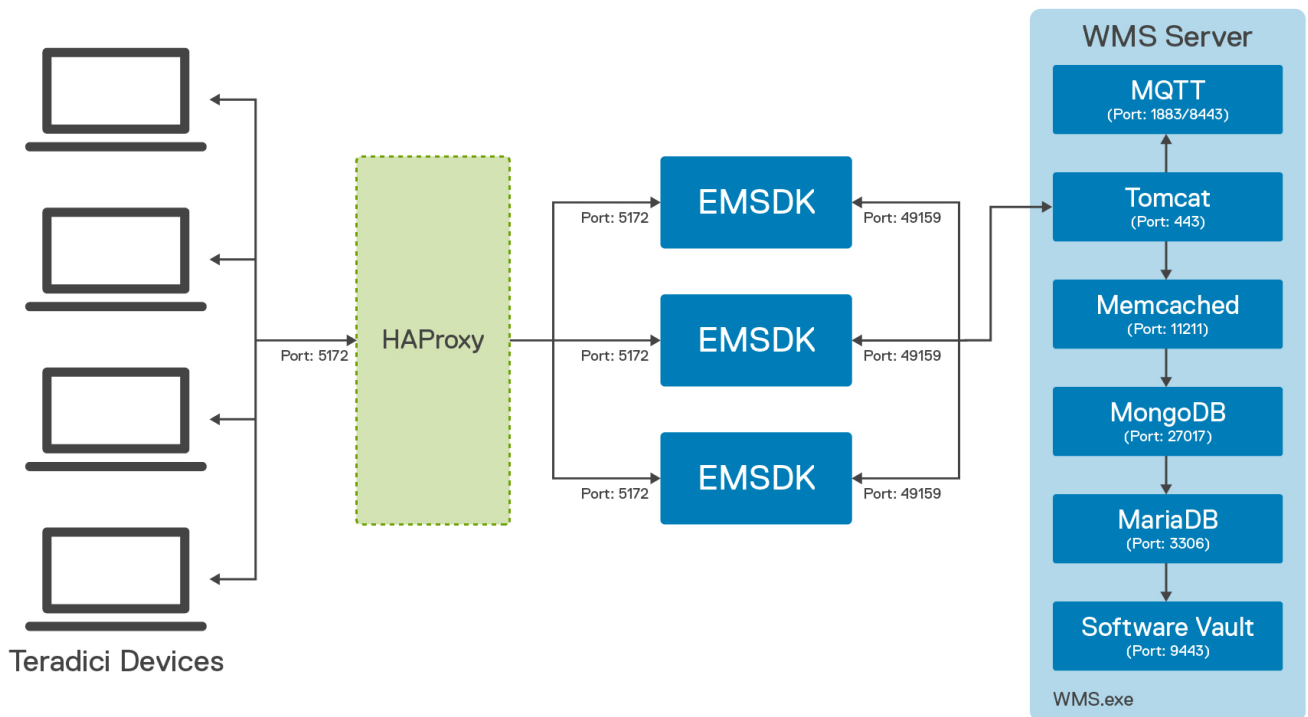


Deployment Architecture of Wyse Management Suite with EMSDK on a single VM (supports up to 5000 Teradici devices)

Figure 4. Wyse Management Suite with EMSDK on a single VM

Deployment to support more than 5,000 Teradici devices

The following diagram explains deployment architecture of Wyse Management Suite on a single VM with multiple remote EMSDKs:



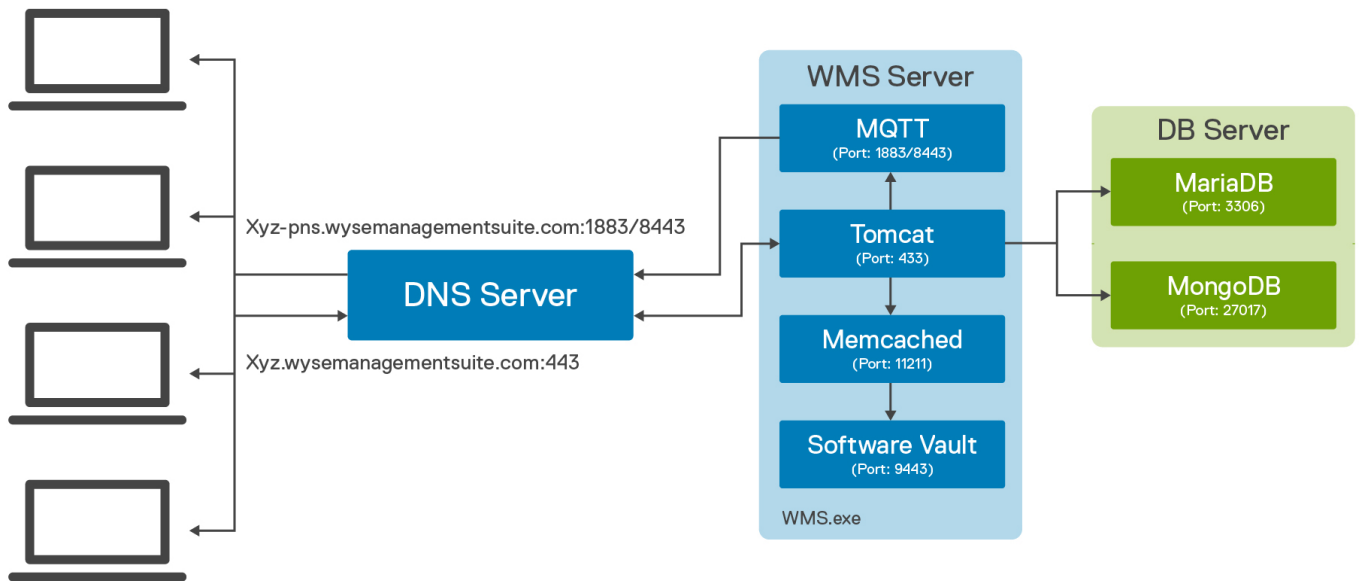
Deployment Architecture of Wyse Management Suite on a single VM with multiple remote EMSDK's
(Each instance of EMSDK supports up to 5000 Teradici devices)
HAProxy is optional for non-HA Deployment

Figure 5. Wyse Management Suite on a single VM with multiple remote EMSDKs

Wyse Management Suite on a separate database server

This section explains the deployment architecture of Wyse Management Suite on a separate database server. MongoDB and MariaDB may be on the same server or on separate servers.

The following diagram depicts the deployment architecture of Wyse Management Suite on a separate database server.



Deployment Architecture of Wyse Management Suite on a single VM Remote Database

Figure 6. Wyse Management Suite on a separate database server

Custom port configurations

Wyse Management Suite uses the following port as the default port for the applications that are installed:

About this task

- Apache Tomcat: 443
- MariaDB database: 3306
- Mongo database: 27017
- MQTT Broker: 1883
- Memcached: 11211
- Software vault: 9443
- EMSDK: 5172, 49159—optional and required only to manage Teradici devices

It is recommended that you use the default port for one or more of the preceding services. If you have a port conflict and are unable to use the default port, Wyse Management Suite enables you to change the default port during installation.

To use a non-default port for one or more of the preceding services, use **Custom** install option during Wyse Management Suite installation. The option that is listed in the following screen enables you to use the local database for MongoDB and MariaDB or use the remotely installed database:

 **NOTE:** You can configure only the Tomcat connection port 49159 for Teradici. You cannot configure the device port 5172.

For more information about the custom installation, see the Custom installation section in *Dell Wyse Management Suite 2.x Quick Start Guide* at support.dell.com/manuals.

Topics:

- [Change the Tomcat service port](#)
- [Change the MQTT port](#)
- [Change the MariaDB port](#)
- [Change the MongoDB database port](#)
- [Remote repository](#)

Change the Tomcat service port

This section explains how to change the port after installing Wyse Management Suite. Reinstall using Custom installation mode to change ports. If reinstallation is not an option, the following sections explain the procedure to change the ports manually:

Prerequisites

To change the Tomcat service port, do the following:

Steps

1. Stop the Tomcat service. The Tomcat service is identified by **Dell WMS: Tomcat Service** entry.
2. Edit the file `<INSTALLDIR>\Tomcat-9\conf\server.xml` in a text editor.
3. Find and replace all occurrences of port entry 443 with the port number you need to use. It is optional to change the references to port 8443.
4. Save the `server.xml` file and exit.
5. Start the Tomcat service.

6. Enter the port number in the URL (default port 443 can be omitted from the URL). For example, **https://xyz.wysemanagementsuite.com:553/ccm-web**. The port that is specified in the URL must be used for both portal access and for device registration.

 **NOTE:** The Memcached port can be changed during Wyse Management Suite installation. Dell recommends not to change the Memcached port detail after installation.

Change the MQTT port

Steps

1. Stop the Tomcat and MQTT services.
2. Perform the following steps to configure the MQTT broker service:
 - a. Edit the file <INSTALLDIR>\wmsmqtt\mqtt.conf in a text editor.
 - b. Note the following entries:

```
# Port to use for the default listener
#port 1883
```
 - c. Uncomment the port 1883 entry and change the port number to your preferred port. For example, port 2883.
 - d. Save the file, and start the MQTT broker service.
 - e. Check the following entry to confirm that the MQTT broker service is running on the new port:

```
ps> get-nettcpconnection -LocalPort 2883
```
3. To configure Tomcat, do the following:
 - a. Open a command prompt session, and go to cd C:\Program Files\DELL\WMS\MongoDB\bin.
 - b. Run the following command at the command prompt:

```
>mongo stratus -u stratus -p <mongodbPassword> -eval
"db.bootstrapProperties.update({'name': ' mqtt.server.url'}, {'name': '
mqtt.server.url' , 'value' : 'tcp://xyz-pns.wysemanagementsuite.com:2883',
'isActive' : 'true', 'committed' : 'true'}, {upsert:true})"
```
 - c. Start Tomcat Service identified in **Local Services** as Dell WMS: Tomcat Service and re-register all the devices, so that the MQTT URL is referring to the new port.

Change the MariaDB port

Steps

1. Start the Tomcat service and stop the MariaDB service. To configure the MariaDB, do the following:
 - a. Edit the file <INSTALLDIR>\Database\SQL\my.ini in a text editor.
 - b. Change the port number for both mysqld and client to your preferred port. The port numbers should be of the same value. For example:

```
[mysqld]
datadir=C:/Program Files/DELL/WMS/Database/SQL
port=3308
[client]
port=3308
```
 - c. Save the file, and start the MariaDB service.
2. To configure Tomcat, do the following:
 - a. Edit the file <INSTALLDIR>\Tomcat-8\webapps\ccm-web\WEB-INF\classes\bootstrap.properties in a text editor.
 - b. Update the properties in the file with your preferred port number details. For example:

```
jpa.connection.url=jdbc:mysql://localhost:3308/stratus?
useUnicode=true&characterEncoding=utf-8&useLegacyDatetimeCode=false&serverTimezone=
America/Los_Angeles
```

```
jpa.connection.port=3308
```

- c. Save the file, and start the Tomcat service. Verify that the services are running on the configured port. For example:

```
ps>get-nettcpconnection -LocalPort 3308
```

Change the MongoDB database port

Steps

1. Stop the Tomcat and MongoDB services.
2. To configure the MongoDB port entry, do the following:
 - a. Edit the file <INSTALLDIR>\MongoDB\mongod.cfg in a text editor.
 - b. Update the property in the file with your preferred port number. For example: port=27027.
 - c. Save the file, and start the MongoDB service. Confirm that it is running on the new port.
3. To configure Tomcat, do the following:
 - a. Edit the file <INSTALLDIR>\Tomcat-8\webapps\ccm-web\WEB-INF\classes\bootstrap.properties in a text editor.
 - b. Update the properties in the file with your preferred port number. For example:
mongodb.seedList=localhost:27027.
 - c. Save the file, and start the Tomcat service. Verify that the service is running on the required port. For example:
ps>get-nettcpconnection -LocalPort 27027.

Remote repository

Wyse Management Suite allows you to have local and remote repositories for applications, operating system images and so on. If the user accounts are distributed across geographies, it would be efficient to have a separate local repository for each of the distributed user account so the devices can download images from its local repository. This flexibility is provided with WMS_Repo.exe software. The WMS_Repo.exe is a Wyse Management Suite file repository software that helps to create distributed remote repositories which can be registered with Wyse Management Suite. The WMS_Repo.exe is available only for **Pro** license subscribers only.

Prerequisites

- If you are using Wyse Management Suite with cloud deployment, go to **Portal Administration > Console Settings > File Repository**. Click **Download version x.x** and download the WMS_Repo.exe file
- The server requirements to install Wyse Management Suite repository software are:
 - Windows 2012 R2 or Windows 2016 Server Standard
 - 4 CPU
 - 8 GB RAM
 - 40 GB storage space

NOTE: 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.

About this task

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

Steps

1. Log in as **Administrator**, and install WMS_Repo.exe on the repository server.
2. Click **Next** and follow the instructions on the screen to complete the installation.

3. Click **Launch** to launch the **WMS Repository registration** screen on the web browser.
4. Select the **Register to public WMS Management Portal** if you are registering on the public cloud.

Figure 7. Register on a public cloud

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

NOTE: Unless you register with Wyse Management Suite version 1.0, you cannot use MQTT Server URL.
 - b. WMS Repository URL (update the URL with the domain name)
 - c. Wyse Management Suite administrator login username information
 - d. Wyse Management Suite administrator login password information
 - e. Repository path information

NOTE: You must provide the read and write access to the folder captured in the **Repository Location** field. The access must be configured for **Dell WMS Repository Tomcat Service** windows service.
6. Click **Register**.
7. If the registration is successful, the **Registration** window is displayed:

Figure 8. Registration successful

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

Generic Client Registration Two-Factor Authentication Reports	☐	☒	WMS Repo - WMS51V441 https://100.106.41.105:443	31 days ago	3.5.0	48	Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: No Subnets:
	☐	☒	WMS Repo - wms75100 https://100.106.75.110:443	5 hours ago	3.5.0	45	Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: No Subnets:
	☐	☒	WMS Repo - WIN-QPTNQCK993C https://WIN-QPTNQCK993C.WMSAD97.COM:443	4 hours ago	3.5.0	80	Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: No Subnets:
Account Custom Branding Subscription	☐	☒	WMS Repo - Wyse6175 https://100.106.61.75:443	32 minutes ago	3.3.2	44	Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: No Subnets:
	☐	☒	WMS Repo - WIN-1K849ISE7KB https://192.168.29.200:443	1 minute ago	3.5.0	44	Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: No Subnets:
	☐	☒					

Figure 9. Registration successful on the portal

9. HTTPS is by default enabled with WMS_Repo.exe, and is installed with the self-signed certificate. To install your own domain-specific certificate, scroll down the registration page to upload the SSL certificates.

Server SSL Certificates: Enabled

SSL Certificate Guide

Current Certificate

Issued to: .com

Issued from: .com

Valid to: August 18, 2118

PKCS-12

Key/Certificate Pair

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

PKCS-12 file

Browse...

Password for PKCS file

Intermediate certificate

Browse...

Upload

Figure 10. Certificate upload

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

▼ Server SSL Certificates: Enabled SSL Certificate Guide

Current Certificate

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

PKCS-12 Key/Certificate Pair

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

PKCS-12 file Browse...

Password for PKCS file *

Intermediate certificate ⓘ Browse...

Upload

Figure 11. SSL certificate enabled

11. If the Wyse Management Suite is enabled with self-signed or a private domain certificate, you can upload the certificate on the Wyse Management Suite repository server to validate the Wyse Management Suite CA credentials.

▼ Trust Store Certificates

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

Uploaded Certificate Alias Names:
 None

Upload WMS Server certificate to trust store (CER format)

Certificate Browse...

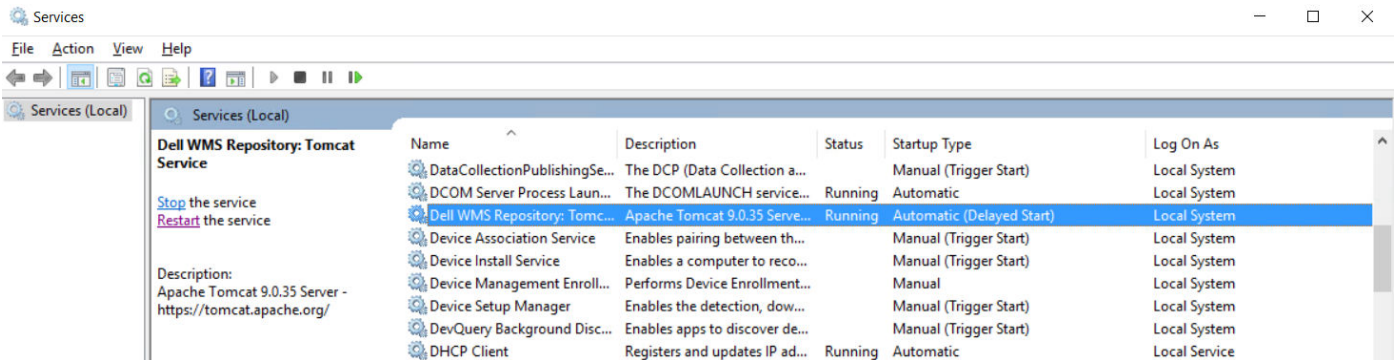
Upload

Figure 12. Trust store certificates

12. Navigate to the `c:\wmsrepo` location that you entered during registration, and you can view the folders where all the repository files are saved and managed.

Manage Wyse Management Suite repository service

Wyse Management Suite repository is displayed as **Dell WMS Repository: Tomcat Service** in the Windows Local Services window and is configured to start automatically when the server restarts.



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.

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.

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.

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**.

i **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.

i **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.

i **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.

i **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.

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**.

i **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.

i **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.

i **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.

i **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.

Software Vault Utility

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

To download the SoftwareVaultUtility-1.x.x.exe files, go to the Drivers & Downloads page of Wyse Management Suite at <https://www.dell.com/support/home/>. If you are using Wyse Management Suite 3.5 or later versions, you can access the utility using the command prompt. You do not have to install the utility. The utility works with Windows command line if you have administrator privileges. The utility is supported with both the default and custom installation of Wyse Management Suite.

Topics:

- [Back up your database](#)
- [Restore your database](#)
- [Export the Software Vault key](#)
- [Import the Software Vault key](#)

Back up your database

Steps

1. Open command prompt where the Wyse Management Suite database is installed.
2. Run the following commands to perform a database backup of MongoDB and MariaDB:
 - MongoDB backup—`mongodump --host localhost -u stratus -p <WMS Mongo DB Password> --authenticationDatabase admin --db stratus --out ".\wmsmongodump"`.
 - MariaDB backup—`mysqldump --routines -hlocalhost -ustratus -p<WMS Maria DB Password> stratus > ".\wmsdump.sql"`.
3. Use the Software Vault utility to export the Software Vault key from the current Wyse Management Suite server. To export the key, see [Export the Software Vault key](#).

Restore your database

Prerequisites

To restore the database on a different Wyse Management Suite server, stop Tomcat services.

Steps

1. Copy the Stratus database folder, which was generated during the backup, to the MongoDB bin folder.
2. Copy the wmsdump.sql file, which was generated during the backup, inside the MariaDB bin folder.
3. Run the following commands to perform a database restore of MongoDB and MariaDB:
 - MongoDB restore—
 - `echo "db.dropDatabase()" | mongo -u stratus -p<WMS Mongo DB Password>--authenticationDatabase admin --host localhost stratus`
 - `mongorestore --host localhost -u stratus -p <WMS Mongo DB Password> --authenticationDatabase admin --db stratus ".\wmsmongodump\stratus"`
 - MariaDB restore—
 - `Mysql.exe --verbose -hlocalhost -ustratus -p<WMS Maria DB Password>-e "DROP DATABASE stratus"`
 - `Mysql.exe --verbose -hlocalhost -ustratus -p<WMS Maria DB Password>-e "CREATE DATABASE stratus DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_unicode_ci"`
 - `Mysql.exe --verbose -hlocalhost -ustratus -p<WMS Maria DB Password>stratus < ".\wmsdump.sql"`

4. Import the Software Vault key from the previous Wyse Management Suite server where the database was backed. To import the key, see [Import the Software Vault key](#).
5. Start the Wyse Management Suite services.
6. Log in to Wyse Management Suite.

NOTE: If you are performing a database backup of the main server and restoring to another server, then the resource files must be uploaded again from Wyse Management Suite user interface. In the new restored Server, dummy entries of the resource file may appear in the Wyse Management Suite user interface or the user interface may not load properly due to unavailability of resource files. For example, the following files which are uploaded from Wyse Management Suite user interface in respective pages must be uploaded again:

- **ThinOS**—Firmware, applications, BIOS, wallpaper, screen saver, and logo.
- **Dell Hybrid Client**—Bundle, applications, logo, and BIOS (cab files).
- **Teradici**—Firmware and Teradici OSD logo
- **WES, ThinLinux, IOT platform**—Wallpaper, Logo, EULA text file, Windows wireless profile, INI file, Locale, Printer Mappings, Font, Hosts, and rules.
- **Custom Branding**—Logo and Favicon

Export the Software Vault key

Steps

1. Open command prompt as an administrator on the server where Wyse Management Suite is installed.
2. Browse to the folder where the utility is copied.
3. Run the .exe file from the command line using the parameters **-mode export -password <password for the zipped file which is created that contains exported keys>**.
For example, **C:\> softwareVaultUtility-1.x.x.x.exe -mode export -password <PASSWORD>**.
A password protected zip file, **keys.zip**, with exported keys and checksum file is generated.
4. Extract and use the same password that was used earlier to check the content of the zip file.

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

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

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

Import the Software Vault key

Steps

1. Copy the utility, keys.zip, and the checksum file to a folder.
2. Run the .exe file from the command line using the parameters **-mode import -password <password for the zipped file which contains exported keys>**.
For example, **C:\> softwareVaultUtility-1.x.x.x.exe -mode import -password <PASSWORD>**.
The keys are imported to the destination end point and the backup.zip file is generated in the same folder. The backup.zip file can be used to rollback the changes.
3. Extract and use the same password that was used to export the keys to check the content of the zip file.
The backup.zip file contains the following files:
 - bootstrap.properties
 - keys.json
 - server.xml
 - configuration.properties
4. After you import the key, restart the Tomcat service.

-  **NOTE:** The password used to export the key must be used to import the key. Use WinRAR or 7z to extract the files. The default Windows extractor cannot extract the password protected files.
-  **NOTE:** Save the backup.zip file in a secure location and do not rename or edit the keys.zip and the checksum file.
-  **NOTE:** Do not rerun the import command. After the keys.zip file is imported, the file is deleted from the system.