Dell Wyse Management Suite

Version 1.0 Quick Start Guide

Notes, cautions, and warnings

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

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

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

2017 - 05

Rev. A00

Contents

1

Introduction

Wyse Management Suite is the next generation management solution for Dell Wyse thin clients that offers advanced feature options such as Cloud versus On-premises deployment, manage-from-anywhere via a Mobile App, enhanced security such as BIOS configuration and port lockdown. Other features include Device Discovery and Registration, the Asset and Inventory management, the Configuration management, OS and Applications deployment, Real-time commands, Monitoring, Alerts, Reporting, and Troubleshooting of endpoints.

NOTE: Dell Cloud Client Manager (CCM) has been rebranded as Wyse Management Suite. This release of Wyse Management Suite includes several major enhancements to CCM R14. For more information, see *Dell Wyse Management Suite Release Notes*. Existing customers can continue to manage their thin clients as before, and take advantage of the new features introduced in this release.

Editions

Wyse Management Suite is available in following editions:

1 **Standard (Free)**:
- Provides core management features for up to 10,000 devices.
- Available for on-premises deployment (only)
- License key or activation is not required.
- Can be upgraded to the Pro edition at a later stage, by importing a Pro license key.

2 **Pro (Paid)**: The Pro subscription must be purchased.

- The following advanced features are available in the Pro version:
  - Delegated administration
  - Two-factor authentication
  - Authentication to Active Directory
  - Automatic Grouping and Configuration of devices
  - Scripting support for customizing application installations
  - Multiple image repositories
  - Reports
  - Mobile App to monitor and manage devices from anywhere.
  - Alerts and Notifications via Email and/or Mobile App
  - BIOS management for supported WES platforms
- Choice of Cloud vs On-premises deployment

  NOTE: Cloud services are hosted in the US and Germany. Customers in countries with data residency restrictions may not be able to take advantage of the cloud-based service.
- Subscription-based licensing for lower upfront cost
- Licenses can be moved at will between Cloud and On-premises installation.

The following information should be considered for selecting the Wyse Management Suite Standard and Pro editions:

Standard

This edition is suited for users with the following requirements:

- Small to midsized deployments
- Small IT staff, do not need features such as Delegated Administration or AD authentication.
- Need core management functions such as the Asset and Inventory management, Configuration, and Apps / Patch management.
- Willing to install and maintain software and infrastructure on-site.

Pro (On-prem)

This edition is suited for users with the following requirements:

- Small, medium, or large deployments
- Need advanced features such as Delegated Administration, Reports, and Two Factor Authentication.
- Want the convenience of “monitor and manage from anywhere” via Mobile App.
- Want to install and maintain software and infrastructure on-site.

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

Pro (Cloud)

This edition is suited for users with the following requirements:

- Small, medium, or large deployments
- Want convenience and cost savings of not having to set up and maintain infrastructure and software.
- Need advanced features such as Delegated Administration, Reports, Two Factor Authentication.
- Want the convenience of “monitor and manage from anywhere” via Mobile App.
- Devices can be configured to communicate with external server either directly or through a forward-proxy service.
- Need to manage devices on non-corporate networks (home office, third party, partners, mobile thin-clients and so on)

Getting started with Wyse Management Suite

Terminologies

The following table lists the important terminologies used in the guide:

Terminology	Definition
Private cloud	Wyse Management Suite Server Installation installed on premise that is private to your organizations datacenter.
WDA	Wyse device agent which resides in the device and acts as an agent for communication b/w server and client.
Local repository	Application, OS Image and File repository that is installed by default that Wyse Management Suite Server.
Remote repository	Application, OS Image and File repositories that can be optionally installed standalone for scalability and reliability accross geographies for content transfer.
Public cloud	Wyse Management Suite hosted on public cloud with convenience and cost savings of not having to setup and maintian infrastructure and software.
Add-on/App	Any component or package which is not a part of the base build and provided as an optional components which can be pushed from management solution. For example: Latest Connection Brokers (from VMware & Citrix)
On-premise	Wyse Management Suite Server Installation installed on premise that is private to your organizations datacenter.
Tenant	A tenant is a group of users who share a common access with specific privileges to Wyse Management Suite access. It is a unique key assigned to specific customer to access the management suite.
Jobs	The scheduled Packages or commands to the devices are known as Jobs. This jobs will be listed in the Job's page.
Users	Local users and users imported from Active Directory can be assigned global administrator, group administrator, and viewer roles to login to Wyse Management Suite. Users are given permissions to perform operations based on roles assigned to them.

Getting started with Wyse Management Suite on public cloud

This section provides you the important information on the general features to help you quickly get started as an administrator and to manage Thin Clients from Dell hosted Wyse Management Suite Cloud portal.

Logging In

This topic provides the basic steps to log in to the management console. To log in to the management console, ensure that you are using your correct User Name and Password.

NOTE:

- You will receive your credentials when you sign up for Wyse Management Suite Trial on www.wysemanagementsuite.com or when you purchase your subscription. You can purchase the Wyse Management Suite subscription at Dell sales or your local Dell partner. For more details, see www.wysemanagementsuite.com
- It is recommended to change your password after logging in for the first time.

1 Use a supported Web browser on any machine with access to the Internet to log in to the management console.

2 You can access Public Cloud (SaaS) edition of Wyse Management Suite by pointing your web browser to following links:
- **US Datacenter**: us1.wysemanagementsuite.com/ccm-web
- **EU Datacenter**: eu1.wysemanagementsuite.com/ccm-web

3 Enter your Username and Password.

NOTE: The default username and password is provided by Account Representative.

4 Click **Sign In** option.

Changing your password

To change the login password, complete the following steps:

1 Click the Account link at the upper-right corner of the management console, and then click **Change Password** option.

2 Enter your current password.

3 Enter a new password.

4 Enter your new password in the **Confirm New Password** box.

5 Click **Change Password** option.

Logging out

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

Getting started with Wyse Management Suite on private cloud

Pre-requisites

Wyse Management Suite Server:

The software can be installed on a physical or virtual machine.

- Supported Operating System – Windows server 2012 R2 and Windows Server 2016
- Minimum Disk Space – 40 GB
- Minimum Memory (RAM) – 8 GB
- Minimum CPU Requirements – 4 CPU

For 50K+ devices:

- Supported Operating System – Windows server 2012 R2 and Windows Server 2016
- Minimum Disk Space –120 GB
- Minimum Memory (RAM) – 16 GB
- Minimum CPU requirements – 4 CPU

Wyse Management Suite repository

The software can be installed on a physical or virtual machine.

- Supported Operating System – Windows server 2012 R2 and Windows Server 2016
- Minimum Disk Space –120 GB
- Minimum Memory (RAM) – 16 GB
- Minimum CPU requirements – 4 CPU

NOTE: For public cloud Wyse Management Suite, the repository must be installed on a server within the DMZ which is externally accessible, and the fully qualified domain name (FQDN) of the server must be registered in public DNS.

OS (Operating System) Language Pack Support for Wyse Management Suite Server

1 English
2 French
3 Italian
4 German
5 Spanish

Browser Support

1 Internet Explorer version 11
2 Chrome version 58.0 and later versions
3 Firefox version 52.0 and later versions
4 Edge browser on Windows (English only)

3

Pre-installation checklist

Before you build your Wyse Management Suite Environment, do the following:

- Obtain and configure all hardware and software, as required.
- Install a supported server operating system on the server machine(s).
- Make sure that all systems are up-to-date with current Microsoft service packs, patches, and updates.
- Make sure that the latest version of the supported browser is available.
- Obtain administrator rights and credentials on all systems involved with the installations.
- Ensure that all required server to server communications ports are available and open for proper communication between servers and clients.
- Obtain a valid Wyse Management Suite License if you need Pro features. Standard edition does not require a license.

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

- Wyse Management Suite Server (Includes repository for application and OS Images)
- Optional: Additional Wyse Management Suite repository servers (for additional image repositories and AD authentication).
- Optional: HTTPS certificate from well-known Certificate Authority.

The Wyse Management Suite server may be optionally configured to interact with the following services in the customer's data center:

- Active Directory: To enable Administrators to log in to the Wyse Management Suite console Web GUI using their AD credentials.
- Email/SMTP Server: To enable Administrators to receive email notifications for Alerts and Two factor authentication.

Client devices can be configured to automatically discover Wyse Management Suite server through either of the following options:

- DHCP Service: via Option Tags
  For more information, see Configuring device using DHCP option tags.
- DNS Service: via SRV records

  For more information, see Configuring device using DNS SRV Record.

4

Installing Wyse Management Suite on-premise and initial setup

Double-click on the installer package, and do the following steps:

1 On welcome screen, go through the license agreement and click **Next** to proceed.

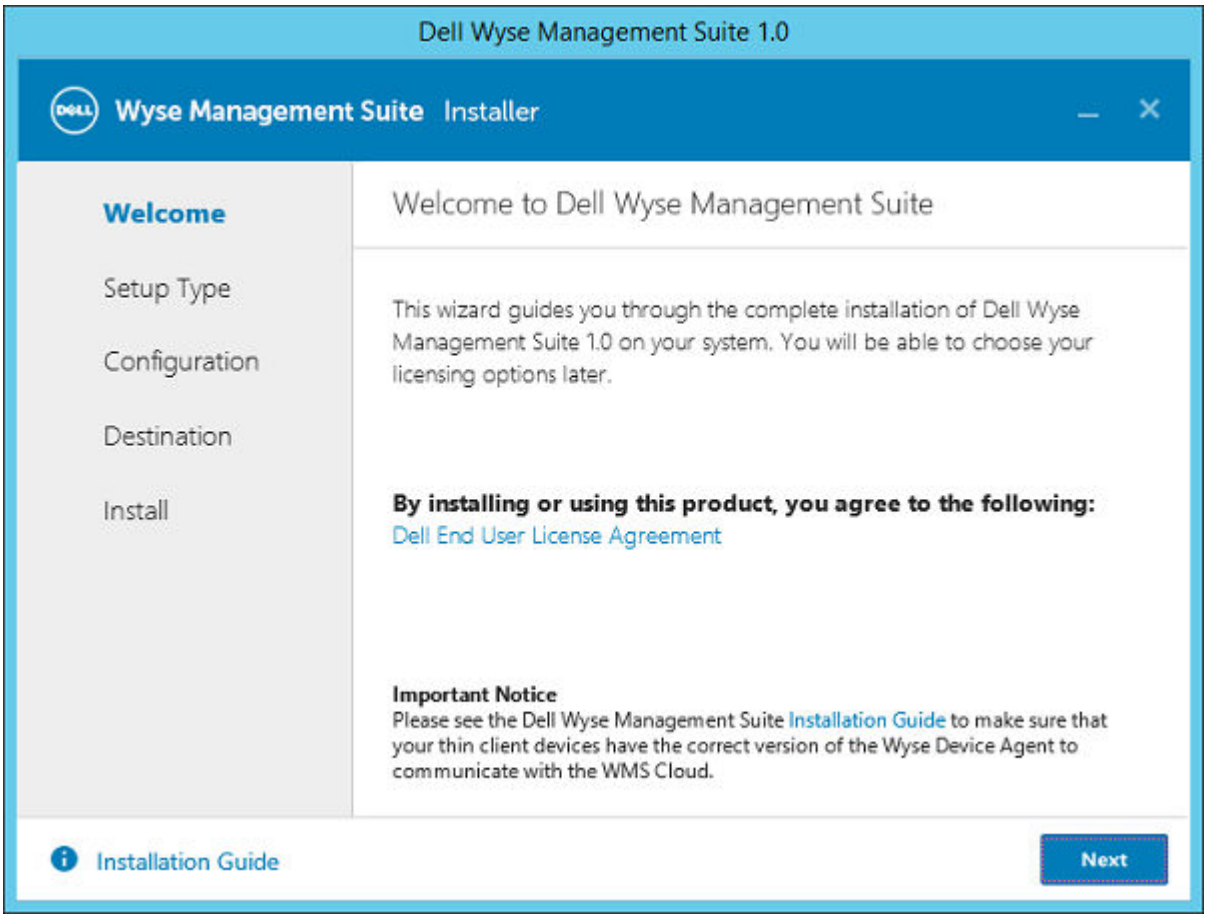

Figure 1. Welcome screen

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

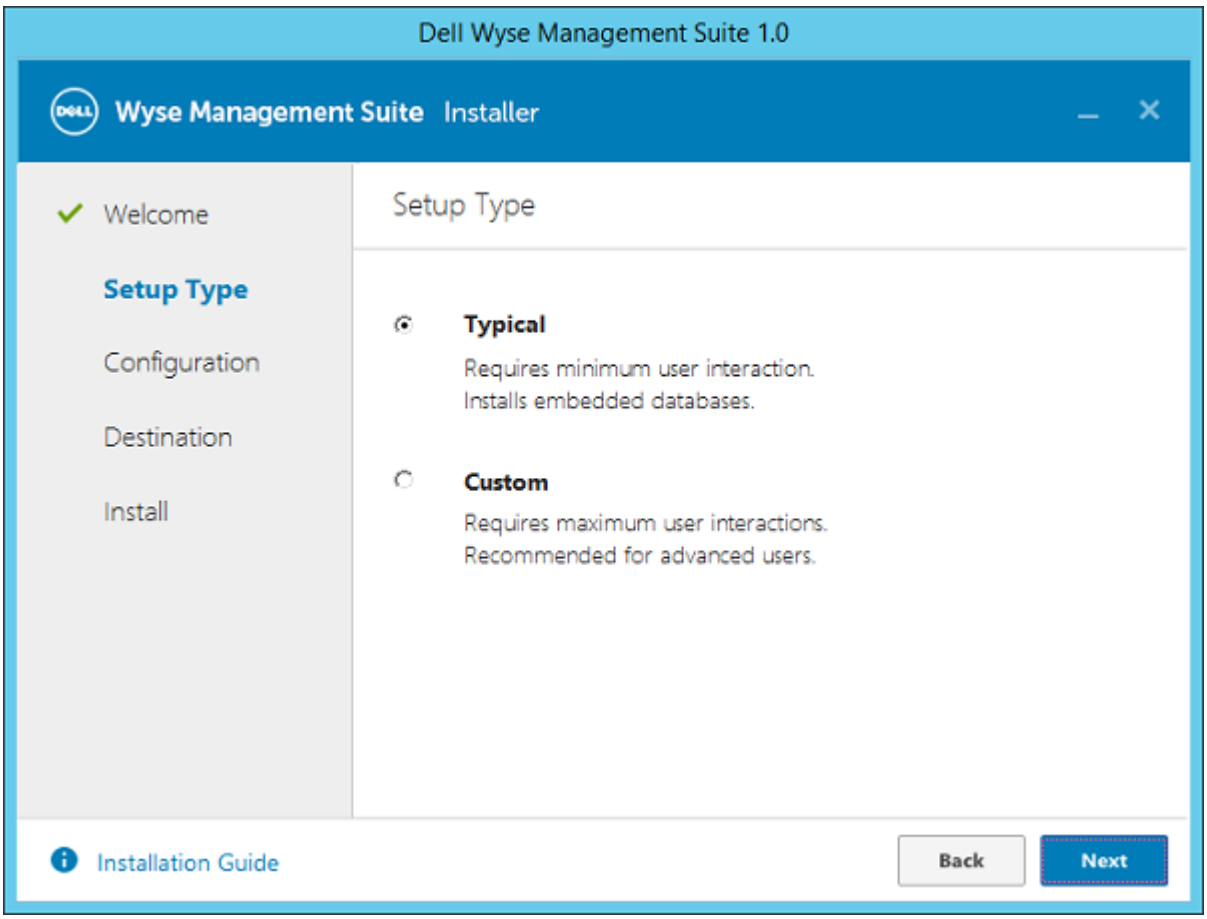

Figure 2. Setup type

- 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

Select the **Setup Type** as typical, enter `Database Credentials` for the embedded databases that are used for the account that Wyse Management Suite uses to connect with embedded databases and enter `Administrator Credentials` and click **Next**. You must remember these credentials to log into Wyse Management Suite web console.

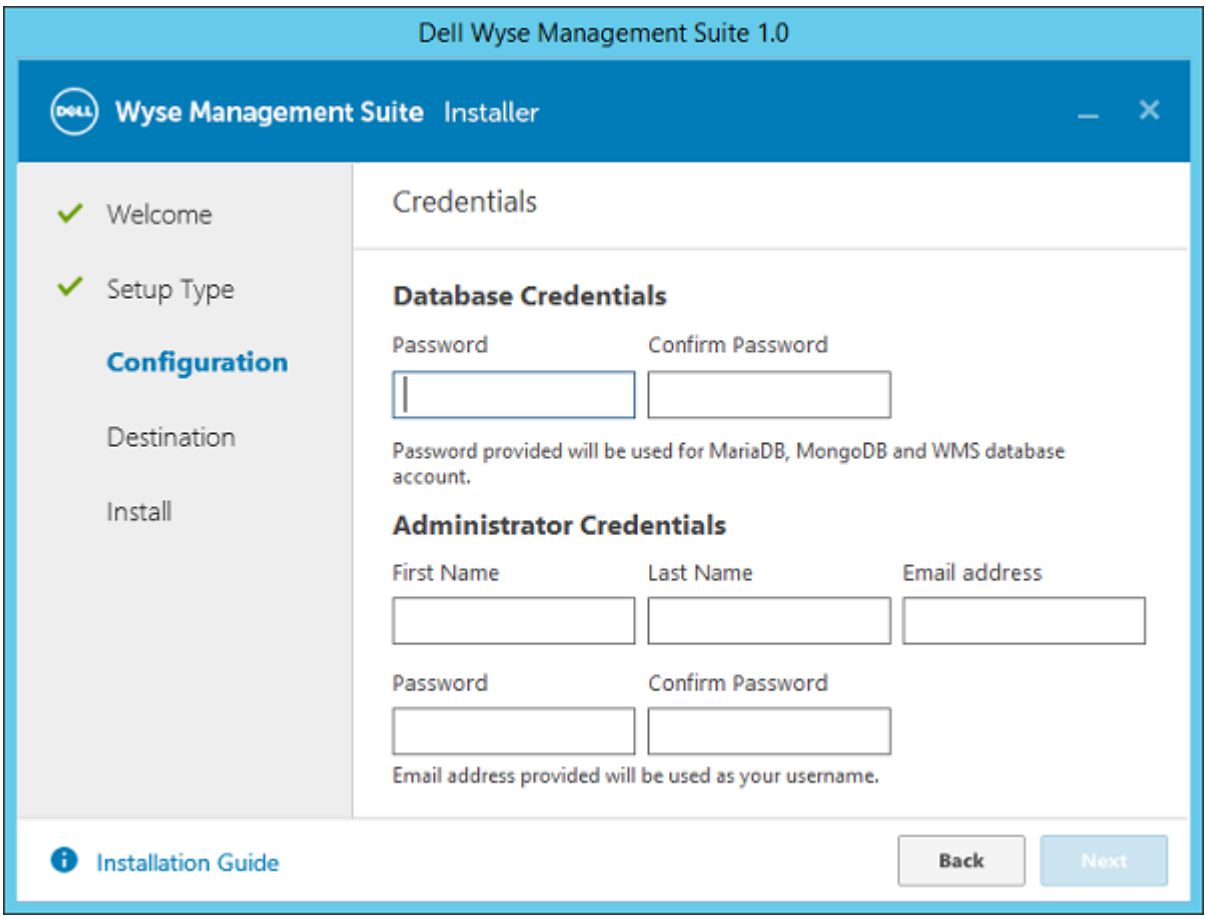

Figure 3. Credentials

3 Select a destination where you want to install Wyse Management Suite. Also, select a local repository where you want to save the tenant files.

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

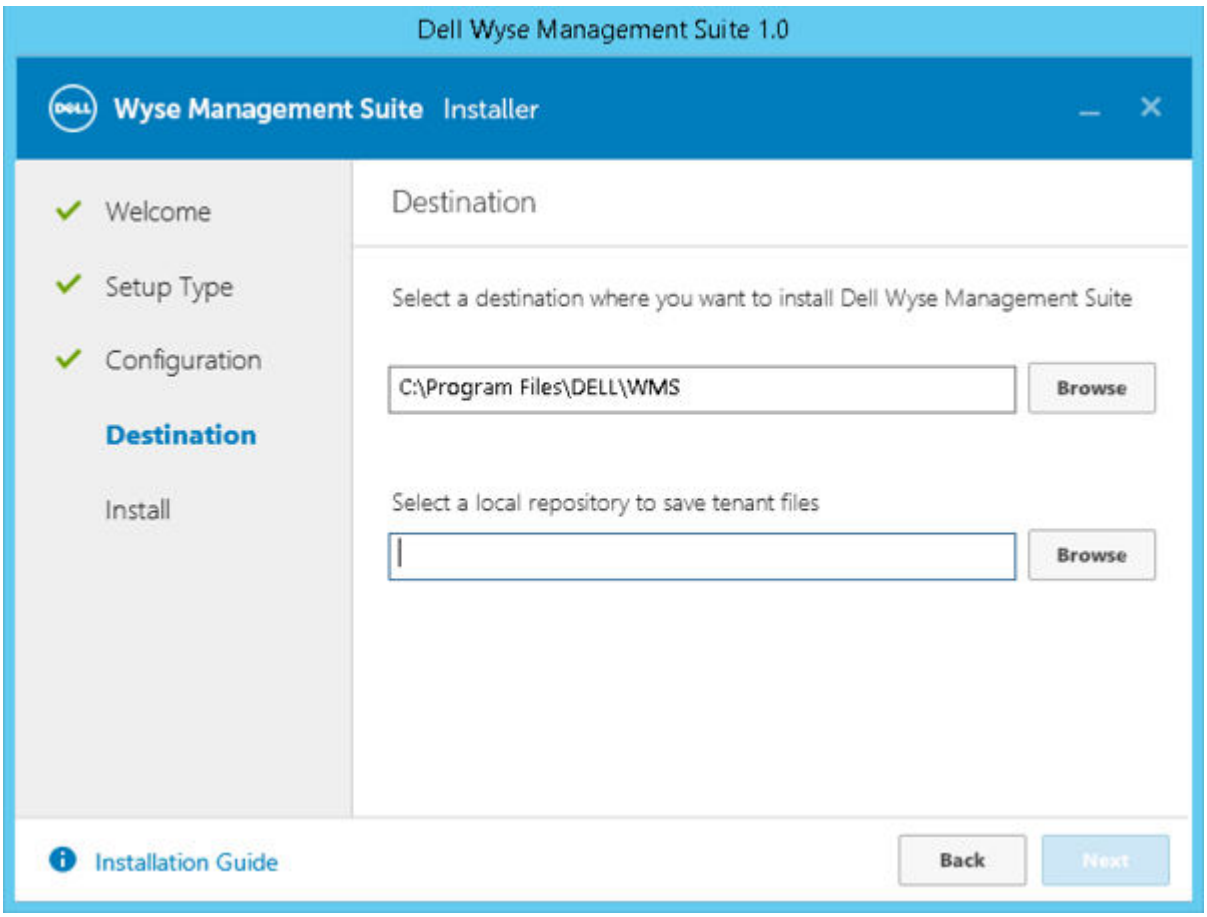

Figure 4. Destination

Click **Next** to install software.

The installer takes approximately 4–5 minutes to install all components. It may take longer time if dependencies such as VC-runtime are not installed on the system.

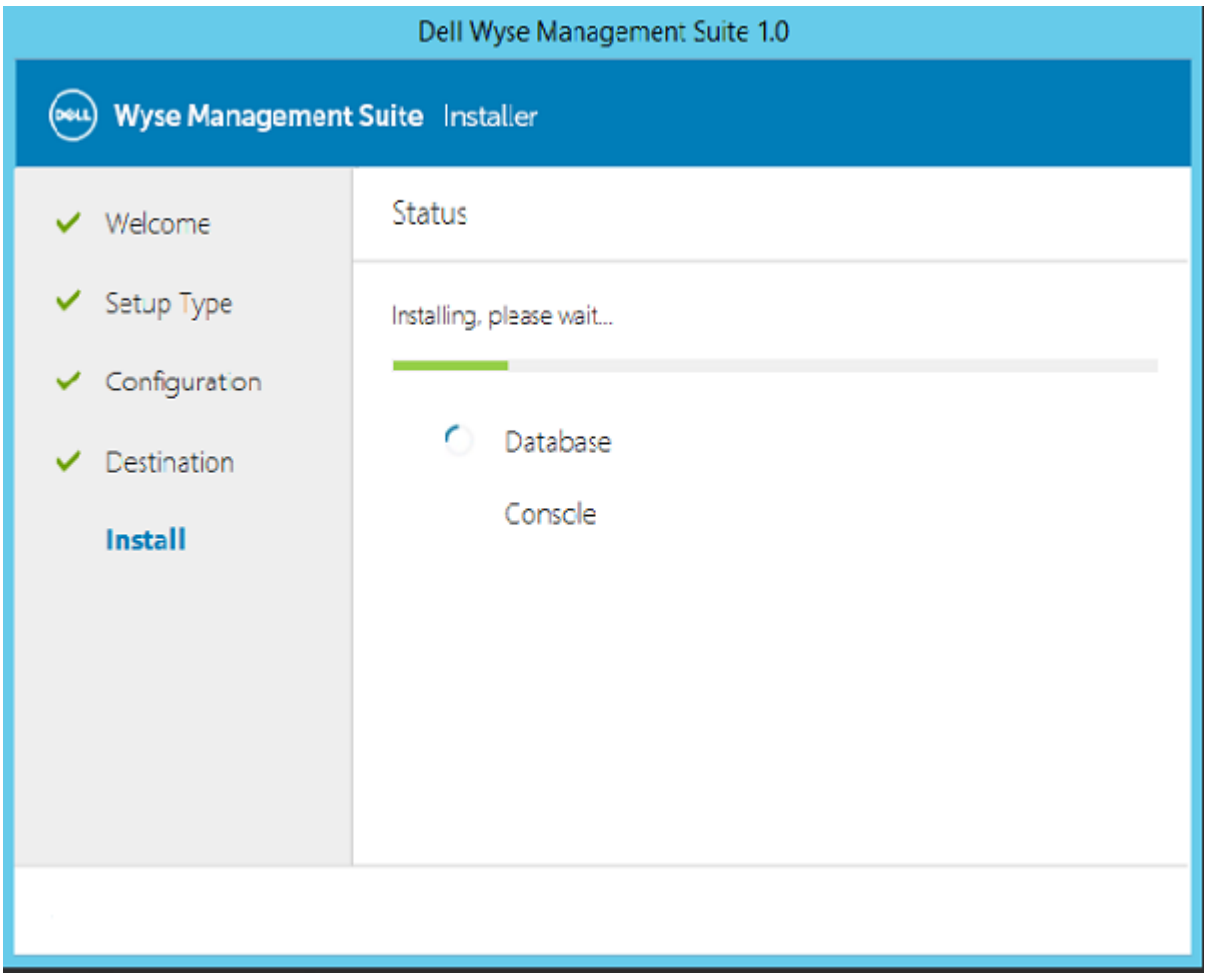

Figure 5. Installation status

4 Click **Launch** to open Wyse Management Suite web console.

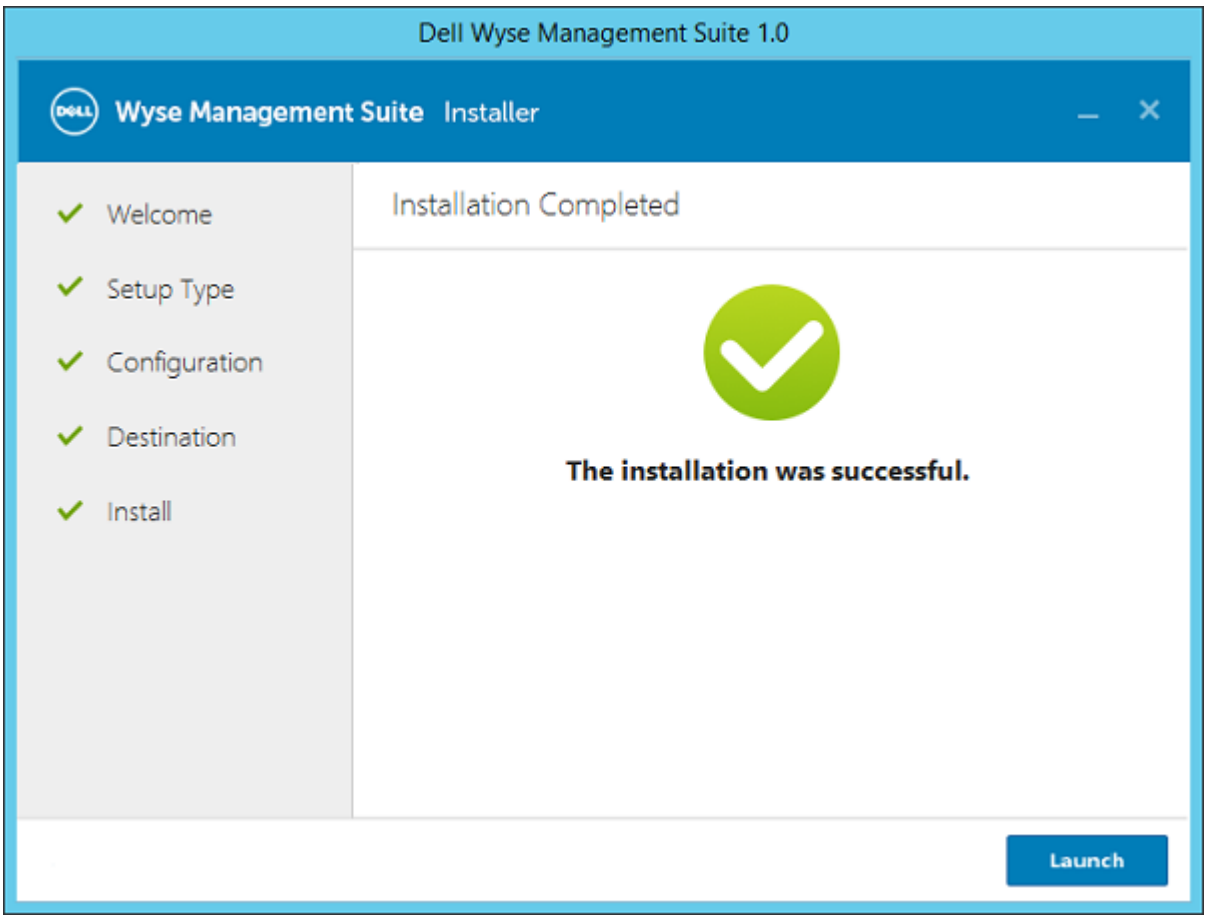

Figure 6. Installation complete status

5 Click the **Get Started** button on the web console to select licence type, setup email notifications, and import SSL certificates.

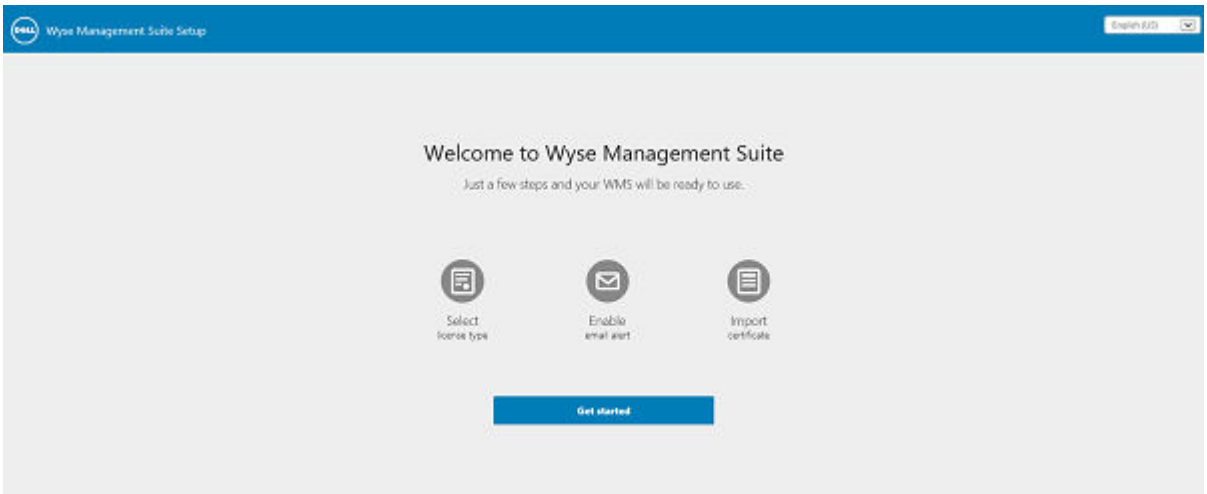

Figure 7. Welcome page

6 To enable Wyse Management Suite on-premise and cloud, select your preferred license. The available types of license are:

- Standard—A free basic device management for on-premises deployment.
- Pro—Enterprise-grade management for on-premises or hosted deployment.

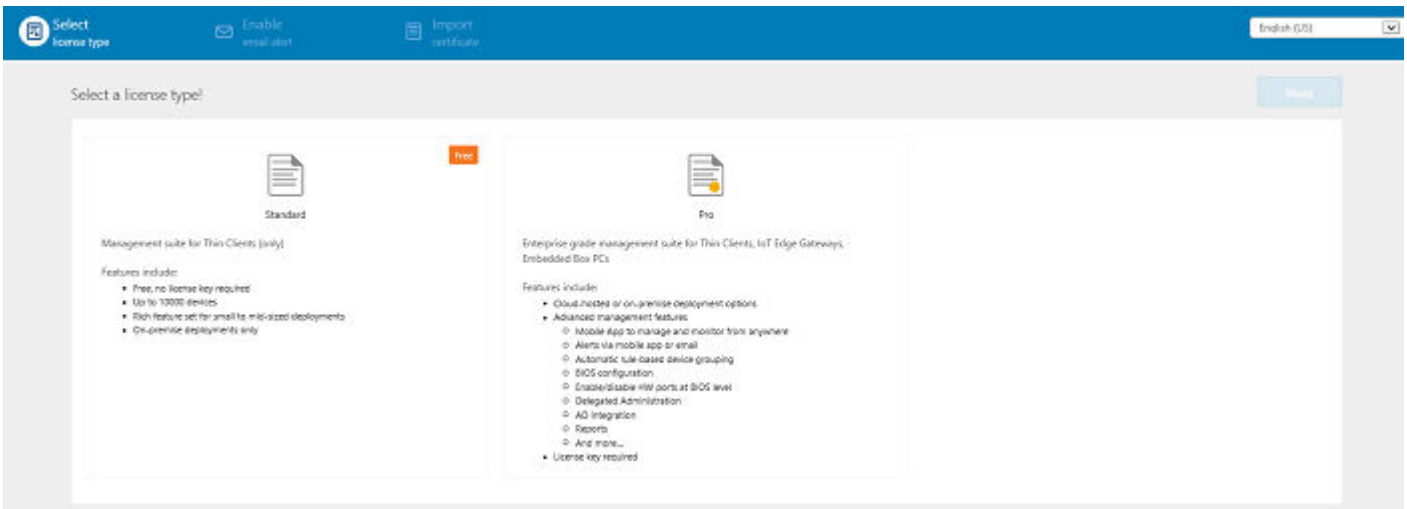

Figure 8. License type

a If you select the license type as **Standard**, then proceed with the standard Wyse Management Suite installation by clicking **Next**.

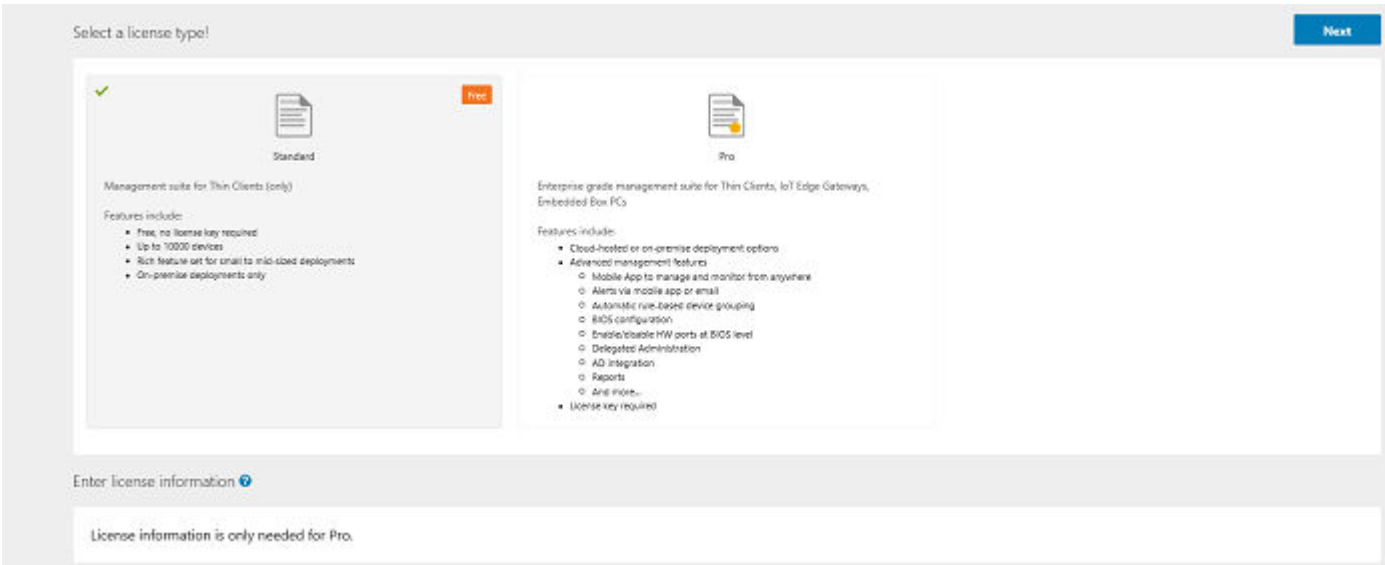

Figure 9. Standard license type

b If you select the license type as **Pro**, you must enter tenant username, password , select the license server datacenter , number of thin client seats and number of Edge Gateway device seats to import the licensing information or import your Wyse Management Suite Pro license key and click **Next**. The summary page shows the details of the license after the license is successfully imported.

> **NOTE: By default, Wyse Management Suite imports self-signed SSL certificate that is generated during installation to secure communication between client and Wyse Management Suite Server. If you do not import valid certificate for your Wyse Management Suite Server, you can see a security warning when accessing Wyse Management Suite web console from a browser on all machines other than server where Wyse Management Suite is installed, because self-signed certificate generated during installation is not signed by well-known Certificate Authority.**

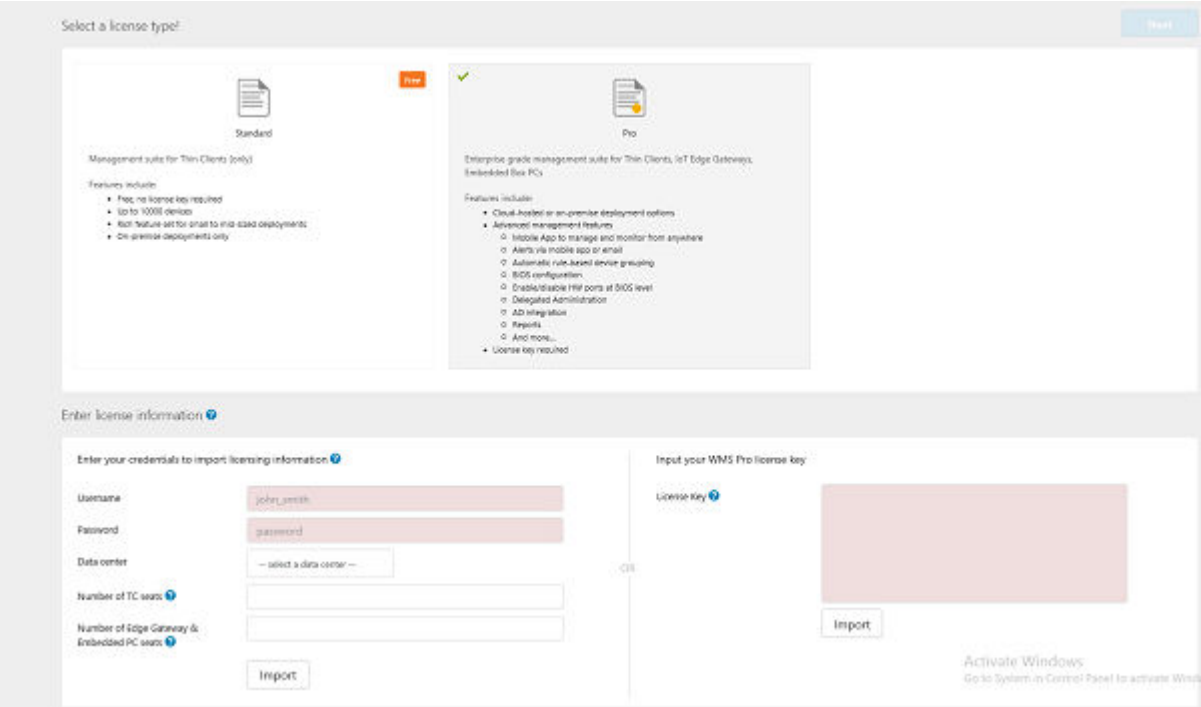

Figure 10. Pro license type

NOTE: License can be upgraded or extended at a later point from the Portal Admin page.

7 Enter information about your SMTP Server, and click **Save**. You may skip this screen and complete this setup or make changes later in the console.

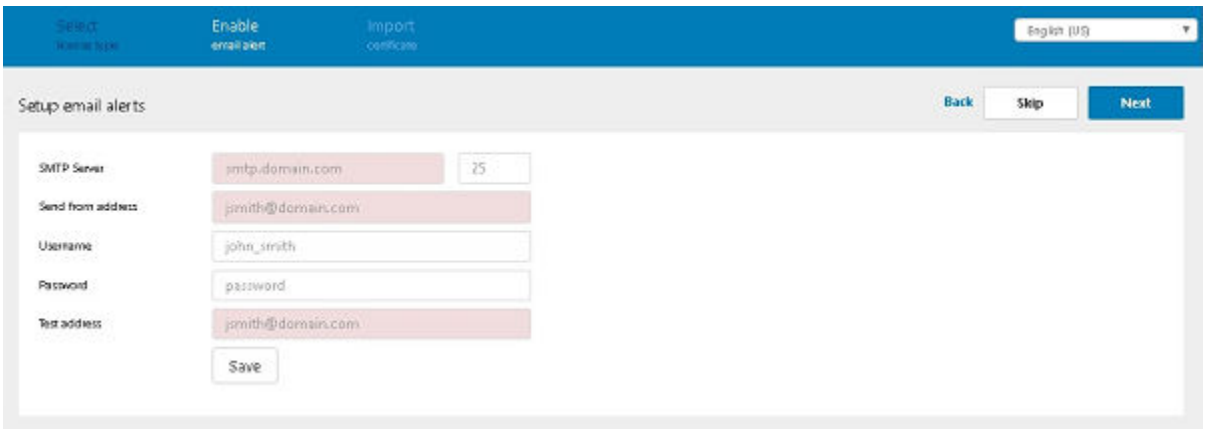

Figure 11. Email alerts

NOTE:

- You must enter valid information about your SMTP server to receive email notifications from Wyse Management Suite.
- If you want to configure SMTP later, this page can be skipped as the SMTP server configuration is not mandatory to configure at this point of time.

8 Import your SSL certificate to secure communications with Wyse Management Suite Server. You need to enter public, private and apache certificate and click the **Import** button. Importing the certificate takes 180 sec of time to configure and restart tomcat services. Click **Next**.

NOTE:

- You can either import .pem or .pfx certificate.
- You may skip this screen and complete this setup or make changes later in the console by logging on to Private cloud and importing from **Portal Admin** page.

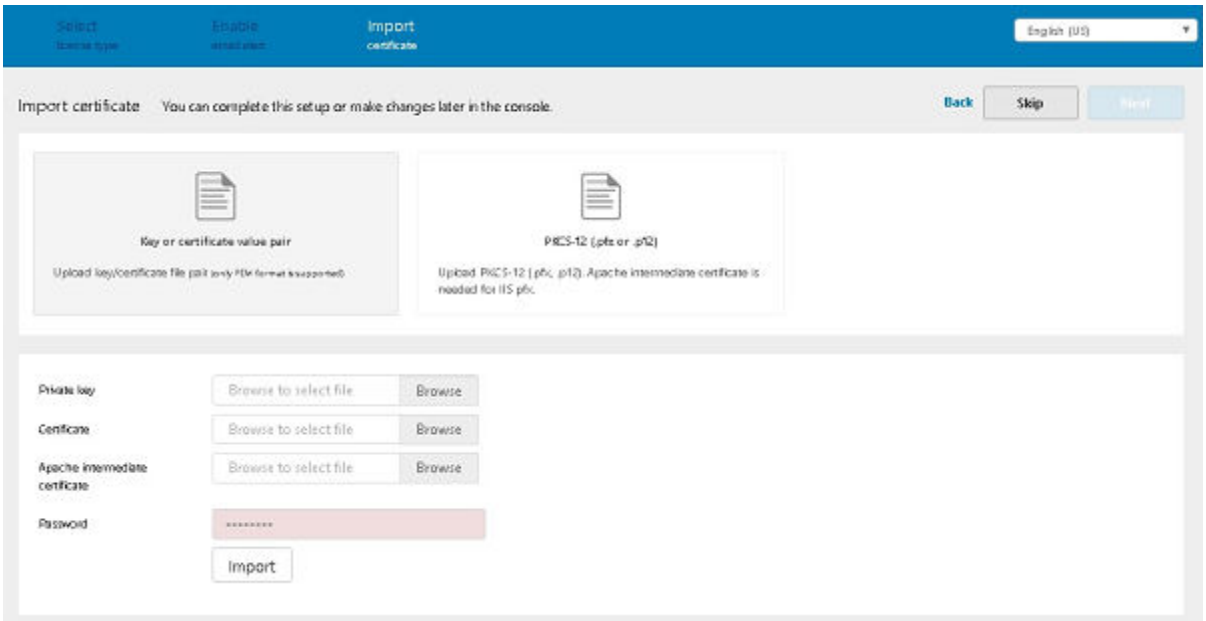

Figure 12. Import certificate

9 Click the **Sign in to WMS** button.

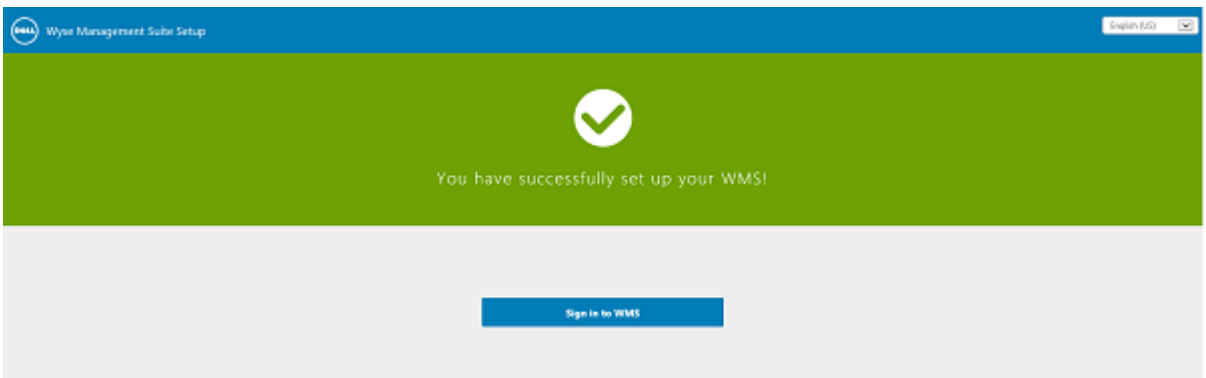

Figure 13. Sign in page

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

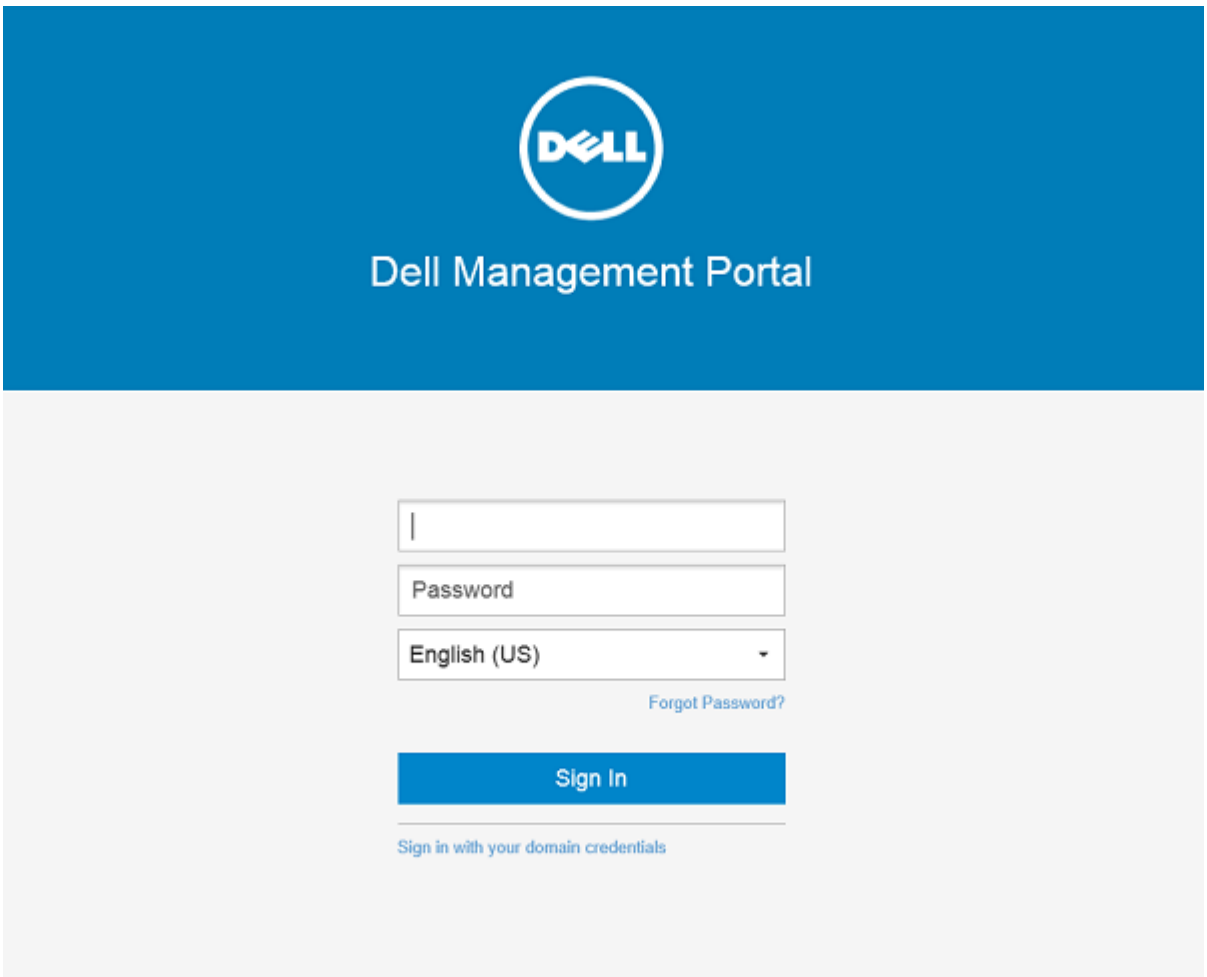

Figure 14. Dell Management Portal

Topics:

- Functional areas of the management console
- Configuring and managing thin clients
- Creating a policy group and updating configuration
- Register a new thin client
- Wyse Management Suite Jobs
- Publishing application to thin clients
- Create and push Advanced Application Policy to thin clients

Functional areas of the management console

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

1 **Dashboard**: This allows you to quickly view important summary of information for each functional area of the system.

2 **Groups**: This allows the flexibility to employ hierarchical Group Policy management for device configuration. Optionally, sub-groups 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.

3 **Users**: Local users and users imported from Active Directory can be assigned global administrator, group administrator, and viewer roles to login to Wyse Management Suite. Users are given permissions to perform operations based on roles assigned to them.

4 **Devices**: This allows you to view and manage Devices, Device Types, and device-specific Configuration.

5 **Apps & Data**: This allows you to manage device Application/OS Image Inventory and Policies, and File Repository Inventory which lists different thin client firmware and certificate files.

6 **Rules**: This allows you to add, edit, and enable or disable rules such as auto grouping and alert notifications.

7 **Jobs**: Creates job for any task such as reboot, WOL, and application/image policy that needs to be pushed to registered devices. Administrator can track status of jobs by navigating to this tab.

8 **Events**: This allows you to view and audit system events and alerts.

9 **Portal Admin**: This allows administrators to perform system administration tasks such as local repositories, Active Directory Connector operations, Subscriptions, and other Self-Service settings/agreements out of the system. You can configure on-premises services and enable two-factor authentication here. For more information, see Managing Administrators and Viewers of the Management Console in the Administration Guide.

Configuring and managing thin clients

The general approach to configure and manage thin clients consists of the following high level steps:

- Configuration management is done through Policy Groups, under the **Groups** tab of the Web Console. Up to 10 levels deep, Wyse Management Suite supports a hierarchy of groups and subgroups. These Groups can be created manually or automatically based on defined rules and needs. You can organize and manage based on functional groups (Example: Marketing, Sales and Engineering etc.). Others may want to organize based on the locations of the devices (Example: Time zone as the first level group, State at the second level, City at the third level, Building at the fourth level, Floor at the fifth level).

  NOTE: You can create rules to automatically create groups or assign devices to existing groups based on device attributes such as subnet, time zone and location.

  - Settings or policies that apply to all the devices in the organization are set at the Default Policy group. This is the global set of parameters that all groups and subgroups will inherit from.
  - Settings or parameters that are configured at lower level groups takes precedence over settings that were configured at the parent or higher level groups.
  - Parameters that are specific to a particular device may be configured from the Device Details page.
  - Configuration parameters are pushed to all devices in that group and all the subgroups, when you create and publish the policy.
  - Once a configuration is published and propagated to the devices, the settings will not be sent again to the devices until the next time you make a change.
  - New devices that are registered receives the configuration policy that is effective for the group to which it was registered.

- Applications, WES OS Image updates and other such operations are done from the Apps and Data tab of the UI.

  - Applications are deployed based on Groups.

    NOTE: Advanced application policy allows you to deploy an application to current and all subgroups based on need. OS Images can be deployed to current group only.

  - Wyse Management Suite supports two types of application deployment policies
    - Standard application
    - Advanced application

    Standard application policy allows you to install a single application package while Advanced application policy allows you to install multiple application packages within a single policy. Advanced application policy also supports execution of pre and post installation scripts that may be needed to customize each application.

    NOTE: For WES devices, a restart is required at the beginning and end of each policy deployment. Since multiple applications can be packaged within a single advanced policy, only two restarts are needed for deploying multiple applications.

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

- Deployment of Application policies and OS images to the thin clients may be scheduled immediately or at a later time based on specific time zone or time zone that is configured on a device.

- Inventory of devices can be located by clicking Devices tab. By default, this shows a paginated, flat list of all the devices in the system. You can choose to view a subset of the devices using a variety of filter criteria, such as Groups or subgroups, device type OS type, status, subnet, platform or time zone.
  - Clicking the device entries listed on this page navigates to the Device Details page for that device. This shows a variety of detailed information for that device
  - The Device Details page also shows all the configuration parameters that apply to that device, and also the group level at which each parameter took effect.
  - This section also enables to set configuration parameters that are specific to that device. Parameters configured in this section overrides any parameters that were configured at the Groups and/or global level.
- You can generate and view canned reports based on predefined filters by navigating to Portal Admin and then clicking the Reports Tab.
- By installing and using mobile application available on Android and iOS devices, you can manage and receive critical notifications from anywhere. Mobile app and its quick start guide can be downloaded by navigating to Portal Admin and then clicking the Alerts and Classification option.

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 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 **WES**.

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

  c Set up some configuration parameters.

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

NOTE:

- For more details on various configuration policies supported by Wyse Management Suite, see *Wyse Management Suite Administrator's Guide*.
- You can choose to create a rule to automatically create a group and/or assign a device to a group based on specific attributes such as subnet, time zone, and location.

Register a new thin client

Thin Client can be registered with Wyse Management Suite manually through registration UI provided by Wyse Device Agent (WDA) or automatically by configuring appropriate option tags on DHCP Server or configuring appropriate DNS SRV records on DNS Server.

Configuring a device manually

WES device can be registered manually by launching **WDA UI** icon on the taskbar.

1 Select **Wyse Management Suite-WMS** as management server.

2 Enter appropriate tenant and group name. If this field is left blank, devices are registered to unmanaged group. (Optional)

3 Click **Register**.

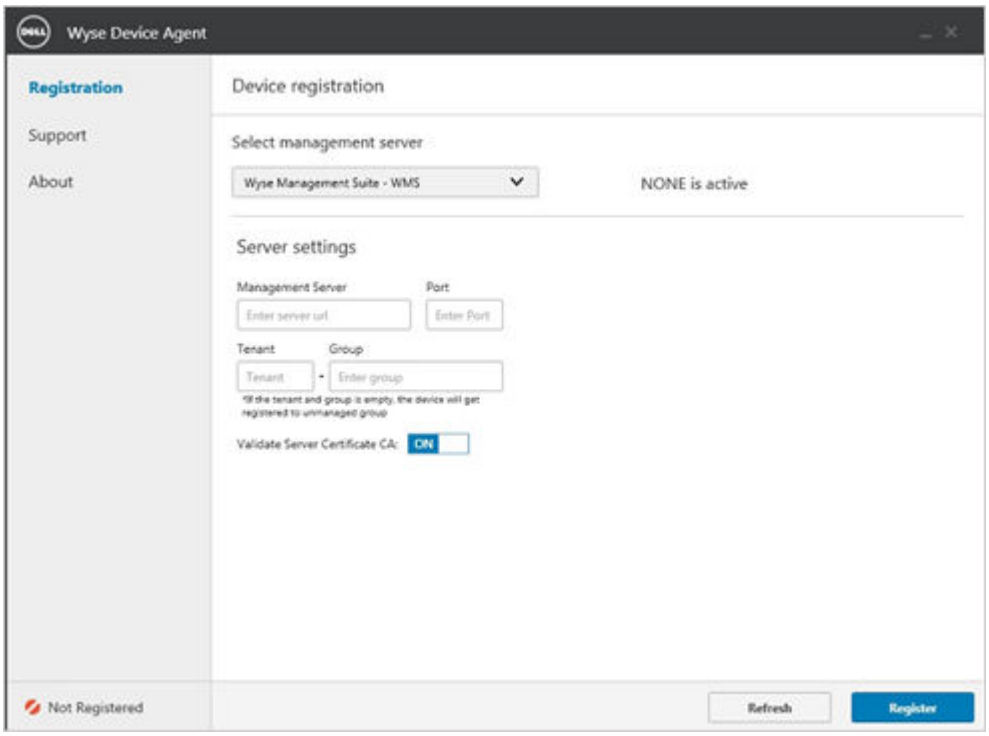

Figure 15. Device registration

Configuring device using DHCP option tags

To configure the DHCP options, do the following:

1 Click the **IPv4** option and select the subnet.

2 Right click **Scope options** and select **Configure** options.

   a In the scope option window select the 165 tag and then enter WMS FQDN along with the port number. For example, https://<FQDN>:<PORT>

   b In the scope option window select the 199 tag and then enter the group token.

   NOTE: This is optional for private cloud installations with only one tenant. If no group token is present, devices will register to unmanaged group.

   c In the scope option window select the 167 tag and set value as TRUE or FALSE for CA Validation, if not configured default value is TRUE.

   d

3 Click **OK**.

Configuring device using DNS SRV record

The instructions described in this section mainly focuses on DNS_SRV record. The DNS record is _tcp_pcoip-tool in the domain that the client is configured to communicate with, and the configurations are expected to be done on the DNS server.

1 Navigate to _tcp under your domain, then right click and select **Other new records**.

2 Select **Service Location (SRV)** from resource record type list.

3 Click **Create Record**... option.

4 Enter the DNS Discovery with following tags:

- **Wyse Management Suite Server URL**
  - DNS Record Type : DNS SRV
  - Record Name : _WMS_MGMT_tcp.<Domain>
  - Value Returned : WMS Server URL
    For example : _WMS_MGMT_tcp.WDADEV.com
- **Group Token** (optional) If this option is not configured, the device will be discovered to the Unmanaged Group.
  - DNS Record Type : DNS Text
  - Record Name : _WMS_GROUPTOKEN.<Domain>
  - Value Returned : Group Token as String
    For example : _WMS_GROUPTOKEN.WDADEV.com
- **CA Validation** (Optional)
  - DNS Record Type : DNS Text
  - Record Name : _WMS_CAVALIDATION.<Domain>
  - Value Returned : TRUE or FALSE (as String). CA Validation value is TRUE by default if not given.
    For example : _WMS_CAVALIDATION.WDADEV.com

    Enter True, if you have installed certificates by well-known certificate for https communication between client and Wyse Management Suite Server. Enter False, if you have not installed certificate on device for https communication.

Wyse Management Suite Jobs

Wyse Management Suite creates job for any task such as reboot, WOL and application/image policy that needs to be pushed to registered devices. Administrator can track the status of job by navigating to **Jobs** tab in Wyse Management Suite web console. For more information, see *Wyse Management Suite Administrator's guide.*

Changing wallpaper for all devices belonging to marketing group

1 To add a wallpaper to Wyse Management Suite repository, do the following:

a Navigate to **Apps & Data** tab.

b Scroll down to bottom of the page and select inventory from navigation bar located on the left pane.

c Click the **Add File** button.

d Browse and point to image that you want to use as a wallpaper.

e For type, select **Wallpaper**.

f Enter description and click on upload.

2 To change configuration policy of group by assigning a new wallpaper, do the following:

a Select a policy group.

b Click **Edit Policies** drop-down and select **WES**.

c Select **Desktop Experience** tab and click **Configure this item** button.

d Select **Desktop Wallpaper** check-box.

e Select wallpaper file from drop-down list.

f Click the **Save and Publish** button.

3 Click on **Jobs** for checking status of configuration policy. You can click the number next to status flag in details column to check devices with particular status.

Publishing application to thin clients

To push applications to WES, Linux and ThinOS thin clients, do the following:

Create and push Application Policy to thin clients

Standard application policy allows you to install single application package and requires reboots before and after each application installation. With advanced application policy, you can install multiple application packages with only two reboots. Advanced application policy also supports execution of pre and post installation scripts that may be needed to install particular application. For more information, see Appendix B.

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

1 Copy application that you would like to push to thin clients in **thinClientApps** folder in local repository.

2 Ensure that the application is registered by navigating to **Apps & Data** tab and selecting **Thin Client** under App Inventory in navigation menu on left of the window.

3 Click the **Thin Client** under **App Policies** in navigation menu on the left pane.

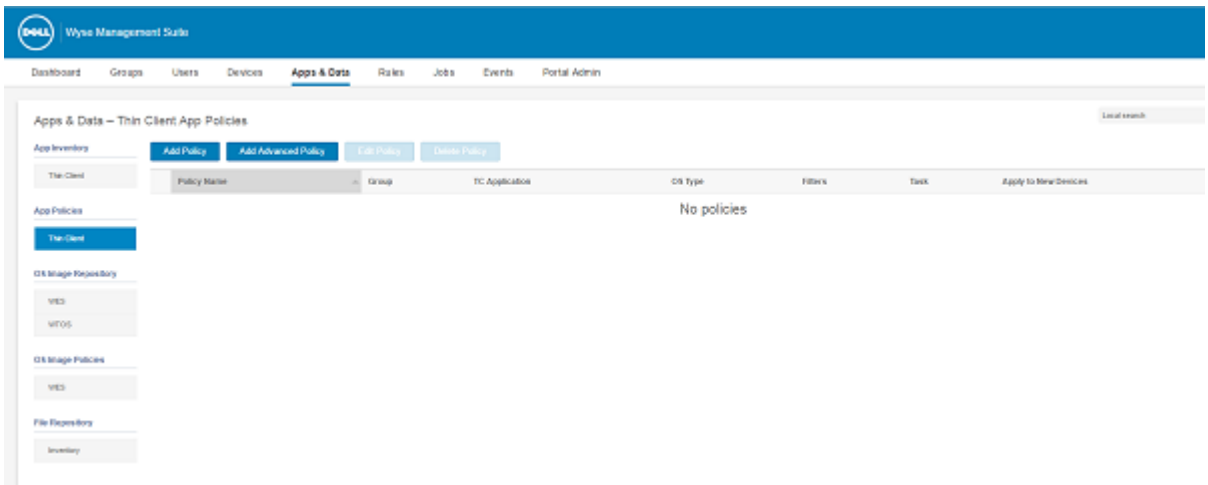

Figure 16. App Policies

4 Click the **Add Policy** button.

5 Enter the appropriate information to create a new application policy.

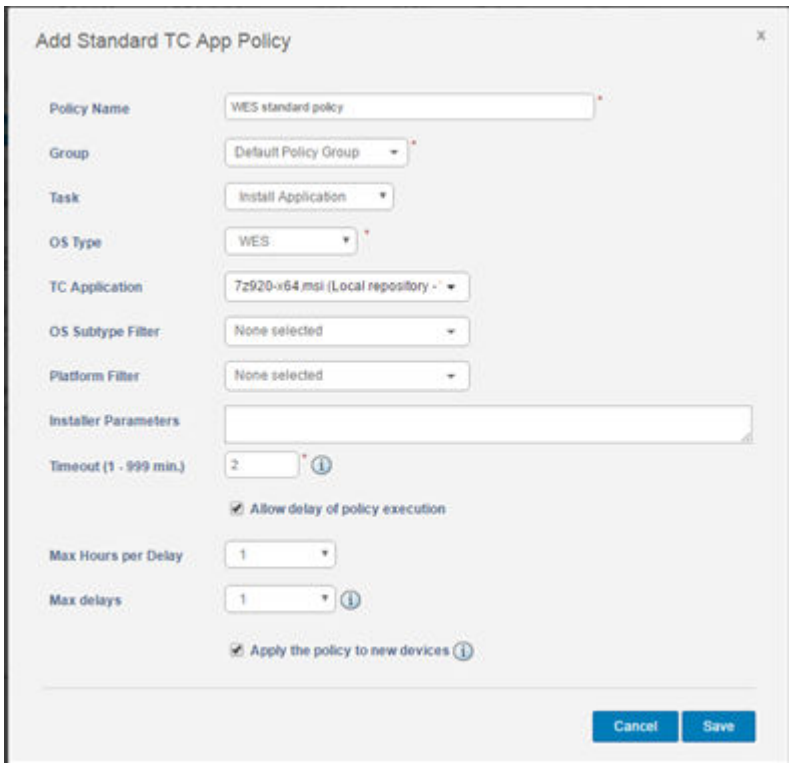

Figure 17. App policy

a You must enter/select Policy Name, Group, Task, Device Type and application.

b You may choose to select OS or Platform filters if you would like to push this policy to specific OS or Platforms.

c Timeout displays a message on the client which gives the user time to save his/her work before the installation begins. Specify the number of minutes the message dialog will be displayed on the client.

d Select **Apply the policy to new devices** if you would like to automatically apply this policy to device that is registered with Wyse Management Suite and belongs to specified group or is moved to specified group.

6 You can select the **Allow delay of policy execution** check box to allow delay of the execution based on 'Max hours per delay' which is 1-24 hours and 'Max Delays' which is 1-3

.

7 You can select **Enable app dependency** to abort app policy at first failure. If unchecked, failure of one app will not affect the policy execution.

8 Click **Save** to create new policy. Dialog will be displayed to allow user to push this policy to devices. Select yes, to push policy now

9 On **Jobs** page click **Schedule App Policy** to push application policy to devices.

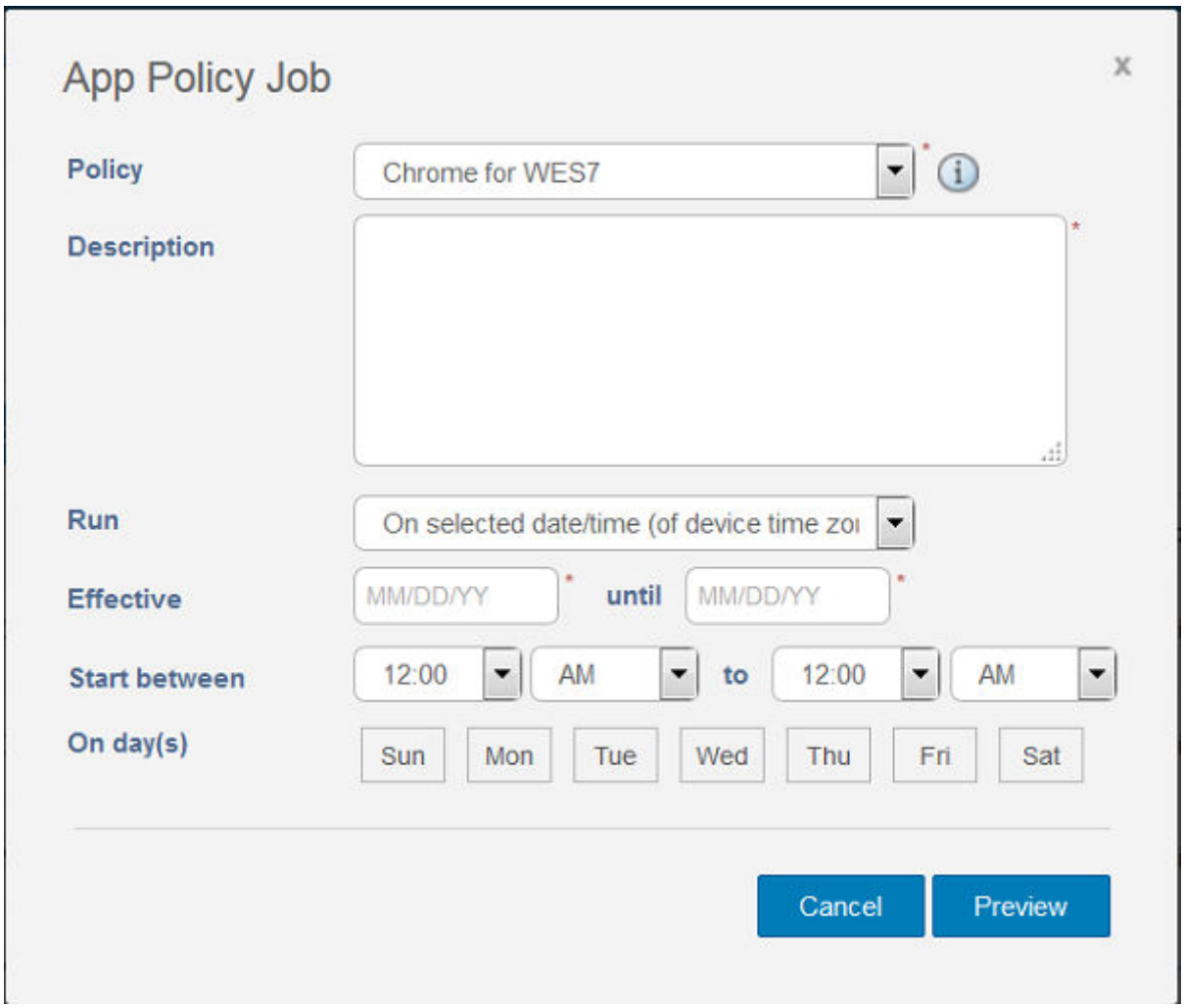

Figure 18. App Policy Job

10 The app / image policy job can Run

a "Immediately": server will run the job right away

b "On device time zone": server will create one 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 one job to be run at the date/time of the designated time zone.

11 Click preview and then schedule on next page to create the Job.

12 You may check the status of Job by navigating to **Jobs** Page at any time.

Create and push Advanced Application Policy to thin clients

Advanced application policy you can install multiple application packages with only two reboots. Advanced application policy also supports execution of pre and post installation scripts that may be needed to install particular application.

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

1 Copy application and Pre, post install scripts (if required) that you would like to push to thin clients in thinClientApps folder in local repository or Wyse Management Suite repository.

2 Ensure that the application is registered by navigating to Apps & Data Tab and selecting thin client under App Inventory in navigation menu on left of the window.

3 Click thin client under App Policies in navigation menu on left of the window.

4 Click the **Add Advanced Policy** button.

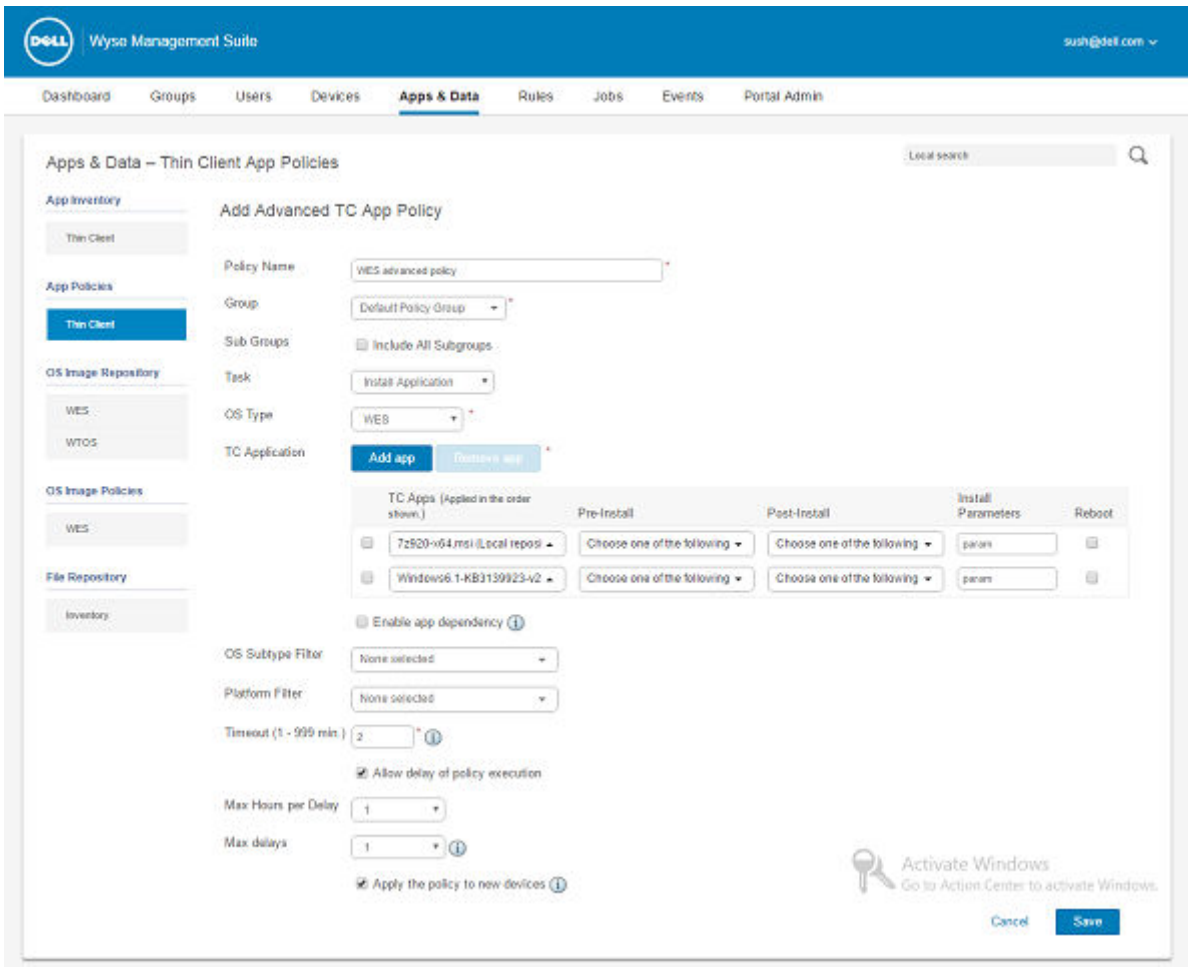

Figure 19. Add Advanced Policy

5 Enter appropriate information to create a new application policy.

a You must enter Policy Name, Group, Task and Device Type.

b Click Add App, you must select one or more application under 'TC apps'. For each application you may optionally select Pre, post install script under section 'pre install' and 'post install' and install parameters. Select reboot if system should reboot after application is successfully installed.

c You can check the checkbox to 'include subgroups', if you want this policy to be applied on all subgroups.

d You may choose to select OS or Platform filters if you would like to push this policy to specific OS or Platforms.

e Timeout displays a message on the client which gives the user time to save his/her work before the installation begins. Specify the number of minutes the message dialog will be displayed on the client.

f Select **Apply the policy to new devices** if you would like to automatically apply this policy to device that is registered with Wyse Management Suite and belongs to selected group or is moved to selected group.

6 You can select the check box 'Allow delay of policy execution' to allow user to delay the execution based on 'Max hours per delay' which is 1-24 hours and 'Max Delays' which is 1-3.

7 You can select checkbox 'Enable app dependency' to abort app policy at first failure, if unchecked, failure of one app will not affect the policy execution.

8 Click Save to create new policy. Pop up will be displayed to allow admin to schedule this policy on devices based on group. Select yes, to navigate to Jobs page.

9 On Jobs page, click the Schedule App Policy to schedule application policy to devices immediately or at scheduled date and time.

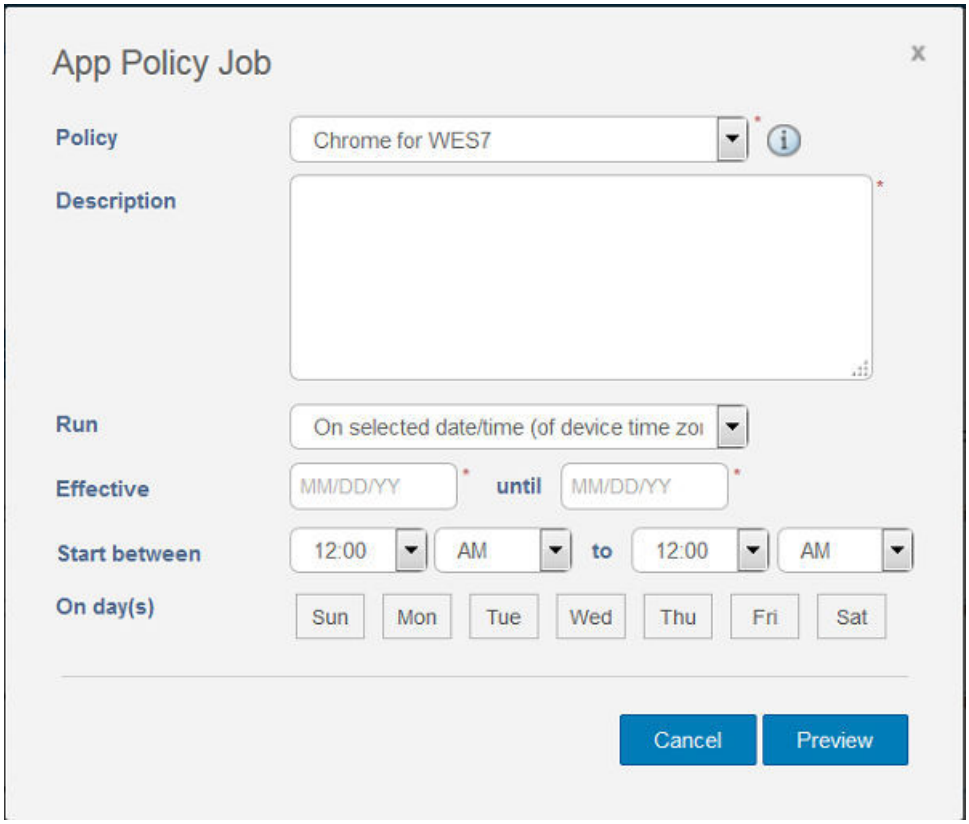

Figure 20. App Policy Job

10 The app/image policy job can Run

a "Immediately": server will run the job right away

b "On device time zone": server will create one 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 one job to be run at the date/time of the designated time zone.

11 Click on preview and then schedule on next page to create the Job.

12 You may status of Job by navigating to Jobs Page at any time.

5

Uninstalling Wyse Management Suite

To uninstall Wyse Management Suite, do the following:

1 Double click the **WMS** icon.

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

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

A

Custom installation

If you select the **Setup Type** as **Custom**, you can choose either **Embedded MongoDB** or **External MongoDB** as the Mongo Database Server.

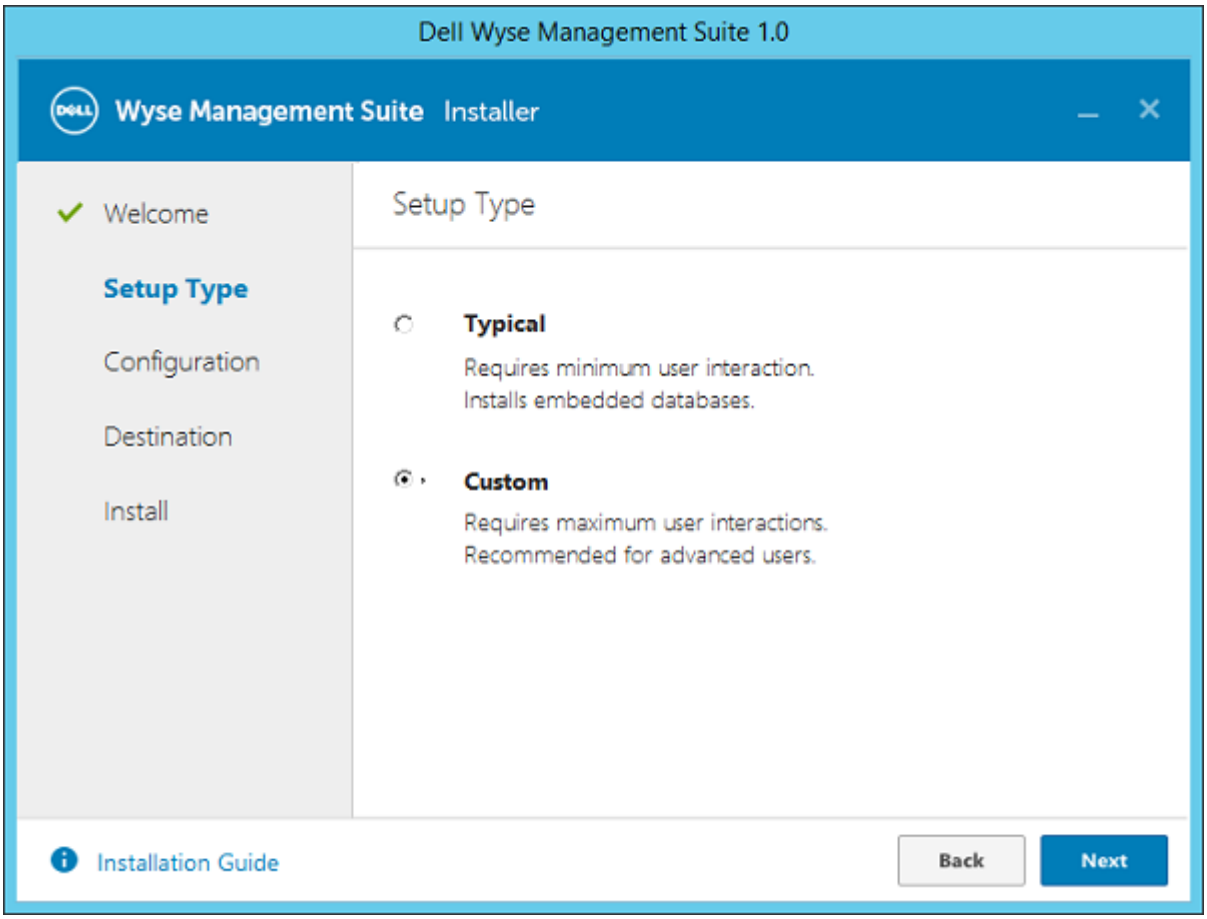

Figure 21. Setup type

- If **Embedded MongoDB** is selected, then provide your password and then click **Next**.

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

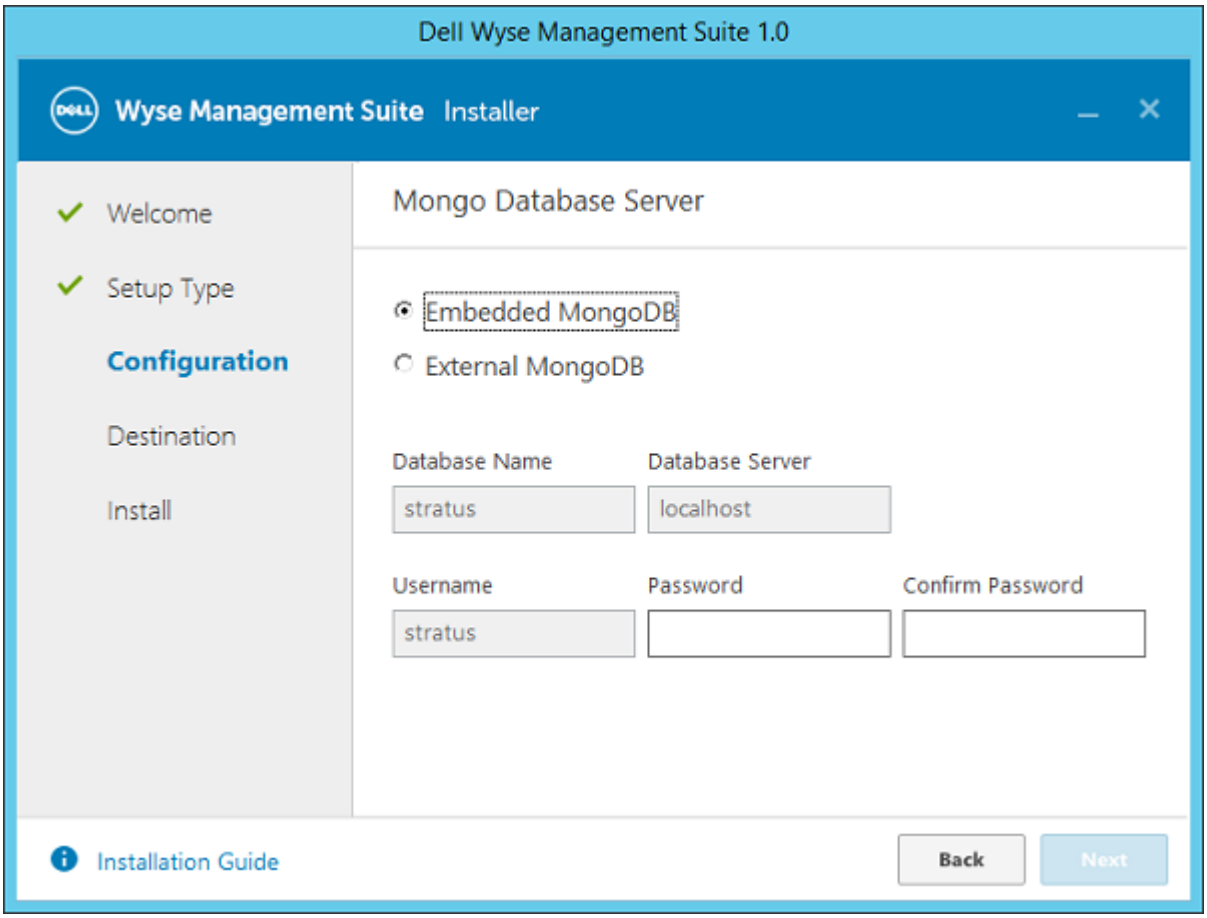

Figure 22. Mongo Database Server

- If **External MongoDB** is selected, then provide username, password and database server details, and then click **Next**.

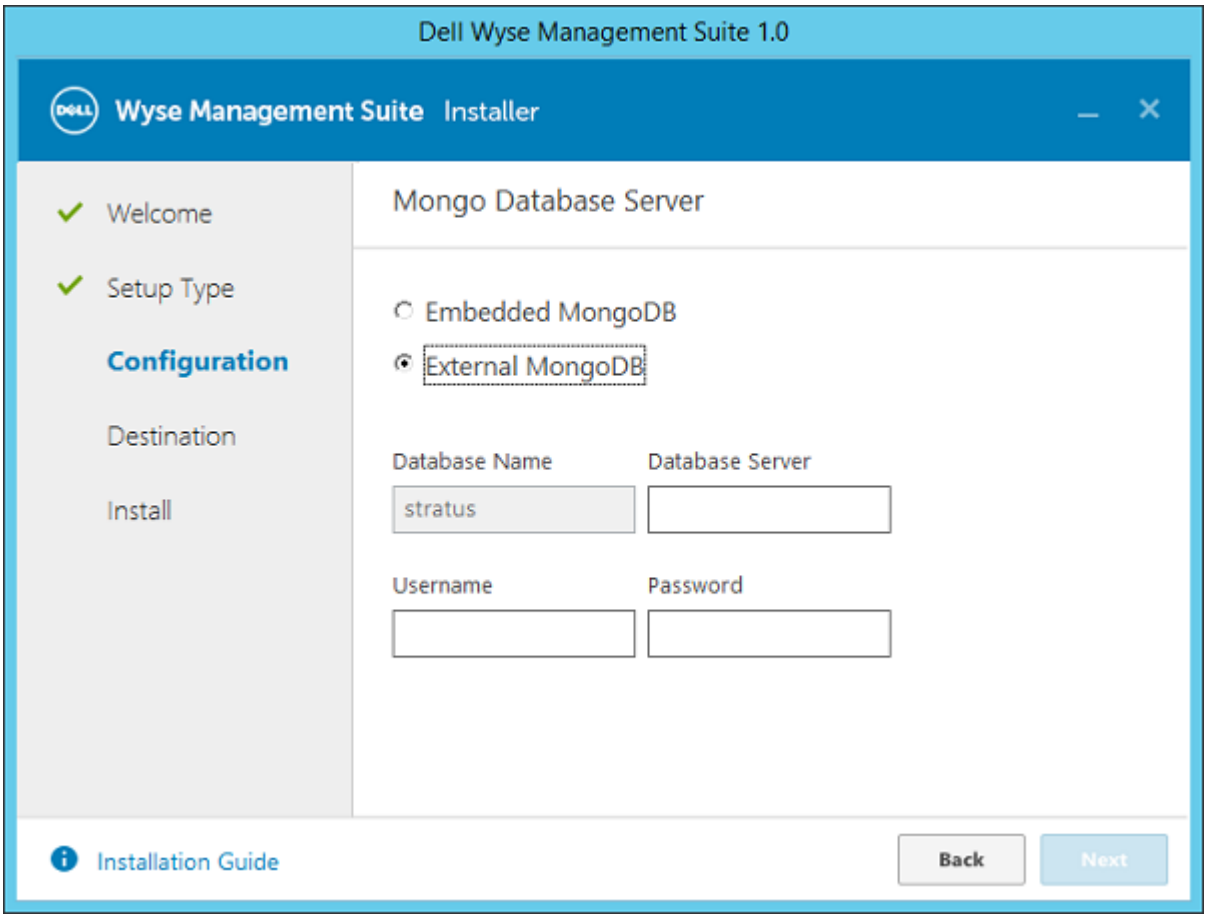

Figure 23. Mongo Database Server

- If **Embedded MariaDB** is selected, then provide username and password and then click **Next**.

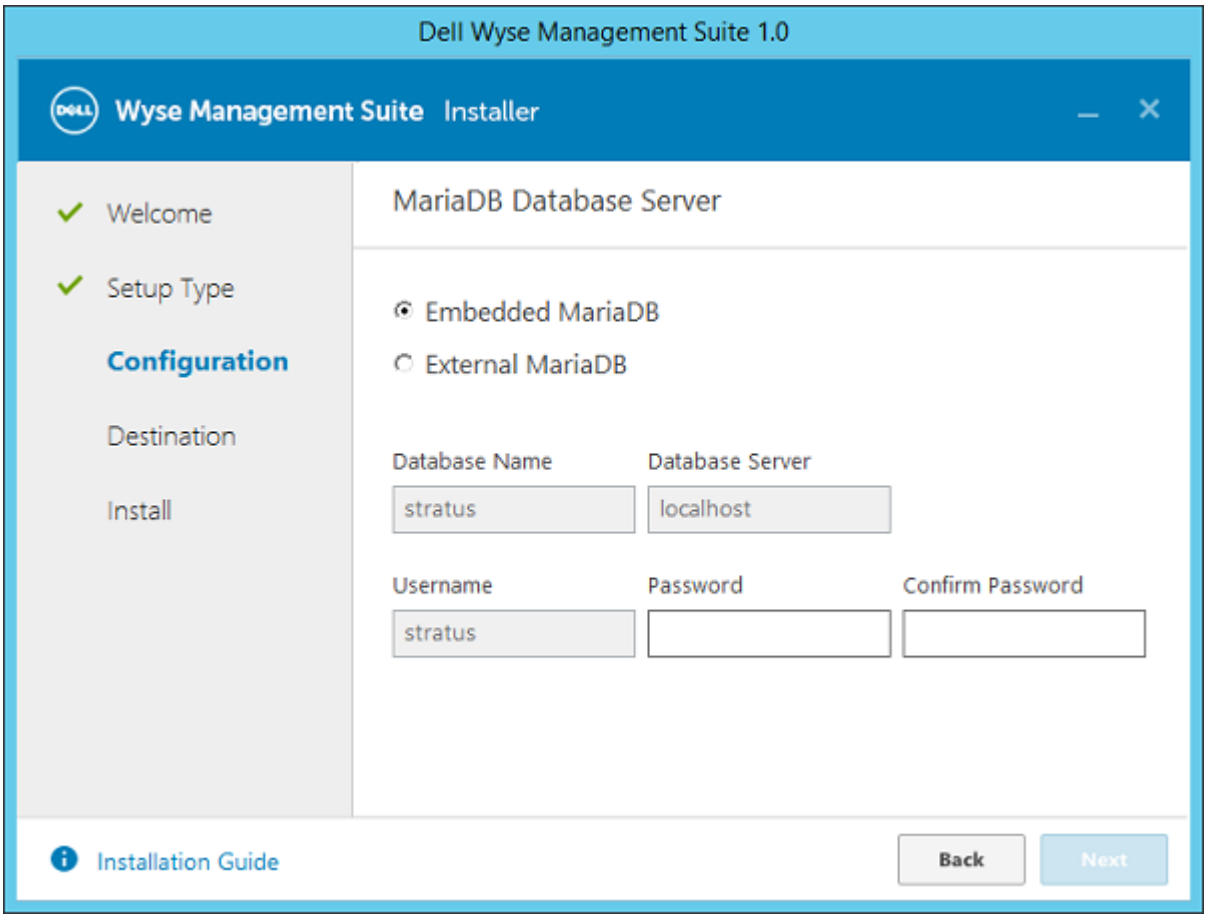

Figure 24. MariaDB Database Server

- If **External MariaDB** is selected, then provide username, password and database server details, and then click **Next**.

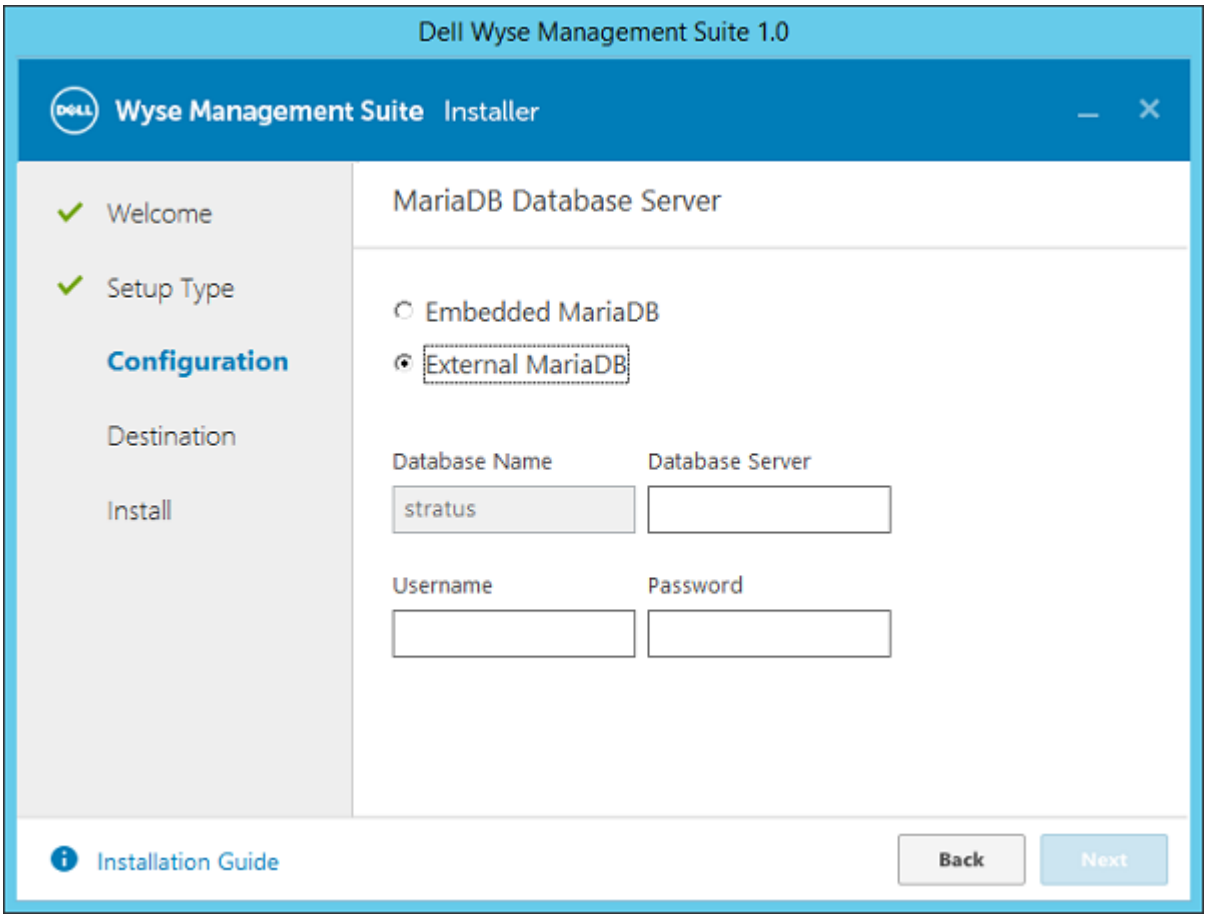

Figure 25. MariaDB Database Server

Follow the steps in the section Installing WMS on-premise and initial setup, to complete the installation.

B

Feature matrix

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

Table 1. Feature Matrix for each Subscription type

Features	Wyse Management Suite Standard	Wyse Management Suite Pro Private cloud	Wyse Management Suite Pro Cloud edition
Highly scalable solution to manage thin clients	Free Up to 10,000 devices	50,000 devices and more	1 million devices and more
Group based management	Yes	Yes	Yes
Multi Level Groups and Inheritance	Yes	Yes	Yes
Configuration Policy management	Yes	Yes	Yes
OS Patch and Image management	Yes	Yes	Yes
View effective configuration at device level after inheritance	Yes	Yes	Yes
Application policy management	Yes	Yes	Yes
Asset, Inventory & Systems management	Yes	Yes	Yes
Automatic Device discovery	Yes	Yes	Yes
Real-time commands	Yes	Yes	Yes
Smart Scheduling	Yes	Yes	Yes
Alerts, Events and Audit logs	Yes	Yes	Yes
Secure communication (HTTPS)	Yes	Yes	Yes
Manage devices behind firewalls	Limited	Limited	Yes
Mobile App	No	Yes	Yes
Alerts via Email and Mobile app	No	Yes	Yes
Scripting support for customizing application installation	No	Yes	Yes
Bundle Applications to simplify deployment and minimize reboots	No	Yes	Yes
Delegated Administration	No	Yes	Yes

Features	Wyse Management Suite Standard	Wyse Management Suite Pro Private cloud	Wyse Management Suite Pro Cloud edition
Dynamic group creation and assignment based on device attributes	No	Yes	Yes
Two-factor authentication	Yes	Yes	Yes
Active directory authentication for role based administration.	No	Yes	Yes
Multi-tenancy	No	Yes	Yes
Enterprise Grade Reporting	No	Yes	Yes
Multiple repositories	No	Yes	Yes
Enable/Disable HW ports on supported platforms	No	Yes	Yes
BIOS Configuration on supported platforms	No	Yes	Yes

C

Supported thin clients

The following table provides information about the supported thin clients:

Table 2. Supported thin clients

Thin Clients	Device Type	Tested OS
Linux	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client	11.3.106
ThinLinux	Wyse 5020 thin client Wyse 5060 thin client Wyse 7020 thin client Wyse 3030 LT thin client	1.0.3
WES7	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client Wyse 3030 thin client Wyse 7010 Extended thin client	895
WES7P	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client Wyse 7010 Extended thin client	896
	Wyse 7040 thin client	7020
	Latitude 3460 mobile thin client	7041
	Latitude E7270 mobile thin client	7010
	Wyse 5060 thin client	7038

Thin Clients	Device Type	Tested OS
Windows 10 IoT	Wyse 5020 thin client Wyse 7020 thin client	0A0F
WE8S	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client	924
ThinOS	Wyse 5040 AIO Wyse 3010 thin client Wyse 3020 thin client, Wyse 5010 thin client (ThinOS, PCOIP) Wyse 7010 thin client Wyse 3030 LT thin client Wyse 5060 thin client Wyse 3040 Thin Client	8.3 HF, 8.4