Edge Device Manager Quick Start Guide

Version R15

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

Edge Device Manager is the next generation management solution for Edge Gateway Devices 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, and Applications deployment, Real-time commands, Monitoring, Alerts, Reporting, and Troubleshooting of endpoints.

NOTE: Wyse Management Suite UI will be re-branded to Edge Device Manager (EDM) after a valid license has been imported.

The following information should be considered for selecting the EDM Public vs Private cloud editions:

Private cloud

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)

Public 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, and so on)

Topics:

Getting started with Edge Device Manager

Terminology

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

Terminology	Definition
Private cloud	Edge Device Manager Server Installation, installed on premise that is private to your organization's data-center.
WDA	Wyse device agent which resides in the device and acts as an agent for communication between server and client.
Local repository	Application, and File repository that is installed by default in the Edge Device Manager Server.
Remote repository	Application, and File repositories that can be optionally installed as standalone for scalability and reliability across geographies for content transfer.
Public cloud	Edge Device Manager hosted on public cloud with convenience and cost savings of not having to setup and maintain 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	Edge Device Manager Server Installation, installed on premise that is private to your organizations data-center.
Tenant	A tenant is a group of users who share a common access with specific privileges to Edge Device Manager 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 Edge Device Manager. Users are given permissions to perform operations based on roles assigned to them.

Getting started with EDM on public cloud

This section provides you the important information on the general features to help you quickly get started as an administrator.

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 Edge Device Manager Trial on www.wysemanagementsuite.com or when you purchase your subscription. You can purchase the Edge Device Manager 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 Edge Device Manager by pointing your web browser to following links:
   - US Datacenter: us1.wysemanagementsuite.com
   - EU Datacenter: eu1.wysemanagementsuite.com
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 EDM on private cloud

Support information

EDM 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

Edge Device Manager 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 EDM, 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 EDM Server

1 English
2 French
3 Italian
4 German
5 Spanish

Browser Support

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

2

Pre-installation checklist

Before you build your EDM 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 Edge Device Manager License.

A simple installation of EDM consists of the following:

- EDM Server (Repository for application)
- Optional: Additional Wyse Management Suite repository servers.
- Optional: HTTPS certificate from well-known Certificate Authority.

The EDM 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 Edge Device Manager 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 Edge Device Manager 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.

3

Installing Edge Device Manager 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.

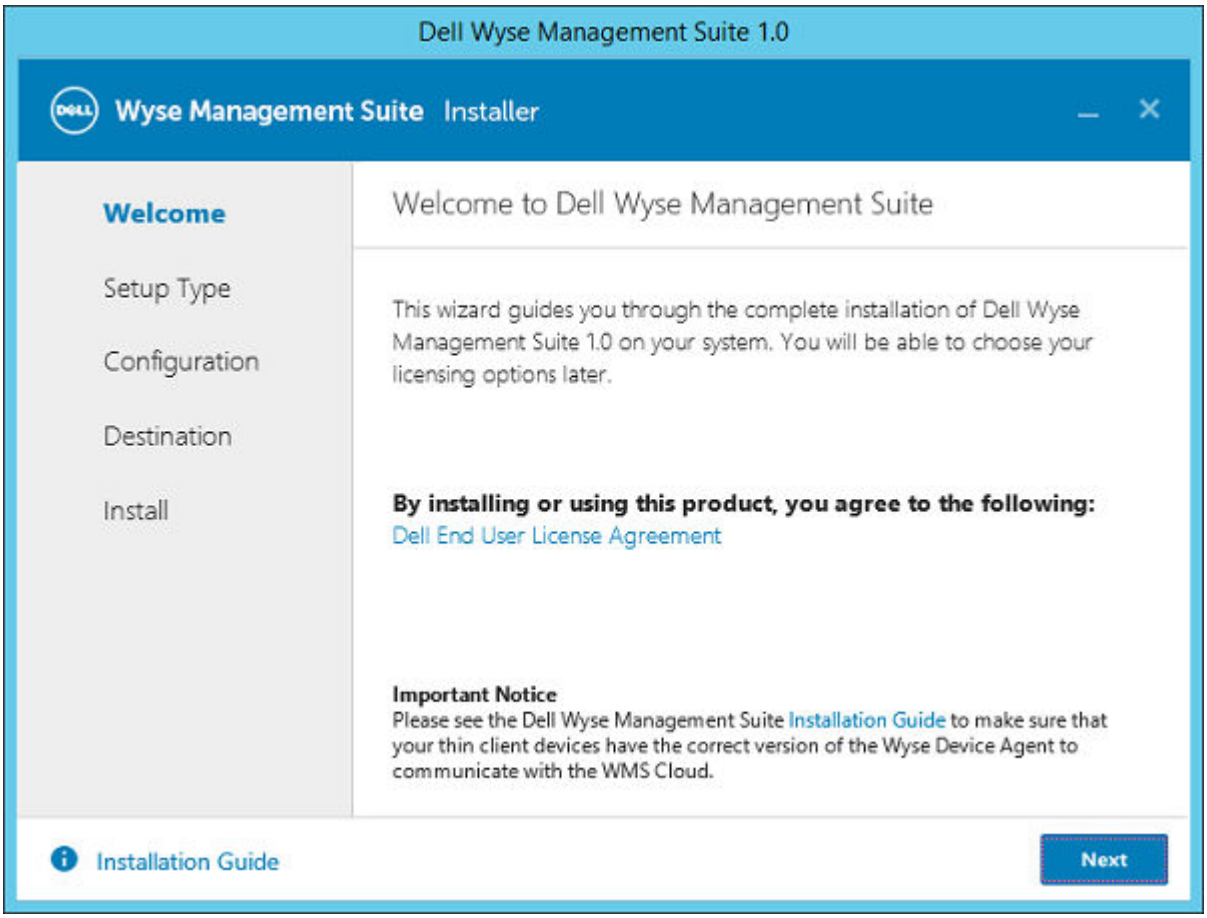

Figure 1. Welcome screen

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

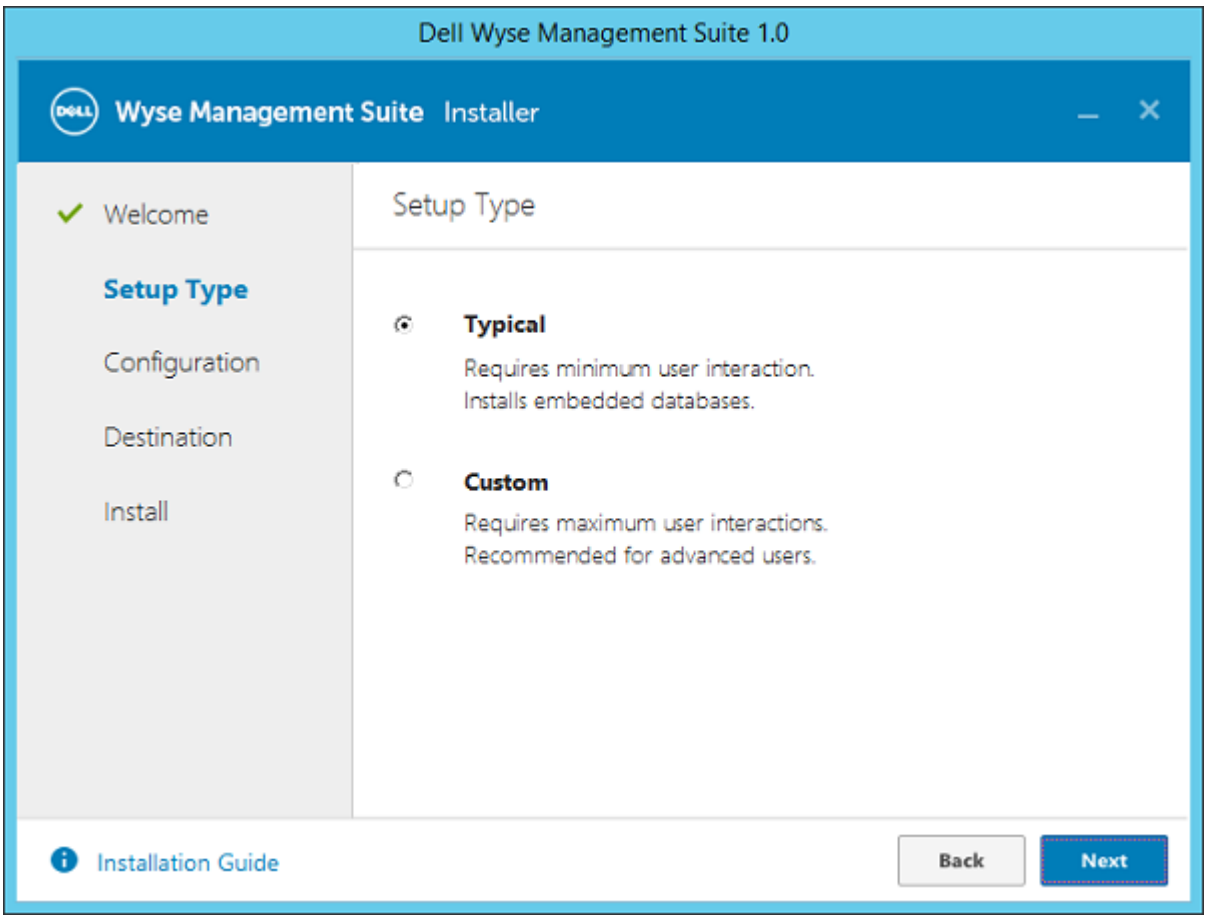

Figure 2. Setup type

- Typical—Requires minimum user interaction and installs embedded databases.
- Custom—Requires maximum user interactions and is recommended for advanced users.

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

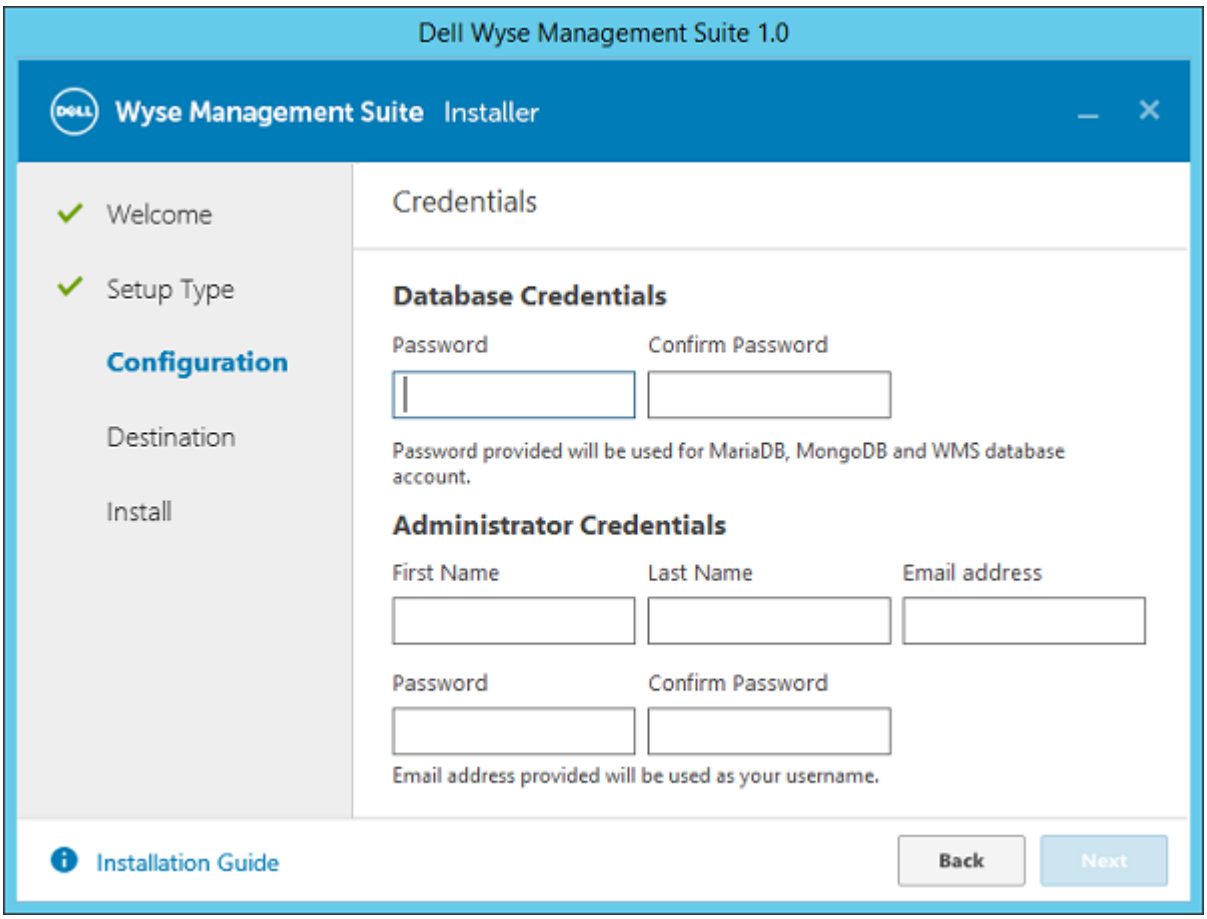

Figure 3. Credentials

3 Select a destination where you want to install Edge Device Manager. 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.

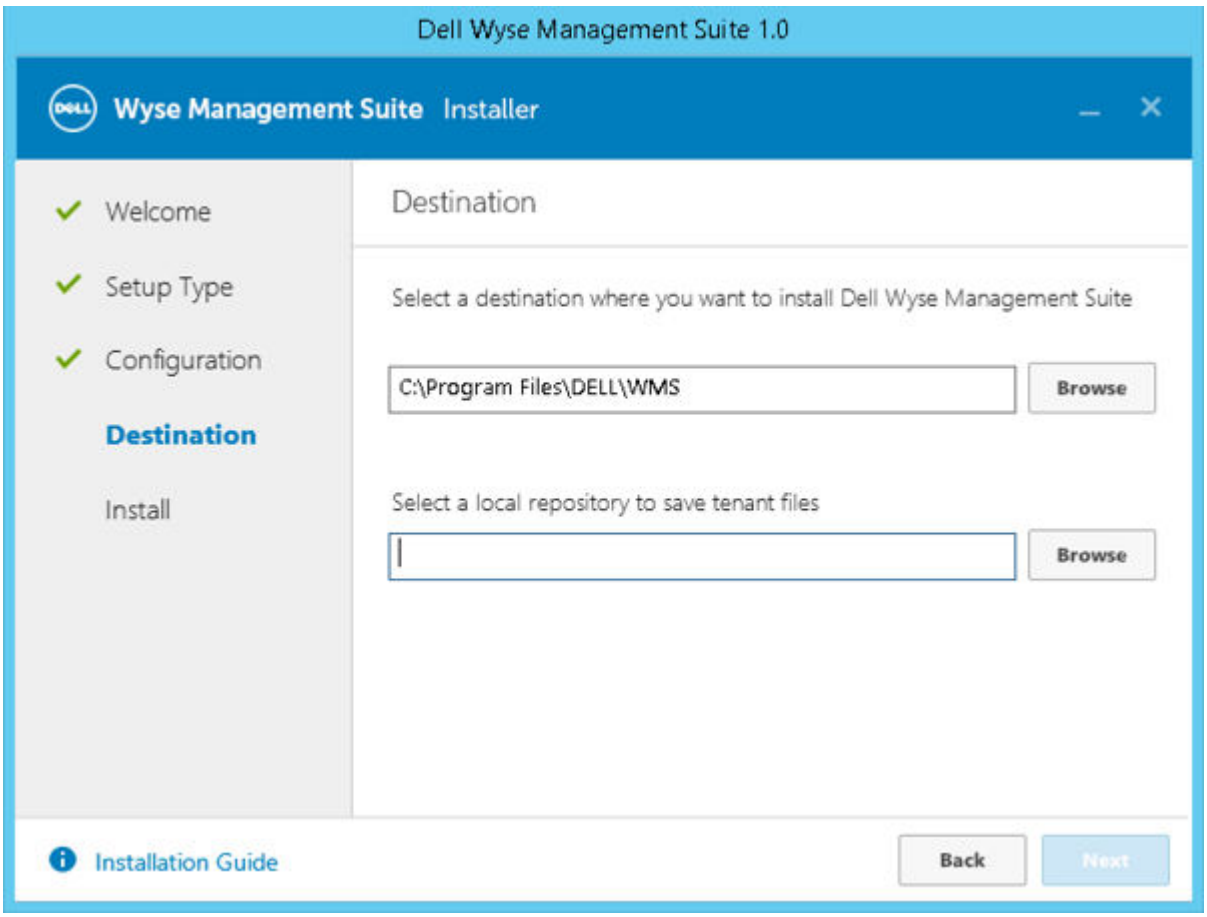

Figure 4. Destination

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.

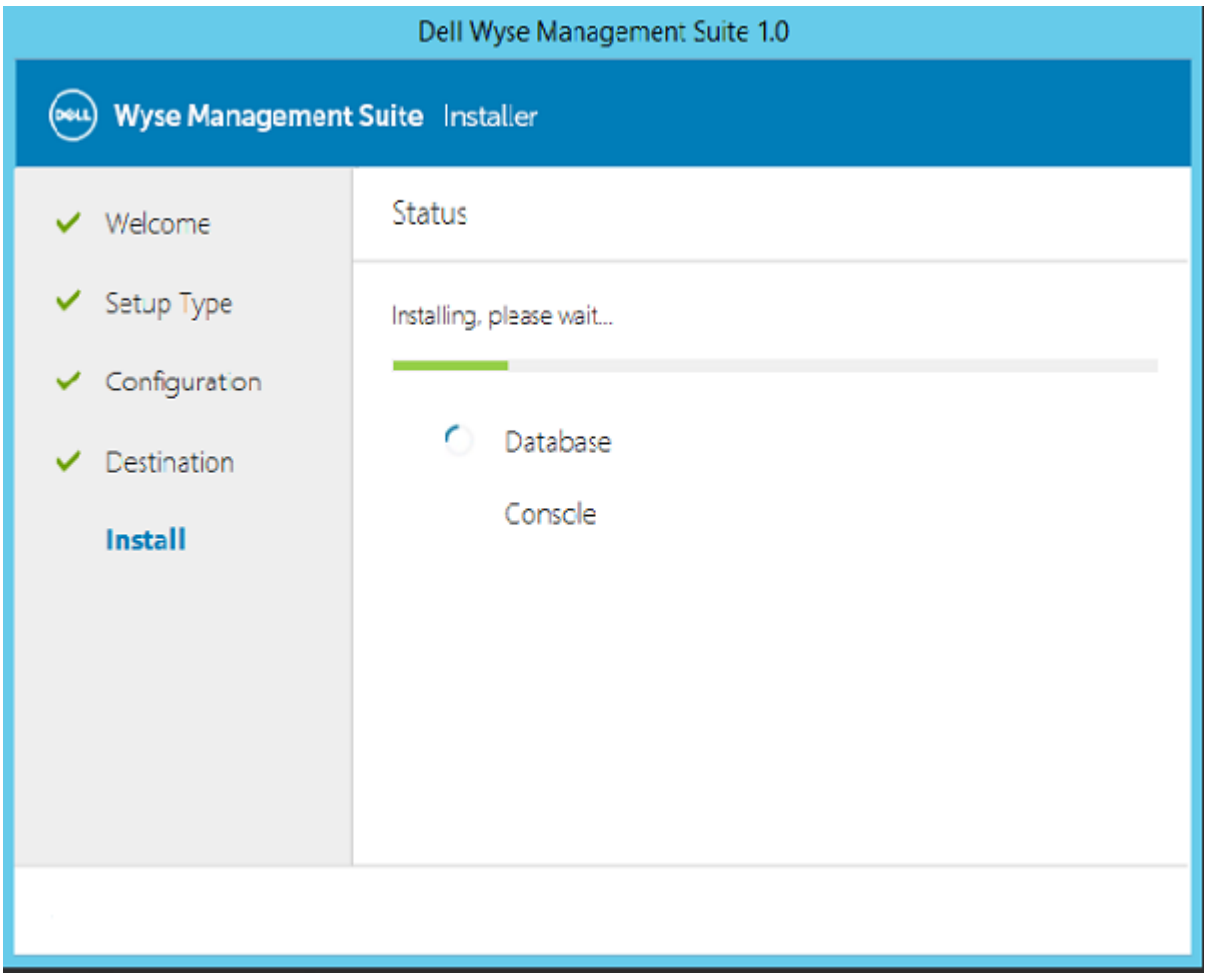

Figure 5. Installation status

4 Click **Launch** to open Edge Device Manager web console.

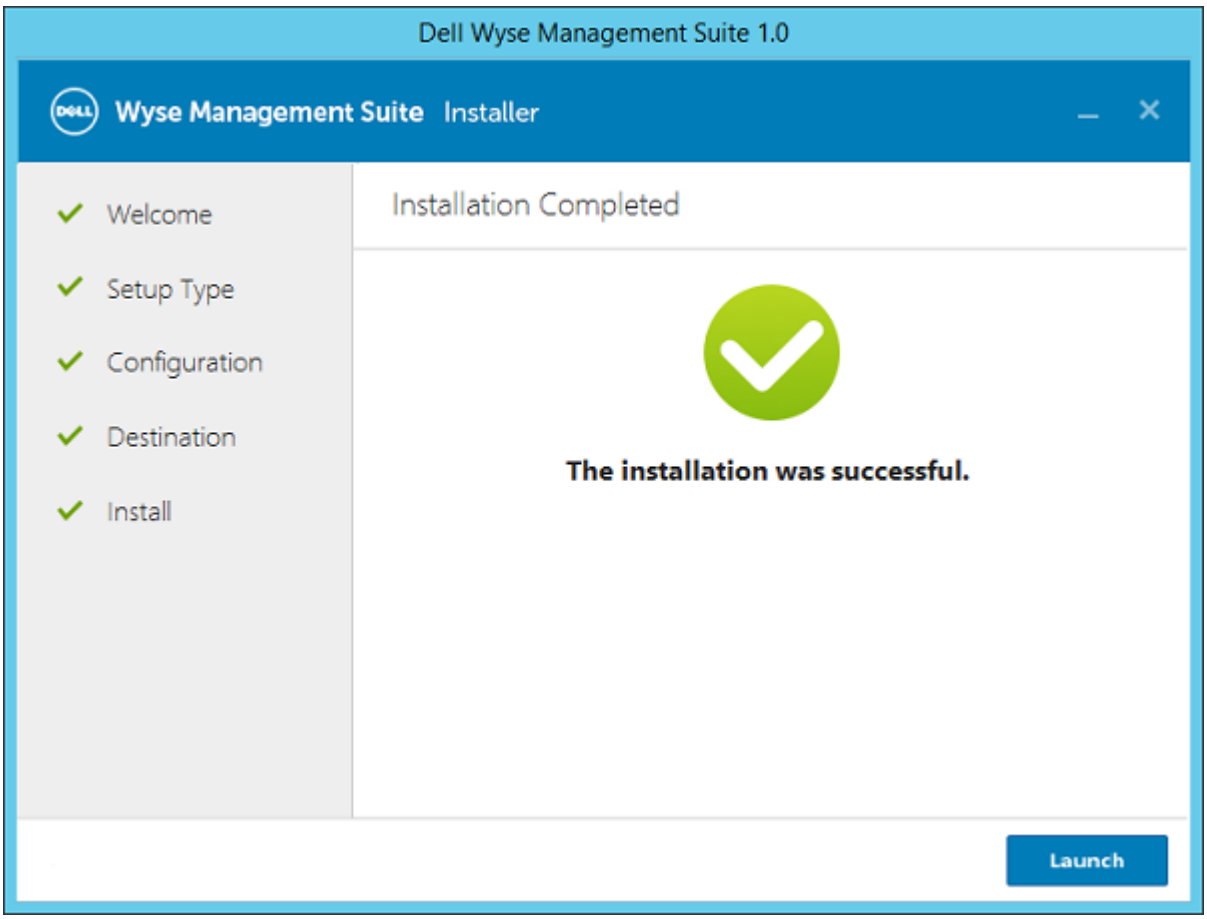

Figure 6. Installation complete status

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

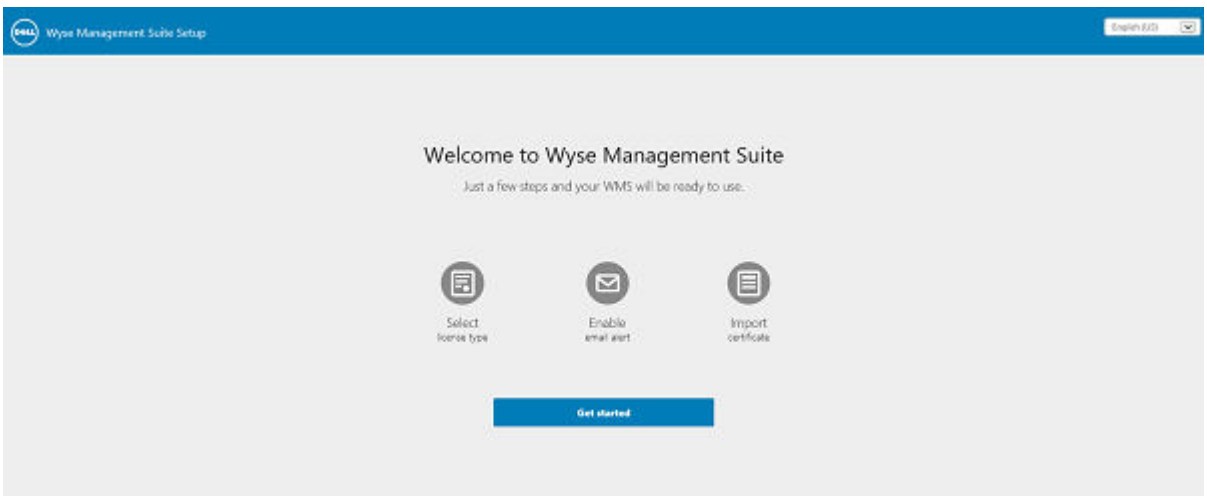

Figure 7. Welcome page

6 To enable Edge Device Manager on-premise and cloud, select the license type as pro.

- Pro—Enterprise-grade management for on-premises or hosted deployment.

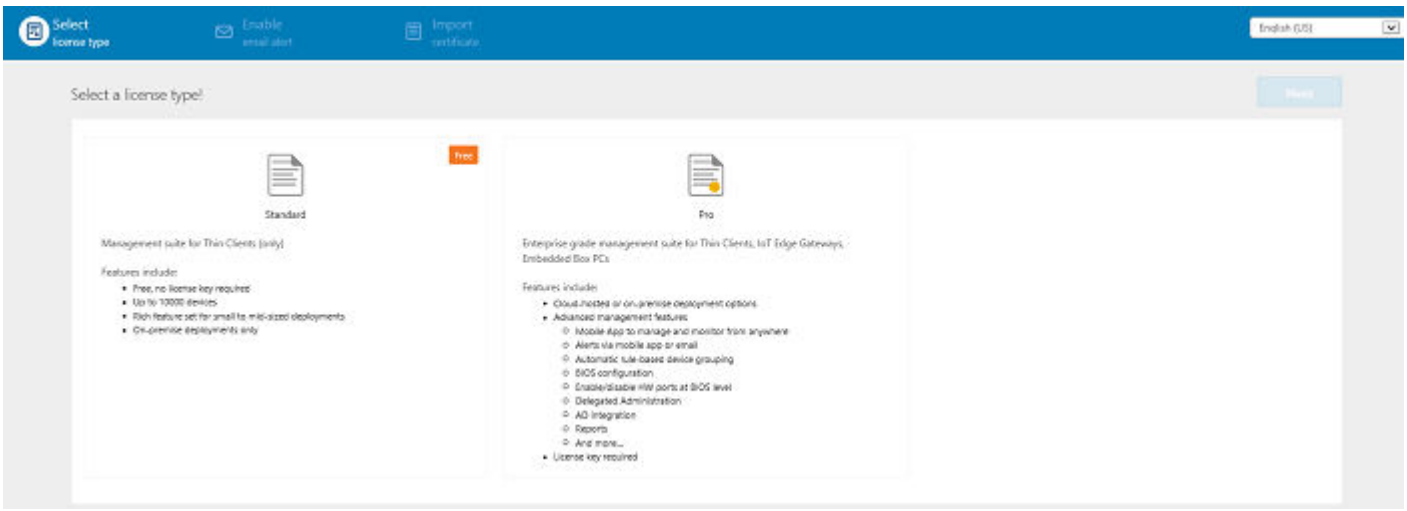

Figure 8. License type

a Select the license type as Pro. If you have internet connectivity, import EDM license from your public cloud account by entering your credentials and selecting number of seats. For installations without internet connectivity, you must export the key from public cloud and import it into license key textbox. License key can be exported by logging into your Wyse Management Suite public cloud account and then selecting **Portal Admin** > **Subscription** tab. On this page, enter number of seats and click **Export**.

> **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.**

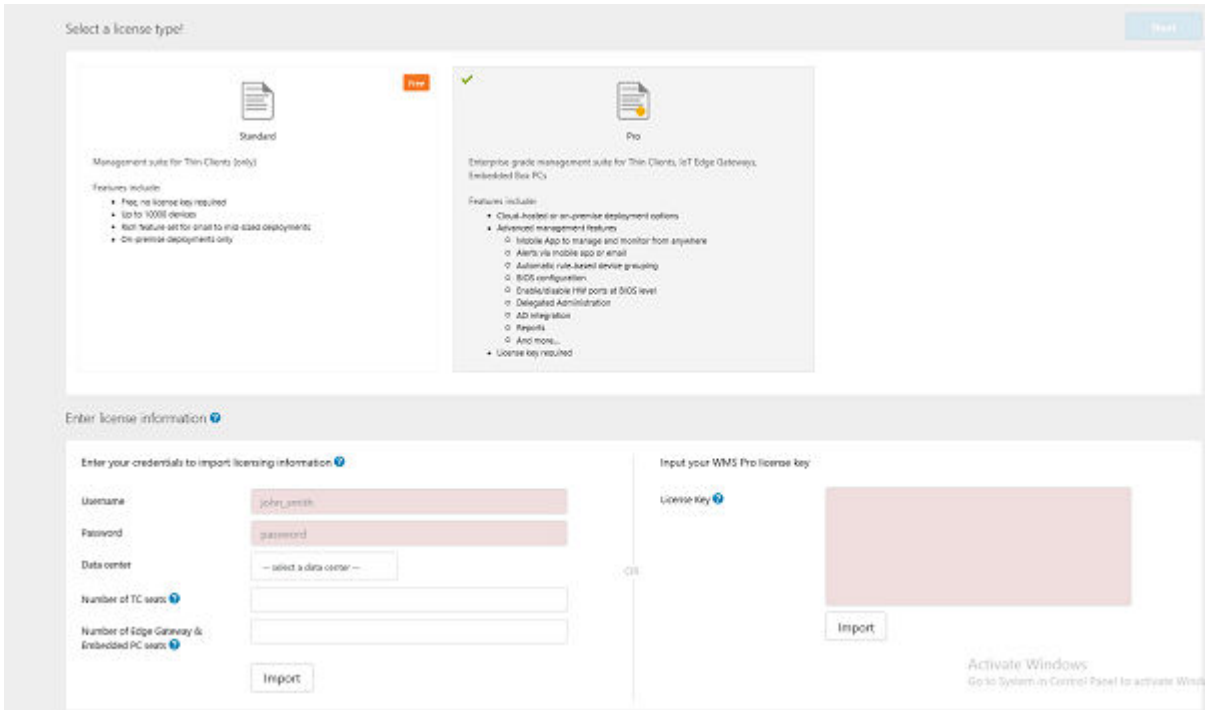

Figure 9. Pro license type

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.

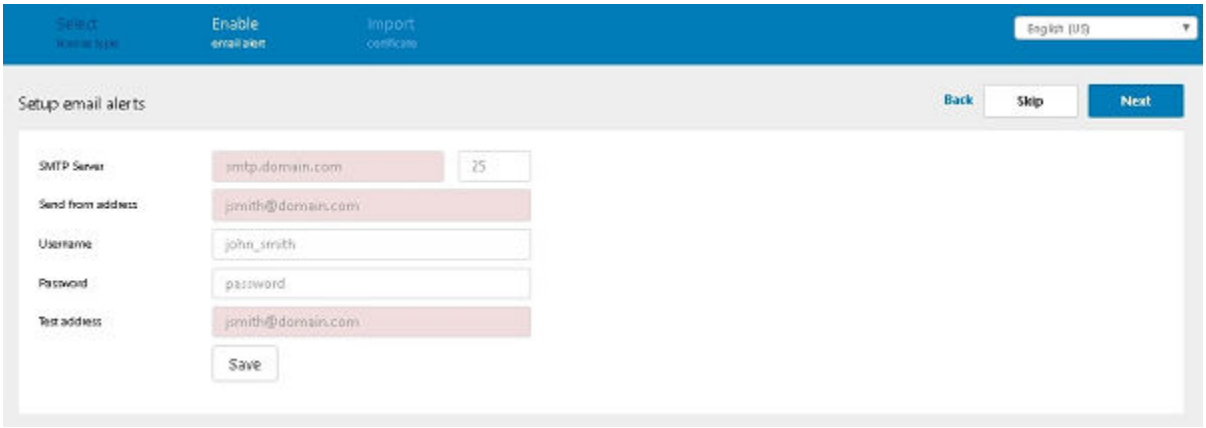

Figure 10. Email alerts

NOTE:

- You must enter valid information about your SMTP server to receive email notifications from Edge Device Manager.
- 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 Edge Device Manager 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.

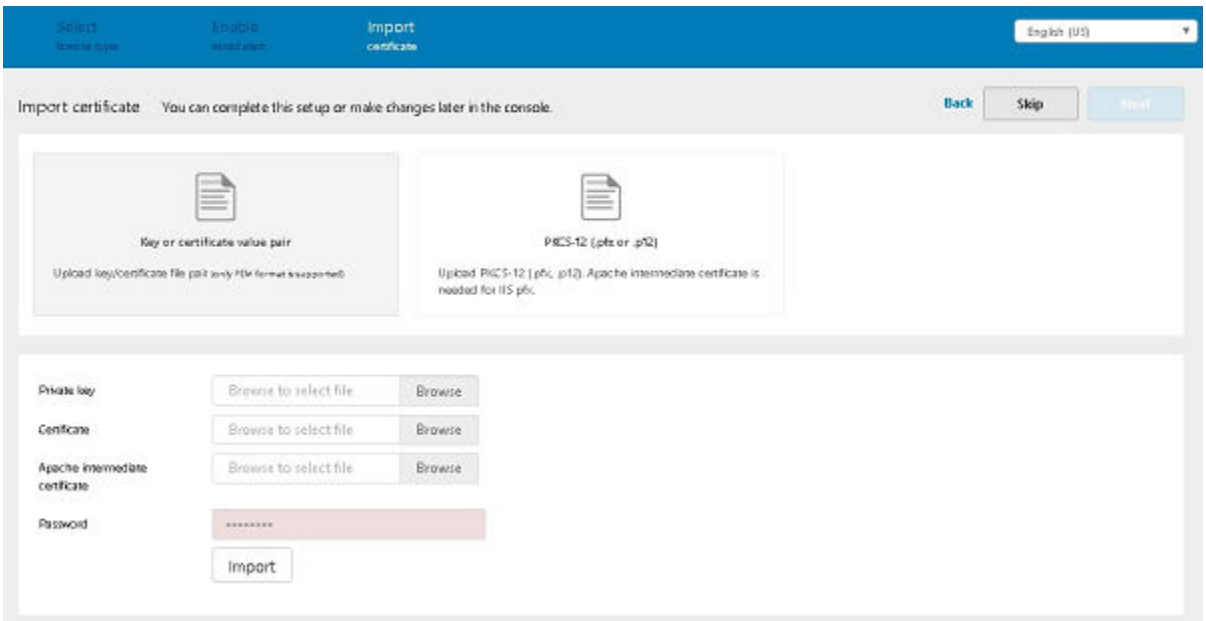

Figure 11. Import certificate

9 Click the **Sign in to Wyse Management Suite** button.

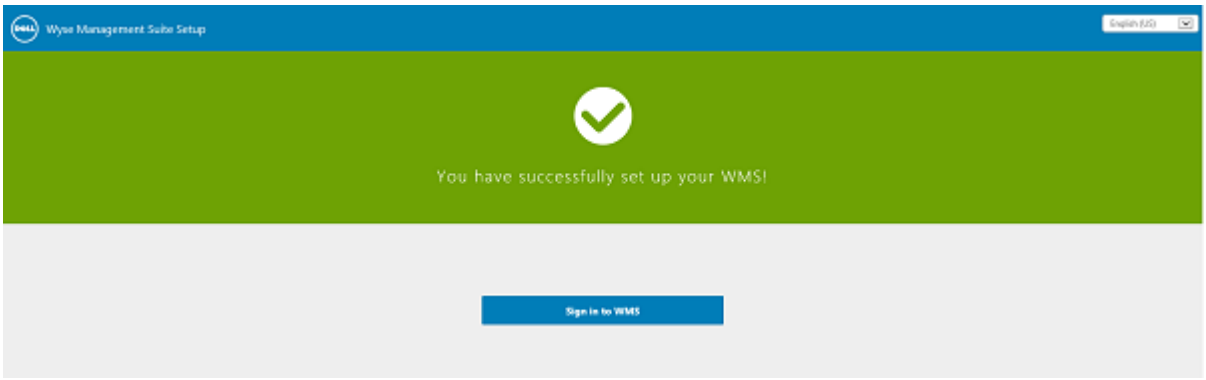

Figure 12. Sign in page

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

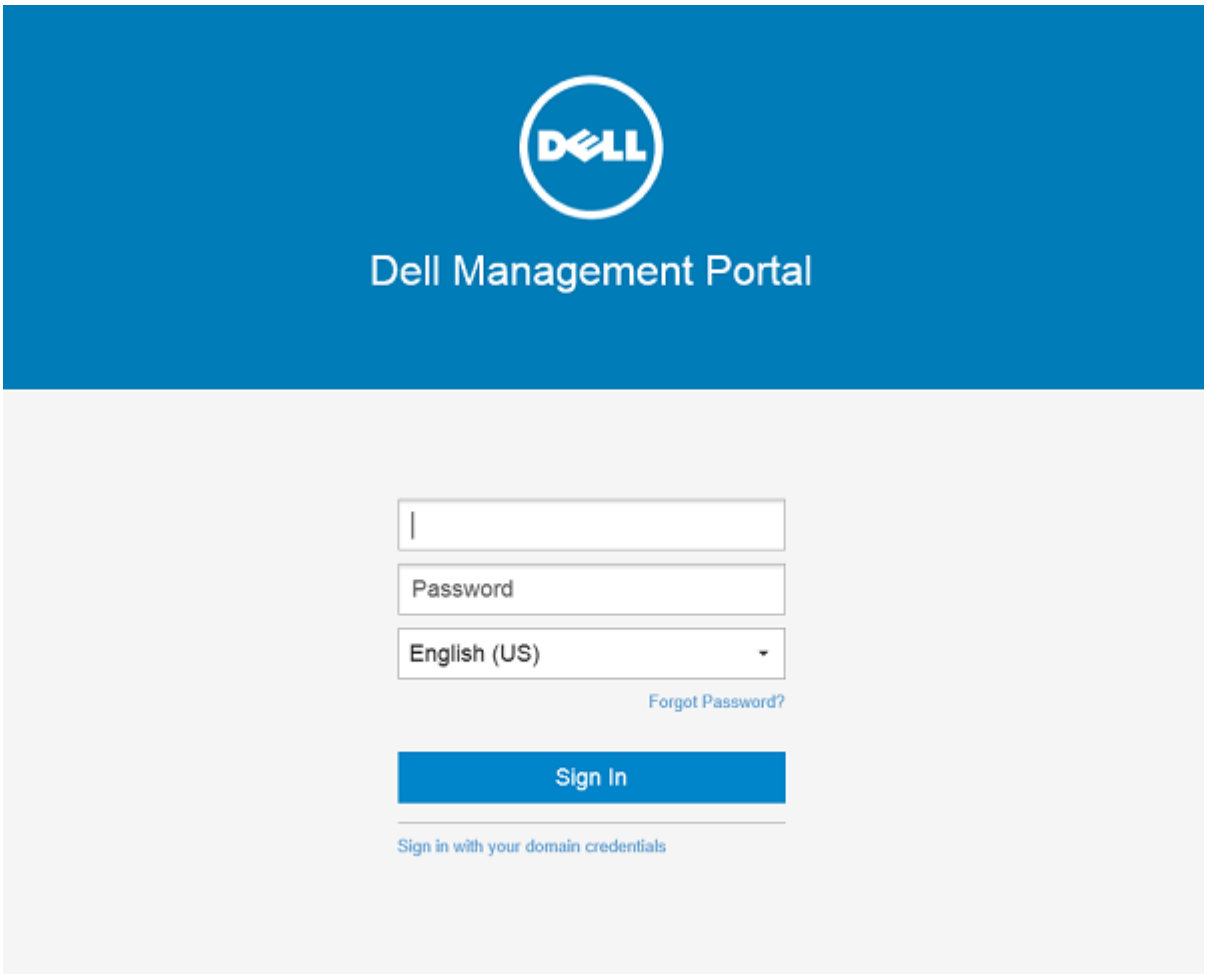

Figure 13. Dell Management Portal

Topics:

- Functional areas of the management console

- Configuring and managing Edge Gateway devices
- Creating a policy group and updating configuration
- Registering devices to Edge Device Manager
- Edge Device Manager Jobs
- Publishing application to Edge Gateway/Embedded PC devices

Functional areas of the management console

The EDM 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 EDM. 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 inventory and policies.
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 Edge Gateway devices

The general approach to configure and manage Edge Gateway devices 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, EDM 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 tenant account 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 the Administrator makes a change.
  - New devices that are registered receives the configuration policy that is effective for the group to which it was registered.
  - New devices that are registered receives the configuration policy that is effective for the group to which it was registered.
- Applications, updates, and other such operations are done from the Apps and Data tab of the UI.
  - Applications are deployed based on Policy Groups.

- Deployment of Application policies to the devices may be scheduled immediately or 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.
- You will receive an alert notification and manage devices using mobile app is available for Android and iOS devices. 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 **Snappy**.

  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 R15 Administrator's Guide*.

Registering devices to Edge Device Manager

Devices can be registered with EDM based on following methods:

1. Configuring appropriate option tags on DHCP Server.

2. Configuring appropriate DNS SRV records on DNS Server.

3. USB based registration.

4. 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 will be registered to the Unmanaged Group if the group token is not provided.

Automated registration of devices 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 for New Agent and required for Old Agent)
     - 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

Automated registration of devices 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 Wyse Management Suite 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**.

Edge Gateway and Embedded PC Registration from USB Device

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

1 Insert a USB drive into a PC or 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 inside the **ccm-wda** folder on the USB drive.
6 Safely eject the USB drive and insert into the Edge Gateway/Embedded PC device and then, 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 EDM server.
2 Navigate to **Portal admin** > **Edge gateway and embedded PC registeration**.
3 Download the Bootstrap file for the group to which you want to register.
4 Copy the file into:
   - Snappy/Ubuntu Desktop Devices: **\root\config\ccm-wda** path on your device.
   - Windows Devices: **C:\config\ccm-wda** path on your device.
5 Restart the device.

Edge Device Manager Jobs

Edge Device Manager creates job for any task such as reboot, WOL and application policy that needs to be pushed to registered devices. Administrator can track the status of job by navigating to **Jobs** tab in Edge Device Manager web console. For more information, see *Edge Device Manager R15 Administrator's guide*.

Publishing application to Edge Gateway/Embedded PC devices

To push applications to Edge Gateway/Embedded PC, do the following:

Create and push Application Policy to Edge Gateway Devices

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

1 Select **Edge Gateway - Snappy** to add App to the inventory and click **Add App**.

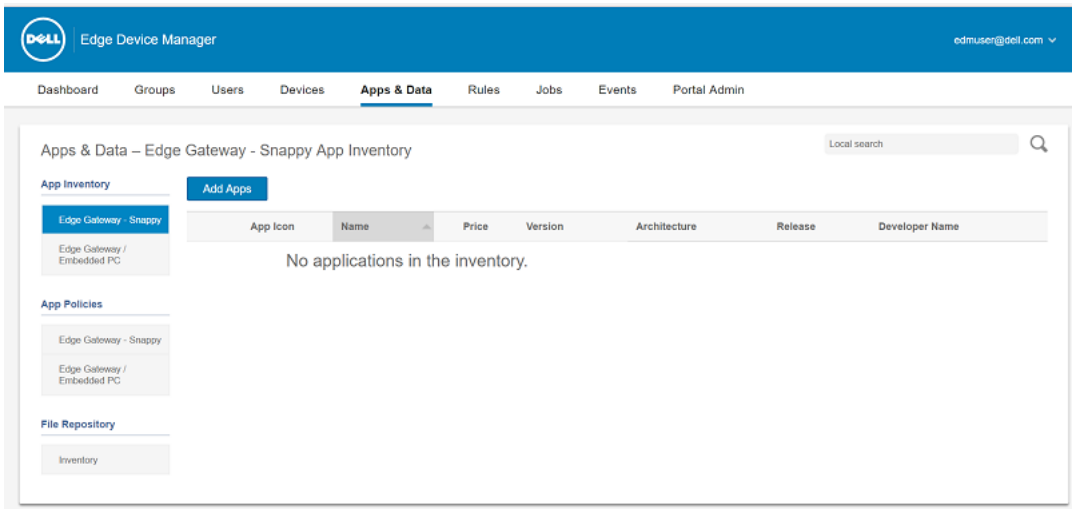

Figure 14.

2 Click the **Edge Gateway – Snappy** under **App Policies** in navigation menu on the left pane.

3 Click the **Add Policy** button.

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

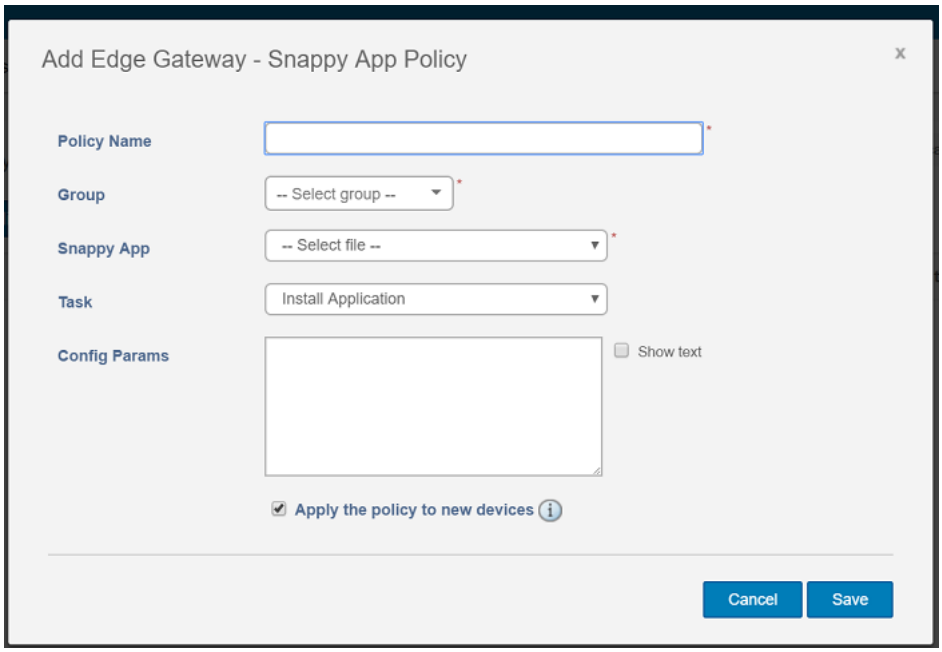

Figure 15.

a You must enter/select Policy Name, Group, Snappy App, Task and Config Params.

b Select **Apply the policy to new devices** if you would like to automatically apply this policy to device that is registered with Edge Device Manager and belongs to specified group or is moved to specified group.

5 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

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

7 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.

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

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

4

Uninstalling Edge Device Manager

To uninstall EDM, do the following:

1 Go to Add/Remove Programs and select Wyse Management Suite.
The uninstaller wizard is initiated, and the **EDM uninstaller** screen is displayed.

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

A

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 via 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 HW ports
- BIOS configuration

B

Supported devices

Supported devices

- Edge gateway 5000 running Windows 10 LTSB 15
- Edge gateway 3001 running Windows 10 LTSB 16
- Edge gateway 3002 running Windows 10 LTSB 16
- Edge gateway 3003 running Windows 10 LTSB 16
- Edge gateway 5000 running Ubuntu 16.04
- Edge gateway 3001 running Ubuntu 16.04
- Edge gateway 3002 running Ubuntu 16.04
- Edge gateway 3003 running Ubuntu 16.04
- 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 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 LTSB 15
- Embedded PC 5000 running Windows 10 Pro
- Embedded PC 3000 running Ubuntu 16.04
- Embedded PC 5000 running Ubuntu 16.04