



# SureMDM

## User Guide



The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of 42Gears Mobility Systems Pvt. Ltd

## Table of Content

<b>Introduction .....</b>	<b>8</b>
<b>Getting started with SureMDM.....</b>	<b>10</b>
Download and install SureMDM Nix Agent .....	10
Set up SureMDM Nix Agent on Android Devices.....	10
Download .....	10
Install .....	10
Configuring SureMDM Nix Agent Settings .....	11
Set up SureMDM Nix Agent on Windows devices .....	17
Download .....	17
Install .....	17
<b>Configuring SureMDM Nix Agent Settings .....</b>	<b>17</b>
Set up SureMDM Nix Agent on iOS devices.....	19
Download and Install.....	19
Configuring SureMDM Nix Agent Settings .....	19
Set up SureMDM Nix Agent on Android Wear devices.....	20
Download and install .....	20
Configuring SureMDM Nix Agent Settings .....	21
Set up SureMDM Nix Agent on Linux devices .....	25
Pre-requisite .....	25
Download and Install.....	25
Troubleshooting .....	28
Set up SureMDM Nix Agent on macOS Devices .....	28
Download and install .....	28
Login to SureMDM Web Console .....	29
New User Sign Up.....	29
Login as Existing User .....	30
<b>SureMDM Web Console.....</b>	<b>31</b>
<b>Approve the devices in the Web Console .....</b>	<b>33</b>
Unapproved.....	33
Preapproved.....	33
Blacklist the devices.....	34
Enrollment .....	35
Generate QR code for new device enrollment.....	35
Generate QR code for enrollment and assign it to a Group .....	36
Generate QR code for enrollment and name the device .....	36
<b>Home .....</b>	<b>38</b>

Device Groups .....	38
Create a new Group .....	39
Rename a Group .....	40
Delete a Group .....	40
Group Properties .....	41
Apply Job to a Group .....	42
Job Queue .....	42
Tags .....	43
Add a device to a tag .....	44
View devices under a tag .....	44
Device List .....	45
Right-Click Operations .....	45
Device Information Panel .....	48
Device Toolbar .....	49
Quick Action Toolbar .....	51
Utility Panel .....	55
System Log .....	56
<b>Dashboard.....</b>	<b>57</b>
<b>Inbox.....</b>	<b>58</b>
<b>Create and Deploy Jobs .....</b>	<b>59</b>
Jobs for Android .....	60
Install Application .....	60
File Transfer .....	62
Text Message.....	63
Run Script.....	64
Remote Data Wipe.....	65
Lock Device.....	65
Nix Agent Settings.....	66
Composite Job .....	67
Notification Policy .....	69
SureLock Settings .....	70
SureFox Settings.....	72
SureVideo Settings .....	73
Location Tracking.....	74
Security Policy.....	74
Password policy .....	75
Peripheral Settings.....	76
Application Settings.....	77

Wi-Fi/Hotspot Settings .....	78
Email Configuration Settings.....	79
Create an Email Account .....	79
Delete an Email Account.....	80
Telecom Management Policy.....	81
Call Log Tracking .....	82
SMS Log Tracking.....	83
Geo Fence.....	84
Time Fence .....	85
Network Fence .....	87
Remote Buzz.....	88
Compliance Job .....	89
Jobs for Windows.....	90
Install Application .....	90
File Transfer .....	91
Execute Program .....	92
Send Text Message .....	92
Run Script.....	93
Lock Device.....	94
Composite Job .....	95
Notification Policy.....	96
SureLock Settings .....	97
SureVideo Settings .....	98
Telecom Management Policy.....	99
Geo Fence.....	100
Time Fence .....	102
Wi-Fi Settings.....	103
Proxy Settings .....	104
FireWall Policy.....	105
Jobs for iOS .....	106
Geo Fencing.....	106
Data Usage Policy.....	107
Lost Mode.....	109
Push Custom Payload.....	110
Compliance Job .....	110
Reboot.....	112
Shut Down.....	112
Uninstall App .....	113

Time Fence .....	114
Nix Settings .....	115
Send Text Message .....	116
Jobs for Android Wear .....	117
File Transfer .....	117
Text Message .....	118
Run Script.....	119
Nix Agent Settings.....	119
Composite Job .....	121
Notification Policy .....	122
SureLock Settings .....	123
Location Tracking.....	124
Wi-Fi Settings .....	125
Telecom Management Policy.....	126
Call Log Tracking .....	128
SMS Log Tracking.....	128
Remote Buzz.....	129
Jobs for Linux .....	130
Run Script.....	130
File Transfer .....	131
<b>Profiles .....</b>	<b>132</b>
Profiles for Android.....	132
Create Android Work Profile and push it to the enrolled devices .....	132
Password Policy .....	132
System Settings .....	134
Application Policy .....	134
Network Settings .....	135
Certificate .....	136
Mail Configuration .....	137
Wi-Fi Configuration .....	138
File Sharing Policy .....	139
Profiles for iOS .....	140
Create iOS Profile and push it to the enrolled devices .....	141
Blacklist/Whitelist Apps .....	142
Web Content Filter .....	144
Branding .....	146
Passcode Policy .....	147
Single App Mode Profile.....	148

Restriction Profile .....	148
Application Policy .....	149
Configuration Profile.....	150
Wi-Fi Configuration .....	151
Mail Configuration .....	152
Global HTTP Proxy .....	153
VPN .....	154
Certificate .....	155
Exchange ActiveSync .....	156
File Sharing Policy .....	157
<b>Profiles for Windows .....</b>	<b>158</b>
Enroll devices to EMM Windows.....	158
Create Windows profile and push it to the enrolled devices .....	159
Password Policy .....	159
Mail Configuration .....	160
Restriction Policy.....	161
App Locker .....	162
Wi-Fi Configuration .....	163
VPN Configuration .....	164
Exchange Active Sync .....	165
Application Policy .....	165
Configuration Profile.....	166
Periodic App Launch .....	167
Certificate .....	167
File Sharing Policy .....	168
<b>Profiles for macOS .....</b>	<b>169</b>
Create macOS profile and push it to the enrolled devices.....	169
Blacklist/Whitelist Apps .....	171
Wi-Fi Configuration .....	172
Certificate .....	173
Passcode Policy .....	174
Mail Configuration .....	175
Exchange ActiveSync .....	176
<b>App Store .....</b>	<b>177</b>
App Store for Android.....	177
Create an Enterprise App Store .....	177
Create an Application Policy profile .....	178

Apply the created profile on desired devices .....	178
App Store for iOS .....	178
Create an Enterprise App Store .....	179
Create an Application Policy profile .....	179
Apply the created profile on desired devices .....	180
<b>File Store .....</b>	<b>181</b>
Upload the file(s) to File Store.....	181
Create a File Sharing Policy profile.....	181
Apply the created profile on desired Windows devices .....	182
<b>Reports.....</b>	<b>183</b>
On Demand Reports .....	183
Schedule Reports.....	185
Custom Reports .....	186
<b>Settings .....</b>	<b>188</b>
Device Enrollment .....	188
Account Settings .....	188
Branding Info.....	188
Device Enrollment Rules.....	189
Miscellaneous Settings .....	190
Single Sign-On .....	191
Alert Template.....	192
Customize Toolbar .....	192
Customize Nix/ SureLock.....	193
iOS Enrollment Settings .....	194
Certificate Management.....	194
Configure SCEP .....	195
User Management.....	195
Add a New User .....	196
Create Role-based Admin.....	200
Create Device Group based Admin .....	202
Create Job-based Admin .....	203
Create Column Set based Admin.....	204
License Management.....	206
Change Password.....	206
Logout .....	206

## Introduction

**SureMDM** is an intuitive and powerful unified endpoint management (UEM) solution for Android, iOS, Windows, macOS, wearOS and Linux platforms. It helps to secure, monitor and manage company owned devices for dedicated use as well as employee owned devices used to access company data (BYOD).

### Platform Support

- Android
- Windows
- iOS
- Android Wear
- Linux
- macOS

### Key Features

- Remote Support
- Android Scripting
- Composite Jobs
- Custom Reporting Tool
- Location Tracking
- Dashboard
- SureLock/SureFox compatibility
- iOS screen sharing
- Geo, Network and Time Fence



- Enterprise App and File Store
- Telecom Expense Management
- Device Grouping
- Two-Way Messaging
- Remotely monitor Device Health
- Silent installations without user interference
- Push Applications and Software Patches

## Getting started with SureMDM

To get started with **SureMDM**, follow these steps:

1. Download and install **SureMDM Nix Agent** on the device (**Android/ Windows/ iOS/ Linux/ Android Wear/ macOS**).
2. Login to **SureMDM Web Console**.

### Download and install SureMDM Nix Agent

#### Set up SureMDM Nix Agent on Android Devices

##### Download

**SureMDM Nix Agent** is downloaded as *Android Application Package file (.apk)* in the device from:

- [Google Play](#)
- [42Gears website](#)

##### Install

To install **SureMDM Nix Agent** on the device, follow these steps:

1. Search for **SureMDM Nix Agent** in the device and tap **Install**.
2. Once the installation is complete, tap **Get Started**.
3. Tap **Allow** on the permission prompts – Location/ Pictures and record video / Contacts / Phone calls / Media files / SMS messages.
4. Read the **Android Administrator Permissions** and tap **proceed**.
5. Read the request for Admin privileges and tap **Activate this device administrator**.

6. Under **Enter SureMDM Account ID**, enter the **Account ID** (Account ID will be sent to the registered email address after sign up) and tap **Register** or **Scan QR** to scan the QR code for [enrollment](#).
7. Go through the **Android Administrator Permissions** and tap **Proceed**.
8. On **Activate device administrator** prompt, tap **Activate**.

**SureMDM Home Screen** appears.

## Configuring SureMDM Nix Agent Settings

On **SureMDM Nix Agent Home Screen**, there are two options:

- **Settings** - Tap **Settings** to configure **Nix Agent Settings**
- **Mailbox** - Tap **Mailbox** to send/read /reply the messages from admin

Tap **Settings** to see the following options:

### 1. Enable Nix Service

This option allows the user to enable or disable the communication between **Nix Agent** and **SureMDM** account. This feature has to be disabled before making changes in the Nix settings.

### 2. Change Device Name

To change the **Device Name**, follow these steps:

1. **On SureMDM Nix Agent Home Screen, tap Settings.**
2. On **Settings** screen, tap **Change Device Name**.
3. Select one of the following options to set the Device Name:
  - **Set Device Name Manually** - Enter the Device Name in the field.
  - **Use IMEI Number** - IMEI number of the device is auto-populated in the field.

- **Use MAC Address-** MAC address of the device is auto-populated in the field.

4. Tap **Set Device Name** to display the **Device Name** in **SureMDM Web Console**.

### 3. Account ID

**Account ID** is the identification number for the **SureMDM** account. Tap on this option to change the **Account ID**.

### 4. Change Password

Password to access Nix Agent Settings can be changed using **Change Password** option.

To change the password, follow these steps:

1. Enter the **Old Password**
2. Enter **New Password** twice and tap **Change** to replace with the new password.



**Note:** Nix Agent password has no restrictions on the format.

### 5. Server Path

The user has the option to change the **Server Path**. By default, the **Server Path** will be **suremdm.42gears.com**.

### 6. Device ID

The **Device ID** generated by **SureMDM** server is a unique identification for the device.

### 7. Enable Admin

Once this option is enabled for the user, SureMDM admin will get following privileges on the device:

- Disable Camera
- Disable Lock Screen
- Encrypt Device

- Set Password Expiry
- Lock Device
- Set Password Restrictions
- Reset Device Password
- Set Device Proxy
- Monitor Unauthorized Login
- Wipe Device

## 8. Use https

Tap on this option to enable the use of **https** for secured connection.

## 9. Allow http fallback

Tap on this option to enable the use of **http** for unsecured connection.

## 10. Enroll Device Using QR Code

Tap on this option to scan the **QR** code and enroll the device to a **SureMDM** account.

To enroll QR Code, see [Enrollment](#).

## 11. SureMDM Nix Connectivity

The user has the following network connectivity options through which the device gets connected to the internet.

- **Any**
- **WiFi Only**
- **Mobile Data Only**

To configure **SureMDM Nix Connection** settings, follow these steps:

1. On **SureMDM Nix Agent** Home Screen, tap **SureMDM Nix Connectivity**.

2. On **Connection Settings** screen, tap **Connectivity Preference**.
3. Select **Connection Preference (Any/ WiFi Only/Mobile data Only)**.
4. Tap **Done**.
5. Enter **Connection Timeout** (in minutes).

Connection Timeout is the time period of non-connectivity of **SureMDM Nix Agent** with the internet. After this specified timeout, the device will restart **SureMDM Nix Agent** by itself.

6. Tap **Done** to complete.

## 12. Prefer Mobile Data

Select this option to use Mobile Data connection by default even if the device is connected to Wi-Fi network.

## 13. Schedule Reboot Settings

Select **Enable Schedule Reboot** to schedule the reboot of the device on selected days.

## 14. Change Polling Mechanism

In Polling Mechanism, the processor periodically checks each of its input and output devices to see if any of them have a request that it needs to handle.

To change the Polling Mechanism, tap **Change Polling Mechanism** and select from following options:

- Normal Polling
- Periodic Polling

## 15. Application Lock PIN

The user has the option to lock the applications by configuring a pin for all the installed applications on the device. **Application Lock PIN** helps the user to change the Lock PIN for these installed applications.

## 16. Remote Support Diagnostic

Select this option to allow the **SureMDM** to remote into the selected device.

## 17. Android Enterprise

Once the **SureMDM** account is enrolled with **Android Enterprise**, the device also needs to get enrolled with **Android Enterprise**.

To enable Android Enterprise on the device, navigate to **SureMDM Nix** home screen, select **Settings > Android Enterprise > Enroll your device**.

Android Enterprise can be enrolled for two different profiles:

- [BYOD profile](#)
- [COSU profile](#)

## 18. Mailbox

Select this option to show **Mailbox** option on the **SureMDM Nix Home Screen**.

## 19. Keep CPU On

Enable **Keep CPU On** option will keep **SureMDM Nix Agent** running all the time.

## 20. Enable Log

Select this option to record the SureMDM Nix Agent activities on the device in the form of logs.

## 21. User Privacy

Admins can select the following options under **User Privacy** and select **Done**.

- Unattended Remote Support
- Unattended Location Tracking
- Unattended Call Log Tracking
- Unattended SMS Log Tracking
- Show Download Notification(s)
- Text to Speech
- Disable Reply Button
- Disable Close Button

## 22. Ignore Block Mobile Data Till Next Cycle

Select this option to ignore blocking of mobile data even if mobile data usage exceeds for the current cycle.

## 23. Agent Version

**Agent Version** shows the version of installed **SureMDM Nix Agent**.

## 24. Uninstall SureMDM Nix

Tap on this option to uninstall **SureMDM Nix Agent** from the device.

## 25. Deregister Suremdm Nix

Deregister device from the current **SureMDM** server.

## 26. Import/Export Settings

Use this option to export the current Nix Agent settings to a File or cloud. This option can also be used to import settings from Cloud or file.



Admins can use exported settings to Cloud and create a QR code for quick and easy configuration.

## Set up SureMDM Nix Agent on Windows devices

### Download

**SureMDM Nix Agent** is downloaded as a *nix\_installer\_win* file (.exe) on the device from [42Gears Website](#).

### Install

To install **SureMDM Nix Agent** on the device, tap on the downloaded *nix\_installer\_win.exe* file and tap **Install**. On successful installation, tap on the **Nix Agent** icon and **SureMDM Nix Agent Home Screen** will appear.

## Configuring SureMDM Nix Agent Settings

On **SureMDM Nix Agent Home Screen**, there are two options:

- **Settings** - Tap the **Settings** to configure **Nix Agent Settings**
- **Mailbox** – Tap **Mailbox** to send/read /reply the messages from admin

Tap **Settings** to see the following options:

### 1. Enable Nix Service

This option allows the user to enable or disable the communication between **Nix Agent** and **SureMDM** account. This feature has to be disabled before making changes in the Nix settings.

## 2. Change Device Name

To change the **Device Name**, follow these steps:

1. On **SureMDM Nix Agent Home Screen**, tap **Settings**.
2. On **Settings** screen, tap **Change Device Name**.
3. Select one of these options to set as **Device Name**:
  - **Set Device Name Manually** – Enter the device name in the box
  - **Use MAC Address**- MAC address of the device is auto-populated in the box
4. Tap **Set Device Name** to display the **Device Name** on the **SureMDM** Web Console.

## 3. Account ID

**Account ID** is the identification number for the **SureMDM** account. Tap this option and enter new **Account ID** and tap **Ok**.

## 4. Server Path

The user has the option to change the **Server Path**. By default, the **Server Path** will be **suremdm.42gears.com**.

## 5. Device ID

The **Device ID** generated by **SureMDM** server is a unique identification for the device.

## 6. Use https

Tap on this option to enable the use of **https** for secured connection.

## 7. Mailbox

Select this option to show **Mailbox** option on the **SureMDM Nix Home Screen**.

## 8. Agent Version

**Agent Version** shows the version of installed **SureMDM Nix Agent**.

## Set up SureMDM Nix Agent on iOS devices

### Download and Install

To download and install **SureMDM Nix Agent**, follow these steps:

1. Download and install **SureMDM Nix Agent** from **App Store**.
2. Once installed, launch **SureMDM Nix Agent**.
3. On **SureMDM Nix** Welcome Screen, tap **Enroll Device**.
4. On **Enroll Device** screen, select one of the following two options:
  - **Register** - If admins want to use the **Account ID** and register manually (**Account ID** will be sent to the user's registered email address after sign up)
  - **Scan QR** - Use this option if admins want to log into **SureMDM Web Console** directly and use **Enrollment** option to scan QR code and configure the **Nix Agent**.
5. On **Install Profile** screen, tap **Install**.
6. Once profile installed, tap **Done**.

On successful configuration, **SureMDM Nix Home Screen** should show **Online** and in [SureMDM Web Console](#), the device gets listed under **Unapproved** list.

### Configuring SureMDM Nix Agent Settings

On **SureMDM Nix Agent Home Screen**, there are two options:

- **Online** – On successful enrollment of device in the **SureMDM** console, the status of the device in **Nix** will show as **Online**.
- **Mailbox** - Tap **Mailbox** to send/read /reply the messages from admin.

Tap **Settings** to see the following options:

### 1. **Server Path**

By default, the **Server Path** will be **https://suremdm.42gears.com**.

### 2. **Location Tracking Status**

Enable **Location Tracking** to allow **SureMDM** admin to remotely track the device location.

### 3. **How to use Location tracking with SureMDM**

Tap on this option to play a short video on location tracking.

### 4. **Background App Refresh**

Allows **SureMDM Nix** agent to run in the background even when the user is not using it.

### 5. **Location Services**

Allows **SureMDM Nix** agent to fetch approximate device location from iOS Location Services.

### 6. **Version**

**Version** displays the version of installed **SureMDM Nix Agent**.

## Set up SureMDM Nix Agent on Android Wear devices

### Supports

Android Smartwatch version 1.0-1.5,2.0,2.6

### Download and install

**SureMDM Nix for Smartwatches** can be downloaded from the following source:

- [Google Play](#)

Download the application on Android smartwatch.

To install **SureMDM Nix for Smartwatches** on the device, follow these steps:

1. Search for **SureMDM Nix for Smartwatches** application on the device and tap **Install**.
2. Once the installation is complete, tap **Open**.
3. Tap **Allow** on the permission prompts to access the following options: Device Location/ Pictures and record video / Contacts / Phone calls / Media files / SMS messages.
4. On **SureMDM Wear Device Management** prompt, tap **Get Started**.
5. Under **Enter SureMDM Account ID**, enter the **Account ID** (Account ID will be sent to the registered email address after sign up) and tap **Register**.
6. On **Configure Device Name** prompt, select an option from the following to configure the device name:
  - Set device name manually
  - Use IMEI number
  - Use MAC address
  - Use system generated name

On successful configuration, **SureMDM Nix Home Screen** should show **Online** and in [SureMDM Web Console](#), the device gets listed under **Unapproved** list.

### Configuring SureMDM Nix Agent Settings

On **SureMDM Nix Agent Home Screen**, there are two options:

- **Settings** - Tap the **Settings** to configure **Nix Agent Settings**
- **Mailbox** - Tap **Mailbox** to send/read /reply the messages from admin

Tap **Settings** to see the following options:

## 1. Enable Nix Service

This option allows the user to enable or disable the communication between **Nix Agent** and **SureMDM** account. This feature has to be disabled before making changes in the Nix settings.

## 2. Change Device Name

To change the **Device Name**, follow these steps:

1. On **SureMDM Nix Agent Home Screen**, tap **Settings**.
2. On **Settings** screen, tap **Change Device Name**.
3. Select one of the following options to set the **Device Name**:

**Set Device Name Manually** - Enter the Device Name in the field.

**Use IMEI Number** - IMEI number of the device is auto-populated in the field.

**Use MAC Address**- MAC address of the device is auto-populated in the field.

4. Tap **Set Device Name** to display the **Device Name** in **SureMDM Web Console**.

## 3. Account ID

**Account ID** is the identification number for the **SureMDM** account. Tap on this option to change the **Account ID**.

## 4. Change Password

Password to access Nix Agent Settings can be changed using **Change Password** option.

To change the password, follow these steps:

1. On **SureMDM Nix Agent Home Screen**, tap **Settings**.
2. On **Settings** screen, tap **Change Password**.
3. Enter the **Old Password**.
4. Enter **New Password** twice and tap **Change** to replace with the new password.



**Note:** Nix Agent password has no restrictions on the format.

## 5. Server Path

The user has the option to change the **Server Path**. By default, the **Server Path** will be **suremdm.42gears.com**.

## 6. Device ID

The **Device ID** generated by **SureMDM** server is a unique identification for the device.

## 7. Use https

Tap this option to enable the use of https for secured connection.

## 8. SureMDM Nix Connectivity

The user has the following network connectivity options to choose from to get connected to the internet.

- **Any**
- **WiFi Only**
- **Mobile Data Only**

To configure **SureMDM Nix Connection** settings, follow these steps:

1. On **SureMDM Nix Agent Home Screen**, tap **SureMDM Nix Connectivity**.
2. On **Connection Settings** screen, tap **Connectivity Preference**.
3. Select **Connection Preference (Any/ WiFi Only/Mobile data Only)**.
4. Tap **Done**.
5. Enter **Connection Timeout** (in minutes).

Connection Timeout is the time period of non-connectivity of **SureMDM Nix Agent** with the internet. After this specified timeout, the device will restart **SureMDM Nix Agent** by itself.

6. Tap **Done** to complete.

## 9. Change Polling Mechanism

In Polling Mechanism, the processor periodically checks each of its input and output devices to see if any of them have a request that it needs to handle.

To change the Polling Mechanism, tap **Change Polling Mechanism** and select from following options:

- Normal Polling
- Periodic Polling

## 10. Mailbox

Select this option to show **Mailbox** option on the **SureMDM Nix Home Screen**.

## 11. Keep CPU On

Enable **Keep CPU On** option will keep **SureMDM Nix Agent** running continuously on the Smartphone.

## 12. Enable Log

Select this option to record the log information of the device in **SureMDM Web Console**.

## 13. Agent Version

Agent Version option displays the version of installed **SureMDM Nix Agent**.

## 14. Uninstall SureMDM Nix

Tap on this option to uninstall **SureMDM Nix Agent** from the device.

## 15. Deregister Suremdm Nix

Deregister device from the **SureMDM** server.

## 16. Import/Export Settings

Use this option to export the current **Nix Agent** settings to a File or Cloud. This option can also be used to import settings from Cloud or file.



## Set up SureMDM Nix Agent on Linux devices

### Pre-requisite

Open JDK 7 OR above. Refer to <http://openjdk.java.net/install/> for details

or

Oracle JDK 7 OR above. Refer to


<http://www.oracle.com/technetwork/java/javase/downloads/index.html> for details

### Download and Install

To download and install **SureMDM Nix Agent**, follow these steps:

1. Download **SureMDM Nix Agent** from website using the below command.

```
wget https://suremdm.42gears.com/nix/nix.tar.gz
```



```
suremdm@ubuntu:~/Desktop$ wget https://suremdm.42gears.com/nix/nix.tar.gz
--2017-06-30 10:58:57-- https://suremdm.42gears.com/nix/nix.tar.gz
Resolving suremdm.42gears.com (suremdm.42gears.com)...
Connecting to suremdm.42gears.com (suremdm.42gears.com)| |:443... connect
HTTP request sent, awaiting response... 200 OK
Length: 3230520 (3.1M) [application/x-gzip]
Saving to: 'nix.tar.gz'

nix.tar.gz          100%[=====]
2017-06-30 10:59:48 (122 KB/s) - 'nix.tar.gz' saved [3230520/3230520]

suremdm@ubuntu:~/Desktop$
```

2. Use the below command to extract tar file:

```
tar -xvzf nix.tar.gz
```

```

nix/
nix/app/
nix/app/nix.jar
nix/app/nix.conf
nix/app/lib/
nix/app/lib/jetty-client-9.2.23.v20171218.jar
nix/app/lib/jetty-http-9.2.23.v20171218.jar
nix/app/lib/websocket-common-9.2.23.v20171218.jar
nix/app/lib/jna-platform-4.5.1.jar
nix/app/lib/commons-io-2.5.jar
nix/app/lib/elfinder.jar
nix/app/lib/websocket-api-9.2.23.v20171218.jar
nix/app/lib/slf4j-simple-1.7.25.jar
nix/app/lib/oshi-core-3.4.4.jar
nix/app/lib/commons-exec-1.3.jar
nix/app/lib/jna-4.5.1.jar
nix/app/lib/commons-codec-1.10.jar
nix/app/lib/gson-2.8.2.jar
nix/app/lib/threetenbp-1.3.6.jar
nix/app/lib/slf4j-api-1.7.25.jar
nix/app/lib/jetty-util-9.2.23.v20171218.jar
nix/app/lib/jetty-io-9.2.23.v20171218.jar
nix/app/lib/websocket-client-9.2.23.v20171218.jar
nix/app/nixr.jar
nix/pilot/
nix/pilot/probe.jar
nix/installnix.sh
nix/legacy/
nix/legacy/sysvinit.sh
nix/legacy/remotesupport_fix.sh
nix/legacy/nix
nix/legacy/nixr
nix/bootstrap/
nix/bootstrap/nixr.service
nix/bootstrap/nix.service
nix/bootstrap/systemd.sh
nix/canontcal/
nix/canontcal/nix.conf
nix/canontcal/nixr.conf
nix/canontcal/upstart.sh
[sudo] password for [redacted]

```

3. Install **SureMDM Nix Agent** using the below command.

**Command for SaaS:** `sudo ./nix/installnix.sh [-y] [-c<Account Id>]`

where

- y is assumed to be **Always yes** while upgrading Nix agent.

- c is **Customer ID**

**Example:** `sudo nix/installnix.sh -y -c1111111`

```

[~]$ sudo nix/installnix.sh -y -c
[sudo] password for sowmya:
SureMDM Nix Installer version 1.06
Found systemd init system.
Assuming YES for all prompts
Customer Id = 031800581
Assuming SureMDM Server = https://suremdm.42gears.com
Server = suremdm.42gears.com
Use HTTPS = true
Nix files will be installed to /usr/share/java/nix
Overwriting existing Nix installation
Customer Id : 031800581
SureMDM Server : https://suremdm.42gears.com
https://suremdm.42gears.com is running
Proceeding Nix installation
Environment Variables for Remote Support are: /home/sowmya/.Xauthority AND :0
● nix.service - SureMDM Nix Agent
   Loaded: loaded (/lib/systemd/system/nix.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2018-04-12 14:38:00 IST; 33ms ago
   Main PID: 7066 (java)
   CGroup: /system.slice/nix.service
           └─7066 /usr/bin/java -jar /usr/share/java/nix/nix.jar

Apr 12 14:38:00 sowmya-Inspiron-3542 systemd[1]: Started SureMDM Nix Agent.
● nixr.service - Remote Support Agent for Nix
   Loaded: loaded (/lib/systemd/system/nixr.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2018-04-12 14:38:00 IST; 13ms ago
   Main PID: 7076 (java)
   CGroup: /system.slice/nixr.service
           └─7076 /usr/bin/java -jar /usr/share/java/nix/nixr.jar

Apr 12 14:38:00 sowmya-Inspiron-3542 systemd[1]: Started Remote Support Agent for Nix.
Installation Complete
  
```

**Command for On Premise:** `sudo /nix/installnix.sh [-y] [-<Account Id>] [-s"<Server Path>"]`

where

- **y** is assumed to be **Always yes** while upgrading Nix agent.
- **c** is the **Customer ID**
- **s** is the **SureMDM server path**

Example: `sudo nix/installnix.sh -y -c11111 -s"http://0.0.0.0/suremdm"`

```

[~]$ sudo nix/installnix.sh -y -c -s"https://
SureMDM Nix Installer version 1.06
Found systemd init system.
Assuming YES for all prompts
Customer Id =
SureMDM Server = https://suremdm.42gears.com
Server = suremdm.42gears.com
Use HTTPS = true
Nix files will be installed to /usr/share/java/nix
Overwriting existing Nix installation
Customer Id :
SureMDM Server : https://suremdm.42gears.com
https://suremdm.42gears.com is running
Proceeding Nix installation
Environment Variables for Remote Support are: /home/sowmya/.Xauthority AND :0
● nix.service - SureMDM Nix Agent
   Loaded: loaded (/lib/systemd/system/nix.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2018-04-05 17:40:33 IST; 33ms ago
   Main PID: 27130 (java)
   CGroup: /system.slice/nix.service
           └─27130 /usr/bin/java -jar /usr/share/java/nix/nix.jar

Apr 05 17:40:33 sowmya-Inspiron-3542 systemd[1]: Started SureMDM Nix Agent.
● nixr.service - Remote Support Agent for Nix
   Loaded: loaded (/lib/systemd/system/nixr.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2018-04-05 17:40:33 IST; 12ms ago
   Main PID: 27140 (java)
   CGroup: /system.slice/nixr.service
           └─27140 /usr/bin/java -jar /usr/share/java/nix/nixr.jar

Apr 05 17:40:33 sowmya-Inspiron-3542 systemd[1]: Started Remote Support Agent for Nix.
Installation Complete
  
```



**Note:** Enter Linux user password if password prompt appears during this process.

**SureMDM Nix Agent** will get installed on the Linux machine and will be enrolled to **SureMDM Web Console**.

## Troubleshooting

1. wget command: In case 'wget' command is not installed, please use the below command.

**Command:**

```
sudo apt-get install wget
```

Or

```
sudo yum install wget
```

2. Below mentioned are the commands helpful in managing and monitoring SureMDM Nix agent

- a. **To check SureMDM Nix Agent service status:** `sudo service nix status`
- b. **To start SureMDM Nix agent:** `sudo service nix start`
- c. **To stop SureMDM Nix agent:** `sudo service nix stop`
- d. **To restart SureMDM Nix agent:** `sudo service nix restart`

## Set up SureMDM Nix Agent on macOS Devices

### Download and install

**SureMDM Nix Agent** can be downloaded as **.pkg** on the device from the following link:

- [Download](#)

To install **SureMDM Nix Agent**, follow these steps:

1. Once **SureMDMNix** is downloaded, double-click on the **.pkg** file to launch **Nix Agent Installer**.
2. In **Installer** window, go through each step one by one starting from **Introduction** to **Summary**.  
**SureMDM Nix Agent** will get installed on the device.
3. Click **Nix Agent** icon to launch **Enroll Device** prompt.
4. On **Enroll Device** prompt, enter **SureMDM Account ID** and click **Register**.

The device will get enrolled to **SureMDM Web Console**.

5. On **SureMDM Nix** screen, there are two options available :

**Status** - Once the device is enrolled to **SureMDM**, the status will show as **Online** .

**Settings** - Under **Settings** option, there are two features:

**Server Path** - Enter the **Server Path** (before clicking on **Register** if server path is apart from <https://suremdm.42gears.com>)

**Version** - Displays the **SureMDM Nix Agent** version

## Login to SureMDM Web Console

Two types of users can login to **SureMDM Web Console**:

- New User Sign up
- Login as Existing User

### New User Sign Up

To login into **SureMDM Web Console** as a new user, follow these steps:

1. Launch browser on the device.

2. Access [SureMDM Web Console](#).
3. On the **SureMDM** login page, click **Signup**.
4. Enter the **Email ID, Password, Confirm Password** and click **Next**.
5. Enter the required details and select **I accept terms and conditions**.
6. Click **Sign Up**.

A link for activation will be sent to the registered mail id with the **Account ID**.

7. Click on the link to navigate to the **SureMDM** Login Page. To login to **SureMDM Web Console**, use steps under [Login as Existing User](#).

## Login as Existing User

To login into **SureMDM Web Console** as an existing user, follow these steps:

1. Launch browser on the device.
2. Access [SureMDM Web Console](#).
3. On **SureMDM** login page, enter the **User Name, Password** and click **Login**.

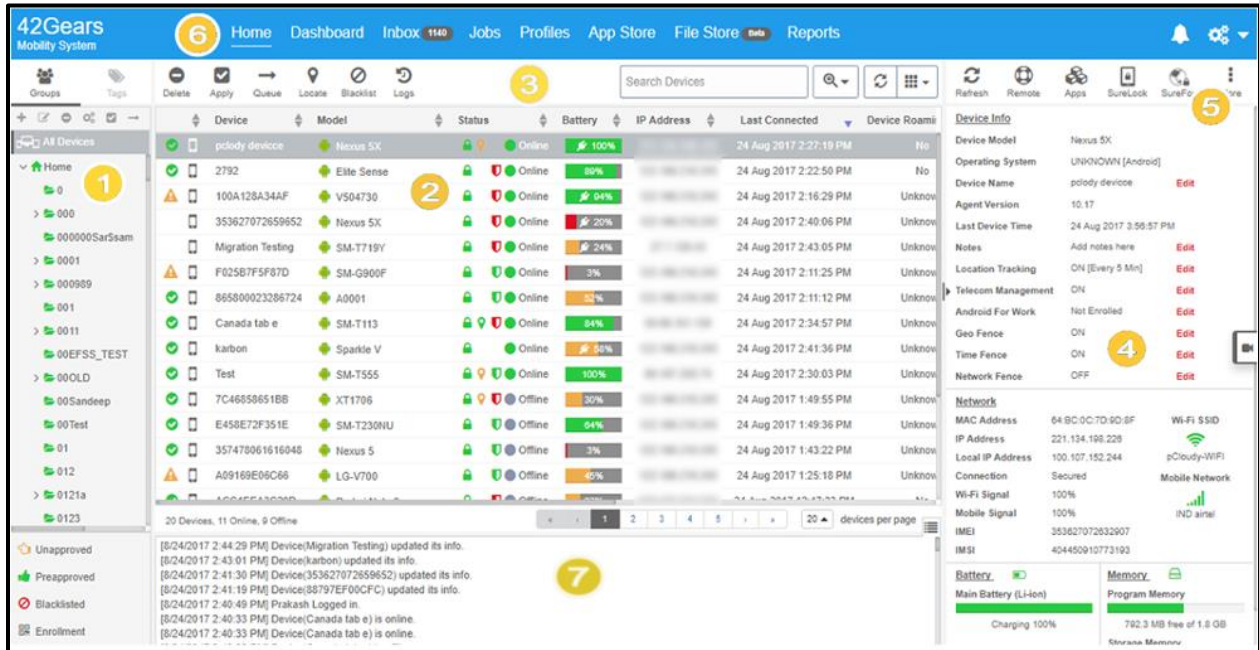
**SureMDM Web Console** page appears.



**Note:** *If the user enters wrong credentials for 10 times continuously, then the account will get blocked for 30 minutes.*



















# SureMDM Web Console

**SureMDM Web Console** is a web-based console which provides a centralized view of all enrolled devices and allows the admins to remotely manage these devices.



- 1. [Device Groups/Tags](#)
- 2. [Device List](#)
- 3. [Device Toolbar](#)
- 4. [Device Information Panel](#)
- 5. [Quick Action Toolbar](#)
- 6. [Utility Panel](#)
- 7. [System Log](#)

The description of visual indicators in the web console are given in the following table:

Icons	Description
<p><b>Device Groups</b></p>    	<p>Unapproved</p> <p>Pre-approved</p> <p>Blacklisted</p> <p>Enrollment</p>
<p><b>Jobs Status</b></p>   	<p>Jobs successfully deployed</p> <p>Jobs pending to push</p> <p>Jobs deployed with error</p>
<p><b>Device Status</b></p>        	<p>Secured Connection</p> <p>Tracking On, Location latest available</p> <p>Tracking On, Location available</p> <p>Tracking On, Location not available</p> <p>Device secured with SureLock</p> <p>Device Unsecured. SureLock is not running</p> <p>Online</p> <p>Offline</p>
<p><b>Battery Status</b></p>   	<p>Above 80%</p> <p>Less than 60%</p> <p>Less than 20%</p>



## Approve the devices in the Web Console

The devices need to get enrolled to the web console that enables the admin to remotely manage and control them. When a new device is enrolled, it either reflects under **Unapproved** / **Preapproved** option.

### Unapproved

Once the Nix Agent is configured with an **Account ID** and **Nix service is enabled** on a device, admin can see the devices awaiting approval under **Unapproved** list.

To approve a device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **Device Groups** section, click **Unapproved** (Unapproved devices are indicated by a notification badge).
3. **Unapproved** screen will have following details:
  - Device Name
  - Model
  - Platform
  - Last Connected
4. Select the device and click **Approve**.

The approved device will get added to the device list.

### Preapproved

Devices can be enrolled in two ways in **Preapproved** page:

- Once **Automatically approve all devices** under **Preapproved** option is selected on the console and from the device **Nix Settings, Account ID, SureMDM path** is entered and **Nix service** is enabled, the devices will get automatically approved without reflecting under **Unapproved** section.
- **SureMDM** makes it easy by allowing importing a list of pre-approved devices details.

To enroll the device using import preapproved list, follow these steps:

1. Login to **SureMDM Web Console**.
2. Under **Device Groups** section, click **Preapproved**.
3. On **Preapproved** page, select/ deselect **Automatically approve all devices** and click **Download Preapprove Template**.

A template in **CSV** format will download.

4. Fill the list of device details in the **CSV** file.
5. Click **Import**.

Preapproved list or **CSV** file will get imported to the console.

6. On the device, enter the **Account ID, SureMDM Path** and enable **Nix service** in **SureMDM Nix Agent Settings**.

Whenever a new device is enrolled, **SureMDM** checks with the preapproved list and approves the device automatically without reflecting under **Unapproved** section, if listed in the preapproved list.

## Blacklist the devices

**Blacklisted** section of web console will have the list of enrolled devices that are blacklisted from the **Device List**. Such devices will not have any communication with the **SureMDM** account.

To blacklist a device, follow these steps:

1. Login to **SureMDM Web Console**.
2. Select the device from **Device List**.
3. Click **Blacklist** from the **Device Toolbar**.
4. Click **Yes** to complete.

The devices will be moved to the **Blacklisted** section under **Device Groups**.



**Note:** i. The blacklisted device can be whitelisted to **Device List** by selecting **Whitelist** option.

ii. To whitelist the device, go to **Blacklisted Device** section, select the device and click **Whitelist**.

## Enrollment

Enrollment section has the options to

- Generate QR code for new device enrollment
- Generate QR code for enrollment and assign it to a Group.
- Generate QR code for enrollment and name the device

### Generate QR code for new device enrollment

If the **Nix Agent** is configured without **Account Id**, then the new device enrollment can be done through scan **QR Code**.

To enroll a new device in the web console, follow these steps:


1. On successful login to web console, below **Groups**, click **Enrollment**.

A **QR Code** will appear.

2. Scan the QR code from the device.


The device gets enrolled in the web console.

or

1. On successful login to the web console, click  **Settings** located at top right of the console.
2. Select **Device Enrollment** from the drop-down menu.  
A **QR Code** will appear.
3. Scan the **QR** code from the device.  
The device gets enrolled in the web console.


## Generate QR code for enrollment and assign it to a Group

To enroll and assign the device to a group, follow these steps:

1. On successful login to the web console, click  **Settings** located at top right of the console.
2. Select **Device Enrollment** from the drop-down menu.
3. Scan the **QR** code from the device.
4. Click **Options**.
5. On **Device Enrollment** prompt, select a group and click **Generate QR Code**.
6. Scan the **QR** code from the device.

## Generate QR code for enrollment and name the device

To enroll and name the device, follow these steps:

1. On successful login to the web console, click  **Settings** located at top right of the console.
2. Select **Device Enrollment** from the drop-down menu and click **Options**.

3. On **Device Enrollment** prompt, **Select Device Name** from the drop-down menu and click **Generate QR Code**.



**Note:** Naming the device option is available only for **Android** devices.

A **QR Code** will appear.

4. Scan the **QR** code from the device.



**Note:** To download and print the **QR Code**, click **Download** and **Print** options.

## Home

On successful login to **SureMDM Web Console**, by default the console opens with **Home** tab.

**Home** tab consists of following options:

Device Groups

Tags

Device List

Device Toolbar

Device Information Panel

Quick Action Toolbar

Utility Panel

System Logs

Settings

## Device Groups








Devices can be assigned to one or more groups or subgroups. Creating **Device Groups** is very helpful when the admins want to push job(s) to multiple devices or to a group with just a single click.

Created groups and subgroups are listed under **Home** section of the **Device Groups**.




**Note:** A single device can be assigned to only a single group.

The description of icons in the **Device Group** is given in the following table:

Buttons	Description
 <b>Add</b>	Add a new group
 <b>Rename</b>	Rename the group
 <b>Delete</b>	Delete the group
 <b>Properties</b>	<p>View group properties details such as total number of devices under a group, total number of subgroups under a group, total devices in the current group, total number of devices that are online, total number of devices that are online in the current group and ping all devices will convert all offline devices to online in a group.</p> <p> <b>Note:</b> <i>Ping All Devices</i> option is applicable only for GCM devices.</p>
 <b>Apply</b>	Push the job(s) to the selected group
 <b>Job Queue</b>	View Job Queue of a group

## Create a new Group

To create a new group and assign devices to the group, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **Device Groups** section, click  .
3. On **New Group Name** prompt, enter the desired name and click **OK**.

The newly created group will get listed under **Home**.

4. There are two ways to move the devices to a group:

- Drag and drop the devices from **Device List** to the group.

or


- Select and right-click the device(s), click **Move to Group** option from the context menu.



**Note:** Alternate option to create a new group is to right-click the selected group or subgroup and click **Add**.

## Rename a Group

To rename a group, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **Device Groups** section, select the group and click .

The existing group name will get displayed in the **New Group Name** field.


3. On **Rename existing group** prompt, clear the existing group name and enter the desired name in **New Group Name** field and click **OK**.



**Note:** Alternate option to **Rename a Group** is to right-click on the group or subgroup and select **Rename**.

## Delete a Group

To delete a group, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **Device Group** section, select a group.
3. Click  to delete a group or subgroup.
4. On the confirmation prompt, click **Ok** to complete.






**Note:** i. Deleting a group will delete the devices in the group and its subgroups.

ii. Alternate option to **Delete a Group** is to right-click a group or subgroup and select **Delete**.

## Group Properties

To view total number of devices and subgroups in a group, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **Device Groups** section, click and select a group.
3. Click  to launch **Group Properties** prompt.
4. **Group Properties** prompt will have the following options:
  - **Total Devices** - Number of devices in a group
  - **Total Subgroups** - Number of subgroups in a group
  - **Total Devices in Current Group** - Number of devices in the current group
  - **Total Online** - Number of devices that are online in the group
  - **Total Online in Current Group** - Number of devices that are online in the current group
  - **Default Jobs** - Jobs that are automatically pushed to the devices enrolled in a group by default



**Note:** i. In **Default Jobs**, the user has options to add or delete the jobs.

ii. The group color turns blue when default jobs are added to a group.


5. Click **Ok** to complete.



**Note:** Alternate option to access **Group Properties** is to right-click a group or subgroup and select **Properties**.

## Apply Job to a Group

To push job(s) to a group at a scheduled time, follow these steps:

1. On **SureMDM Web Console**, select a group.
2. Click  from the **Device Toolbar**.
3. On **Apply Job To Group** prompt, select the job(s) from the list.
4. Select **Configure Schedule Time** to launch **Schedule Job** prompt.
5. Select an option for **Push the job to device**:
  - **Immediately**
  - **Periodically**
  - **Schedule Days and Time**
  - **Schedule Date and Time**



**Note:** *Immediately* option is selected by default.


6. Click **Apply** to complete.




**Note:** *Alternate option to push a job to a group or subgroup, right-click a group or subgroup and select **Apply**.*

## Job Queue

If the job is applied to the device and the device is online then the job gets pushed to the device(s) immediately. If the device is offline, the job will get queued in **Job Queue** section with the **Status** as **Pending**.

Click  on **Device Toolbar** to view the status of the jobs. The status of the jobs are categorized as the following:


**Pending** - Jobs that are paused or queued. Also, admin has an option to Re Apply  the pending / error jobs.

**Success** - Jobs that are pushed to the group successfully

**Failed** - Jobs that are failed to be applied to the device

The **Pending** jobs can be reapplied once the device comes online.

To re-apply the job, follow these steps

1. On **SureMDM Web Console**, select a group from the **Device Group**.
2. Click  from the **Device Toolbar**.
3. On **Job Queue** prompt under **Pending** section, select a job from the list and click **Retry**.
4. Select **Configure Schedule Time** to launch **Schedule Job** prompt.



**Note:** i. Alternate option to view the job status is to right-click a group or subgroup and select **Job**

**Queue.**

ii. The jobs under the status (*Pending / Success / Failed*) can be deleted from the list using





**Remove Job.**

## Tags

Tagging in **SureMDM** allows admins to create tags and assign multiple tags to a single device.

Admins can easily categorize and view list of all the devices with a particular tag and push jobs to this list.

The description of icons in **Tags** section is given in the following table:

Buttons	Description
 <b>Add</b>	Add a new tag
 <b>Rename</b>	Rename the tag
 <b>Delete</b>	Delete the tag
 <b>Apply</b>	Push the job(s) to the selected tag

## Add a device to a tag

To add a device to a tag, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web console**, select and right-click the desired device from **Device List**.
3. Click **Tag** from the context menu.
4. On **Tag List** prompt, select from the existing tags or create a new tag by entering a new name in **Create Custom Tag** field.
5. Click **Save** to complete.

## View devices under a tag

To view a tag, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Home >Tags**.
3. Under **Tags** section, click the desired tag to view the list of devices.

## Device List

**Device List** section displays a list of enrolled devices with their details in a tabular format.

At the bottom of the **Device List**, following options are displayed:

- Total Number of devices in the device list
- Number of online and offline devices
- Page navigation
- Select to display **Devices per page (20/50/100)**


















Device	Model	Status	Battery	IP Address	Last Connected	Device Roaming	Signal	Agent Version
ASB100010CBA1	SM-T350	Offline	41%		4 Dec 2017 4:32:48 P...	Unknown	0	10.80
42gears-getsoft	SmartTab1	Online	100%		4 Dec 2017 4:05:08 P...	Unknown	0	10.62
3544	SM-T285YD	Offline	33%		4 Dec 2017 3:55:03 P...	Unknown	0	10.80
911554050020788	Elite Sense	Online	98%		4 Dec 2017 4:21:01 P...	No	100	10.22
3537	SM-T230NU	Online	38%		4 Dec 2017 4:20:59 P...	Unknown	0	10.81
3547	DL-Axist	Offline	5%		4 Dec 2017 3:47:55 P...	Unknown	0	9.45
firewall blocking	SM-G930F	Online	82%		4 Dec 2017 3:43:23 P...	Unknown	0	10.22
3538	V400414	Online	49%		4 Dec 2017 4:29:45 P...	No	89	10.81
DESKTOP-BDJJQR4	Inspiron 15-3567	Offline	98%		4 Dec 2017 2:14:43 P...	Unknown	N/A	1.3
100A128A34AF	V504730	Offline	27%		4 Dec 2017 1:58:27 P...	Unknown	0	10.81
0027155094AA	V455120	Offline	22%		4 Dec 2017 12:58:37 ...	Unknown	0	9.45
42Gears Test	iPad Air 16 GB S...	Offline	100%		4 Dec 2017 12:43:29 ...	Unknown	N/A	3.1
sandhya	XT1088	Offline	34%		4 Dec 2017 12:42:04 ...	No	88	10.22
088E01732398	VSD220	Offline	100%		4 Dec 2017 12:38:42 ...	Unknown	0	9.45
3075121B1D39	D2105	Offline	7%		4 Dec 2017 12:13:13 ...	No	0	9.45
Tab	IdeaTabA 1000L-F	Offline	2%		4 Dec 2017 11:50:22 ...	Unknown	0	9.45
3533	A0001	Offline	89%		4 Dec 2017 11:09:10 ...	Unknown	0	10.81
iPad	iPad mini 4	Offline	11%		4 Dec 2017 10:20:07 ...	Unknown	N/A	3.1
personal dont touch	vivo Y21L	Offline	94%		4 Dec 2017 9:49:20 A...	No	100	10.22















20 Devices, 7 Online, 13 Offline











1 2 3 4 5 ... 20 devices per page

## Right-Click Operations

More operations can be performed on the selected devices in **Device List**. Right-click the device, following options appear in the context menu:

Device	Buttons	Description
Android	 <b>Refresh</b>	Refresh the device
	 <b>Remote</b>	Initiate a remote connection with a device
	 <b>Reboot</b>	Reboot the device
	 <b>Move to Group</b>	Move the device to a <b>Group</b>
	 <b>Tag</b>	Move the device to the <b>Tag</b>
	 <b>Delete</b>	Delete device(s) from the <b>Device List</b>
	 <b>Push Application</b>	Upload an application
	 <b>Push File</b>	Upload a file
	 <b>SureLock</b>	 Deactivate <b>SureLock</b> license  Install <b>SureLock</b>
	 <b>SureFox</b>	 Install <b>SureFox</b>
	 <b>SureVideo</b>	 Install and manage <b>SureVideo</b>
iOS	 <b>Configure Nix</b>	Configure Nix Settings on the device
	 <b>Refresh</b>	Refresh the device

Device	Buttons	Description
iOS	 <b>Move to Group</b>	Move the device to a <b>Group</b>
	 <b>Tag</b>	Move the device to the <b>Tag</b>
	 <b>Delete</b>	Delete device(s) from the <b>Device List</b>
Windows	 <b>Refresh</b>	Refresh the device
	 <b>Reboot</b>	Reboot the device
	 <b>Move to Group</b>	Move the device to a <b>Group</b>
	 <b>Tag</b>	Move the device to the <b>Tag</b>
	 <b>Delete</b>	Delete device(s) from the <b>Device List</b>
Android Wear	 <b>Refresh</b>	Refresh the device
	 <b>Move to Group</b>	Move the device to a <b>Group</b>
	 <b>Tag</b>	Move the device to the <b>Tag</b>
	 <b>Delete</b>	Delete device(s) from the <b>Device List</b>
	 <b>Push File</b>	Upload a file
Linux	 <b>Refresh</b>	Refresh the device

Device	Buttons	Description
Linux	 <b>Remote</b>	Remote into the selected device only when the device is online.
	 <b>Reboot</b>	Reboot the device
	 <b>Move to Group</b>	Move the device to a <b>Group</b>
	 <b>Tag</b>	Move the device to a <b>Tag</b>
	 <b>Delete</b>	Delete device(s) from the <b>Device List</b>
macOS	 <b>Refresh</b>	Refresh the device
	 <b>Remote</b>	Remote into the selected device only when the device is online.
	 <b>Move to Group</b>	Move the device to a <b>Group</b>
	 <b>Tag</b>	Add the device to a existing <b>Tag</b> / create a new <b>Tag</b> / remove the <b>Tag</b>
	 <b>Delete</b>	Delete device(s) from the <b>Device List</b>

## Device Information Panel

**Device Information Panel** displays information on Device, Network, Battery and Memory status of the selected device. The information includes following details:

- **Device** - Device Model, Operating System, Device Name, Agent Version, Last Device Name, Notes, Location Tracking, Test



- **Network** - MAC Address, IP Address, Connection, Wi-Fi Signal
- **Battery** - Main Battery status
- **Memory** - Program Memory, Storage Memory

The screenshot displays a mobile device management interface with the following sections:

- Device Info:**
  - Device Model: SM-T350
  - Operating System: MARSHMALLOW [Android]
  - Device Name: A88195619C8A1 [Edit](#)
  - Agent Version: 10.80
  - Last Device Time: 4 Dec 2017 4:32:34 PM
  - Notes: Add notes here [Edit](#)
  - Location Tracking: OFF [Edit](#)
  - Telecom Management: ON [Edit](#)
  - Android For Work: Not Enrolled [Edit](#)
  - Geo Fence: OFF [Edit](#)
  - Time Fence: OFF [Edit](#)
  - Network Fence: OFF [Edit](#)
- Network:**
  - MAC Address: [Redacted]
  - IP Address: [Redacted]
  - Local IP Address: [Redacted]
  - Connection: Secured
  - Wi-Fi Signal: 100%
  - Mobile Signal: 0%
- Battery:**
  - Main Battery (Li-ion): 41%
- Memory:**
  - Program Memory: 394.9 MB free of 1.4 GB
  - Storage Memory: 3.3 GB free of 11.1 GB

## Device Toolbar











Device Toolbar contains shortcut options to manage and perform actions on selected devices or a device group.

The Device Toolbar includes the following elements:


- Action Icons:** Delete, Apply, Queue, Locate, Blacklist, Logs.
- Table Headers:** Device, Model, Status, Battery, IP Address, Last Connected, Device Roaming, Signal, Agent Version, SureLock Version.
- Table Row:**

083D888970ED	SM-T350	Offline	89%		24 Nov 2017 11:58:49...	No	97	10.67	Not Installed
--------------	---------	---------	-----	--	-------------------------	----	----	-------	---------------

The description of the icons in **Device Toolbar** is given in the following table:

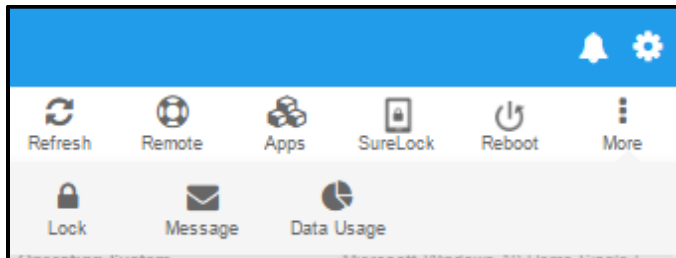
Buttons	Description
 <b>Delete</b>	Delete the selected device(s) from the list
 <b>Apply</b>	Push a job to the selected device(s)
 <b>Queue</b>	View Job(s) that are deployed, pending / error jobs in the queue.
 <b>Locate</b>	Locate the device using GPS
 <b>Blacklist</b>	Blacklist the selected device(s) from the list
 <b>Logs</b>	View log information of a selected device
 <b>Search</b>	Search device(s) on the basis of matching pattern
 <b>Export</b>	Export all device details from <b>Device List</b> in <b>.csv</b> format
 <b>Refresh</b>	Refresh the device
 <b>Columns</b>	View to customize the display of device details








**Note:** Jobs can be successfully applied to online devices, however, if the devices are offline, the applied jobs can be re-applied once the devices come online. To re-apply the job, click **Queue** >  displayed under **Status**.














## Quick Action Toolbar















This section provides easy to use buttons to perform an action or apply jobs on a specific device. These jobs are called **Dynamic Jobs**. Dynamic Jobs can be pushed to a specific device remotely only once.























The description of icons/ dynamic jobs in **Quick Action Toolbar** for different platforms is given in the following table:

Platform	Icons / Dynamic Jobs	Description
Android	 <b>Refresh</b>	Refresh the device status
	 <b>Remote</b>	Initiate a remote connection with a device
	 <b>Apps</b>	Displays all native and installed applications on the device
	 <b>SureLock</b>	Push and apply settings of <b>SureLock</b> Application to a device
	 <b>SureFox</b>	Push and apply settings of <b>SureFox</b> Application to a device

Platform	Icons / Dynamic Jobs	Description	
Android	 More	 Call Logs	View and import call log details of a device
		 SMS Logs	View and import SMS log details of a device
		 Reboot	Reboot the device
		 Reset	Reset device password remotely
		 Lock	Initiate device lock remotely
		 Message	Send an instant message to enrolled devices
		 SureVideo	Push and apply settings of <b>SureVideo</b> Application to a device
		 Wipe	Wipe the data from device remotely
		 Data Usage	Track data usage information remotely based on the connectivity preference (Mobile Data / Wi-Fi Data) for a specific period
		 Remote Buzz	Locate the device by creating a buzzing sound when misplaced or lost
Windows	 Refresh	Refresh the device status	
	 Remote	Initiate a remote connection with a device	

Platform	Icons / Dynamic Jobs	Description		
Windows	 <b>Apps</b>	Displays all native and installed applications on the device		
	 <b>SureLock</b>	Push and apply settings of <b>SureLock</b> Application to a device		
	 <b>Reboot</b>	Reboot the device remotely		
	 <b>More</b>	 <b>Lock</b>	Initiate device lock remotely	
		 <b>Message</b>	Send an instant message to enrolled devices	
		 <b>Data Usage</b>	Track data usage information remotely based on the connectivity preference (Mobile Data / Wi-Fi Data) for a specific period	
iOS	 <b>Refresh</b>	Refresh the device status		
	 <b>Apps</b>	Displays all native and installed applications on the device 1. Locks the Application of a device 2. Runs the application at startup of selected device		
	 <b>Reboot</b>	Reboot the device remotely		
	 <b>Reset</b>	Reset the device remotely		
	 <b>Lock</b>	Initiate device lock remotely		
	 <b>More</b>		Send an instant message to enrolled devices	

Platform	Icons / Dynamic Jobs	Description	
iOS	 More	 Message	
		 Wipe	Wipe the data from device remotely
		 Data Usage	Track data usage information remotely based on the connectivity preference (Mobile Data / Wi-Fi Data) for a specific period
		 Shut Down	Power Off the device remotely
Android Wear	 Refresh	Refresh the device status	
	 SureLock	Push and apply settings of <b>SureLock</b> Application to a device	
	 Call Logs	Track call logs of the enrolled device	
	 SMS Logs	Track SMS logs of the enrolled device	
	 Message	Send an instant message to enrolled devices	
	 More	 Data Usage	Track data usage information remotely based on the connectivity preference (Mobile Data / Wi-Fi Data) for a specific period
 Remote Buzz		Locate the device	
	 Refresh	Refresh the device status	

Platform	Icons / Dynamic Jobs	Description
Linux	 Remote	Initiate a remote connection with a device
	 Reboot	Reboot the device remotely
macOS	 Refresh	Refresh the device status
	 Apps	Displays all native and installed applications on the device
	 Lock	Initiate device lock remotely
	 Wipe	Wipe the data from device remotely



**Note:** The customized jobs created will get added under **More** option. To know how to customize jobs, see [Customize Toolbar](#).

## Utility Panel

This section allows users to access dashboard, emails, manage jobs, view/generate reports, create profiles and manage files using **File Store**, create enterprise **App Store**, get information by typing or voicing the requirement using **Deep Thought**.

## System Log

**SureMDM** keep a log which has recorded list of actions happening on an account. These logs are updated in a chronological order and even displays log information of other users who are logged into the same account.



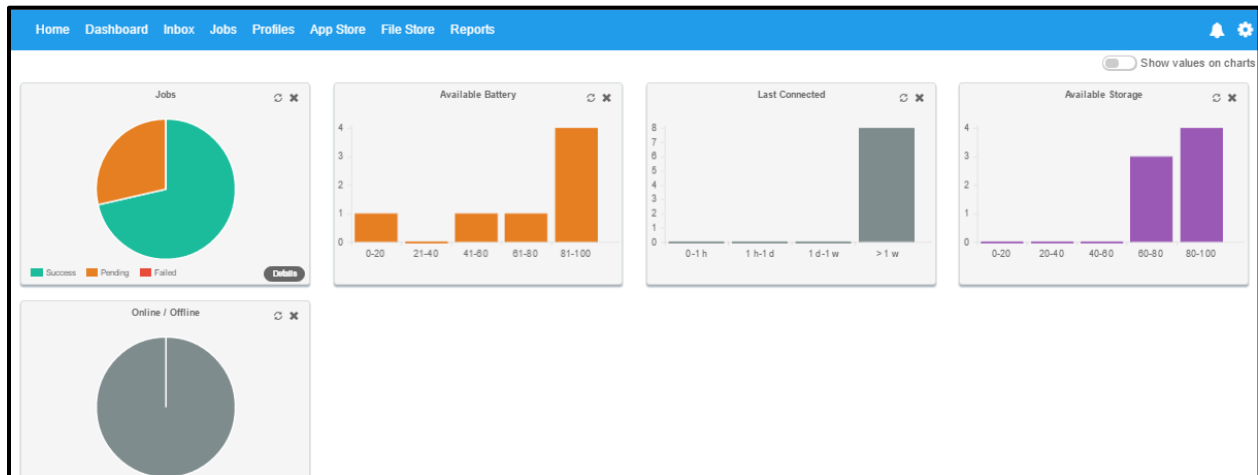
**Note:** The log information can be exported as a *.txt* file using **Export** option located at the right corner of the **System Logs** section.



## Dashboard

**SureMDM Web Console** has an HTML5 based dashboard. Admins can sort, filter and organize to get customized panels with summarized views of device parameters. It is an easy-to-comprehend, one-page graphical representation view of device details, their status, alerts, notifications and more.

To view **SureMDM Dashboard**, click **Dashboard** from **Utility Panel**. Based on the parameters selected in the left panel, corresponding charts will get displayed on the dashboard.



**Note:** i. In some charts, admins can select, view and export the device details.

For example: If admins want to view the pending jobs of all platforms, click **Pending** section of the **Jobs** chart and view the device and job details that are pending to apply.

ii. To display values on the charts, turn on **Show values on charts**.

## Inbox

**SureMDM Web Console** offers two-way messaging. Admins can send messages to individual devices or broadcast to groups. **Inbox** tab will have a notification count icon which indicates the number of unread messages.

Admins can remotely perform actions such as reply to the messages, select and mark the message as unread, delete the message, clean-up the inbox of messages older than (15/30/60/90) days

To send a message to the device user using web console, follow these steps:

1. Login to **SureMDM Web Console**.
2. Select the device from **Device List**.
3. On **Quick Action Toolbar** section, click **Message**.
4. On **Send Message** prompt, enter the following details:
  - Subject
  - Body
5. Select **Get Read Notification** to get read receipt of the message.
6. Select **Force read message** to auto-launch the message on the device for the user to read.
7. Click **Send** to complete.

## Create and Deploy Jobs

Jobs refers to the tasks which admins can create and remotely push it to the enrolled devices for execution. All the created jobs are saved under **Jobs List** and jobs can be either pushed to the devices immediately or scheduled to be pushed on a specific date and time.



**Note:** Jobs can be successfully applied to online devices. If the devices are offline, the jobs will be applied once the devices come online.

Jobs available under different platforms are given below:

### Android

<a href="#">Install Application</a>	<a href="#">File Transfer</a>	<a href="#">Text Message</a>
<a href="#">Run Script</a>	<a href="#">Remote Data Wipe</a>	<a href="#">Lock Device</a>
<a href="#">Nix Agent Settings</a>	<a href="#">Composite Job</a>	<a href="#">Notification Policy</a>
<a href="#">SureLock Settings</a>	<a href="#">SureFox Settings</a>	<a href="#">SureVideo Settings</a>
<a href="#">Location Tracking</a>	<a href="#">Security Policy</a>	<a href="#">Application Settings</a>
<a href="#">Wi/Fi / Hotspot Settings</a>	<a href="#">Email Configuration Settings</a>	<a href="#">Telecom Management Policy</a>
<a href="#">Call Log Tracking</a>	<a href="#">SMS Log Tracking</a>	<a href="#">Geo Fence</a>
<a href="#">Time Fence</a>	<a href="#">Network Fence</a>	<a href="#">Remote Buzz</a>
<a href="#">Compliance Job</a>		

### Windows

<a href="#">Install Application</a>	<a href="#">File Transfer</a>	<a href="#">Execute Program</a>
<a href="#">Send Text Message</a>	<a href="#">Run Script</a>	<a href="#">Lock Device</a>
<a href="#">Composite Job</a>	<a href="#">Notification Policy</a>	<a href="#">SureLock Settings</a>
<a href="#">SureVideo Settings</a>	<a href="#">Telecom Management Settings</a>	<a href="#">Geo Fence</a>
<a href="#">Time Fence</a>	<a href="#">Wi-Fi Settings</a>	<a href="#">Proxy Settings</a>

[Firewall policy](#)**iOS**[Geo Fencing](#)[Data Usage Policy](#)[Lost Mode](#)[Push Custom Payload](#)[Compliance Job](#)[Reboot](#)[Shut Down](#)[Uninstall App](#)[Time Fence](#)[Nix Settings](#)[Send Text Message](#)**Android Wear**[File transfer](#)[Notification Policy](#)[Call Log Tracking](#)[Text Message](#)[SureLock Settings](#)[SMS Log Tracking](#)[Run Script](#)[Location Tracking](#)[Remote Buzz](#)[Nix Agent Settings](#)[Wi-Fi Settings](#)[Composite Job](#)[Telecom Management Policy](#)**Linux**[Run Script](#)[File Transfer](#)

## Jobs for Android

### Install Application

**Install Application** job will remotely install or upgrade an application on enrolled devices.

To create **Install Application** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.

3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Install Application**.
6. On **Configure Job** screen, enter **Job Name** and click **Add**.
7. On **Install Job** prompt, enter following details:

**File Path/URL** - Browse and select the **apk** file from the system or type file **URL**

**Device Path** - Enter the location for the file to save

**Install After Copy** - Select this option to copy and install on the device

**Use Authentication** - If the user has specified the selected file or URL in **File Path/URL** field as password protected, then the file or URL can be accessed only by giving login credentials.



**Note:** *This feature works only when the apk downloaded device supports authentication.*

8. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

9. Go back to **Home** tab and select the Android device(s) or a group.
10. Click **Apply** to launch **Apply Job To Device** prompt.
11. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.



**Note:** *i. When the job is applied to a device and if the device is online then the job gets pushed to the device(s) immediately. If the device is offline, the job will get queued in **Job Queue** section with status showing **Pending**.*

*ii. Check **Logs** window to see the progress of applied job.*

## File Transfer

**File Transfer** job will transfer files to an enrolled device(s) or a group of devices.

To create **File transfer** job and push it to the device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **File Transfer**.
6. On **Configure Job** screen, enter **Job Name** and click **Add**.
7. On **File Transfer Properties** prompt, enter following details:

**File Path/URL** - Browse and select the file from the system or specify the link where the file is hosted

**Device Path** - Enter the location for the file to save

**Use Authentication** - If the user has specified the selected file or URL in **File Path/URL** field as password protected, then the file or URL can be accessed only by giving login credentials.



**Note:** *This feature works only when the apk downloaded device supports authentication.*

8. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

9. Go back to **Home** tab and select the **Android** device(s) or a group.
10. Click **Apply** to launch the **Apply Job To Device** prompt.
11. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Text Message

**Text Message** job helps the admins to remotely send text messages or broadcast messages on an enrolled devices.

To create a job to compose a message and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Text Message**.
6. On **Create Text Message** prompt, enter the following details:

**Job Name** - Name of the Job

**Subject** - Subject for the message

**Body** - Message

**Get Read Notification** - Select this option to get read receipt of the message

**Force Read Message** - Select this option to force the device users to read the message. A message prompt will appear on the device user's screen.

7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Run Script

**Run Script** job allows admins to remotely run customized scripts on an enrolled devices.

To create a job to run customized scripts and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job** and select **Android**.
4. On **Select Job Type** screen, select **Run Script**.
5. On **Run Script** prompt, enter **Job Name** and **Script**.

or

To add a pre-defined script in the **Script** box, follow these steps:

- a. Select a feature under **All/Knox/EA/Shell**.
- b. On **Run Script** prompt, insert the script in the blank space (if required) and click **Validate**.

A confirmation on successful validation will get displayed.

- c. Click **Insert** to complete.
  6. Click **Save**.
- The newly created job will get listed in the **Jobs List** section.
7. Go back to **Home** tab and select the Android device(s) or a group.
  8. Click **Apply** to launch **Apply Job To Device** prompt.
  9. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.



## Remote Data Wipe

**Remote Data Wipe** job remotely wipes all the data on an enrolled device.

To create a job to wipe data on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Remote Data Wipe**.
6. On **Remote Data Wipe** prompt, enter **Job Name** and turn on **Wipe All Data**.
7. Select **Wipe Data If Device Is Offline** to wipe the data when the device goes offline.
8. Click **Ok**.

The newly created job will get listed in **Jobs List** section.

9. Go back to **Home** tab and select the Android device(s) or a group.
10. Click **Apply** to launch **Apply Job To Device** prompt.
11. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Lock Device

**Lock Device** job remotely locks the device or change existing device password. This feature is helpful when an enrolled device is lost or stolen.

To create a job to lock the device and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.

4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Lock Device**.
6. On **Lock Job** prompt, enter **Job Name** and select following options:
  - Lock the device
  - Change password



**Note:** *Change password* option will work only when a password is already configured and enabled on the device.

7. Click **Ok**.  
  
The newly created job will get listed in the **Jobs List** section.
8. Go back to **Home** tab and select the Android device(s) from **Device List**.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Nix Agent Settings

**Nix Agent Settings** job remotely configures or updates **SureMDM Nix Agent settings** on enrolled devices.

To create a job to configure **Nix Agent Settings** and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Nix Agent Settings**.

6. On **Nix Agent Settings** prompt, enter **Job Name** and select the following options:
  - Enable time synchronization with server** - Select the **Periodicity** from drop-down menu to synchronize with the server in specified time.
  - Enable device info update** - Select the **Periodicity** from drop-down menu to update device info in specified time.
  - Enable Nix Password** - Enter the password to configure **Nix Agent** settings.
  - Enable Schedule Reboot** - Schedule for device reboot at a specified time on selected **Days**.
  - Enable Schedule Shutdown** - Schedule for device shutdown at a specified time on selected **Days**.
  - Connection Type** - Select the **Connection Type (Any / Wi-Fi Only/ Mobile Data)** from the drop-down menu to connect the internet.
7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.
8. Go back to **Home** tab and select the Android device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Composite Job

SureMDM allows the user to deploy a combination of job types by a special job called **Composite Job**. The composite job can have a combination of multiple jobs such as installation, send messages, nix settings and more. Composite Jobs helps the user to apply multiple jobs on an enrolled device(s) with just a single job.

To create a composite job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Composite Job**.
6. On **Configure Job** screen, enter **Job Name** and click **Add**.



**Note:** *Add Delay* option will delay for the specified time on executing the job.

7. On **Select Job(s) To Add** prompt, select the job(s).



**Note:** Use **Ctrl** key to select multiple jobs.

8. Go back to **Configure Job** screen.



**Note:** Use the controls, **Move Up** and **Move Down** to prioritize the desired jobs in a sequence.

9. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

10. Go back to **Home** tab and select the Android device(s) or group.
11. Click **Apply** to launch the **Apply Job To Device** prompt.
12. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Notification Policy

**SureMDM** allows the creation of notification policies for enrolled devices. Once this job is pushed to the enrolled device, automatic notifications will be sent when the device goes beyond the set threshold.

To configure **Notification Policy** on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Notification Policy**.
6. On **Notification Policy** screen, select or enter the following details:

**Job Name** - Enter **Job Name**.

**Disable Notification Policy** - Select this option to disable all the notification settings for a specific Job.

**Enable Battery Policy** - Select this option to set the value (in %) for battery threshold. This option notifies the user (Device/Admin/E-mail address) when an enrolled device battery power falls below the set threshold.

**Enable Connection Policy** - Select this option to set the time (in min). This option notifies the user (Device/Admin/Email address) when an enrolled device is offline in SureMDM for a specified period of time.

**Enable Data Usage Policy** - Select this option to set the data usage (in **KB/MB/GB**). This option notifies the user (Device/Admin/E-mail address) when an enrolled device data consumption exceeds the set threshold.

**Notify when device comes online** – This option notifies the user (device/admin/e-mail address) when an enrolled device comes online after being offline.

**Notify when SIM is changed** – This option notifies the user (device/admin/e-mail address) when an enrolled device sim card is changed.

**Notify when device is rooted or Nix has been granted with root permission** - Sends notification when the device has granted root access or when the Nix has got advance management permissions after rooting.

**Send Alert to** - The user has the option to send notification to one of the following:

- **SureMDM Web Console**
- **Device**
- **E-Mail Notification**

7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android device(s) or a group.

9. Click **Apply** to launch the **Apply Job To Device** prompt.

10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## SureLock Settings

Admin can configure **SureLock Settings** remotely on enrolled devices.

To create **SureLock Settings** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.

4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **SureLock Settings**.
6. On **SureLock Settings** prompt, select the desired option from the following and configure the settings and then click **Save**.
  - a. Allowed Applications
  - b. SureLock Settings
  - c. Samsung Knox Settings
  - d. Allowed Widgets
  - e. Manage Shortcuts
  - f. Phone Settings
  - g. Multi-User Profile Settings
  - h. Import/Export Settings
  - i. About SureLock
7. Enter **Job Name, Password** and click **Ok**.

The newly created job will get listed in the **Jobs List** section.
8. Go back to **Home** tab and select the Android device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.



**Note:** Admin has the following options to select from:

- i. Download the **surelock.settings** file using **Save As File**.
- ii. To edit the **SureLock** settings in XML form, click **Edit XML**.
- iii. To install and activate **SureLock** on a device remotely, click **Advanced Option** and enter the **Activation Code**.

## SureFox Settings

Admin can configure **SureFox Settings** remotely on enrolled devices.

To create **SureFox Settings** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **SureFox Settings**.
6. On **SureFox Settings** prompt, select the desired option from the following and configure the settings and then click **Save**.
  - a. Allowed Website
  - b. Blocked Website
  - c. Manage Categories
  - d. Browser Preferences
  - e. SureFox Pro Settings
  - f. Samsung Knox Settings
  - g. Display Settings
  - h. Import/Export Settings
  - i. About SureFox

7. Enter **Job Name**, **Password** and click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.



10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.



**Note:** Admin has the following options to select from:

- i. Download the `surelock.settings` file using **Save As File**.
- ii. To edit the **SureFox** settings in XML form, click **Edit XML**.
- iii. To install and activate **SureFox** on a device remotely, click **Advanced Option** and enter the **Activation Code**.

## SureVideo Settings

Admin can configure **SureVideo Settings** remotely on enrolled devices.

To create **SureVideo Settings** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **SureVideo Settings**.
6. On **SureVideo Settings** prompt, enter the **Job Name** and **Password**.
7. Type or copy the XML code in **Source** box and click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Location Tracking

Location tracking job enables the admins to remotely enable Location Tracking on an enrolled device and set tracking periodicity.

To create a **Location Tracking** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Location Tracking**.
6. On **Location Tracking** screen, enter **Job Name**.
7. Select **Enable Location Tracking**.
8. Select a value from the spin box (in minutes) in **Tracking Periodicity**.
9. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

10. Go back to **Home** tab and select the Android device(s) or a group.
11. Click **Apply** to launch the **Apply Job To Device** prompt.
12. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Security Policy

**Security Policy** job remotely configures security policy on an enrolled device(s). There are two kinds of security policies to choose from: **Password Policy** and **Peripheral Settings**.

## Password policy

Admin can remotely configure password policy on the enrolled devices.

To create **Security Policy** job for password and push it on an enrolled device(s) remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Security Policy**.
6. On **Security Policy** prompt, select **Password policy** tab and select the following settings:
  - Disable password policy on device-
  - Enforce Password Policy on Device
  - Minimum Password Length
  - Password Strength
  - Time lapse before device auto-locks
  - Maximum Failed Password Attempts Before Device Wipes

7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android device(s).
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Peripheral Settings

Admin can remotely configure peripheral settings on the enrolled devices.

To create **Security Policy** job for **Peripheral Settings** and push it on an enrolled device(s) remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Security Policy**.
6. On **Security Policy** prompt, select **Peripheral Settings** tab and select the following settings:
  - Enforce Peripheral Settings on Device
  - Disable Bluetooth
  - Disable WiFi
  - Disable Camera
  - Mobile Data
  - GPS
7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android device(s).
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Application Settings

**Application Settings** job helps the user to manage the applications remotely with following **Job**

**Types:**

- **Lock Apps** - Lock the application with password
- **Run at startup** - Run the application on device booting
- **Uninstall applications** - Remove the application from the device
- **Clear data** - Delete the data of an application

To create **Application Settings** job and push it to the device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Application Settings**.
6. On **Application Settings** prompt,
  - a. Enter **Job Name**.
  - b. Select the **Application Name(s)** from the list.
  - c. Click **Add** to move **Application Names** in the right-side box.
  - d. Click **Remove** to remove the **Application Names** from the right- side box.
  - e. Select the desired **Job Type**.
  - f. Click **Advanced** to set the **Password** in **Advanced Settings** prompt.
7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select Android device(s) from **Device List**.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Wi-Fi/Hotspot Settings

Admins can remotely configure Wi-Fi/Hotspot settings on the enrolled device(s).

To create **Wi-Fi/Hotspot Settings** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Wi-Fi Configuration**.
6. On **WiFi Configuration Settings** screen, click **Add**.
7. On **Add Wi-Fi/Hotspot Config** prompt,
  - a. Enter **SSID**.
  - b. Enter **Password**.
  - c. Select an option from **Security Type**.
  - d. Select **Auto Connect** or **Hotspot** to connect the device automatically to Wi-Fi/Hotspot.
  - e. Select **Hidden Network** to connect to the different network manually.
8. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

9. Go back to **Home** tab and select Android device(s) or a group.
10. Click **Apply** to launch the **Apply Job To Device** prompt.

11. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Email Configuration Settings

Admins can remotely configure an email account or delete a configured email account on the enrolled devices using **SureMDM Web Console**.

### Create an Email Account

To create a job to configure an email account and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Email Configuration Settings**.
6. On **Email Configuration Settings** prompt,
  - a. Click **Create E-mail Account** tab.
  - b. Enter **Job Name**.
  - c. Enter **User Name, Password**.
  - d. Select **Server Type** from the drop-down menu.
  - e. Enter **Incoming Server Address, Outgoing Server Address**.
  - f. Select **Security Type** from the drop-down menu.
  - g. Select a value from the spin box for **Incoming Port** and **Outgoing Port**.
  - h. Enter the **Signature**.
  - i. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

7. Go back to **Home** tab and select the Android device(s) or group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.



**Note:** This feature is currently available for Samsung KNOX devices only.

## Delete an Email Account

To create a job to delete an email account and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job** and select **Android**.
4. On **Select Job Type** screen, select **Email Configuration Settings**.
5. On **Email Configuration Settings** prompt,
  - a. Click **Delete Email Account** tab.
  - b. Enter the **Job Name, User Name**.
  - c. Select **Server Type** from the drop-down menu.
  - d. Enter **Incoming Server Address**.
  - e. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

6. Go back to **Home** tab and select the Android device(s) or a group.
7. Click **Apply** to launch the **Apply Job To Device** prompt.
8. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.



**Note:** This feature is currently available for Samsung KNOX devices only.



## Telecom Management Policy

This job allows admin to remotely set thresholds for data usage on an enrolled device(s) or group of devices. Admin can use this job to receive automatic notifications and even block mobile data of the device if the data usage goes beyond the set threshold limit.

To create **Telecom Management Policy** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Telecom Management Policy**.
6. On **Telecom Management Policy** prompt,
  - a. Select **Data Usage Tracking** tab.
  - b. Select **Enable Telecom Management**.
  - c. Select an option from **Configure Billing Cycle** drop-down menu.



**Note:** *Billing Start Date / Day will be auto-populated based on the option selected in the **Configure Billing Cycle**.*

- d. Under **Configure Mobile Data Limits**, enter the value to set the **threshold** for the data usage for **Limit 1** and **Limit 2**.



**Note:** ***Block Data, Send Device Alert, Send MDM Alert, Send Email Alert** options are enabled once the value for the threshold is entered.*

- e. Under **Action**, select the following:

**Block Data** - Will block the data when the data usage exceeds the set threshold.

**Send Device Alert** - Notifies the device user when the data usage exceeds the set threshold.

**Send MDM Alert** - Notifies the **MDM** admins when the data usage exceeds the set threshold.

**Send Email Alert** - Notifies the admins by email when the data usage exceeds the set threshold.

- f. Select **Call Log Tracking** tab.
  - g. Select an option from the **Call Log Tracking** drop-down menu.
  - h. Select a value from the spin box to set **Tracking Periodicity** (in minutes).
  - i. Select **SMS Log Tracking** tab.
  - j. Select an option from the **SMS Log Tracking** drop-down menu.
  - k. Select a value from the spin box to set **Tracking Periodicity** (in minutes).
7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Call Log Tracking

Admins can remotely track call logs of an enrolled device(s).

To create **Call Log Tracking** job and push it on an enrolled device(s) remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.

3. On **Jobs** screen, click **New Job** and select **Android**.
4. On **Select Job Type** screen, select **Call Log Tracking**.
5. On **Call Log Tracking** prompt,
  - a. Enter **Job Name**.
  - b. Select an option from the **Call Log Tracking** drop-down menu.
  - c. Select a value from the spin box to set **Tracking Periodicity** (in minutes).
6. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.
7. Go back to **Home** tab and select the Android device(s) or a group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## SMS Log Tracking

Admins can remotely track SMS logs of an enrolled device(s).

To create **SMS Log Tracking** job and push it on an enrolled device(s) remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **SMS Log Tracking**.
6. On **SMS Log Tracking** prompt,
  - a. Enter **Job Name**.
  - b. Select an option from **SMS Log Tracking** drop-down menu.

- c. Select a value from the spin box to set **Tracking Periodicity** (in minutes).
- d. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

7. Go to **Home** tab and select the Android device(s) or a group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.


## Geo Fence

Geo Fence option creates a virtual fence around a geographical location. Admins can configure policies on the devices by assigning jobs when they enters or exits the fence.



**Note:** *Geo Fence requires GPS capability on the device.*

To create a **Geo Fence** job and push it to the device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM** Web Console, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Geo Fence**.
6. Select **Enable Geo Fencing**.
7. On **Geo Fence** screen, **Select Fence** and click **Search** to enter the location.
8. Click  **Draw Fence**, place the cursor at the center of the location, click and move the cursor until it covers the desired area. Click again to set the boundary.
9. On **Geo Fence Details** prompt, enter the fence **Name** and click **Add**.

The newly created fence gets listed in the **Fence Details** section.



**Note:** Radius of the circle (fence) is auto-populated. Select the unit for the fence as **Meter/ Kilometer / Mile**.

10. Select **Fence Entered** tab, click **Add** to select the job(s) that will be activated on the device when it enters the fenced area.
11. On **Select Jobs to Add** screen, select the multiple jobs from the list using **Ctrl** key.
12. Select the **Alert Type** from the following options, who will receive an alert when the device enters the fenced area:  
  
**Device**  
  
**MDM**  
  
**Email**
13. Click **Save**.
14. Select **Fence Exited** tab and repeat the steps 10 to 13.  
  
The newly created job will get listed in the **Jobs List** section.
15. Go back to **Home** tab and select the android device(s) or group.
16. Click **Apply** to launch the **Apply Job To Device** prompt.
17. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Time Fence

Time Fence option creates a periodical boundary for mobile devices to behave or function a specified way. Admins can assign jobs to be executed at scheduled start time and after the end time using this feature.

To create a **Time Fence** job and push it on an enrolled device(s) remotely, follow these steps:

1. Login to **SureMDM Web Console**.

2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select Operating System** screen, click **Android**.
5. On **Select Job Type** screen, click **Time Fence**.
6. On **Time Fence** prompt, select **Enable Time Fencing**.
7. Click **Select Fence** tab, click **Add Fence**.



**Note:** *Multiple Time Fences can be added.*

8. Enter the **Start Time**, **End Time** and select the **Days**.
9. Select **Fence Entered** tab, click **Add** to select the job(s) that will be activated on the device when it enters the fenced area.
10. On **Select Jobs to Add** screen, select the multiple jobs from the list using **Ctrl** key.
11. Select a user from the following options, who will receive an alert when the device enters the fenced area:
  - Device**
  - MDM**
  - Email**
12. Click **Save**.
13. Select **Fence Exited** tab and repeat the steps 9 to 12.

The newly created job will get listed in the **Jobs List** section.
14. On the **Job Details** window, enter the **Job Name**.
15. Go back to **Home** tab and select the Android device(s) or group.
16. Click **Apply** to launch the **Apply Job To Device** prompt.
17. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Network Fence

Network Fence option creates a network boundary for the mobile devices to behave or function a certain specified way. Admins can configure policies on the devices by assigning jobs when the device enters or exits a certain Wi-Fi network.

To create a **Network Fence** job and push it on an enrolled device(s) or a group, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Network Fence**.
6. On **Network Fence** prompt, select **Enable Network Fencing**.
7. Click **Select Fence** tab, click **Add Fence**.
8. Enter the **SSID**.



***Note:** Multiple Network Fences can be added.*

9. Select **Fence Entered** tab, click **Add** to select the job(s) that will be activated on the device when it enters the fenced area.
10. On **Select Jobs to Add** screen, select the multiple jobs from the list using **Ctrl** key.
11. Select a user from the following options, who will receive an alert when the device enters the fenced area:

**Device**

**MDM**

**Email**

12. Select **Fence Exited** tab and repeat the steps 9 to 11.

13. Click **Save**.

14. On the **Job Details** window, enter the **Job Name**.

The newly created job will get listed in the **Jobs List** section.

15. Go back to **Home** tab and select the android device(s) or group.

16. Click **Apply** to launch the **Apply Job To Device** prompt.

17. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Remote Buzz

When a device is lost or misplaced, **Remote Buzz** job helps admin to locate the device by pushing a job which forces it to make a sound.

To create a **Remote Buzz** job remotely to locate the device and push it to the device(s)/group, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Remote Buzz**.
6. Enter **Job Name** and click **Ok**.

The newly created job will get listed in the **Jobs List** section.

7. Go back to **Home** tab and select the android device(s) or group.

8. Click **Apply** to launch the **Apply Job To Device** prompt.

9. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.



Once this job is applied on an enrolled device, a buzzing sound will be created from the device.

## Compliance Job

**Compliance Job** is used to detect threats such as rooting/ jailbreaking, SIM card changes, password in compliance and proactively trigger specified measures like blacklisting the devices or wiping data off a device. This job allows admins to set alerts and notifications on detection of such vulnerabilities.

To create a **Compliance Job** and remotely push it to the device(s) or group, follow these steps:

1. Login to SureMDM Web Console.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. **Select the OS** screen, select **Android**.
5. On **Select Job Type** screen, select **Compliance Jobs**.
6. On **Compliance Job** prompt, enter the **Job Name**, select **Enable Compliance Job** and select from given options:
  - OS Version
  - Jailbroken/Rooted
  - Online Device Connectivity
  - SIM Change
  - Password Policy
7. Select the option to configure **Compliance Rules** and **Out Of Compliance Actions**.
8. Click **Add Action** to add additional **Out of Compliance Actions**.
9. Click **Save**.

The newly created job will get listed in the **Jobs List** section.

10. Go back to **Home** tab and select the Android device(s) or a group.
11. Click **Apply** to launch the **Apply Job To Device** prompt.
12. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Jobs for Windows

### Install Application

**Install Application** job will remotely install or upgrade an application on an enrolled device.

To create **Install Application** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **Install Application**.
6. On **Configure Job** screen, enter the **Job Name** and click **Add**.
7. On **Install Job** prompt, enter the following details:

**File Path/URL** - Browse and select the **exe** file from the system or type file **URL**

**Device Path** - Enter the location for the file to save

**Install After Copy** - Select this option to copy and install on the device

**Silent Install** - Select this option to install silently without user intervention

**Execute Path** - Select this option to execute the file located on the specified path.

8. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

9. Go back to **Home** tab and select the Windows device(s) or a group.
10. Click **Apply** to launch the **Apply Job To Device** prompt.
11. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.



**Note:** Check **Logs** window to see the progress of the applied job.

## File Transfer

**File Transfer** job will transfer the files to an enrolled device(s) or a group of devices.

To create **File transfer** job and push it to the device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **File Transfer**.
6. On **Configure Job** screen, enter the **Job Name** and click **Add**.
7. On **File Transfer Properties** prompt, enter the following details:

**File Path/URL** - Browse and select the file from the system or specify the link where the file is hosted

**Device Path** - Enter the location of the file to save

8. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

9. Go back to **Home** tab and select the Windows device(s) or a group.
10. Click **Apply** to launch the **Apply Job To Device** prompt.

11. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Execute Program

**Execute Program** job will launch the files on an enrolled device(s) or a group of devices.

To create **Execute Program** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **Execute Program**.
6. On **Configure Job** screen, enter the **Job Name**, **Device Path** and **Parameters**.
7. Click **OK**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Windows device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Apply** to complete.

## Send Text Message

**Send Text Message** job helps the admins to remotely send text messages or broadcast messages on an enrolled device(s).

To create a job to compose a message and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the Windows** screen, select **Windows**.
5. On **Select Job Type** screen, select **Send Text Message**.
6. On **Create Text Message** prompt, enter the following details:

**Job Name** - Name of the Job

**Subject** - Subject for the message

**Body** - Message



**Note:** *Get Read Notification* option is applicable only to the Android devices.

**Force Read Message** - Select this option to force the device users to read the message. A message prompt will appear on the device users' screen.

7. Click **OK**.  
The newly created job will get listed in the **Jobs List** section.
8. Go back to **Home** tab and select the Windows device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Run Script

**Run Script** job will run customized scripts on the enrolled devices.

To create a job to run customized scripts and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.

3. On **Jobs** screen, click **New Job** and select **Windows**.
4. On **Select Job Type** screen, select **Run Script**.
5. On **Run Script** prompt, enter the **Job Name** and **Script**.
6. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

7. Go back to **Home** tab and select the Windows device(s) or group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Lock Device

**Lock Device** job remotely locks the device. This feature is helpful when the device is lost or stolen.

To create a job to lock the device and push it on an enrolled device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **Lock Device**.
6. On **Lock Job** prompt, enter **Job Name** and select **Lock the device**.



**Note:** Password should be configured and enabled for device lock to work.

7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Windows device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Composite Job

SureMDM allows the user to deploy a combination of job types by a special job called Composite Job. The composite job can have a combination of multiple jobs such as installation, send messages, update security policies and more. Composite Jobs helps the user to apply multiple jobs on an enrolled device(s).

To create a composite job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **Composite Job**.
6. On **Configure Job** screen, enter **Job Name** and click **Add**.
7. On **Select Job(s) To Add** prompt, select the job(s).



**Note:** Use **Ctrl** key to select multiple jobs.

8. Go back to **Configure Job** screen.



**Note:** Use the controls, **Move Up** and **Move Down** to arrange the sequence of jobs.

9. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

10. Go back to **Home** tab and select the Windows device(s) or a group.
11. Click **Apply** to launch the **Apply Job To Device** prompt.
12. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Notification Policy

**SureMDM** allows creation of notification policies for enrolled devices. Once this job is pushed to an enrolled device, automatic notifications will be sent when the device goes beyond the set threshold.

To configure **Notification Policy** on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **Notification Policy**.
6. On **Notification Policy** screen, select or enter following details:

**Job Name** - Enter the Job Name.

**Disable Notification Policy** - Select this option to disable all the notification settings.

**Enable Battery Policy** - Notifies the user (Device/Admin/E-mail address) when an enrolled device battery power falls below the set threshold.

**Enable Connection Policy** - Notifies the user (Device/Admin/E-mail address) when an enrolled device is not connected to a network for a specified period of time.

**Notify when device comes online** - Notifies the user (Device/Admin/E-mail address) when an enrolled device comes online after being offline.



**Send Alert to** - The admins have the option to send notifications to following recipients:

- **SureMDM Web Console**
- **Device**
- **E-Mail Notification**

7. Click **OK**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Windows device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## SureLock Settings

Admin can remotely configure **SureLock** settings on enrolled devices.

To create **SureLock Settings** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. **Login to SureMDM Web Console.**
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **SureLock Settings**.
6. On **SureLock Settings** prompt, select the desired option from the following and configure the settings and click **Save**.
  - a. Allowed Applications
  - b. Allowed Websites
  - c. SureLock Settings

- d. Browser Settings
  - e. Import/Export Settings
  - f. Peripheral Settings
  - g. About SureLock
7. Enter **Job Name**, **Password** and click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Windows device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.



**Note:** Admin has the following options to select from:

- i. Download the `surelock.settings` file using **Save As File**.
- ii. To edit the **SureLock** settings in XML form, click **Edit XML**.

## SureVideo Settings

Admin can remotely configure **SureVideo Settings** remotely on enrolled devices.

To create **SureVideo Settings** job and push it to the device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **SureVideo Settings**.
6. On **SureVideo Settings** prompt, enter the **Job Name**

7. Enter the XML code in **Source box** and click **OK**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Windows device(s) or group.

9. Click **Apply** to launch the **Apply Job To Device** prompt.

10. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Telecom Management Policy

This job allows admin to remotely set thresholds for data usage on an enrolled device(s) or group of devices. Once this job is pushed to an enrolled device, automatic notifications will be sent or mobile data will be blocked if the device goes beyond set data usage threshold limit.

To create **Telecom Management Policy** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On Select the **OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **Telecom Management Policy**.
6. On **Telecom Management Policy** prompt,
  - a. Enter **Job Name**.
  - b. Select **Enable Telecom Management**.
  - c. Select an option from **Configure Billing Cycle** drop-down menu.



**Note:** *Billing Start Date / Day will be auto-populated based on the option selected in the **Configure Billing Cycle**.*

- d. Under **Configure Mobile Data Limits**, enter the value to set the threshold for the data usage for **Limit 1** and **Limit 2**.



**Note:** *Block Data, Send Device Alert, Send MDM Alert, Send Email Alert options are enabled once the value for the threshold is entered.*

- e. Under **Action**, select the following:

**Block Data** - Will block the data when the data usage exceeds the set threshold.

**Send Device Alert** - Notifies the device user when the data usage exceeds the set threshold.

**Send MDM Alert** - Notifies the **MDM** admins when the data usage exceeds the set threshold.

**Send Email Alert** - Notifies the admins by email when the data usage exceeds the set threshold.

7. Click **OK**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the windows device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Geo Fence

**Geo Fence** option creates a virtual fence around a geographical location. Admins can configure jobs to be applied on the devices when users enter or exit this geographical fence.



**Note:** *Geo Fence requires GPS capability on the device.*

To create a **Geo Fence** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **Geo Fence**.
6. Select **Enable Geo Fencing**.
7. On **Geo Fence** screen, Select **Fence** and click **Search** to enter the location.
8. Click  **Draw Fence**, place the cursor at the center of the location, click and move the cursor until it covers the desired area. Click again to set the boundary.
9. On **Geo Fence Details** prompt, enter the **Fence Name** and click **Add**.

The newly created fence gets listed in the **Fence Details** section.



**Note: Radius of the circle (fence) is auto-populated. Select the unit for the fence as *Meter / Kilometer / Mile*.**

10. Select **Fence Entered** tab, click **Add** to select the job(s) which will be activated on the device when it enters the fenced area.
11. On **Select Jobs to Add** screen, select the multiple jobs from the list using **Ctrl** key.
12. Select a user from the following options, who will receive an alert when the device enters the fenced area:

**Device**

**MDM**

**Email**

13. Click **Save**.

14. Select **Fence Exited** tab, Repeat steps 10 to 13.

The newly created job will get listed in the **Jobs List** section.

15. Go back to **Home** tab and select the windows device(s) or a group.
16. Click **Apply** to launch the **Apply Job To Device** prompt.
17. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Time Fence

Time Fence option creates a periodical boundary for mobile devices to behave or function a specified way. Admins can assign jobs to be executed at scheduled start time and after the end time using this feature.

To create a **Time Fence** job and push it on an enrolled devices remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select Operating System** screen, click **Windows**.
5. On **Select Job Type** screen, click **Time Fence**.
6. On **Time Fence** prompt, select **Enable Time Fencing**.
7. Select the **Optional Time** from the options given below:

**Console Time**

**Device Time**

8. Click **Select Fence** tab, click **Add Fence**.



**Note:** Multiple Time Fences can be added.

9. Enter the **Start Time**, **End Time** and select the **Days**.

10. Select **Fence Entered** tab, click **Add**.
11. On **Select Jobs to Add** screen, select the jobs from the list which will be activated on the device when it enters the fenced area.
12. Select a user from the following options, who will receive an alert when the device enters the fenced area:  
  
**Device**  
  
**MDM**  
  
**Email**
13. Click **Save**.
14. Select **Fence Exited** tab, Repeat steps 9 to 12.  
  
The newly created job will get listed in the **Jobs List** section.
15. On the **Job Details** window, enter the **Job Name**.
16. Go back to **Home** tab and select the windows device(s) or a group.
17. Click **Apply** to launch the **Apply Job To Device** prompt.
18. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Wi-Fi Settings

Admins can remotely configure Wi-Fi settings on an enrolled device(s).

To create **Wi-Fi Settings** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**

5. On **Select Job Type** screen, select **Wi-Fi Settings**.
6. On **WiFi Configuration Settings** screen, click **Add**.
7. On **Add Wi-Fi Config** prompt,
  - a. Enter **SSID**.
  - b. Select an option from **Security Type**.
  - c. Select **Auto Connect** to connect the device automatically to Wi-Fi.
  - d. Select **Hidden Network** to connect to the different network manually
8. Click **Ok**.

The newly created job will get listed in the **Jobs List**.
9. Go back to **Home** tab and select the windows device(s).
10. Click **Apply** to launch the **Apply Job To Device** prompt.
11. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Proxy Settings

Admin can remotely monitor and block access to certain websites on enrolled devices.

To create **Proxy Settings** job and push it on enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **ProxySettings**.
6. Enter **Job Name**.
7. Select **Enable Proxy**.



8. Select **Proxy Type**.
  - When **Proxy Type – Auto** is selected, enter the URL in **Proxy PAC URL**.
  - When **Proxy Type – Manual** is selected, enter **Proxy Server** and **Proxy Port**.
9. Click **Save**.

The newly created job will get listed in the **Jobs List**.
9. Go back to **Home** tab and select the windows device(s).
10. Click **Apply** to launch the **Apply Job To Device** prompt.
11. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## FireWall Policy

Admin can remotely Whitelist or Blacklist the URLs on the enrolled devices.

To create **Firewall Policy** job and push it on enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Windows**.
5. On **Select Job Type** screen, select **Firewall Policy**.
6. Select **Enable** option.
7. Select **Domain List (Whitelist /Blacklist the list)**.
8. Enter **Domain Names**.

## Jobs for iOS


### Geo Fencing

**Geo Fence** option creates a virtual fence around a geographical location. Admins can configure jobs to be applied on the devices when user enters or exits this geographical fence.



**Note:** *Geo Fence requires GPS capability on the device.*

To create a **Geo Fence** job and push it to the device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM** Web Console, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **iOS**.
5. On **Select Job Type** screen, select **Geo Fence**.
6. Select **Enable Geo Fencing**.
7. On **Geo Fence** screen, **Select Fence** and click **Search** to enter the location.
8. Click  **Add Fence**, place the cursor at the center of the location, click and move the cursor until it covers the desired area. Click again to set the boundary.
9. On **Geo Fence Details** prompt, enter the **Name** for the fence and click **Add**.

The newly created fence gets listed in the **Fence Details** section.



**Note:** *Radius of the circle (fence) is auto-populated. Select the unit for the fence as **Meter/***

***Kilometer / Mile.***

10. Select **Fence Entered** tab, click **Add** to select the job(s) that will be activated on the device when it enters the fenced area.
11. On **Select Jobs to Add** screen, select the multiple jobs from the list using **Ctrl** key.

12. Select **Alert Type** from the following options to send notification when the device enters the fenced area:

**Device**

**MDM**

**Email** (multiple email id's can be added to receive the notifications)

13. Click **Save**.

14. Select **Fence Exited** tab, Repeat steps 10 to 13.

The newly created job will get listed on the **Jobs List** section.

15. Go back to **Home** tab and select the iOS device(s) or group.

16. Click **Apply** to launch the **Apply Job To Device** prompt.

17. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Data Usage Policy

This job allows admins to remotely set thresholds for data usage on the enrolled device(s) or group of devices.



**Note:** Once this job is pushed to the enrolled device, automatic notifications will be sent when the device reaches the allowed threshold limit. This will work only when **SureMDM Alert Type** is enabled.

To create **Data Usage Policy** job and push it to the device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.

4. On **Select the OS** screen, select **iOS**.
5. On **Select Job Type** screen, select **Data Usage Policy**.
6. On **Data Usage Policy** prompt,
  - a. Enter **Job Name**.
  - b. Select **Enable Data Usage Policy**.
  - c. Select an option from **Configure Billing Cycle** drop-down menu.



**Note:** *Billing Start Date / Day will be auto-populated based on the option selected in the **Configure Billing Cycle**.*

- d. Under **Configure Mobile Data Limits**, enter the value (in **MB/GB**) to set the threshold for the data usage for **Limit 1** and **Limit 2**.



**Note:** *Send MDM Alert, Send Email Alert, Apply Profile and Block Data options are enabled once the value for the threshold is entered.*

- e. Under **Action**, select the following:

**Send MDM Alert** - Notifies the **MDM** admins when the data usage exceeds the set threshold.

**Send Email Alert** - Notifies the admins by email when the data usage exceeds the set threshold.

**Apply Profile** - Apply the selected profile when the data usage exceeds the set threshold.



**Note:** *Only one **Profile** can be added.*

**Block Data** - Will block the data when the data usage exceeds the set threshold.

7. Click **OK**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the iOS device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Lost Mode

When an enrolled device is lost, admin can push **Lost Mode** job on the enrolled device. This will lock down the device and displays specified message on the device screen.

To create a **Lost Mode** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **iOS**.
5. On **Create Job** prompt, select **Lost Mode**.
6. On **Lost Mode** prompt,
  - a. **Job Name** - Enter the job name.
  - b. **Lost Mode** - Turn-on **Lost Mode**
  - c. **Message** - Enter the message
  - d. **Phone Number** - Enter the Phone number
  - e. **Footer** - Enter the message for the Footer

The newly created job will get listed on **Jobs List** section.

7. Go back to **Home** tab and select the **iOS** device(s) or a group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Push Custom Payload

**Push Custom Payload** job allows admins to remotely run customized scripts on enrolled devices.

To create a job to run customized scripts on enrolled device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job** and select **iOS**.
4. On **Select Job Type** screen, select **Custom MDM Payload**.
5. On **Run Script** prompt, enter **Job Name** and **Command**.
6. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

7. Go back to **Home** tab and select the **iOS** device(s) or group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Compliance Job

**Compliance Job** is used to detect threats such as rooting/ jailbreaking, SIM card changes, password in compliance and proactively trigger specified measures like blacklisting the devices or wiping data off a device. This job allows admins to set alerts and notifications on detection of such vulnerabilities.

To create a **Compliance Job** and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. **Select the OS** screen, select **iOS**.
5. On **Select Job Type** screen, select **Compliance Jobs**.
6. On **Compliance Job** prompt, enter the **Job Name**, select **Enable Compliance Job** and select from given options:
  - OS Version
  - Jailbroken/Rooted
  - Online Device Connectivity
  - SIM Change
  - Password Policy
7. Select between the iOS versions under **Compliance Rules**.
8. Select an **Action Type** under **Out Of Compliance Actions** from the following options when the device goes beyond the **Compliance Rules**:
  - Send Message
  - Move to Blacklist
  - Wipe the Device
  - Lock Device
  - E-Mail Notification
  - Apply Job
9. Click **Add Action** to add additional **Out of Compliance Actions**.
10. Click **Save**.

The newly created job will get listed in the **Jobs List** section.

11. Go back to **Home** tab and select the iOS device(s) or a group.
12. Click **Apply** to launch the **Apply Job To Device** prompt.
13. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Reboot

Reboot job allows the admins to reboot the enrolled device remotely.

To create a **Reboot** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **iOS**.
5. On **Select Job Type** screen, select **Reboot**.
6. On **Reboot Device** prompt, enter **Job Name** and click **Ok**.

The newly created job will get listed in the **Jobs List** section.

7. Go back to **Home** tab and select the iOS device(s) or a group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.



**Note:** *Device Reboot* is supported only on supervised devices, **iOS 10.3** onwards.

## Shut Down

**Shut Down** job allows the admin to power off the enrolled device remotely.

To create a **Shut Down** job and push it to on an enrolled device(s) or group remotely, follow these steps:



1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **iOS**.
5. On **Select Job Type** screen, select **Shut Down**.
6. On **Shut Down Device** prompt, enter **Job Name** and click **Ok**.

The newly created job will get listed on **Jobs List** section.

8. Go back to **Home** tab and select the iOS device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.



**Note:** *Device Shut Down is supported only on supervised devices, iOS 10.3 onwards.*

## Uninstall App

Uninstall App job enables the admins to uninstall applications remotely on the enrolled devices.

To create an **Uninstall App** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **iOS**.
5. On **Select Job Type** screen, select **Uninstall App**.
6. On **Uninstall App** prompt, enter the **Job Name** and select an option from the **Bundle Id** drop-down menu and click **Ok**.

The newly created job will get listed on **Jobs List**.

8. Go back to **Home** tab and select the iOS device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Time Fence

Time Fence option creates a periodical boundary for mobile devices to behave or function a specified way. Admins can assign jobs to be executed at scheduled start time and after the end time using this feature.

To create a **Time Fence** job and push it on an enrolled devices remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select Operating System** screen, click **iOS**.
5. On **Select Job Type** screen, click **Time Fence**.
6. On **Time Fence** prompt, select **Enable Time Fencing**.
7. Click **Select Fence** tab, click **Add Fence**.



**Note:** *Multiple Time Fences can be added.*

8. Enter **Start Time**, **End Time** and select the **Days**.
9. Select **Fence Entered** tab, click **Add**.
10. On **Select Jobs to Add** screen, select multiple jobs from the list using **Ctrl** key.
11. Select **Alert Types** from the following options to receive notification when the device enters the fenced area:

**Device**

**MDM****Email**

12. Click **Save**.
13. Select **Fence Exited** tab, Repeat steps 9 to 12.

The newly created job will get listed in the **Jobs List** section.

14. On the **Job Details** window, enter the **Job Name**.
15. Go back to **Home** tab and select the device(s) or group.
16. Click **Apply** to launch the **Apply Job To Device** prompt.
17. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Nix Settings

**Nix Agent Settings** job remotely configures the password settings for **SureMDM Nix Settings** on an enrolled device(s).

To create a job to configure password settings for **Nix Agent** and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **iOS**.
5. On **Select Job Type** screen, select **Nix Agent Settings**.
6. On **Nix Agent Settings** prompt, enter **Job Name**.
7. Select **Enable Password** and enter **Password**.
8. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the iOS device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Send Text Message

**Send Text** job helps the admins to remotely send text messages or broadcast messages on an enrolled device(s).

To create a job to compose a message and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **iOS**.
5. On **Select Job Type** screen, select **Text Message**.
6. On **Create Text Message** prompt, enter the following details:

**Job Name** - Name of the Job

**Subject** - Subject for the message

**Body** - Message that needs to be conveyed

7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the **iOS** device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Jobs for Android Wear

To deploy few jobs such as install/uninstall/update applications on Android Wear devices, **ADB Debugging** has to be enabled on the device.

To enable **ADB Debugging** on the device, follow these steps:

1. Access device's **Settings** option.
2. Select **System > About >** tap 5 or 6 times on **Build Number**.

**Developer Option** will be enabled and will be available in main **Settings** page.

3. Go to **Developer Option**, enable **ADB Debugging** and **Debug Over WiFi**.

## File Transfer

**File Transfer** job allows the IT admins to push the files on an enrolled device(s) or a group.

To create **File transfer** job and push it on an enrolled device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **File Transfer**.
6. On **Configure Job** screen, enter **Job Name** and click **Add**.
7. On **File Transfer Properties** prompt, enter the following details:

**File Path/URL** - Browse and select the file from the system or specify the link where the file is hosted

**Device Path** - Enter the location of the file to save

8. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

9. Go back to **Home** tab and select the Android Wear device(s) or a group.

10. Click **Apply** to launch the **Apply Job To Device** prompt.

11. On **Apply Job To Device** prompt, select the job(s) and click **Ok** to complete.

## Text Message

**Text Message** job helps the admins to remotely send text messages or broadcast messages on an enrolled device(s).

To create a job to compose a message and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **Text Message**.
6. On **Create Text Message** prompt, enter the following details:

**Job Name** - Name of the Job

**Subject** - Subject for the message

**Body** – Message that needs to be conveyed



**Note:** *Get Read Notification* option is applicable only for Android devices and **Force Read**

*Message* option is applicable only to Android and Windows devices.

7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android Wear device(s) or a group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Run Script

**Run Script** job allows admins to remotely run customized scripts on enrolled devices.

To create a job to run a customized script and push it on an enrolled device(s) or a group remotely for execution, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job** and select **Android Wear**.
4. On **Select Job Type** screen, select **Run Script**.
5. On **Run Script** prompt, enter **Job Name** and **Script** in XML.
6. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

7. Go back to **Home** tab and select the Android Wear device(s) or a group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Nix Agent Settings

**Nix Agent Settings** job remotely configures or updates **SureMDM Nix Agent settings** on an enrolled device(s).

To create a job to configure **Nix Agent Settings** and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **Nix Agent Settings**.
6. On **Nix Agent Settings** prompt, enter **Job Name** and select the following options:
  - Enable time synchronization with server** - Set the periodicity to synchronize **Nix Agent** settings with the server at specified time.



**Note:** *This option works only on Knox devices.*

**Enable device info update** - Set the Periodicity to update device information at specified time.

**Enable Nix Password** - Admin can restrict the access to **Nix Agent Settings** by configuring a password.

**Connection Type** - Select the **Connection Type (Any/ Wi-Fi Only/ Mobile Data Only)** from the drop-down menu to connect to the internet.

8. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android Wear device(s) or group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.



## Composite Job

**SureMDM** allows the user to deploy a combination of job types by a special job called Composite Job. The composite job can have a combination of multiple jobs such as installation, send messages, lock the device and more. Composite Job helps the admin to apply multiple jobs on an enrolled device(s) or a group, with just a single job.

To create a composite job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **Composite Job**.
6. On **Configure Job** screen, enter **Job Name** and click **Add**.



**Note:** *Add Delay* option will delay the job execution for the specified period of time.

7. On **Select Job(s) To Add** prompt, select the job(s).



**Note:** Use **Ctrl** key to select multiple jobs.

8. Go back to **Configure Job** screen.



**Note:** Use the controls, **Move Up** and **Move Down** to arrange the sequence of jobs.

9. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

10. Go back to **Home** tab and select the Android Wear device(s) or group.
11. Click **Apply** to launch the **Apply Job To Device** prompt.

12. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Notification Policy

**SureMDM** allows the creation of notification policies for enrolled devices. Once this job is pushed to the enrolled device, automatic notifications will be sent when the device goes beyond the set threshold.

To configure **Notification Policy** on the enrolled device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **Notification Policy**.
6. On **Notification Policy** screen, following options are available:

**Job Name** - Enter the **Job Name**.

**Disable Notification Policy** - Select this option to disable all the notification settings for a specific Job.

**Enable Battery Policy** - Notifies the user when an enrolled device battery power falls below the set threshold.

**Enable Connection Policy** - Notifies the user when an enrolled device is not connected to a network for a specified period of time.

**Enable Data Usage Policy** - Select this option to set the data usage (in **KB/MB/GB**).  
Notifies the user when an enrolled device data usage exceeds the set threshold.

**Notify when device comes online** - Notifies the user when an enrolled device comes online after being offline.

**Notify when SIM is changed** - Notifies the user when an enrolled device's sim card is changed.

**Send Alert to** - Admins has the option to send the notification to following recipients:

- **SureMDM Web Console**
- **Device**
- **E-Mail Notification** (multiple email ids can be included to receive the notification)

7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android Wear device(s) or group.

9. Click **Apply** to launch the **Apply Job To Device** prompt.

10. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## SureLock Settings

Admin can configure **SureLock** settings remotely on the enrolled devices.

To create **SureLock Settings** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to SureMDM Web Console.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **SureLock Settings**.
6. On **SureLock Settings** prompt, enter **Job Name**, **Password**, **Source** (in XML) and click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android Wear device(s) or a group.

9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Location Tracking

Location tracking job enables the admins to remotely enable Location Tracking on an enrolled device and set tracking periodicity.

To create a **Location Tracking** job and push it on an enrolled device(s) or group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **Location Tracking**.
6. On **Location Tracking** screen, enter **Job Name**.
7. Select **Enable Location Tracking**.
8. Select a value from the spin box (in minutes) in **Tracking Periodicity**.
9. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

10. Go back to **Home** tab and select the Android Wear device(s) or a group.
11. Click **Apply** to launch the **Apply Job To Device** prompt.
12. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## Wi-Fi Settings

Admins can remotely configure Wi-Fi settings on an enrolled device(s).

To create **Wi-Fi Configuration Settings** job and push it on an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **Wi-Fi Settings**.
6. On **WiFi Configuration Settings** screen, click **Add**.
7. On **Add Wi-Fi Config** prompt,
  - a. Enter **SSID** and **Password**.
  - b. Select an option from **Security Type** drop-down menu.
  - c. Select **Auto Connect** to connect the device automatically to Wi-Fi.
  - d. Select **Hidden Network** to connect to the different network manually.
8. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

9. Go back to **Home** tab and select the Android Wear device(s) or group(s).
10. Click **Apply** to launch the **Apply Job To Device** prompt.
11. On **Apply Job To Device** prompt, select the job(s) and click **Apply** to complete.

## Telecom Management Policy

This job allows admins to remotely set thresholds for data usage on an enrolled device(s) or group of devices. Once this job is pushed to the enrolled device, automatic notifications will be sent or mobile data will be blocked if the device goes beyond the set data usage threshold limit. Apart from this, Call logs (incoming/outgoing/missed calls) and SMS logs can be tracked at specified tracking periodicity.

To create **Telecom Management Policy** job and push it to an enrolled device(s) or a group remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **Telecom Management Policy**.
6. On **Telecom Management Policy** prompt,
  - a. Select **Data Usage Tracking** tab.
  - b. Select **Enable Telecom Management**.
  - c. Select an option from **Configure Billing Cycle** drop-down menu.



**Note:** *Billing Start Date / Day* will be auto-populated based on the option selected in the **Configure Billing Cycle**.

- d. Under **Configure Mobile Data Limits**, enter the value to set the **threshold** for the data usage for **Limit 1** and **Limit 2**.



**Note:** *Send Device Alert, Send MDM Alert, Send Email Alert* options are enabled once the value for the threshold is entered.

e. Under **Action**, select the following:

**Send Device Alert** - Notifies the device user when the data usage exceeds the set threshold.

**Send MDM Alert** - Notifies the **MDM** admins when the data usage exceeds the set threshold.

**Send Email Alert** - Notifies the admins by email when the data usage exceeds the set threshold.

f. Select **Call Log Tracking** tab.

g. Select **On** from **Call Log Tracking** drop-down menu.

h. Select a value from the spin box to set **Tracking Periodicity** (in minutes).



**Note:** This option is enabled only when **Call Log Tracking** is **On**.

i. Select **SMS Log Tracking** tab.

j. Select **On** from **SMS Log Tracking** drop-down menu.

k. Select a value from the spin box to set **Tracking Periodicity** (in minutes).



**Note:** This option is enabled only when **SMS Log Tracking** is **On**.

7. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

8. Go back to **Home** tab and select the Android Wear device(s) or a group.

9. Click **Apply** to launch the **Apply Job To Device** prompt.

10. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.



**Note:** This feature may not work on certain Android Wear /Smartwatches.

## Call Log Tracking

Admins can remotely track call logs on the enrolled devices.

To create **Call Log Tracking** job and push it on an enrolled device(s) remotely, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job** and select **Android Wear**.
4. On **Select Job Type** screen, select **Call Log Tracking**.
5. On **Call Log Tracking** prompt,
  - a. Enter **Job Name**.
  - b. Select an option from the **Call Log Tracking** drop-down menu.
  - c. Select a value from the spin box to set **Tracking Periodicity** (in minutes).
6. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

7. Go back to **Home** tab and select the Android Wear device(s) or group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.



**Note:** This feature may not work on certain Android Wear /Smartwatches.

## SMS Log Tracking

Admins can remotely track SMS logs on the enrolled device(s).

To create **SMS Log Tracking** job and push it on an enrolled device(s) remotely, follow these steps:



1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **SMS Log Tracking**.
6. On **SMS Log Tracking** prompt,
  - a. Enter **Job Name**.
  - b. Select an option from **SMS Log Tracking** drop-down menu.
  - c. Select a value from the spin box to set **Tracking Periodicity** (in minutes).
  - d. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

7. Go to **Home** tab and select the Android Wear device(s) or group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.



**Note:** This feature may not work on certain Android Wear /Smartwatches.

## Remote Buzz

When a device is lost or misplaced, **Remote Buzz** job helps admin to locate the device by pushing a job which forces it to make a sound.

To create a **Remote Buzz** job remotely to locate the device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.

4. On **Select the OS** screen, select **Android Wear**.
5. On **Select Job Type** screen, select **Remote Buzz**.
6. Enter **Job Name** and click **Ok**.

The newly created job will get listed in the **Jobs List** section.

7. Go back to **Home** tab and select the Android Wear device(s) or group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

Once this job is applied on an enrolled device, a buzzing sound will be heard from the device.

## Jobs for Linux

### Run Script

**Run Script** job will run customized scripts on an enrolled device(s).

To create a job to remotely run the customized script and push it on an enrolled device(s) or a group, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job** and select **Linux**.
4. On **Select Job Type** screen, select **Run Script**.
5. On **Run Script** prompt, enter **Job Name** and **Script**.
6. Click **Advanced Settings** to enter the **File Name, Default Path, Permission**.
7. Click **Browse** and select the file from the location.
8. Click **Save**.

The newly created job will get listed in the **Jobs List** section.

9. Go back to **Home** tab and select the Linux device(s) or group.
10. Click **Apply** to launch the **Apply Job To Device** prompt.
11. On **Apply Job To Device** prompt, select the job and click **Ok** to complete.

## File Transfer

**File Transfer** job allows the IT admins to remotely push the files on the enrolled devices.

To create **File transfer** job and push it on an enrolled device(s) or a group, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Jobs**.
3. On **Jobs** screen, click **New Job**.
4. On **Select the OS** screen, select **Linux**.
5. On **Select Job Type** screen, select **File Transfer**.
6. On **Configure Job** screen, enter **Job Name** and click **Add**.
7. On **File Transfer Properties** prompt, enter the following details:

**File Path/URL** - Browse and select the file from the system or specify the link where the file is hosted

**Device Path** - Enter the location of the file to save

8. Click **Ok**.

The newly created job will get listed in the **Jobs List** section.

9. Go back to **Home** tab and select the Linux device(s) or group.
10. Click **Apply** to launch the **Apply Job To Device** prompt.
11. On **Apply Job To Device** prompt, select the job(s) and click **Ok** to complete.

## Profiles

Profiles in **SureMDM** allows admins to control the functions and settings of specific installed apps and enrolled devices.

Profiles created under different platforms are given below:

### Profiles for Android

#### Create Android Work Profile and push it to the enrolled devices

Work Profile allows admins to create below mentioned profiles:

- [Password Policy](#)
- [System Settings](#)
- [Application Policy](#)
- [Network Settings](#)
- [Certificate](#)
- [Mail Configuration](#)
- [Wi-Fi Configuration](#)
- [File Sharing Policy](#)

#### Password Policy

**Password Policy** allows admin to configure password settings on the enrolled devices. The settings can be configured for the device or for the applications in the container or both.

To create a password policy profile, follow these steps:

1. Login to **SureMDM Web Console**
2. On **SureMDM Web Console**, select **Profiles**.

3. On **Profiles** screen, select **Android** and click **Add**.
4. On **Work Profile** panel, click **Password Policy > Configure**.
5. Enter **Profile Name**.
6. Select the **Profile Type (Device Security/ Work Security/ Device & Work Security)**.
  - When **Device Security Profile Type** is selected, following fields are listed.
    - ✓ Device Minimum Password Quality
    - ✓ Device Minimum Password Length
    - ✓ Device Maximum Failed Attempts
    - ✓ Device Maximum Password Age (in hours)
    - ✓ Device Enforce Password History
    - ✓ Device Maximum Time to Lock (in seconds)
  - When **Work Security Profile Type** is selected, following fields are listed.
    - ✓ Work Profile Minimum Password Quality
    - ✓ Work Profile Minimum Password Length
  - When both **Device & Work Security Profile Type** is selected, following fields are listed.
    - ✓ Device Minimum Password Quality
    - ✓ Device Minimum Password Length
    - ✓ Device Maximum Failed Attempts
    - ✓ Device Maximum Password Age (in hours)
    - ✓ Device Enforce Password History
    - ✓ Device Maximum Time to Lock (in seconds)
    - ✓ Work Profile Minimum Password Quality
    - ✓ Work Profile Minimum Password Length
7. Enter the details in the fields.
8. Click **Save** to complete.

The newly created profile gets listed in the **Profiles** section.

9. Go back to **Home** tab and select the device(s) or group.
10. Click **Apply** to launch the **Apply Job To Device prompt**.
11. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## System Settings

**System Settings** allows admin to set policies to enable or disable certain system settings like USB debugging, install from unknown sources and more on the enrolled devices.

To create a system settings profile, follow these steps:

1. Login to **SureMDM Web Console**
2. On **SureMDM Web Console**, select **Profiles**.
3. On **Profiles** screen, select **Android** and click **Add**.
4. On **Work Profile** panel, select **System Settings > Configure**.
5. Enter **Profile Name**.
6. On **System Settings** prompt, select the desired system settings options.
7. Click **Save** to complete.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.
9. Click **Apply** to launch the **Apply Job To Device prompt**.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Application Policy

**Application Policy** allows admin to configure policies for App Store, Play For Work and System Applications on the enrolled devices.

To create **Application Policy** profile, follow these steps:

1. Login to **SureMDM Web Console**
2. On **SureMDM Web Console**, select **Profiles**.
3. On **Profiles** screen, select **Android** and click **Add**.
4. On **Work Profile** screen, click **Application Policy > Configure**.
5. Enter **Profile Name**.
6. Click **Add**.
7. On **Select Application Source** prompt, select an option from the following:
  - a. **SureMDM App Store**
  - b. **Play For Work**
  - c. **Configure System Apps**
8. Select or enter the required details.
9. Click **Save** to complete.

The newly created profile gets listed in the **Profiles** section.
10. Go back to **Home** tab and select the device(s) or group.
11. Click **Apply** to launch the **Apply Job To Device** prompt.
12. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Network Settings

**Network Settings** allows admin to configure policies for network connection on the enrolled devices.

To create a **Network Settings** profile, follow these steps:

1. Login to **SureMDM Web Console**
2. On **SureMDM Web Console**, select **Profiles**.
3. On **Profiles** screen, select **Android** and click **Add**.
4. On **Work Profile** panel, click **Network Settings > Configure**.

5. Enter **Profile Name**.
6. On **Network Settings** screen,
  - a. Select **Proxy Type** from the drop-down menu.
  - b. Enter **Package Name**.
  - c. Select **Disable network access when VPN is not connected**.



**Note:** It will work only when VPN is connected.

7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.
8. Go back to **Home** tab and select the device(s) or group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Certificate

**Certificate** in **Profiles** allows admins to remotely upload corporate certificates and other certificates that is necessary to authenticate the device access to the network.

To create a **Certificate profile**, follow these steps:

1. Login to **SureMDM Web Console**
2. On **SureMDM Web Console**, select **Profiles**.
3. On **Profiles** screen, select **Android** and click **Add**.
4. On **Work Profile** screen, click **Certificate > Configure**.
5. On **Certificate** prompt,
  - To fetch the existing SCEP certificate from CA server, follow these steps:
    - a. Deselect **Create Certificate Using SCEP**.
    - b. Select **Certificate Usage (VPN and Apps / Wi-Fi)** from the drop-down list.



- c. Upload **Certificate** file from saved location.
  - d. Enter **Password** and click **Add**.
- To get SCEP certificate from another CA server, follow these steps:
    - a. Select **Create Certificate Using SCEP**.
    - b. Select **Certificate Usage (VPN and Apps / Wi-Fi)** from the drop-down list.
    - c. Select **Override Account-Wide SCEP Settings**.

This will enable admin to create and configure another certificate using SCEP. To configure SCEP in **SureMDM**, see the steps under [Configure SCEP](#).

- d. Click **Add**.

The newly created profile gets listed in the **Profiles** section.

6. Enter **Profile Name**.
7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.
9. Click **Apply** to launch the **Apply Job To Device prompt**.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Mail Configuration

**Mail Configuration** allows admin to configure the email account settings on the enrolled devices.



**Note:** Currently this feature support settings configuration for **POP** or **IMAP** email accounts.

To create a **Mail Configuration** profile, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Android > Add**.

4. On **Work Profile** screen, click **Mail Configuration > Using Gmail App**.

5. Enter **Profile Name**.

6. On **Mail Configuration** screen, enter the following details:

- Email Address
- Hostname or Host
- Username
- Device Identifier
- SSL Required
- Trust all Certificates
- Login Certificate Alias
- Default Email Signature
- Default Sync Window

7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.

9. Click **Apply** to launch the **Apply Job To Device** prompt.

10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.



**Note:** When **Mail Configuration** profile is deployed on multiple devices to configure multiple email accounts then **wild card** characters can be used to refer **Email Address** as “**\$Email Address\$**” and **Username** as “**\$Username\$**”. So that the device users can login with their Email Address and Username. For the Wild card option to work, the device should be enrolled with OAuth (G Suite, ADFS and Azure AD).

## Wi-Fi Configuration

**Wi-Fi Configuration** allows admin to configure Wi-Fi settings on the enrolled devices.

To configure **Wi-Fi** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Android > Add**.
4. On **Work Profile** screen, click **Wi-Fi Configuration > Configure**.
5. Enter **Profile Name**.
6. On **WiFi Configuration** prompt, enter the following:
  - SSID
  - Password
  - Security Type
  - Auto Connect
  - Hidden Network
7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## File Sharing Policy

**File Sharing Policy** offers a secure way to share and distribute enterprise files on devices through **File Store** option. This option allows the IT Admins to create a document library using **File Store** feature and share documents like images, videos and other files across enrolled devices.

To share a file using **File Sharing Policy**, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.

3. On **Profiles** screen, click **Android > Add**.
4. On **Work Profile** screen, click **File Sharing Policy > Configure**.
5. Enter **Profile Name**.
6. Click **Add** to launch **File Store** prompt.
7. Select the desired files or folders and click **Add**.  

The selected files will get listed in the box located on the right side of the screen.
8. Click **Done**.  

The selected files will get listed in the **File Sharing Policy** section.
9. Click **Save**.  

The newly created Profile gets listed in the **Profiles** section.
10. Go back to **Home** tab and select the device(s) or group.
11. Click **Apply** to launch the **Apply Job To Device** prompt.
12. On Apply Job To Device prompt, select the created profile and click Apply to complete.

## Profiles for iOS

To use remote features in **SureMDM** like **Single App Mode** and **Silent App Installation** on enrolled iOS devices, the user needs to activate **Supervised Mode** on the device or has to be **DEP** enrolled.



**Note:** Select **Supervised Mode** to wipe all data from iOS device. For security reasons, Apple does not allow to supervise the device if **Find My iPhone** option is selected.

To activate **Supervised Mode** on an iOS device, follow these steps:

1. Download and install **Apple Configurator2** on Mac.
2. Attach iOS device to the Mac.
3. Run the **Apple Configurator2**.

4. Select the device and click **Prepare**.
5. Select **Manual** from the drop-down and click **Next**.
6. Select **Do not enroll in MDM** from the **Server** drop-down menu and click **Next**.
7. On **Supervise Devices** screen, select **Supervise Device** and **Allow devices to pair with other computer** and click **Next**.
8. On **Create an Organisation** prompt, enter the details and click **Next**.
9. Select **Generate a new supervision identity** and click **Next**.
10. On **Configure iOS Setup Assistant** prompt, configure **Setup Assistant** and click **Prepare** to complete.

The device will wipe all data and reboot the device.

## Create iOS Profile and push it to the enrolled devices

**iOS MDM Profile** allows admins to create below mentioned policies:

- [Blacklist/Whitelist Apps](#)
- [Web Content Filter](#)
- [Branding](#)
- [Passcode Policy](#)
- [Single App Mode Profile](#)
- [Restriction Profile](#)
- [Application Policy](#)
- [Configuration Profile](#)
- [Wi-Fi Configuration](#)
- [Mail Configuration](#)
- [Global HTTP Proxy](#)

- [VPN](#)
- [Certificate](#)
- [Exchange ActiveSync](#)
- [File Sharing Policy](#)

## Blacklist/Whitelist Apps

Admins can allow or disallow certain applications to function on an enrolled device.

### Blacklist Apps

Disables desired applications from functioning on iOS devices and app icon will not be visible on the screen for launching.

To blacklist applications, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS MDM Profile** screen, select **Blacklist/Whitelist Apps** and click **Blacklist Apps Configure**.
5. On **Blacklist Apps** page, click **Add**.
6. On **Application List** prompt, choose the app from **App Name** drop-down menu.



**Note:** *App Id* is auto-populated when *App Name* is selected.

The selected app gets listed under **Blacklist Apps** section.

7. Enter **Profile Name** and click **Save.Ap**

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or a group.
9. Click **Apply** to launch **Apply Job To Device** prompt.

10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

### Whitelist Apps

Allows only desired apps to function on an iOS device and restricts all other apps.

To whitelist applications, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS MDM Profile** screen, select **Blacklist/Whitelist Apps** and click **Whitelist Apps Configure**.
5. On **Whitelist Apps** page, click **Add**.
6. On **Application List** prompt, choose the app from **App Name** dropdown menu and click **Add**.



**Note:** *App Id* will be auto-populated when **App Name** is selected.

The selected app gets listed under **Whitelist Apps** section.

7. Enter **Profile Name** and click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or a group.
9. Click **Apply** to launch **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.



**Note:** *Contacts* and *Settings* are two native apps that cannot be blacklisted. Admins can use **Restrictions Profile** option to disable specific settings under **Settings**.

## Web Content Filter

**Web Content Filter** is an in-built option to assist web filtering for supervised iOS devices.

Following options are available in **Web Content Filter**:

- **Blacklist URLs** - Block specific URLs from being accessed on enrolled iOS devices.

To blacklist URLs on enrolled iOS devices, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS MDM Profile** screen, click **Web Content Filter** and click **Configure**.
5. On **Web Content Filter** screen, click **Blacklisted URLs** tab and then click **Add**.
6. Enter the **URL** to be blacklisted and click **Add**.

The blacklisted URL will get listed under **Blacklisted URL** section.

7. Enter **Profile Name** and click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or a group.
9. Click **Apply** to launch **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

- **Whitelisted Bookmarks** - Allows access to the selected bookmarks on enrolled iOS devices.

To whitelist bookmarks on enrolled iOS devices, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.



4. On **iOS MDM Profile** screen, click **Web Content Filter** and click **Configure**.
5. On **Web Content Filter** screen, click **Whitelisted Bookmarks** tab and then click **Add**.
6. On **Whitelist Bookmark** prompt, enter the following details and click **Add**.

- **Title** – Name
- **URL** – URL of the bookmark
- **Bookmark Path** – Path of the bookmark

The bookmark that is allowed to access will get listed in **Whitelisted Bookmarks**.

7. Enter **Profile Name** and click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or a group.
9. Click **Apply** to launch **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

- **Auto Filter** - Automatically blocks all web pages with adult content or allow browsing of only selected URLs.

To **Auto Filter web contents** on enrolled iOS devices, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS MDM Profile** screen, click **Web Content Filter** and click **Configure**.
5. On **Web Content Filter** screen, select **Auto Filter > Enable Auto Filtering** to block all webpages with adult content and then click **Add**.
6. On **Filtered URL** prompt, enter the **URL** to be allowed for accessing and click **Add**.

The URL to be allowed for accessing will get listed in **Auto Filter** section.

7. Enter **Profile Name** and click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or a group.
9. Click **Apply** to launch **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Branding

Admin can remotely brand an iOS supervised device by setting a wallpaper for **Home** and **Lock Screen**.

To brand an enrolled iOS device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS MDM Profile** screen, select **Branding**, enter **Profile Name** and click **Configure**.
5. On **Set Wallpaper** page, click **+** to browse and select the desired wallpaper.
6. Select **Use Home Screen wallpaper** option if the user wants to use the same wallpaper for **Lock Screen**.

Or

Disable **Use Home Screen wallpaper** option if the user wants to use some other wallpaper for **Lock Screen**, click **+** to browse and select the desired wallpaper.

7. Click **Save** to complete.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or a group.
9. Click **Apply** to launch **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Passcode Policy

**Passcode Policy** allows admin to configure password settings on the enrolled devices.

To create a password policy and push it on an enrolled device(s), follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS MDM Profile** screen, click **Passcode Policy**, enter the **Profile Name** and click **Configure**.
5. On **Passcode Policy** section, enter following details:
  - Force User To Set Passcode
  - Allow Simple Value
  - Require Alphanumeric Value
  - Minimum Passcode Length
  - Minimum Number Of Complex Characters
  - Maximum Passcode Age (1-730 Days, Or None)
  - Maximum Auto-Lock
  - Passcode History (1-50 Passcodes, Or None)
  - Maximum Grace Period For Device Lock
  - Maximum Number Of Failed Attempts

6. Click **Save** to complete.

The newly created profile gets listed in the **Profiles** section.

7. Go back to **Home** tab and select the device(s) or a group.
8. Click **Apply** to launch **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Single App Mode Profile

Lock down iOS supervised devices with just one application in the foreground all the time.

Once enabled, it disables Home Button, Notifications, and Control Center.

To create a **Single App Mode** profile, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS Work Profile** screen, select **Single App Mode Profile**, enter the **Profile Name** and click **Configure**.
5. On **Single App Mode** screen, enter following details:
  - Lockdown Application
  - Single App Mode
  - Launch Periodically
  - Periodicity (in mins.)



**Note:** Lockdown works only for the apps installed on the device.

6. Click **Save** to complete.

The newly created profile gets listed in the **Profiles** section.

7. Go back to **Home** tab and select the device(s) or a group.
8. Click **Apply** to launch **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Restriction Profile

**SureMDM** offers lockdown of selective settings, functions and media content on enrolled devices.

To create a **Restriction Profile**, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS MDM Profile** screen, click **Restriction Profile**, enter **Profile Name** and click **Configure**.

**Restriction** section lists out all functions on the device under following three categories:

- Functionality
  - Apps
  - Media Content
5. Deselect the desired features from different categories to restrict and click **Save**.  
The newly created profile gets listed in the **Profiles** section.
  6. Go back to **Home** tab and select the device(s) or a group.
  7. Click **Apply** to launch **Apply Job To Device** prompt.
  8. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

### [Application Policy](#)

**Application Policy** allows admin to install and configure apps remotely on the enrolled device(s).

To install and configure application remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS Work Profile** screen, select **Application Policy**, enter the **Profile Name** and click **Configure**.
5. On **Application Policy** section, click **Add**.
6. On **Add App** prompt, select the app name from drop-down menu.

7. Select **Install Silently** to install the app without device user's interference.
8. Click **Add**.

The application details get listed in **Application Policy** section.

9. On **Application Policy** section, select the app and click **Config**.
10. On **Application Configuration** prompt, enter the details for the following:
  - Key
  - Value
11. Click **Save** to complete.

The newly created profile gets listed in the **Profiles** section.

12. Go back to **Home** tab and select the device(s) or a group.
13. Click **Apply** to launch **Apply Job To Device** prompt.
14. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

### Configuration Profile

**Configuration Profile** allows admin to install and configure apps remotely on enrolled devices.

To install and configure application remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS Work Profile** screen, select **Configuration Profile**, enter the **Profile Name** and click **Configure**.
5. On **Configuration** prompt, click **Add**.
6. On **Application Configuration** prompt, select or enter the details:
  - App Name App ID
  - Key
  - Value



**Note:** *App Id* will get auto-populated when an application from **App Name** drop-down is selected.

7. Click **Save**.

The application details will get listed in the **Configuration** section.

8. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

9. Go back to **Home** tab and select the device(s) or a group.

10. Click **Apply** to launch **Apply Job To Device** prompt.

11. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Wi-Fi Configuration

**Wi-Fi Configuration** allows admin to remotely configure Wi-Fi settings on the enrolled device.

To configure **Wi-Fi** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS Work Profile** screen, select **Wi-Fi Configuration**, enter the **Profile Name** and click **Configure**.
5. On **Wi-Fi Configuration** prompt, click **Add**.
6. On **WiFi Configuration** screen, enter the details for following:
  - SSID
  - Security Type (WEP/WPA or WPA Personal /WPA2 Personal/Any/EAP or TLS/PEAP)



**Note:** Entering password is mandatory when **Security Type** is selected as

WEP, WPA, WPA2, Any.

- Hidden Network
- Auto Join
- Proxy Setup

7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or a group.

9. Click **Apply** to launch **Apply Job To Device** prompt.

10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Mail Configuration

**Mail Configuration** profile allows admin to remotely configure email account on an enrolled device.



**Note:** Currently this feature support settings configuration for **POP** or **IMAP** email accounts.

To configure an email account remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS Work Profile** screen, select **Mail Configuration**, enter the **Profile Name** and click **Configure**.
5. On **Mail Configuration** screen, select or enter the following details:
  - Account Description
  - Account Type



- User Display Name
  - Email Address
  - Allow User To Move Message From This Account
  - Allow Recent Addresses To Be Synced
  - Use Only In Mail
6. Enter the following details in **Incoming Mail** and **Outgoing Mail** fields and click **Save**.
- Mail Server and Port
  - Username
  - Authentication Type
  - Use SSL

The newly created profile gets listed in the **Profiles** section.

7. Go back to **Home** tab and select the device(s) or a group.
8. Click **Apply** to launch **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Global HTTP Proxy

**Global HTTP Proxy** profile configures settings for the proxy server. This feature can only be applied to iOS 6 supervised devices and provides data security since all personal and business communication is filtered through the **Global HTTP proxy**.

To configure **Global HTTP Proxy** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS Work Profile** screen, select **Global HTTP proxy**, enter the **Profile Name** and click **Configure**.

5. On **Global HTTP Proxy** screen, enter following details:

- Proxy Type
- Proxy Server And Port
- Username
- Password
- Allow Bypassing Proxy To Access Captive Networks

The newly created profile gets listed in the **Profiles** section.

6. Go back to **Home** tab and select the device(s) or a group.

7. Click **Apply** to launch **Apply Job To Device** prompt.

8. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## VPN

**VPN** profile allows admin to configure the enrolled device to connect to a wireless network via VPN.

To configure **VPN** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS Work Profile** screen, select **VPN**, enter **Profile Name** and click **Configure**.
5. On **VPN** screen, enter the following details:
  - Connection Name
  - Connection Type
  - Server
  - Account
  - User Authentication

- Password
  - Shared Secret
  - Send All Traffic
6. Click **Save**.

The newly created profile gets listed in the **Profiles** section.
  7. Go back to **Home** tab and select the device(s) or a group.
  8. Click **Apply** to launch **Apply Job To Device** prompt.
  9. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Certificate

**Certificate** in **Profiles** allows admin to remotely upload corporate certificates and other certificates that is necessary to authenticate the device access to the network.

To create and configure **Certificate** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS Work Profile** screen, select **Certificate**, enter **Profile Name** and click **Configure**.
5. On **Certificate** prompt,
  - To fetch the existing SCEP certificate from CA server, follow these steps:
    - a. Deselect **Create Certificate Using SCEP**.
    - b. Upload the **Certificate** file from saved location.
    - c. Enter **Password** and click **Add**.
  - To get SCEP certificate from another CA server, follow these steps:
    - a. Select **Create Certificate Using SCEP**.
    - b. Select **Override Account-Wide SCEP Settings**.

This will enable admin to create and configure another certificate using SCEP. To configure SCEP in **SureMDM**, see the steps under [Configure SCEP](#).

b. Click **Add**.

The newly created profile gets listed in the **Profiles** section.

6. Click **Save**.
7. Go back to **Home** tab and select the device(s) or a group.
8. Click **Apply** to launch **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Exchange ActiveSync

When an email account is configured in **Exchange Active Sync**, the device users can schedule to sync their Mails, Contacts, Calendars, Reminders and Notes remotely on enrolled devices.

To configure **Exchange ActiveSync** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS Work Profile** screen, select **Exchange ActiveSync**, enter **Profile Name** and click **Configure**.
5. On **Exchange ActiveSync** screen, enter the following details:
  - Account Name
  - Exchange ActiveSync Host
  - Use SSL
  - User
  - Email Address

- Password
  - Days To Sync
  - Authentication
  - Allow Messages To Be Moved
  - Allow Recent Addresses To Be Synced
  - Use Only In Mail
6. Click **Save**.

The newly created profile gets listed in the **Profiles** section.
  7. Go back to **Home** tab and select the device(s) or a group.
  8. Click **Apply** to launch **Apply Job To Device** prompt.
  9. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## File Sharing Policy

**File Sharing Policy** offers a secure way to share and distribute enterprise files on enrolled devices. This option allows the IT Admins to share documents like images, videos and other files on enrolled devices.

To share a file using **File Sharing Policy**, upload the file to **File Store** and follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **iOS > Add**.
4. On **iOS Work Profile** screen, select **File Sharing Policy**, enter **Profile Name** and click **Configure**.
5. On **File Sharing Policy** screen, click **Add** to launch **File Store** prompt.
6. On **File Store** prompt, select the desired document or folder and click **Add**.

The selected files will get listed in the box located on the right side of the screen.

7. Click **Done**.

The selected files will get listed in the **File Sharing Policy** section.

8. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

9. Go back to **Home** tab and select the device(s) or a group.

10. Click **Apply** to launch the **Apply Job To Device** prompt.

11. On **Apply Job To Device** prompt, select the Profile(s) and click **Apply** to complete.

## Profiles for Windows

In order to create profile policies for Windows devices, the device needs to be registered with EMM Windows.

### Enroll devices to EMM Windows

To enroll devices to **EMM Windows**, follow these steps:

1. Launch **Settings** on the Windows device.
2. Search for **Work** and select **Access Work or School**.
3. Select **Enroll Only in Device Management (MDM)**.
4. Click **Connect**.
5. Enter **Email Address** in the box and click **Continue**.
6. Enter **MDM Server URL**.
7. Enter **Customer Id** and click **Enroll Device**.

A confirmation prompt appears on successful enrollment.



**Note:** EMM features in **Profiles** is applicable only for **Windows 10** platform.

## Create Windows profile and push it to the enrolled devices

Windows Profile allows admins to create below mentioned profiles:

- [Password Policy](#)
- [Mail Configuration](#)
- [Restriction Policy](#)
- [App Locker](#)
- [Wi-Fi Configuration](#)
- [VPN Configuration](#)
- [Exchange ActiveSync](#)
- [Application Policy](#)
- [Configuration Profile](#)
- [Periodic App Launch](#)
- [Certificate](#)
- [File Sharing Policy](#)

### Password Policy

**Password Policy** allows admin to configure password settings on the enrolled devices.

To create Password Policy profile, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** screen, select **Password Policy > Configure**.
5. Enter **Profile Name**.

6. On **Device Password Policy** section, enable **Device Lock** and enter the following details:

- Minimum Password Length
- Maximum Password Failed Attempts
- Password Expiration (in days)
- Password History
- Maximum Inactivity Time to Device Lock (in minutes)

7. Click **Save** to complete.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.

9. Click **Apply** to launch the **Apply Job To Device prompt**.

10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Mail Configuration

**Mail Configuration** profile allows admin to remotely configure an email account on the enrolled device.



**Note:** Currently this feature support settings configuration for **POP** or **IMAP** email accounts.

To configure an email account on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** screen, click **Mail Configuration > Configure**.
5. Enter the **Profile Name** and click **Add**.
6. On **Mail Configuration** screen, enter following details:
  - Account Name



- Your Name
  - Account Type
  - Email Address
  - Username
  - Password
7. Select or enter the following details in **Incoming Mail**, **Outgoing Mail** tabs and click **Add**.
    - Mail server and Port
    - Use SSL

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Restriction Policy

**SureMDM** offers lockdown of selective settings, functions and media content on enrolled devices. For example, if admins want the device users to have access to everything on the device except **Camera** and use of **Storage Card**, then a **Restriction Profile** can be created using **SureMDM** and apply it remotely to the desired devices.

To create a **Restriction Profile**, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** screen, click **Restriction Policy > Configure**.
5. Enter **Profile Name**.

6. In **Restriction Policy** section, deselect the desired features under the following options to restrict the functionalities on the device.

- Camera
- System
- Experience

7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.

9. Click **Apply** to launch the **Apply Job To Device** prompt.

10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## App Locker

**App Locker** allows admin to remotely lock specific apps on enrolled devices to maintain privacy and security.

To create an **App Locker** policy, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** screen, click **App Locker > Configure**.
5. Enter **Profile Name** and click **Add**.
6. On **App Locker** prompt, enter the following details:
  - a. Select the **Action (Allow / Deny)**.
  - b. Enter **Publisher** and **Package Name**.
7. Click **Add > Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.

9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Wi-Fi Configuration

**Wi-Fi Configuration** allows admin to configure Wi-Fi settings on the enrolled devices.

To configure **Wi-Fi** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** screen, click **Wi-Fi Configuration > Configure**.
5. Enter **Profile Name** and click **Add**.
6. On **WiFi Configuration** prompt, enter the following:
  - SSID
  - Security Type
  - Encryption Type
  - Disable Internet Connectivity Checks
  - Hidden Network
  - Auto Join
7. Click **Add > Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## VPN Configuration

**VPN Configuration** allows admin to create a secured network for the enrolled windows devices.

To configure **VPN** settings, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** screen, click **VPN Configuration > Configure>**
5. Enter **Profile Name**.
6. Enter the following details in **VPN** section,
  - Profile Name
  - Profile Type
  - Application Trigger List
  - Remember Credentials
  - Always On
  - Lock Down
  - DNS Suffix
  - Trusted Network Detection
  - Próxy

7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.
9. Click **Apply** to launch the **Apply Job To Device prompt**.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Exchange Active Sync

When an email account is configured in **Exchange Active Sync**, the device users can sync their Mails, Contacts, Calendars, Reminders and Notes remotely on enrolled devices.

To configure **Exchange ActiveSync remotely** on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** screen, select **Exchange ActiveSync > Configure**.
5. Enter **Profile Name**.
6. Click **Add** and enter the following details:
  - Account Name
  - Exchange ActiveSync Host
  - Username
  - Email Address
  - Password
  - Sync Schedule
  - Days to Sync
7. Click **Add > Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.
9. Click **Apply** to launch the **Apply Job To Device prompt**.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Application Policy

**Application Policy** allows admin to remotely install apps on the enrolled devices.

To create a profile to install an application, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** screen, click **Application Policy > Configure**.
5. Enter **Profile Name**.
6. Click **Add** and enter **Name** and **URL** of the Application in **Add App** prompt.
7. Click **Add > Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.
9. Click **Apply** to launch the **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

### [Configuration Profile](#)

**Configuration Profile** allows admin to remotely configure application settings on the enrolled devices.

To create a profile to configure application settings, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** prompt, select **Configuration Profile > Configure**.
5. Enter **Profile Name**.
6. Click **Add** and enter the following details in **Application Configuration** prompt:
  - App Name
  - Key
  - Value

7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.

9. Click **Apply** to launch the **Apply Job To Device prompt**.

10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Periodic App Launch

**Periodic App Launch** allows admin to remotely launch the application at a specified interval of time on enrolled device.

To create a profile to launch the application periodically, follow these steps:

1. Login to **SureMDM Web Console**.

2. On **SureMDM Web Console**, click **Profiles**.

3. On **Profiles** screen, click **Windows > Add**.

4. On **Windows Profile** prompt, click **Periodic App Launch > Configure**.

5. Enter **Profile Name**.

6. Select an application from **Application** drop-down menu and enter **Periodicity** in **minutes**.

7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or group.

9. Click **Apply** to launch the **Apply Job To Device prompt**.

10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Certificate

**Certificate** in **Profiles** allows admin to remotely upload corporate certificates and other certificates that is necessary to authenticate the device access to the network.

To create and configure **Certificate** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** screen, select **Certificate**, enter **Profile Name** and click **Add Certificate Configure**.
5. On **Certificate** prompt,
  - a. Select **Store Location (Local Machine/ Current User)** for the certificate to save.
  - b. Upload the **Certificate** file from saved location.
  - c. Enter **Password** and click **Add**.

The newly created profile gets listed in the **Profiles** section.

6. Go back to **Home** tab and select the device(s) or a group.
7. Click **Apply** to launch **Apply Job To Device** prompt.
8. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## File Sharing Policy

**File Sharing Policy** offers a secure way to share and distribute enterprise files on enrolled devices. This option allows the IT Admins to share documents like images, videos and other files across enrolled devices.

To share a file using **File Sharing Policy**, upload the file to **File Store** and follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.
4. On **Windows Profile** screen, Select **File Sharing Policy > Configure**.
5. Enter **Profile Name**.



6. Click **Add** to launch **File Store** prompt.
7. Select the desired files or folders and click **Add**.

The selected files will get listed in the box located on the right side of the screen.

8. Click **Done**.

The selected files will get listed in the **File Sharing Policy** section.

9. Click **Save**.

The newly created profile gets listed in the **Profiles** section.



**Note:** *File sharing Policy is not supported in EMM windows.*

10. Go back to **Home** tab and select the device(s) or a group.
11. Click **Apply** to launch the **Apply Job To Device** prompt.
12. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Profiles for macOS

### Create macOS profile and push it to the enrolled devices

**macOS Profile** allows admins to create below mentioned profiles:

[Restriction Profile](#)

[Blacklist/Whitelist Apps](#)

[Wi-Fi Configuration](#)

[Certificate](#)

[Passcode Policy](#)

[Mail Configuration](#)

[Exchange ActiveSync](#)

**SureMDM** offers lockdown of selective settings, functions and media content on enrolled devices.

To create a **Restriction Profile**, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, select **macOS** and click **Add**.
4. On **macOS Profile** prompt, click **Restriction Profile**, enter **Profile Name** and click **Configure**.

**Restriction** section lists out the functions that are enabled on the device:

- Allow use of camera
  - Allow iCloud documents < data
  - Allow iCloud Keychain
  - Allow iCloud Photo Sharing
  - Allow Spotlight Suggestions
  - Allow Touch ID to unlock device
  - Allow Definition Lookup
  - Allow music service
  - Allow profile removal
5. Deselect the desired features from different categories to restrict and click **Save**.  
The newly created profile gets listed in the **Profiles** section.
  6. Go back to **Home** tab and select the device(s) or a group.
  7. Click **Apply** to launch **Apply Job To Device** prompt.
  8. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Blacklist/Whitelist Apps

Admins can allow or disallow certain applications to function on an enrolled device.

### Blacklist Apps

Disables desired applications from functioning on macOS devices and app icon will not be visible on the screen for launching.

To blacklist applications, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, select **macOS** and click **Add**.
4. On **macOS Profile** prompt, click **Blacklist/Whitelist Apps**, enter **Profile Name** and click **Blacklist Apps Configure**.
5. On **Blacklist Apps** page, click **Add**.
6. On **Blacklist Application** prompt, enter **Name**, **Path To Application** and click **Add**.

The selected app gets listed under **Blacklist Apps** section.

7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or a group.
9. Click **Apply** to launch **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

### Whitelist Apps

Allows only desired apps to function on macOS device and restricts all other apps.

To whitelist applications, follow these steps:

1. Login to **SureMDM Web Console**.

2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, select **macOS** and click **Add**.
4. On **macOS Profile** prompt, click **Blacklist/Whitelist Apps**, enter **Profile Name** and click **Blacklist Apps Configure**.
5. On **Whitelist Apps** page, click **Add**.
6. On **Whitelist Application** prompt, enter **Name**, **Path To Application** (path of the application) and click **Add**.

The selected app gets listed under **Whitelist Apps** section.

7. Enter **Profile Name** and click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or a group.
9. Click **Apply** to launch **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Wi-Fi Configuration

**Wi-Fi Configuration** allows admin to remotely configure Wi-Fi settings on the enrolled device.

To configure **Wi-Fi** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, select **macOS** and click **Add**.
4. On **macOS Profile** prompt, click **Wi-Fi Configuration**, enter **Profile Name** and click **Configure**.
5. On **Wi-Fi Configuration** prompt, click **Add**.
6. On **WiFi Configuration** screen, enter following details:

- SSID
- Security Type
- Hidden Network
- Auto Join
- Proxy Setup

7. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to **Home** tab and select the device(s) or a group.
9. Click **Apply** to launch **Apply Job To Device** prompt.
10. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Certificate

**Certificate** in **Profiles** allows admin to remotely upload corporate certificates and other certificates that is necessary to authenticate the device access to the network.

To configure **Certificate** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, select **macOS** and click **Add**.
4. On **macOS Profile** prompt, click **Certificate**, enter **Profile Name** and click **Configure**.
5. On **Certificate** prompt, upload the **Certificate** file from the saved location and enter the **Password** and click **Add**.

The newly created profile gets listed in the **Profiles** section.

6. Go back to **Home** tab and select the device(s) or a group.
7. Click **Apply** to launch **Apply Job To Device** prompt.

8. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Passcode Policy

**Passcode Policy** allows admin to configure password settings on the enrolled devices.

To create a password policy and push it on an enrolled device(s), follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, select **macOS** and click **Add**.
4. On **macOS Profile** prompt, click **Passcode Policy**, enter **Profile Name** and click **Configure**.
5. On **Passcode Policy** section, enter following details:
  - Force User To Set Passcode
  - Allow Simple Value
  - Require Alphanumeric Value
  - Minimum Passcode Length
  - Minimum Number Of Complex Characters
  - Maximum Passcode Age (1-730 Days, Or None)
  - Maximum Auto-Lock
  - Passcode History (1-50 Passcodes, Or None)
  - Maximum Grace Period For Device Lock
  - Maximum Number Of Failed Attempts
6. Click **Save** to complete.

The newly created profile gets listed in the **Profiles** section.

7. Go back to **Home** tab and select the device(s) or a group.

8. Click **Apply** to launch **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Mail Configuration

**Mail Configuration** profile allows admin to remotely configure email account on an enrolled device.



**Note:** Currently this feature support settings configuration for **POP** or **IMAP** email accounts.

To configure an email account remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, select **macOS** and click **Add**.
4. On **macOS Profile** prompt, click **Mail Configuration**, enter **Profile Name** and click **Configure**.
5. On **Mail Configuration** screen, enter following details:
  - Account Description
  - Account Type
  - User Display Name
  - Email Address
6. Enter the appropriate details in **Incoming Mail**, **Outgoing Mail** fields and click **Save**.

The newly created profile gets listed in the **Profiles** section.

7. Go back to **Home** tab and select the device(s) or a group.
8. Click **Apply** to launch **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

## Exchange ActiveSync

When an email account is configured in **Exchange Active Sync**, the device users can sync their Mails, Contacts, Calendars, Reminders and Notes remotely on enrolled devices.

To configure **Exchange ActiveSync** remotely on an enrolled device, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, select **macOS** and click **Add**.
4. On **macOS Profile** prompt, click **Exchange ActiveSync**, enter **Profile Name** and click **Configure**.
5. On **Exchange ActiveSync** screen, enter the following details:
  - Account Name
  - Exchange ActiveSync Host
  - Use SSL
  - User
  - Email Address
  - Password

6. Click **Save**.

The newly created profile gets listed in the **Profiles** section.

7. Go back to **Home** tab and select the device(s) or a group.
8. Click **Apply** to launch the **Apply Job To Device** prompt.
9. On **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.



## App Store

**App Store** allows admins to create their own enterprise app store. They can use **SureMDM Web Console** to compile a list of enterprise apps and push it to the enrolled mobile devices.

App Store can be created on Android and iOS devices.

### App Store for Android

To share an app store with **Android** device, following three steps have to be performed.

1. Create an Enterprise **App Store**
2. Create an **Application Policy** profile
3. Apply the created profile on desired devices

### Create an Enterprise App Store

To create an enterprise **App Store**, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **App Store**.
3. On **App Store** screen, select **Android** tab and click **Add new app**.
4. Select desired option from **Select Options**:

#### **Android**

Upload APK

APK link

Web App

Once the app is successfully added, the application will reflect on **App Store** page.

## Create an Application Policy profile

To create an **Application Policy** profile, follow these steps:

1. On **SureMDM Web Console**, click **Profiles**.
2. On **Profiles** screen, select the **Android** platform and click **Add**.
3. On the **Profile** screen, click **Application Policy** tab.
4. Enter **Profile Name** and click **Configure**.
5. Click **Add** to launch **Select Application Source** prompt.
6. On **Select Application Source** prompt, select **SureMDM App Store**.
7. On **Enterprise App store**, select **App Name** and **Install Silently** and enter **App Version**.
8. Click **Add**.

The application with details will get listed under **Application Policy** section.

9. Click **Save**.

The newly created profile will get listed in the **Profiles** section.

## Apply the created profile on desired devices

To apply the created profile on the desired device(s), follow these steps:

1. On **SureMDM**, select the device(s) or a group.
2. Click **Apply** to launch the **Apply Job To Device** prompt.
3. On **Apply Job To Device** prompt, select the profile and click **Apply**.

On successful completion, the device will have a new App store which will list all enterprise apps on the device.

## App Store for iOS

To share an app store with **Android** device, following three steps have to be performed.

1. Create an Enterprise **App Store**
2. Create an **Application Policy** profile
3. Apply the created profile on desired devices

## Create an Enterprise App Store

To create an enterprise App store, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **App Store**.
3. On **App Store** screen, select **iOS** tab and click **Add new app**.
4. On **Select Options** prompt, select desired option from the following:

Upload ipa

Manifest link

Search from App Store

Web App

On successful creation of enterprise app store, the application will reflect on **App Store** page.

## Create an Application Policy profile

To create an **Application Policy** profile, follow these steps:

1. On **SureMDM Web Console**, click **Profiles**.
2. On **Profiles** screen, select the **iOS** platform and click **Add**.
3. On the **Profile** screen, click **Application Policy** tab.
4. Enter **Profile Name** and click **Configure**.
5. Click **Add** to launch **Add App** prompt.
6. Select the desired app from **App Name** drop-down menu and select **Install Silently**.
7. Click **Add**.

The application details will get **listed under Application Policy** section

#### **8. Click Save.**

The newly created profile will get listed in the **Profiles** screen.

### **Apply the created profile on desired devices**

To push the created profile on the desired device(s), follow these steps:

1. On **SureMDM**, select the device(s) or a group.
2. Click **Apply** to launch the **Apply Job To Device** prompt.
3. On **Apply Job To Device** prompt, select the profile and click **Apply**.

On successful completion, the device will have a new App store which will list all enterprise apps on the device.

## File Store

**File Store** offers a secure way to share and distribute enterprise files on Android, iOS and Windows devices. This option allows the IT admins to create a document library and share documents like images, videos and other files across enrolled Windows devices.

To share a file using **File Store** option in **SureMDM** following three steps have to be performed:

1. Upload the file(s) to File Store
2. Create a File Sharing Policy profile
3. Apply the created profile on desired Windows devices

### Upload the file(s) to File Store

To upload a file to **File Store**, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **File Store**.
3. On **File Store** screen, click **New Folder** to create a new folder.
4. Once the folder is created, double-click the folder and open.
5. Click **Upload files** to browse and upload the desired file(s).

On successful upload, the file will get saved in the folder.

### Create a File Sharing Policy profile

To create a **File Sharing Policy** profile, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Profiles**.
3. On **Profiles** screen, click **Windows > Add**.

4. On **Windows Profile** screen, click **File Sharing Policy > Configure**.
5. Enter **Profile Name**.
6. Click **Add to launch File Store** prompt.
7. Select the desired files or folders and click **Add**.

The selected files will get listed in the box located on the right side of the screen.

8. Click **Done**.

The selected files will get listed in the **File Sharing Policy** section.

9. Click **Save** to complete.

## Apply the created profile on desired Windows devices

To apply the created profile on Windows devices, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Home**.
3. Select the device(s) from **Device List**.
4. Click **Apply** to launch the **Apply Job To Device** prompt.
5. On **Apply Job To Device** prompt, select the Windows Profile and click **Apply** to complete.

## Reports

**Reports** section helps the admins to generate different types of reports such as **On Demand Reports, Schedule Reports** and **Custom Reports**.

### On Demand Reports

On Demand Reports are the reports that can be generated with the predefined format. Some of the **On Demand Reports** are **System Log, Asset Tracking, Call Log Tracking, Jobs Deployed, Installed Job Report, Device Health Report, Device History, Data Usage, Device Connected, App Version**.

To generate an **On Demand Report**, follow these steps:

1. Login to **SureMDM Web Console**.
2. Select **Reports** from the **Utility Panel**.
3. Select **On Demand Reports** and select the type of report to be generated from the following options:
  - **System Log** - This report will list all the activities of enrolled devices for the specified time period.
  - **Asset Tracking** - This report will list all the enrolled devices' details
  - **Call Log Tracking** - This report will list calls details (Incoming/ Outgoing/ Missed/ Rejected) of the selected device or group for the specified time period. There are following types of call logs to select from:
    - Incoming
    - Outgoing
    - Missed

- Rejected
- **Jobs Deployed** - This report will list all deployed jobs of the selected group
- **Installed Job Report** -This report will list devices of a specific group based on the selected job and Applications Name provided.
- **Device Health Report** - This report will list devices with following parameters for the selected group for a specified time period:
  - Battery Percentage
  - Storage Space
  - Physical Memory
- **Device History** - This report will list the history with following parameters for the selected device:
  - Last Connected
  - Device Time
  - Battery Percent
  - Back up Battery percent
  - Available Physical Memory Percent
  - Available Storage Percent
  - Wi-Fi Signal Strength
- **Data Usage** - This report will list all the enrolled devices with their data usage for the specified time period.
- **Device Connected** - Using **Reports** option, admins can view a list of devices last connected to the account at a specific period of time. The following details will be available in the report:
  - Device Name



- Last Connected
- Registered Date
- Devices Status
- **App Version** - This report allows the admins to generate the report on version details of all the installed applications for a selected group.

#### 4. Click **Request Report**.

The request will be added to the queue and the status of the report is updated in the **View Reports** section. The report can be viewed or downloaded from **View Reports** section.

## Schedule Reports

SureMDM allows admins to schedule specific report generation for a specified period and also auto-send the report to email addresses. This means admins can receive the Daily/Weekly report through email without logging into **SureMDM Web Console**.

To schedule reports, follow these steps:

1. Login to **SureMDM Web Console**.
2. Select **Reports > Schedule Reports**.
3. Select a report type (eg: App version) for which report needs to be generated.
4. Click **Schedule New**.
5. On **Schedule New** prompt, specify following details:
  - **Schedule Report Cycle** - Select **Daily/Weekly**
  - **Mail to** - Email addresses of the recipients
  - **Select Group** - Report generated for a specific group
6. Click **Schedule** to complete.

The request will be added to the queue and the status of the report is updated in the **View Reports** section. The report can be viewed or downloaded from **View Reports** section.

## Custom Reports

**Custom Report** option generates customized reports with only the required set of data. Admins can select the required tables and filters to generate tailor-made reports.

To generate and view **Custom Report**, follow these steps:

1. Login to **SureMDM Web Console**.
2. Select **Reports** from the **Utility Panel**.
3. Select **Custom Reports** and click **Add**.
4. Enter **Name** and **Description**.
5. Select the desired items for the report to generate from **Tables List** and click **Add**.

The selected items will get displayed under **Selected Tables List**.



**Note:** When **SureLock Analytics** option is selected and added to the **Selected Tables List**, **Analytics Call Back Url** option will get auto-populated where admin can fetch the analytics data from the URL entered. The data can be filtered and managed as per the requirement from the URL entered.

6. Apply filters to the selected columns in **Add filter** (optional).
7. Select the **Column Name** and **Sort Order** under **Add Sort** option to sort the report in ascending/descending order (optional).
8. Select or enter the following details:
  - **Group By (Column Name)**

- **Aggregate Options** - Merge rows of data with the same value for the column name selected in **Group By** field (optional)
- **Alias Name** - Alternate name given to the column name selected in **Group By** field.

9. Click **Save**.

Custom report will be saved.

10. Go to **On Demand Reports**, select the saved custom report and select the device/group for which report should be generated.

11. Click **Request Report**.

The request will be added to the queue and the status of the report is updated in the **View Reports** section.

12. Go to **View Reports** to view or download the generated report.

## Settings

This toolbar provides account management options such as user management, password change, branding info, license details and more.

### Device Enrollment

Android and iOS devices can be enrolled to the Console using QR Code Enrollment.

See [Enrollment](#) section to know more.

### Account Settings

**Account Settings** is the option to manage the user interface, permission and scope. It helps the admins to configure their account as per their preferences and goals. It helps the user to enable or disable settings in compliance with organizational rules.

It is just a one-click navigation to manage options such as Branding Info, Device Enrollment Rules, Miscellaneous Settings, Single Sign-On, Alert Template, Custom Toolbar.

### Branding Info

**Branding Info** option helps the user to configure and set custom logo and custom title in the title bar of the web console.

To brand **SureMDM Web Console** with desired text or logo, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **Account Settings**.
3. On **Account Settings** prompt, click **Branding Info** tab and configure desired changes in following fields:

- **Use Logo** - Upload logo of the company or any image file

or

**Title** - Enter the desired text

- **Sub-title** - Enter the desired text to appear in small font below the logo or Title

- **Message Footer** - Enter the desired text to appear in the Footer.

4. Click **Apply** to complete.

## Device Enrollment Rules

**SureMDM** allows admins to set device enrollment rules for devices upon enrollment.

To enable auto naming of devices on enrollment, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **Account Settings**.
3. Click **Device Enrollment Rules** tab, on **Account Settings** prompt, enter the following details:
  - **Prefix** - text or numerals added at the beginning of the device name
  - **Suffix** - text or numerals added at the end of the device name
  - **Start Count** - Number from which the count has to start
  - **Count Length** - Number of characters of **Start Count**
  - **Device Authentication Type** - Select the required **Device Authentication Type** from the following options:
    - No Authentication
    - Require Password
    - OAuth Authentication
    - Active Directory Authentication

- Active Directory Authentication using Admin Account



**Note:** On selecting **OAuth Authentication**, two options will get auto-populated and supports the following:

- **Native Application** - Android/iOS/macOS
- **Web Application** - EMM Windows / Deep Thought

4. Click **Apply** to complete.

## Miscellaneous Settings

**Miscellaneous Settings** has the option to configure remote support features for enrolled devices.

The following are the options available in **Miscellaneous Settings**:

1. **Use GCM** - Enable GCM (Google Cloud Messaging).
2. **Default Connectivity Option For Install/File Transfer Job** - Select the connectivity option (Wi-Fi only/ Mobile Data only /Any Network) from the drop-down menu.
3. **Provide Remote Access To 42Gears Support Team** - Click **Grant / Revoke** to grant or revoke the remote access to 42 Gears Support Team.
4. **Enable Global Search** - Search devices in all the groups/subgroups present in MDM Web Console.
5. **Free up SureLock/SureFox/SureVideo licenses from device when it is deleted from SureMDM (only for android)** - Select this option to deactivate the **SureLock / SureFox / SureVideo** licenses when the device is deleted from console and tries to activate the licenses.
6. **Enable Auto Search** - Search will get started once the text is typed on the **Search** box.

7. **Use Old Remote Support** - Select this option when the device supports older version of remote support.
8. **Don't Pause Screen Capture** - Select this option to proceed with the screen capture.
9. **Zip All Downloads** - On selecting this option, the files that are getting downloaded will be zipped by default.

## Single Sign-On

**Single Sign-On (SSO)** is an authentication process that allows a user to access multiple applications with one set of login credentials.

The following are the options available in **Single Sign-On** of **SureMDM Web Console**:

1. **Enable Single Sign-On** - Select **Single Sign-On** option
2. **SSO Type** - Select the **SSO Type** from the drop-down menu
3. **Service Identifier** - Enter the **Service Identifier**
4. **Sign On Service Url** - Enter the **Sign On Service Url**
5. **Logout Service Url** - Enter the **Logout Service Url**



*Note: Generally, the URL for **Sign On Service Url** and **Logout Service Url** will be the same.*

6. Select role permission from **Features Permissions** drop-down menu. See [Create Role-based Admin](#).
7. Select device group permission from **Allowed Device Groups** drop-down menu. See [Create Device Group based Admin](#).
8. Select job folder permission from **Allowed Job Folders** drop-down menu. See [Create Job based Admin](#).
9. **Generate/ Upload Certificate** - This option will be available when there is no certificate is uploaded.

10. **Generate / Delete Certificate** - If the certificate is already uploaded then the admin has the option to delete or download the certificate.

## Alert Template

**Alert Template** helps the admins to create a custom template alert instead of default alert messages for the following options:

- **Battery Policy**
- **Connection Policy**
- **Data Usage Policy**
- **Notify when device comes online**
- **Notify when SIM is changed**
- **Notify when device is rooted or Nix has been granted with root permission**

## Customize Toolbar

**SureMDM** enables the admins to create a customized job.


There are two types of jobs:

1. **Predefined Jobs** - Jobs that are available by default.
2. **User defined Jobs** - Admins can create a customized job with the desired icon.

To create a **User defined job**, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **Account Settings > Customize Toolbar**.
3. Under **User defined Jobs**, click **Add**.
4. On **Add Jobs** prompt,



- a. Enter **Name**.
- b. Click **Browse Icons** to browse and select an icon.
- c. Click  to list all the jobs.
- d. On **Select Jobs to Add** screen, select a job from the list.
- e. Click **OK** to complete.

The newly created customized job will get displayed under **User defined job** section and also gets added to the dynamic jobs.

## Customize Nix/ SureLock


Using this option admins can customize the **Nix Agent** and **SureLock** applications such as renaming the app title, importing and editing the app settings and configuring a customized icon for the app launcher.

To launch a customized **Nix/SureLock** application, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **Account Settings > Customize Nix/SureLock**.
3. Select an application from **Select App** drop-down menu.



**Note:** *App Download URL* field is auto-populated on selecting an application from **Select app** field.

4. Enter the desired **App Title**.
5. In **App Settings** box, click **Import Settings** to import the app settings and click **Edit** to edit the app settings.
6. Click  to upload desired image as **App Launcher Icon**.

7. Click **Generate > Download** to complete.

The apk file will be launched as a System App on the device.

## iOS Enrollment Settings

Enrollment Settings of iOS devices can be configured in this option. Admins can configure and push DEP (Device Enrollment Program) profile to the devices under DEP.

To configure and push DEP profile to the devices, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **Account Settings > iOS Enrollment Settings**.
3. Click **Download**, to download the vendor signed CSR to generate push certificate.
4. Browse for the push certificate from the location and click **Upload**.
5. Under **Device Enrolment Program**,
  - a. In **PEM Certificate**, click **Download** to download **dep** file. Login to **Apple Deployment Programs** and upload the **dep** file.
  - b. Download **SMIME server token** from **deploy.apple.com** and click **Upload** to upload the token in **Server Token**.
  - c. Click **Configure** to configure DEP profile to be pushed to all devices.
  - d. Click **Push** to push the configured DEP profile to all devices.

## Certificate Management

Security for the Wi-Fi / VPN Apps can be configured using SCEP (Simple Certificate Enrollment Protocol) in **SureMDM**.

## Configure SCEP

To configure SCEP in **SureMDM**, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **Account Settings > Certificate Management**.
3. Following options are available in the Certificate Management section:
  - a. **CA Server Address** - URL of the CA server
  - b. **Certificate Template** - Template that is fetched from CA server
  - c. **Certificate Renewal Period** - Renews the certificate automatically before the specified days/weeks/months/years.
  - d. **Common Name Wildcard** - Configure the wild card name as IMEI/ MAC Address/ Device Id/ Serial Number on the CA server.
  - e. **Subject Alternate Name Wildcard** - Configure the alternate wild card name as as IMEI/ MAC Address/ Device Id/ Serial Number /Constant Text on the CA server.
  - f. **Enable OTP** – Enables OTP option
  - g. **User Name and Password** - Enter the Account User Name and Account Password of the CA server.
4. Click **Save** to save the CA server settings.
5. Click **Get Managed Certificates** to renew or revoke the certificate manually.

## User Management







**SureMDM User Management** option allows customizing user permissions for all existing and new administrators using the following set of permissions:

- Roles
- Device Groups Set
- Job Folder Set
- Device Grid Column Set

There are two types of users who can access the web console:

- **Account Admin /Super User** - There can be only one **Super User** for an account. This user type will not have any restrictions on the functions available in the web console.
- **Admin User** – There can be multiple Admin users for an account.

The description of icons in **User Management** is given in the following table:

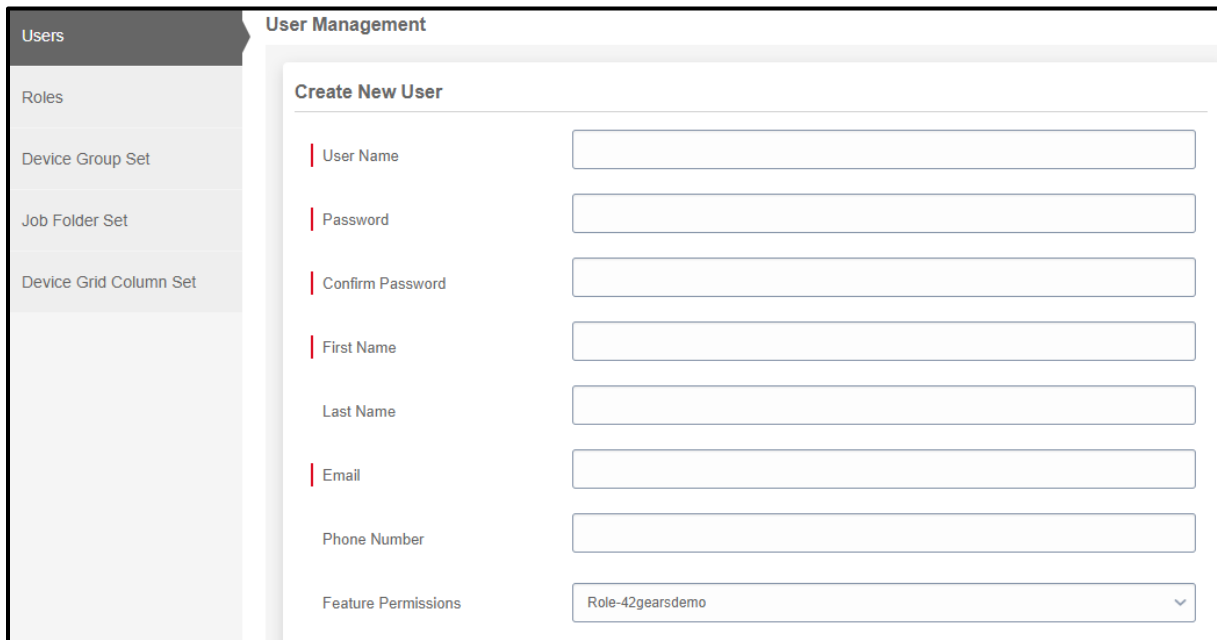
Buttons	Description
 <b>Add User</b>	Add a new user
 <b>Edit User</b>	Edit the user details
 <b>Delete</b>	Delete the user
 <b>Reset Password</b>	Reset the password of the user
 <b>Enable/Disable User</b>	Enable /Disable the user
 <b>Visible Column In Grid</b>	Select only the specific Column set(s) to be visible for a Sub-user

## Add a New User

To add a new user to the web console, follow these steps:

1. Login to **SureMDM Web Console**.

2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **User Management**.
3. On **User Management** screen, click **Add User**.
4. On **Create New User** screen, enter the **User Name, Password, Confirm Password, First Name, Last Name, Email, Phone Number**.



The screenshot shows the 'User Management' interface with a sidebar on the left containing 'Users', 'Roles', 'Device Group Set', 'Job Folder Set', and 'Device Grid Column Set'. The main area is titled 'Create New User' and contains the following fields:

- User Name
- Password
- Confirm Password
- First Name
- Last Name
- Email
- Phone Number
- Feature Permissions (dropdown menu showing 'Role-42gearsdemo')

5. Select a role from **Roles** drop-down menu. See [Create Role-based Admin](#).



**Note:** If no option is selected from **Roles** drop-down, Super User Role will be selected by default.

6. Select a device group from **Device Group Set** drop-down menu. See [Create Device Group based Admin](#).



**Note:** If no option is selected from **Device Group Set** drop-down, Super User Device Group Set will be selected by default.

7. Select a job folder from **Job Folder Set** drop-down menu. See [Create Job-based Admin](#).



**Note:** If no option is selected from **Job Folder Set** drop-down, Super User Job Folder Set will be selected by default.

8. Select a created column set from **Device Grid Column Set** drop-down menu. See [Device Column Set based Admin](#).



**Note:** If no option is selected from **Device Grid Column Set** drop-down, Super User's Device Column Set will be selected by default.

9. Select **Hide Parent Group When No Access to Child Groups** will hide the parent group when child groups are disabled.

For example: Super user can restrict the permission for add/delete/modify jobs for a specific admin user which will hide the **Jobs** module in **Utility Panel**. The **Jobs** module will not be visible to the Admin user.

In **Roles** prompt, disable the child modules(add/delete/modify) which will hide the **Jobs** module in **Utility Panel** as shown below.

Roles
✕

**Name**

**Description**

Select All

- >  Group Permissions
- >  Device Action Permissions
- >  Device Management Permissions
- >  Application Settings Permissions
- Job Permissions
 
  - New Job
  - Delete Job
  - Modify Job
- >  Report Permissions
- >  User Management Permissions
- >  Dashboard Permissions
- >  File Store Permissions

**SureMDM**

Home
 Dashboard
 Inbox
 Profiles
 App Store
 File Store
 Reports





10. Click **Create** to complete.

The newly created Admin user will get listed in the **Users** section.

## Create Role-based Admin

These admins will have access to the functions that are allowed by the Superuser. For example, a superuser can create a user and give him access to everything except remote wiping of enrolled devices.

The description of icons in **User Management > Roles** is given in the following table:

Buttons	Description
 <b>Add</b>	Add a new Role
 <b>Edit</b>	Edit the Role details
 Clone	Duplicate the existing Role
 <b>Delete</b>	Delete the Role

To create role-based admin, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **User Management**.
3. On **User Management** screen, select **Roles** tab and click **Add**.
4. On **Roles** prompt, enter **Name** and **Description**, select the permissions to allow and click **Save**.



Roles

Name

Description

Select All

- >  Group Permissions
- >  Device Action Permissions
- >  Device Management Permissions
- >  Application Settings Permissions
- ∨  Job Permissions
  - New Job
  - Delete Job
  - Modify Job
- >  Report Permissions
- >  User Management Permissions
- >  Dashboard Permissions
- >  File Store Permissions

Save

5. Go to **Users** tab and click **Add**.
6. On **Create New User** screen, enter the details including **User Name** and **Password** and under **Feature Permissions**, select the created role.



**Note:** *Role can also be assigned to the existing user.*

7. Click **Create**.

When new admin user logs in using the created credentials, he will have access to only specified functions allowed by the Super user.

## Create Device Group based Admin

This admin will have access to manage only specified groups and sub-groups.

To create group-based admin, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **User Management**.
3. On **User Management** screen, select **Device Group Set** tab and click **Add**.
4. On **Device Groups** prompt,
  - a. Enter **Name** and **Description**.
  - b. Deselect the group(s) that has to be hidden from the user.
  - c. Enable **Automatically Allow New Groups Added In Future** to allow the Admin user to view the groups that will be added in future and click **Save**.

The screenshot shows the 'Device Groups' configuration window. It features a blue header with the title 'Device Groups' and a close button. Below the header, there are two text input fields: 'Name' and 'Description'. Underneath these fields is a list of device groups with checkboxes. The 'Home' group is expanded, showing sub-groups: 'East', 'North', 'South', 'Test', and 'west'. At the bottom of the list, there is a checkbox for 'Automatically Allow New Groups Added In Future'. A green 'Save' button is located at the bottom center of the form.

5. Go to **Users** tab and click **Add**.
6. On **Create New User** screen, enter the details including User Name and Password for the user and under **Allowed Device Groups**, select the created Device Group set.
7. Click **Create**.

When the new user logs in using the created credentials, he will be able to manage only the specified group(s) allowed by the superuser.

## Create Job-based Admin

This type of admin will have access to apply only specified job folders on the enrolled devices.

To create job-based admin, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **User Management**.
3. On **User Management** screen, select **Job Folder Set** tab and click **Add**.
4. On **Job Folders** prompt,
  - a. Enter **Name** and **Description**.
  - b. Deselect the job folders that have to be hidden from the user.
  - c. Enable **Automatically Allow New Folder Added In Future** to allow the Admin user to view the job folders that will be added in future and click **Save**.

Jobs Folders✕

Name

Description

Select All

▼  Home (Default)

- Alkem Labs
- test

Automatically Allow New Folder Added In Future.

Save

5. Go to **Users** tab and click **Add**.

6. On **Create New User** screen, enter the details including **User Name** and **Password** and under **Allowed Job Folders**, select the created Job Folder set.

7. Click **Create**.

Now when the new user logs in using the created credentials, he will have an option to access only the job folders allowed by the superuser.

## Create Column Set based Admin

This admin can view only the specified column set allowed by the Super user in the device grid.

To create **Device Column set** based admin, follow these steps:

1. Login to **SureMDM Web Console**.

2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **User Management**.
3. On **User Management** screen, select **Device Grid Column Set** tab and click **Add**.
4. On **Grid Column** prompt, enter the **Name** and **Description** and select the desired columns to be allowed for the Admin to view and click **Save**.

The screenshot shows a modal dialog titled "Grid Column" with a blue header and a close button (X) in the top right corner. The dialog contains the following elements:

- A "Name" label followed by a text input field.
- A "Description" label followed by a text input field.
- A "Select All" checkbox.
- A scrollable list of checkboxes for selecting columns:
  - Model
  - Status
  - Battery
  - IP Address
  - Last Connected
  - Last Device Time
  - Device Registered
  - Network Operator
  - Device Roaming
  - Signal
- A green "Save" button at the bottom center.

5. Newly created **Device Grid** column set will get added to this section.
6. Go to **Users** tab and select an Admin user and click **Visible Column in Grid**.
7. On **Device Grid Column Set** prompt, select the newly created column set and click **Ok**.



**Note:** Super user also have the option to use a combination of all four types of permissions. This enables the creation of admin users with tailor-made custom permissions.

## License Management

License Management option displays license details of **SureMDM** such as license purchase date, expiry date, number of enrolled devices.

## Change Password

To change **SureMDM** login password, follow these steps:

1. Login to **SureMDM Web Console**.
2. On **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **Change Password**.
3. On **Change your Account Password** prompt, enter **Old Password**, **New Password** and **Retype New Password**.
4. Click **Ok** to complete.

## Logout

To sign out from **SureMDM Web Console**, click **Settings** icon located at top right of the screen and select **Logout**.