LifeSaver
www.lifesavermobile.com

Deploying LifeSaver through your Unified Endpoint Management (UEM) Software

Here are instructions for deploying the LifeSaver App to your mobile devices using your UEM software.

1. Information Required. There are 3 pieces of information that you will need from LifeSaver Mobile before you begin.

- Public app store links for the LifeSaver App
  - Here is the Apple App Store URL: https://itunes.apple.com/us/app/lifesaver-distracted-driving/id874231222?mt=8
  - The Google Play Store URL is: https://play.google.com/store/apps/details?id=com.lifesaverapp
- The LifeSaver app configuration XML file used by your UEM provider, and
- Your unique **LifeSaver Company ID** (see #4 below).

Contact LifeSaver Customer Success (support@lifesaver-app.com) to request the 2nd and 3rd items listed above. Also refer to the **Appendix** section at the end of this document

2. LifeSaver setup for your UEM

- Using the public app store links above, you can add and deploy the LifeSaver App from the App Store and/or Google Play Store to your UEM implementation.
- If you want LifeSaver to automatically add new driver devices to your LifeSaver Fleet Portal OR if you intend to use the LifeSaver Pro iPhone locking feature, you must configure the mapping of your UEM data for mobile devices as *instructed by LifeSaver Customer Success for your specific UEM provider*.

Device Serial Number	Required to simplify app setup and linking device to portal
Phone Number (Mobile)	Highly recommended to identify, link, and notify driver
Full Name	The full name of the user who owns the enrolled device
LSCompanyid (UDID)	Required to automatically add new drivers to portal (see #4 below)
LSMDMDeviceid	Required for LifeSaver Pro iOS Device Locking (please contact Customer Success to discuss)
Email Address	The email address listed for the user in the UEM (optional.. If not included in portal import spreadsheet this UEM email will update the driver row in portal)

3. App Permission Requests / Verification. Your IT team or your drivers will need to open the LifeSaver App on each phone, and accept the app permission requests (for example, location services and notifications).

- In addition, if your UEM has not provided a serial number via the LifeSaver app configuration XML file, your IT team or your drivers will need to perform a one-time device verification (by signing into the app with the respective cell phone number).

4. Adding Devices to your Portal. If your UEM is set up with the **LifeSaver Company ID,** this will automatically add new driver devices to the “Unassigned” group within your LifeSaver Fleet Portal.

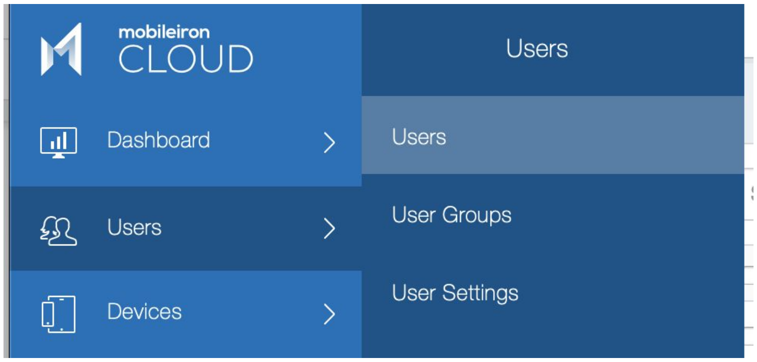
If this option is not available for any reason, please complete our LifeSaver driver template by extracting your driver names, emails, and cell phone numbers from your UEM. LifeSaver Customer Success (support@lifesaver-app.com) will upload the driver information from this spreadsheet into your LifeSaver Fleet Portal, and your driver devices will be automatically linked to your Portal (no Portal invitation is required).

API Setup Requirements

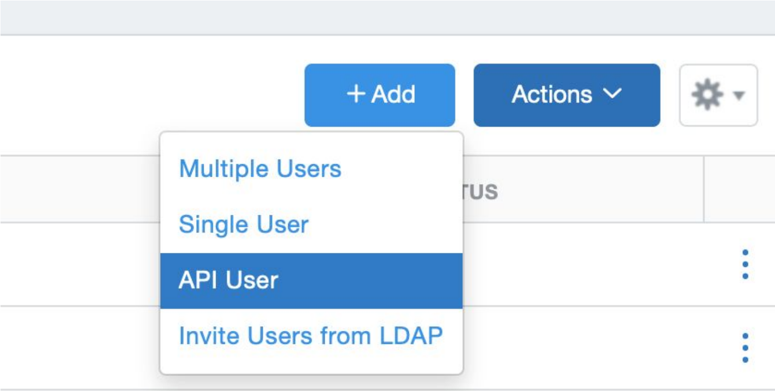
To be able to use the lock API, the admin needs to first create an API user and assign appropriate roles to be able to call the ***Lock API.***

Example using MobileIron Cloud:

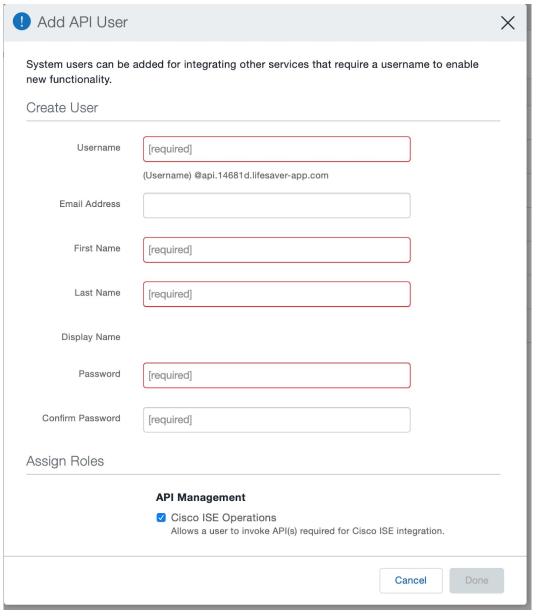
1. Navigate to the Users section



2. Add an API User



3. Make sure you assign the appropriate roles to the API user. Once complete you will need to provide this information to LifeSaver customer support.



Add API User

System users can be added for integrating other services that require a username to enable new functionality.

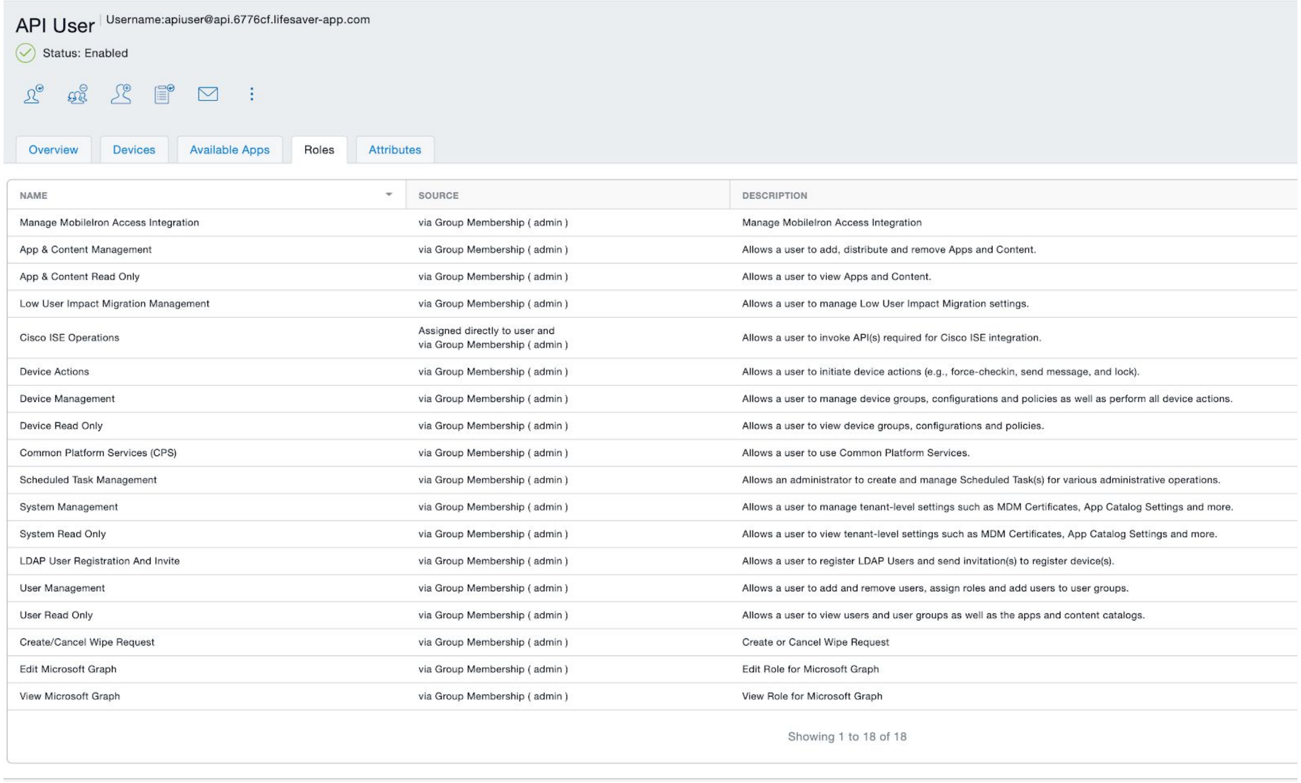
Create User

Username	[required] (Username) @api.14681d.lifesaver-app.com
Email Address	
First Name	[required]
Last Name	[required]
Display Name	
Password	[required]
Confirm Password	[required]

Assign Roles

API Management

☑ Cisco ISE Operations
Allows a user to invoke API(s) required for Cisco ISE integration.



API User

Username:apiuser@api.6776cf.lifesaver-app.com

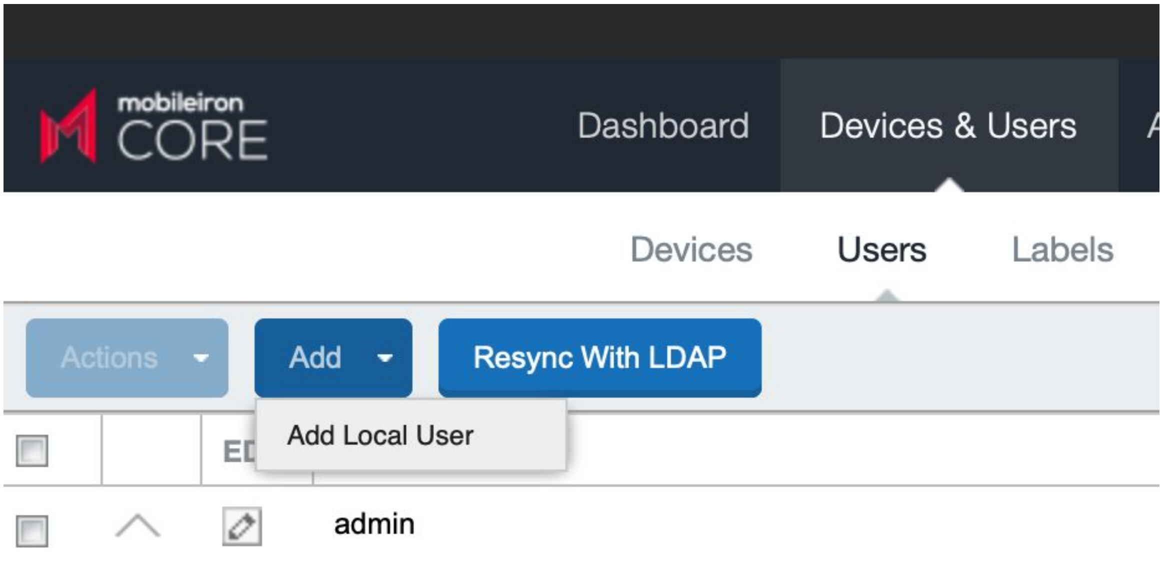
Status: Enabled

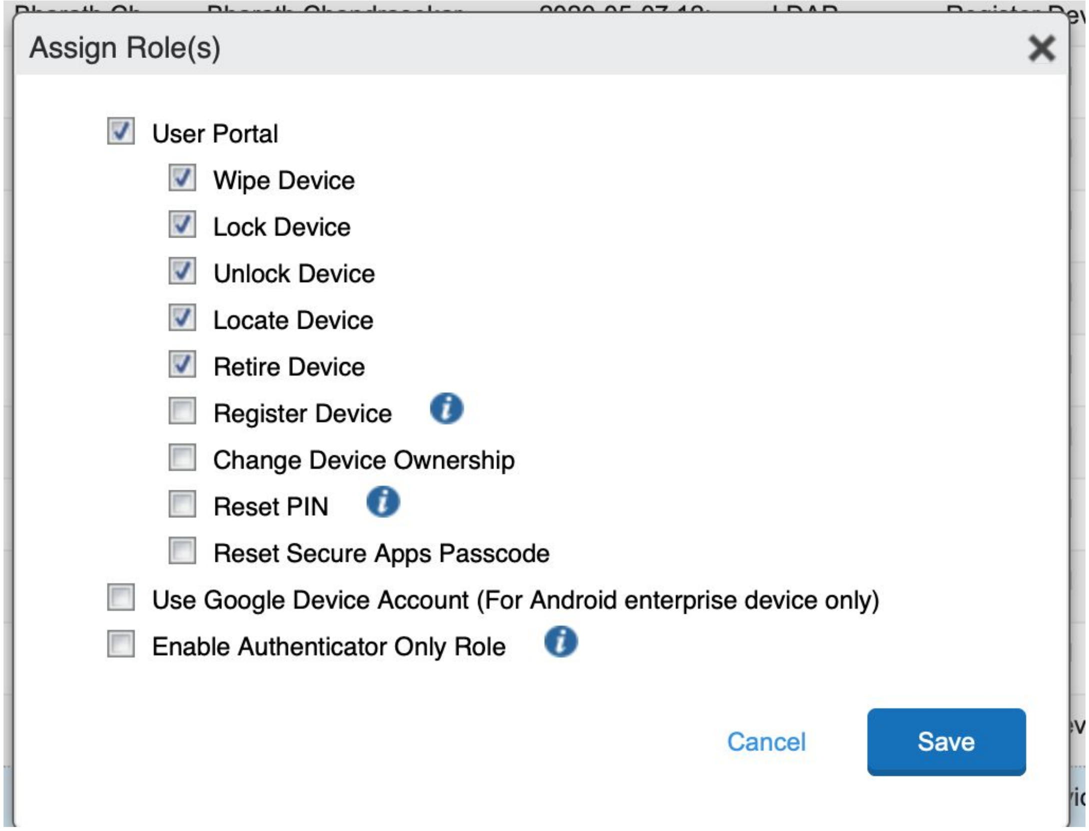
NAME	SOURCE	DESCRIPTION
Manage MobileIron Access Integration	via Group Membership (admin)	Manage MobileIron Access Integration
App & Content Management	via Group Membership (admin)	Allows a user to add, distribute and remove Apps and Content.
App & Content Read Only	via Group Membership (admin)	Allows a user to view Apps and Content.
Low User Impact Migration Management	via Group Membership (admin)	Allows a user to manage Low User Impact Migration settings.
Cisco ISE Operations	Assigned directly to user and via Group Membership (admin)	Allows a user to invoke API(s) required for Cisco ISE integration.
Device Actions	via Group Membership (admin)	Allows a user to initiate device actions (e.g., force-checkin, send message, and lock).
Device Management	via Group Membership (admin)	Allows a user to manage device groups, configurations and policies as well as perform all device actions.
Device Read Only	via Group Membership (admin)	Allows a user to view device groups, configurations and policies.
Common Platform Services (CPS)	via Group Membership (admin)	Allows a user to use Common Platform Services.
Scheduled Task Management	via Group Membership (admin)	Allows an administrator to create and manage Scheduled Task(s) for various administrative operations.
System Management	via Group Membership (admin)	Allows a user to manage tenant-level settings such as MDM Certificates, App Catalog Settings and more.
System Read Only	via Group Membership (admin)	Allows a user to view tenant-level settings such as MDM Certificates, App Catalog Settings and more.
LDAP User Registration And Invite	via Group Membership (admin)	Allows a user to register LDAP Users and send invitation(s) to register device(s).
User Management	via Group Membership (admin)	Allows a user to add and remove users, assign roles and add users to user groups.
User Read Only	via Group Membership (admin)	Allows a user to view users and user groups as well as the apps and content catalogs.
Create/Cancel Wipe Request	via Group Membership (admin)	Create or Cancel Wipe Request
Edit Microsoft Graph	via Group Membership (admin)	Edit Role for Microsoft Graph
View Microsoft Graph	via Group Membership (admin)	View Role for Microsoft Graph

Showing 1 to 18 of 18

Example using MobileIron Core

When creating an API user using MobileIron Core, make sure the roles you assign include Locking and Unlocking a device. Here is an example of the Add User and Roles screen.




Assign Role(s)

☑ User Portal
- ☑ Wipe Device
- ☑ Lock Device
- ☑ Unlock Device
- ☑ Locate Device
- ☑ Retire Device
- □ Register Device
- □ Change Device Ownership
- □ Reset PIN
- □ Reset Secure Apps Passcode

□ Use Google Device Account (For Android enterprise device only)

□ Enable Authenticator Only Role

Appendix: AppConfig Values

- On some UEM's AppConfig values can be automatically filled in for you, except in the case of the company UDID (**LSCompanyId**), which the administrator will have to manually fill in. Please contact LifeSaver Customer Success (support@lifesaver-app.com) for this value.
- Note: All values are of the type **String**

1. Mobile Iron Cloud

KEY	**VALUE**
DeviceSerialNumber	**${deviceSN}**
EmailAddress	**${userEmailAddress}**
PhoneNumber	**${devicePhoneNumber}**
FullName	**${userDisplayName}**
LSCompanyId	**<Company UDID entered manually by the admin>**
LSMDMDeviceId	**${deviceGUID}**

2. MobileIron Core

KEY	**VALUE**
DeviceSerialNumber	**$DEVICE_SN$**
EmailAddress	**$EMAIL$**
PhoneNumber	**$PHONE_NUMBER$**
FullName	**$DISPLAY_NAME$**
LSCompanyId	**<Company UDID entered manually by the admin>**
LSMDMDeviceId	**$DEVICE_UUID$**