magic leap

DEVICE MANAGER

ADMIN GUIDE

Version 1.8

magic leap

TABLE OF CONTENTS

magic leap

DEVICE MANAGER OVERVIEW

THE SOLUTION

Magic Leap provides a method to manage their Magic Leap devices designed to aid customers with integrating these devices into their business and helping to manage their mixed reality solutions. This solution is a web-based management tool that allows administrators to manage their Magic Leap devices via a policy driven mechanism. In this document, we will call this web-based tool, the “Device Manager”. For a full description of the Magic Leap device and this management solution, user agreements, please visit magicleap.com.

GETTING STARTED

Read this Magic Leap Enterprise Admin Guide (“Enterprise Guide”) and our Quick Start Guide available at magicleap.com/quickstart and our Safety Guide available at magicleap.com/safety before using a Magic Leap device. Failure to do so and follow the directions in all guides can result in serious injury, property damage, or damage to your Magic Leap.

CHANGES

Magic Leap may update this Enterprise Guide from time-to-time to keep it accurate and complete. If we issue updates to the Enterprise Guide, please discard any possible copies (hard or soft) and only use the new one. We encourage you to review our Enterprise Guide at magicleap.care from time-to-time to ensure you are reading the latest version.

magic leap

ENTERPRISE ADMIN OVERVIEW

IDENTITY MANAGEMENT

- Employees can securely log in to the Magic Leap device using their enterprise credentials.
- Administrators can use account provisioning restrict who has access to the Device Manager.

DEVICE MANAGEMENT

- Administrators can view and manage devices they own from an easy to use web portal.
- Administrators can configure devices to fit business needs and ease the process of staging devices.
- Administrators can manage devices including:
    - Remotely update profile.
    - Remotely reset a device.
    - Remotely view device logs
- Kiosk mode can be used to lock Magic Leap devices into a single application and prevent users from accessing the launcher.
- Wireless networks can be pre-configured and applied to devices to avoid users from manually connecting to networks.

APPLICATION MANAGEMENT

- Allow enterprise administrators to install applications remotely on all managed devices.
- Configure applications to restrict updates or automatically update.

ACCOUNT PROVISIONING

Enterprise users can log into the Magic Leap device and the Device Manager using their enterprise credentials. The Device Manager uses a third-party identity management solution, Okta, to manage the authentication. Any identity source that is compatible (Active Directory or LDAP) with Okta can be used as a single sign-on solution for Magic Leap devices. The diagram below shows how Magic Leap manages the connection between Okta and the Device Manager and the Magic Leap device. The connection from Okta to the enterprise user database is managed by the enterprise customer. For more information on this connection, visit the links at the bottom of this article

ACCOUNT PROVISIONING

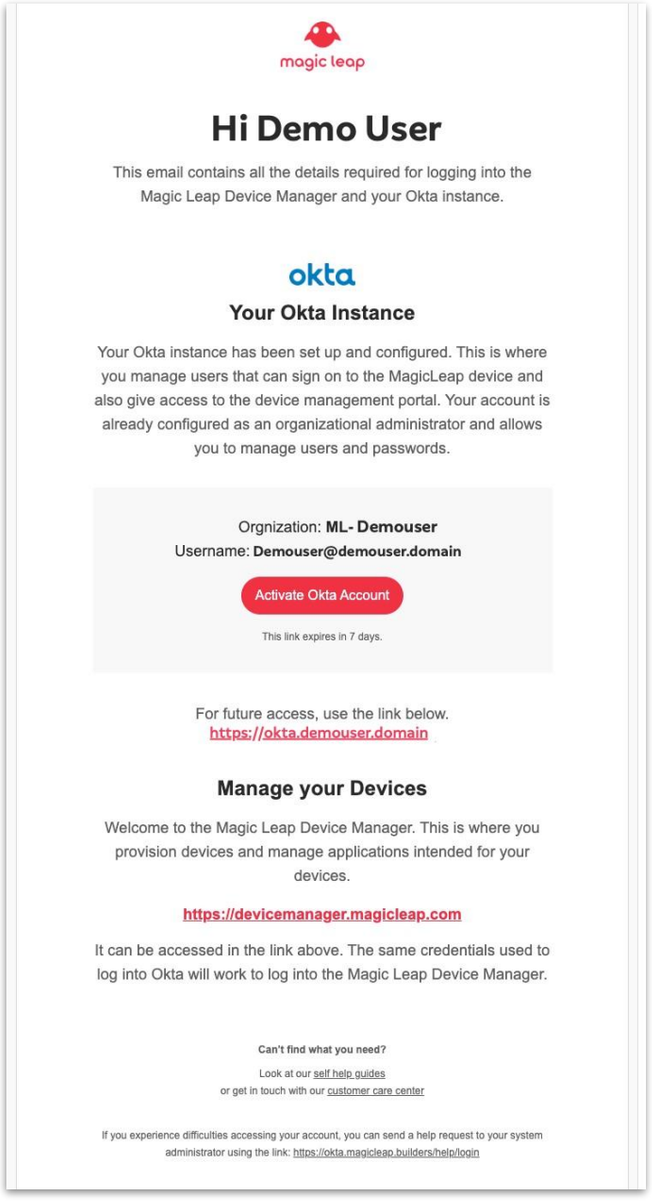
The identified administrator within your organization, will be setup within Okta by the Magic Leap team and will receive an activation email from Okta detailing how to access the site.

Administrators will need to download the Okta Verify applications via their respective mobile app stores to properly authenticate into the Admin section of Okta.

iOS
Android

Upon first visit to your Okta instance, the Administrator will need to change their password
on initial login to their Okta instance.

Password requirements:
at least 8 characters, a lowercase letter, an uppercase letter, a number, no parts of your username. Your password cannot be any of your last 4 passwords.


magic leap

Hi Demo User

This email contains all the details required for logging into the Magic Leap Device Manager and your Okta instance.

okta

Your Okta Instance

Your Okta instance has been set up and configured. This is where you manage users that can sign on to the MagicLeap device and also give access to the device management portal. Your account is already configured as an organizational administrator and allows you to manage users and passwords.

Orgnization: **ML- Demouser**
Username: **Demouser@demouser.domain**

Activate Okta Account

This link expires in 7 days.

For future access, use the link below.
https://okta.demouser.domain

Manage your Devices

Welcome to the Magic Leap Device Manager. This is where you provision devices and manage applications intended for your devices.

https://devicemanager.magicleap.com

It can be accessed in the link above. The same credentials used to log into Okta will work to log into the Magic Leap Device Manager.

Can't find what you need?

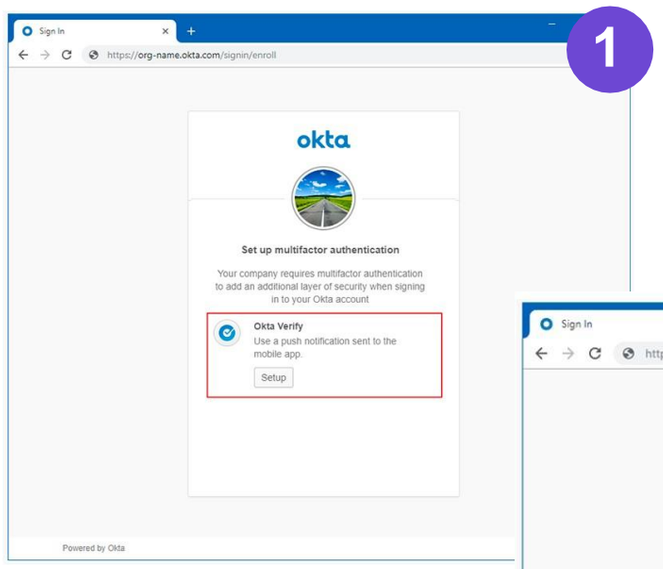
Look at our self help guides
or get in touch with our customer care center

If you experience difficulties accessing your account, you can send a help request to your system administrator using the link: https://okta.magicleap.builders/help/login

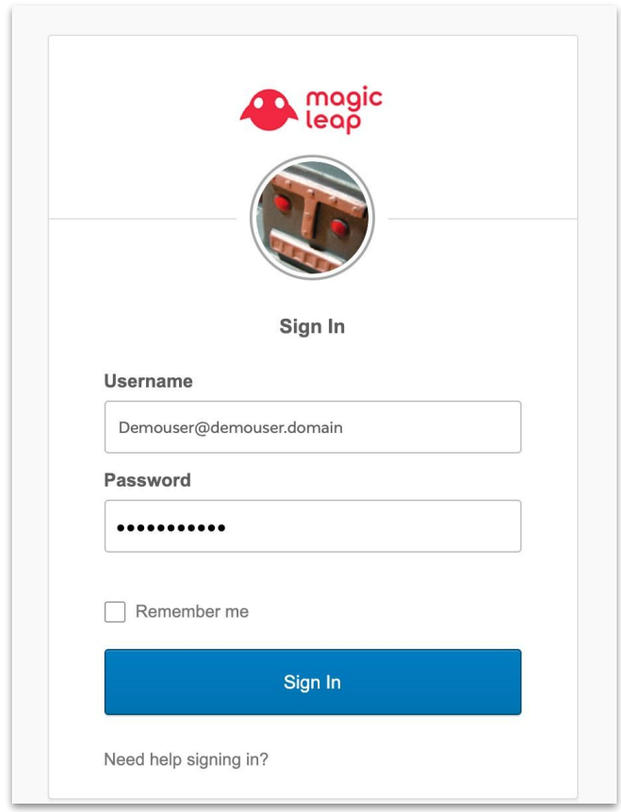
magic leap

ACCOUNT PROVISIONING

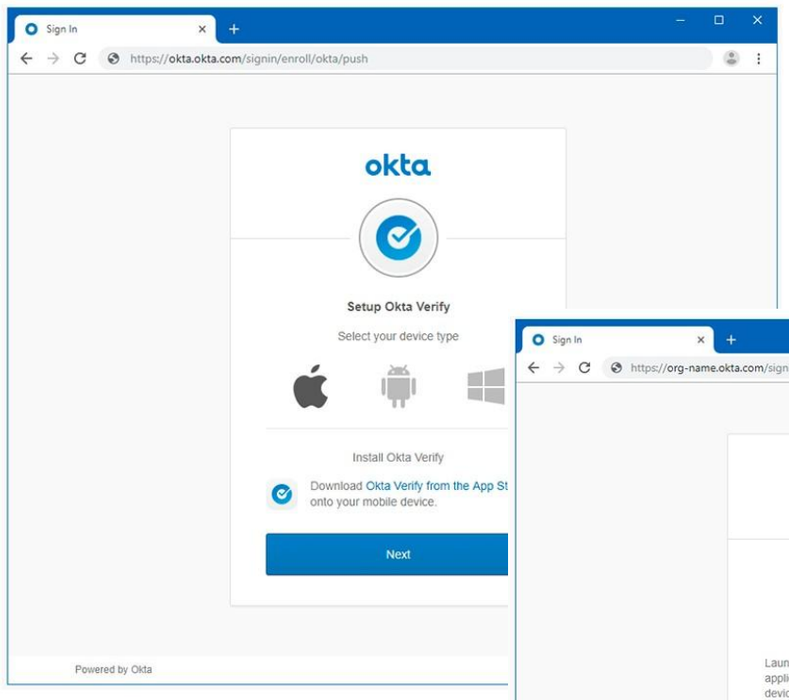
To add additional users to Okta, open a web browser and navigate to the provided Okta instance provided in your activation email (e.g. https://ml-customer.okta.com)



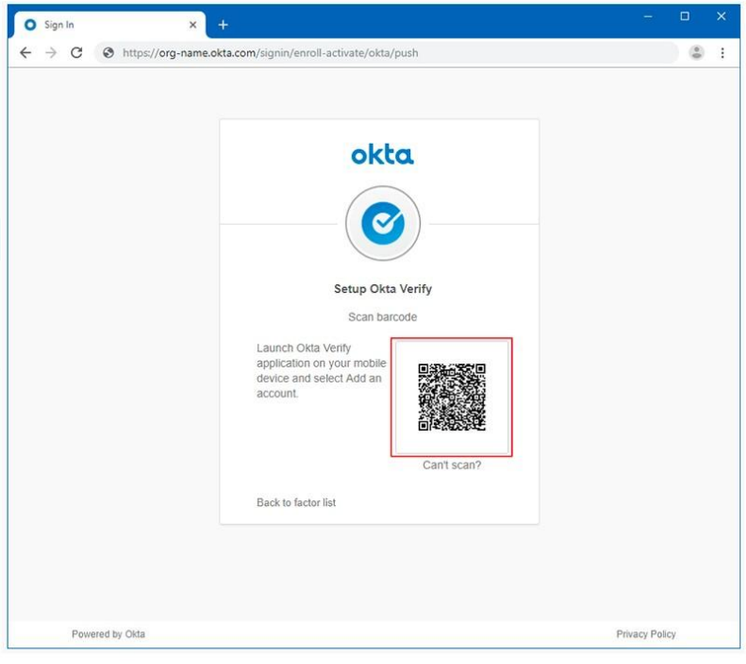
1 When you login for the first time you will presented with the **Setup multi factor authentication** screen



2 Select iOS, Android, or Windows to configure Okta Verify for your platform of choice.



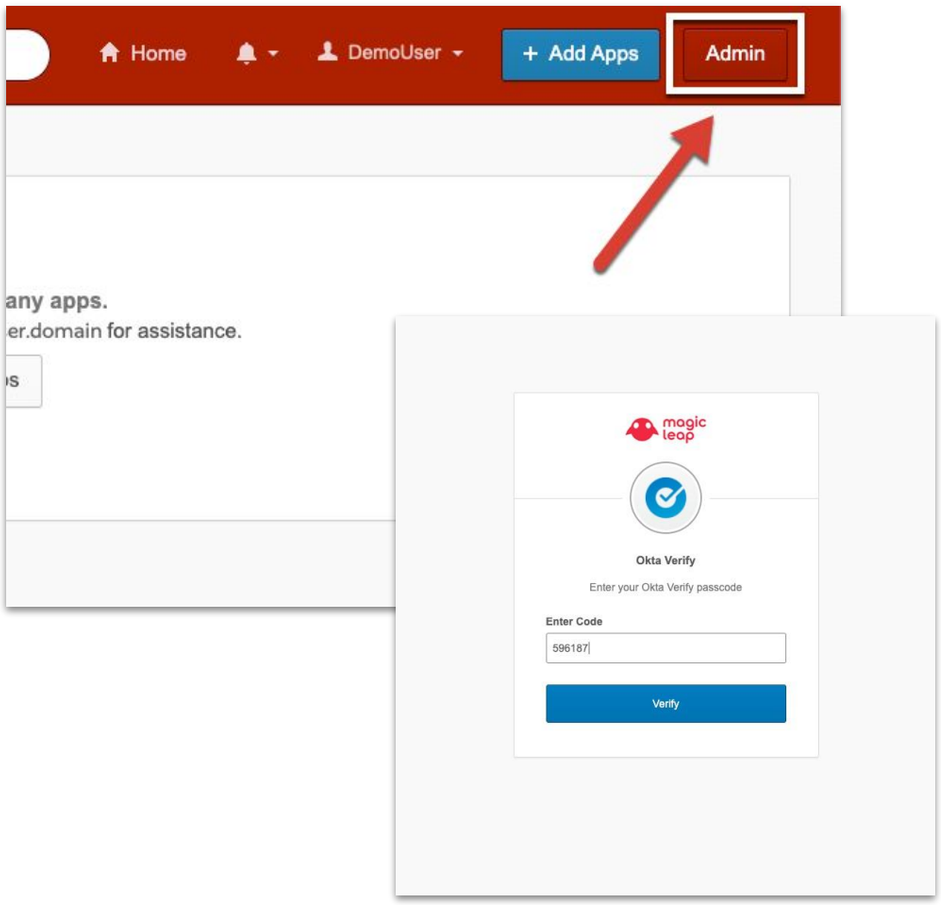
3 Open Okta Verify and click **Add Account** and scan the QR code



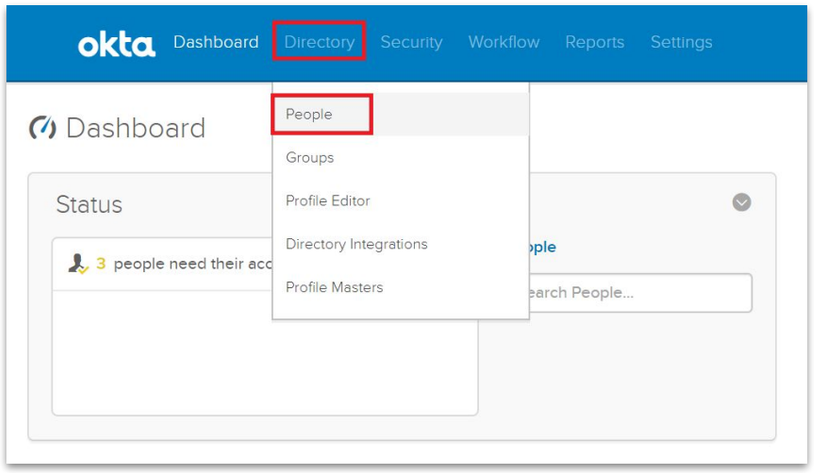
magic leap

ACCOUNT PROVISIONING

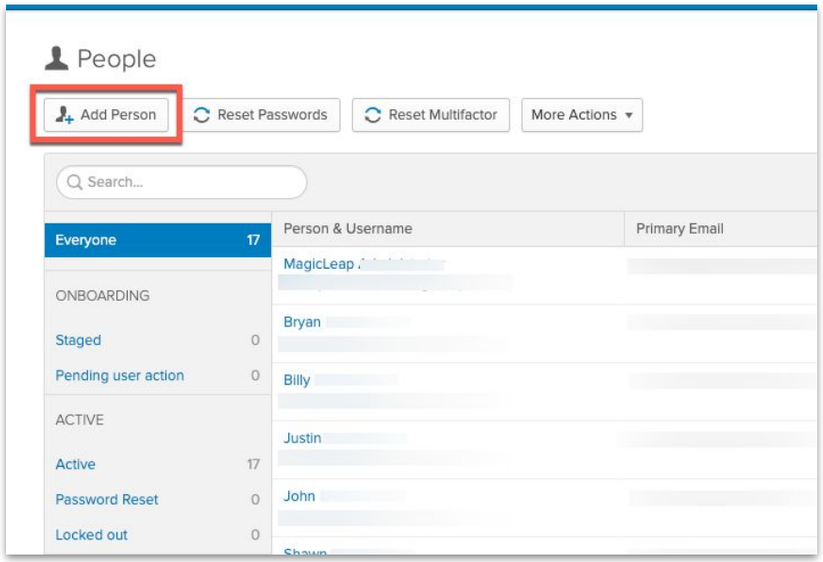
Click on the Admin button in the upper right hand corner and enter the OKTA verify key to authenticate into the Admin console



1 Click on Directory on the toolbar and then People



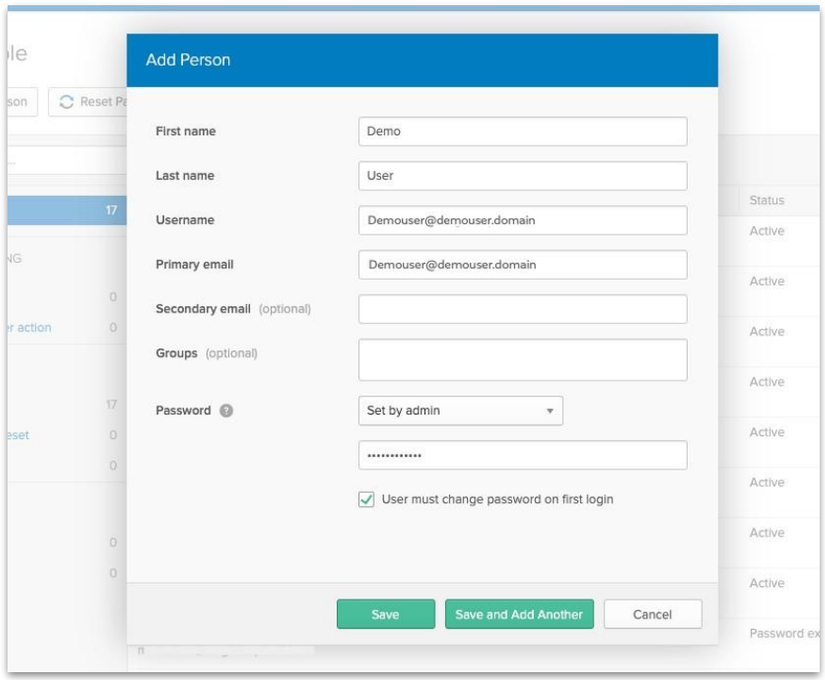
2 Click **Add Person**



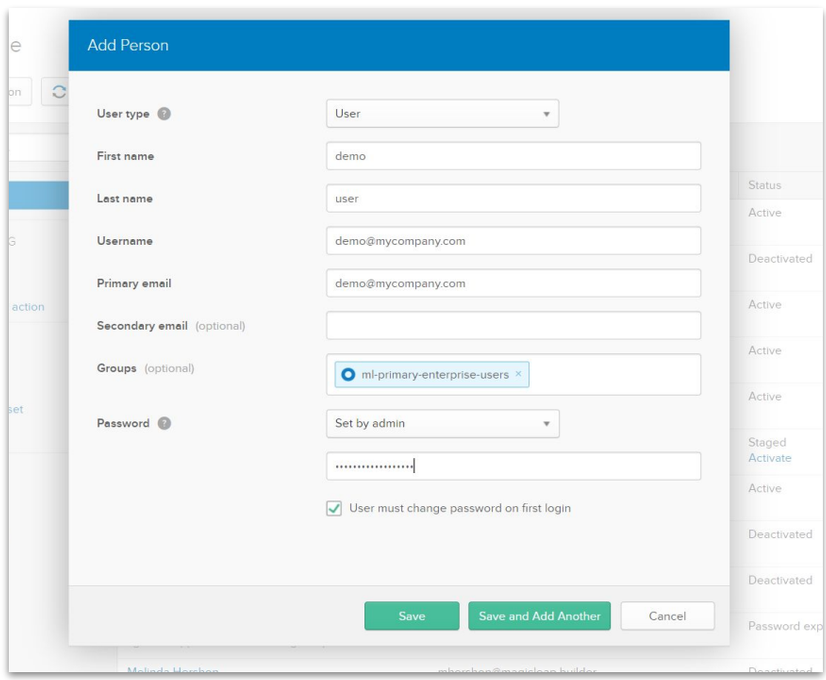
magic leap

ACCOUNT PROVISIONING

3a **Adding Non-Administrators**
For non-administrators, type in their information and click **Save**.

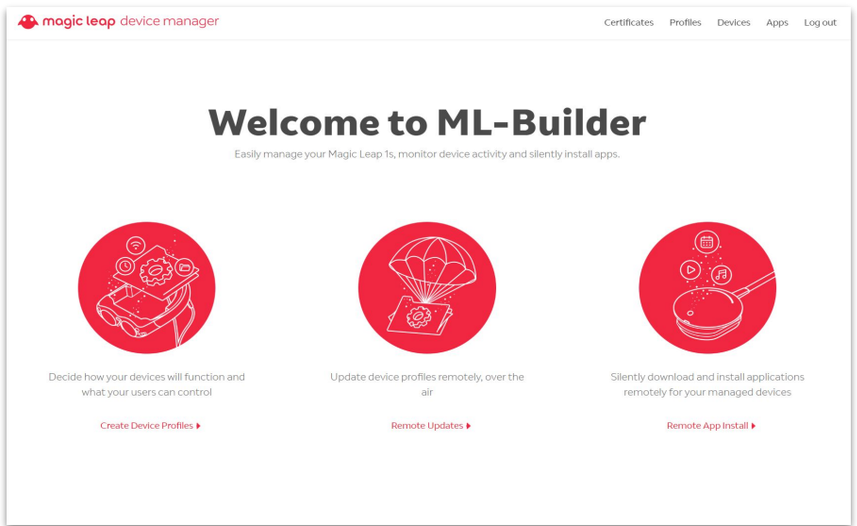


3b **Adding Administrators**
Type in the users information and add the user to the appropriate security group by typing the name of the group. For Device Manager Admins, add group: **ml-primary-enterprise-users**

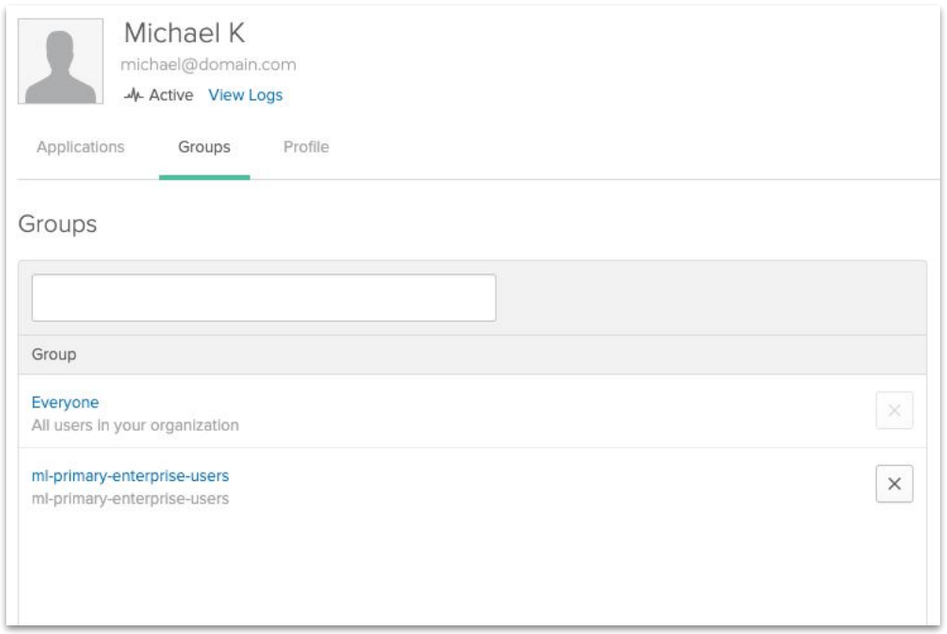


ADDING DEVICE MANAGER ADMINS

In order to login to the Device Manager, an individual(s) identified within your organization will need to be granted permission within OKTA by Magic Leap. Once Magic Leap provisions the initial administrator, that administrator must add the desired users to a predefined security group within OKTA called **ml-primary-enterprise-users**. This group is ONLY for users that need to configure and manage devices within your organization.



This group may also be synced from a compatible Active Directory or LDAP directory using the Okta group sync feature. The screenshot below shows how using OKTA directly to add the user to a specific group.



There are no additional permissions inside the Device Manager. All features of the Device Manager are available to any user with the permission to log into the site.

okta

For the best practices in configuring OKTA for your environment, please review these articles from OKTA.

[Users and Groups]

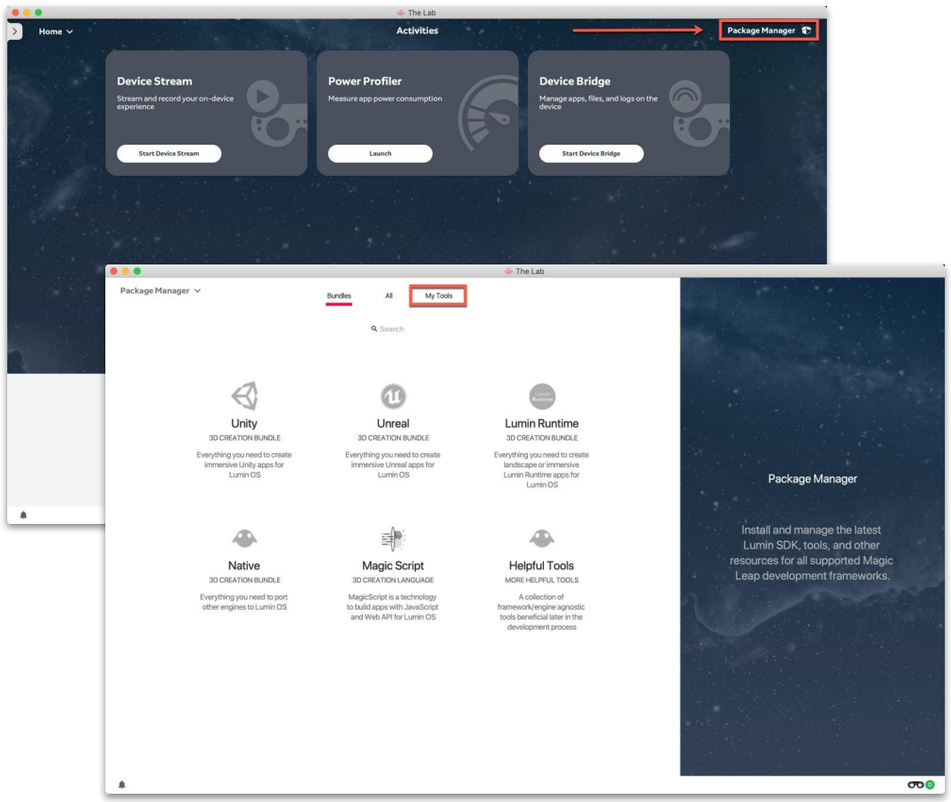
Directory Integrations

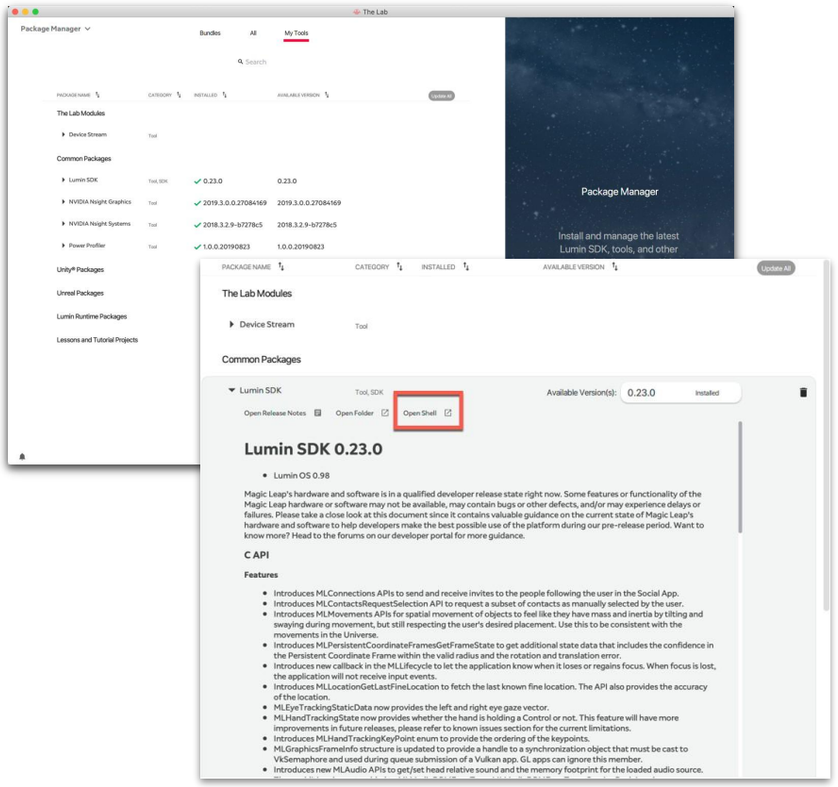
DEVICE PROVISIONING PREREQUISITES

To prepare each device added to your Enterprise, each administrator will need to follow the below steps.

MAGIC LEAP THE LAB

Command-line management (MLDB) of Magic Leap devices is available and will be used with certain aspects of the process. Download the Magic Leap desktop app, “The Lab”, which includes the Package Manager here.





magic leap

DEVICE PROVISIONING PREREQUISITES

Obtaining the MAC Address

Some organizations require the whitelisting of devices before they can utilize network resources. In order to find the MAC address for each device, you will plug in your Magic Leap into a computer. Leveraging the Magic Leap Lab and Package Manager from the link above and select **Lumin SDK** and click on **Shell**.

Once you have opened your shell, you will type in the following:

mldb ifconfig

Within the **wlan0** section you will see the **HWaddr** print out of the MAC address of the device currently connected

magic leap

DEVICE PROVISIONING PREREQUISITES

WiFi Internet Access

Verify that your environment has valid internet connectivity for each device to be configured.

The device supports the following networks: Open, WPA Personal and 3 types of WPA Enterprise: PEAP, TLS, TTLS.

WPA-Personal
Since WPA Personal requires a password, Magic Leap will encrypt that password at the time it is entered on Device Manager. It uses a key specific to the enterprise customer thus allowing for safe storage and retrieval.

WPA Enterprise
TLS will require both CA and Client Certificates. TTLS requires a CA Certificate. Certificates can be uploaded to Device Manager by using the Certificates section from the header menu and must be loaded prior to adding to a profile.

Note: When applying a profile with a pre-configured network, the key file must also be applied to the device. This is done via the MLDB command-line tool available within the Magic Leap Lab and Package Manager, discussed in detail later on in this guide.

App Publishing

If your organization will be deploying an app to your Magic Leap devices, you will need a Publisher account configured on our Developer Portal. Some organizations may choose to leverage a relationship with a 3rd party developer, who will also need to have a Publisher account.

LOGGING INTO DEVICE MANAGER

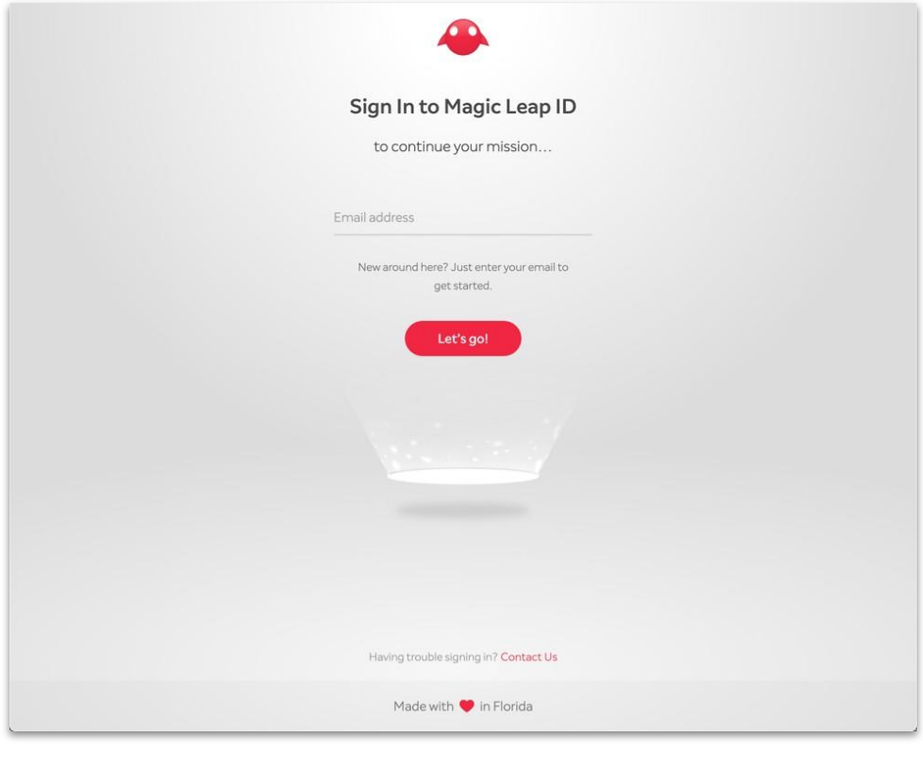
Once the administrator(s) have been added to the ml-primary-enterprise- users group, they can now login to the Device Manager.

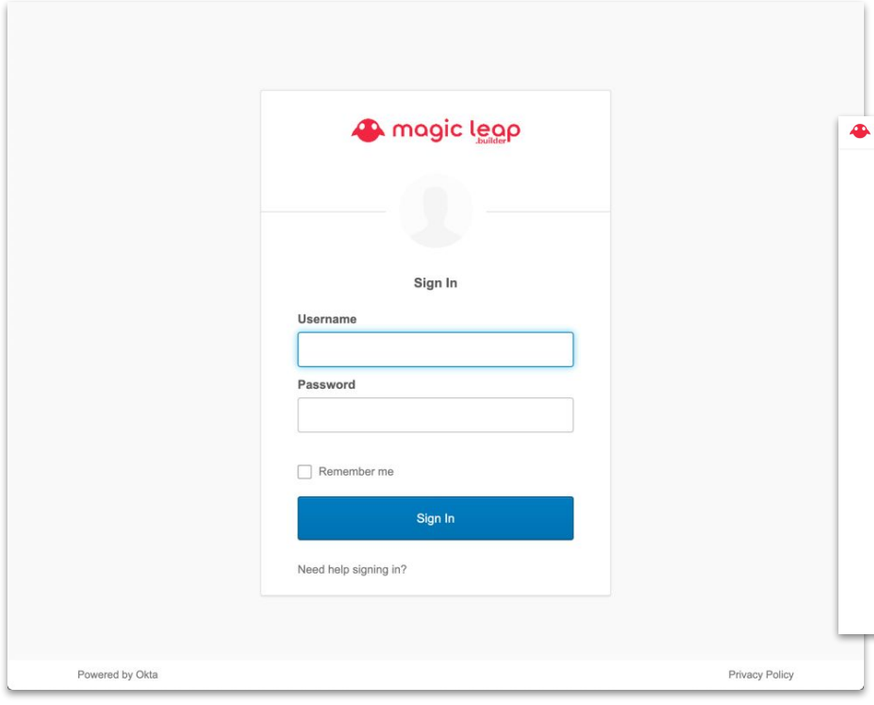
Log into the Magic Leap Device Manager by going to the following website using your browser.

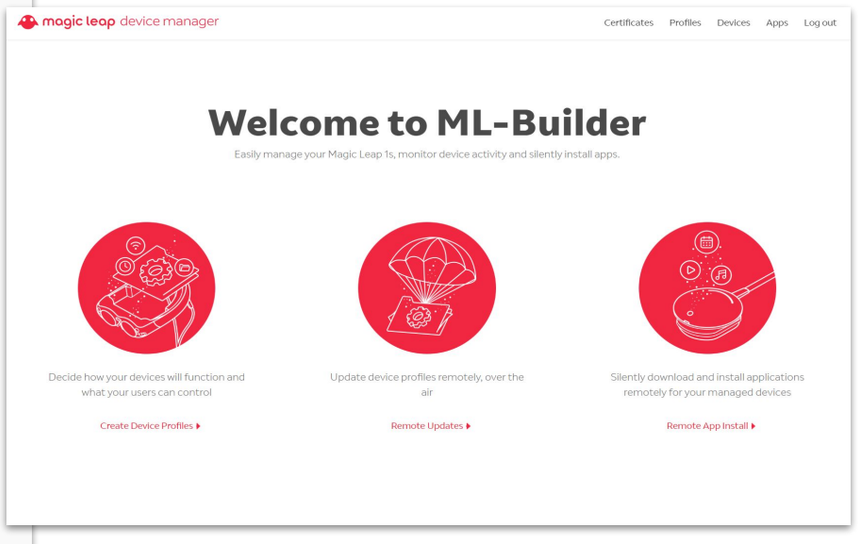
https://devicemanager.magicleap.com

Enter the email address of your existing company login.

You will be redirected to the OKTA login screen. Enter the password associated with your account to log in.







okta

Download Mobile OKTA Authenticator

OKTA (iOS)

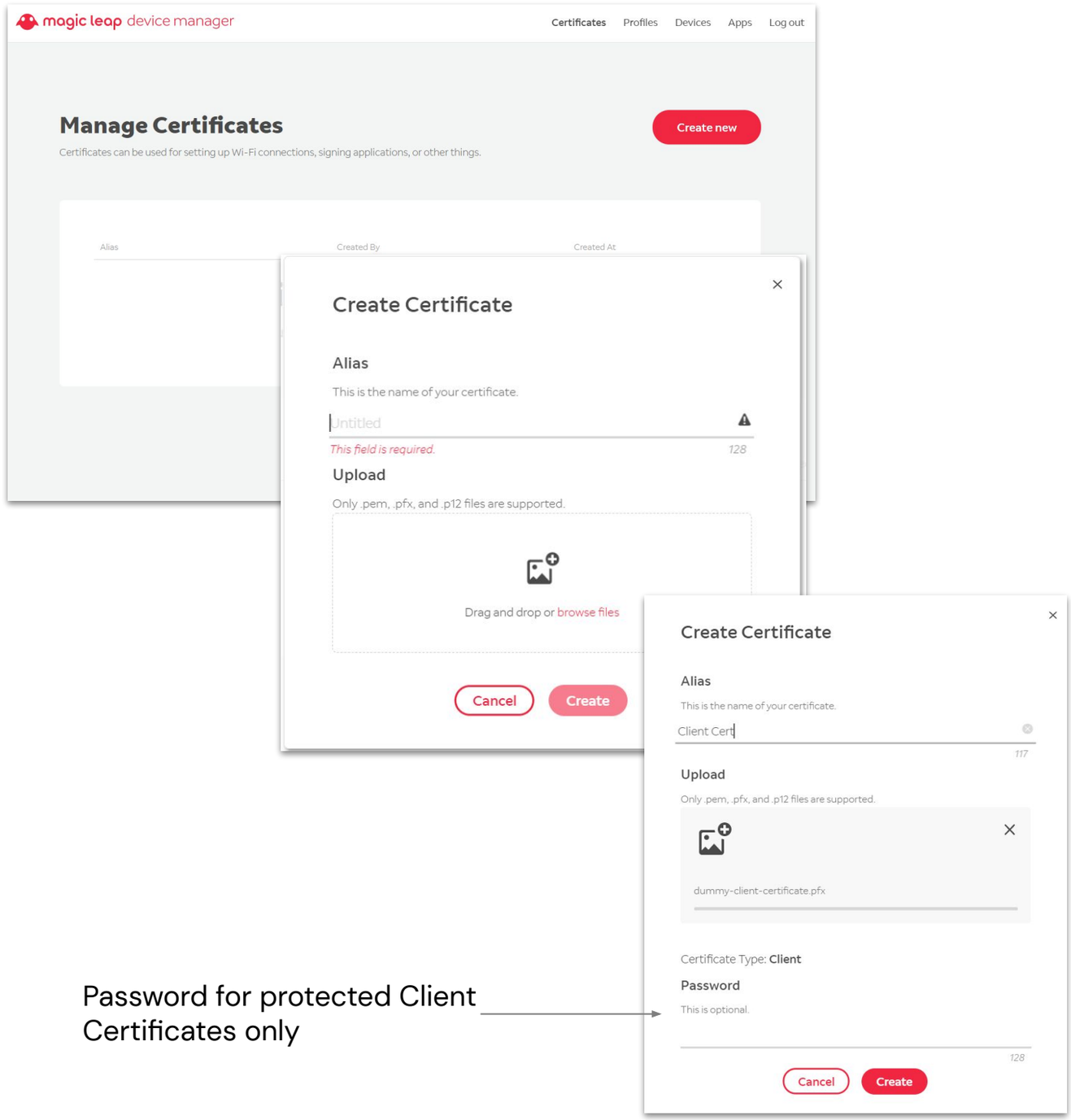
OKTA (Android)

CERTIFICATES

Certificates can be used for setting up Wi-Fi connections. Add a Certificate here and it will then be available when configuring Wifi connections within a profile.

Adding Certificates

- click on Certificates from the top menu
- click “Create new”
- enter an Alias to identify the certificate
- drag a single certificate from your computer to the upload section of the Device Manager Create Certificate window. The certificate type will be automatically detected
- If the Certificate was password protected, please enter the password in the optional password field. Otherwise, leave it blank.
- click Create
- the Certificate will now show in your Manage Certificates list
- add more certs if applicable

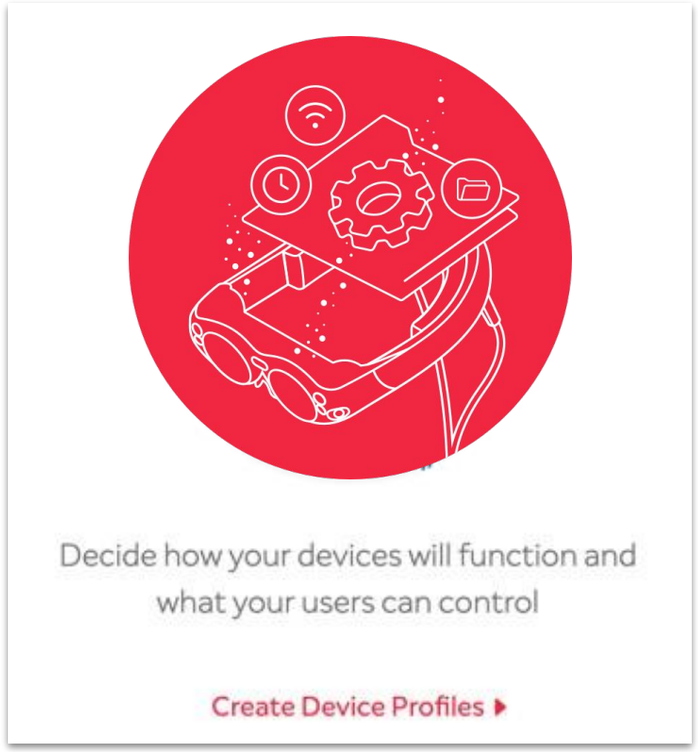


magic leap

PROFILES

Managing devices is done by applying a **provisioning profile** to each device. Each profile contains settings that allow the device to be configured with preset values to customize the device to fit their business needs. Administrators can create multiple provisioning profiles and assign them to different devices.

Profiles are encrypted in a way that only certified Magic Leap devices can decrypt and use these profiles. Profiles are specific to each enterprise customer and cannot be shared outside the organization.



Profile Management

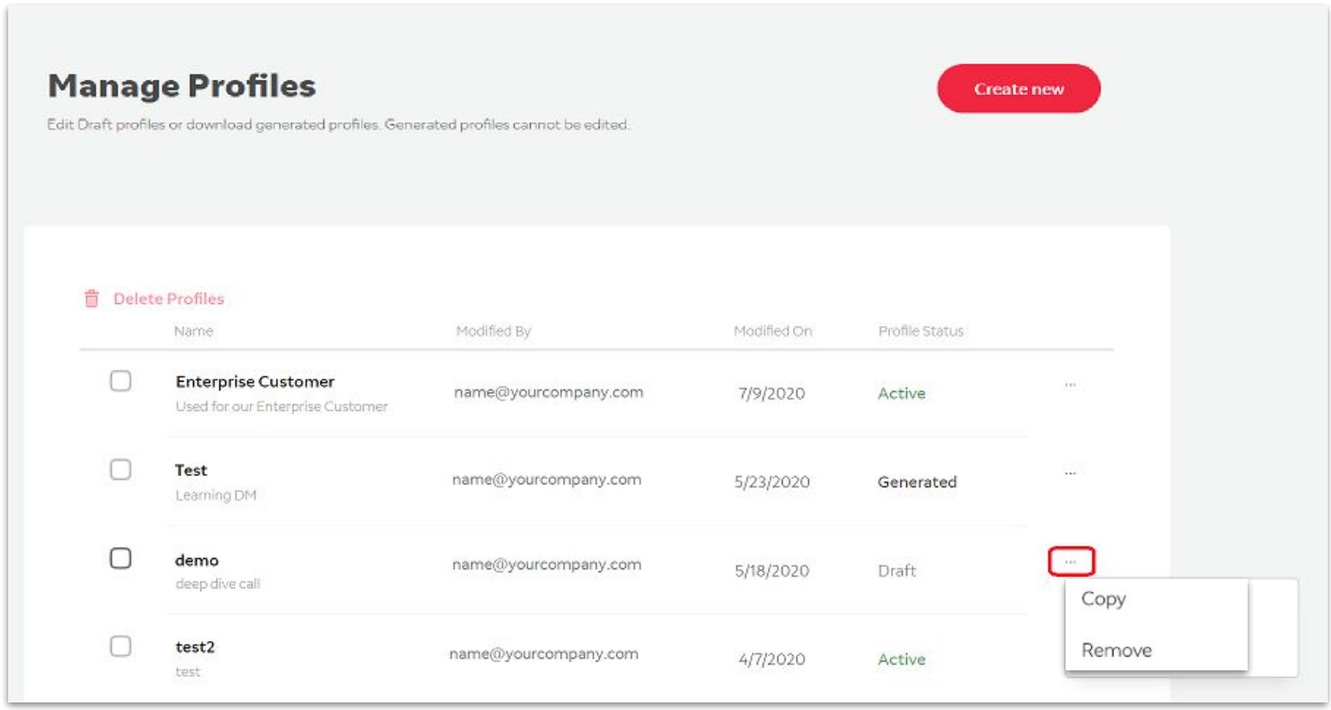
Creating a profile is done in the Device Manager. The Device Manager contains preset values for most fields and requires only a few clicks to get started.

Let's understand the steps needed to create and manage profiles within the Device Manager.

1. To create your first profile, click on **Create Device Profiles** from the Device Manager home page.
2. On the **Manage Profile** page, click on the **Create *new*** button.

PROFILES

The Device Manager has three types of profiles available for use within the environment. Below you will find the details around **DRAFT**, **GENERATED** and **ACTIVE** and what actions can be performed on each**.**
Note: removing a profile cannot be undone



	Can Edit?	Can Download?	Can Copy?	Can Remove?	Description
Draft	Yes	No	Yes	Yes	Profile has not been submitted yet
Generated	No	Yes	Yes	No	Profile has been submitted and ready to be installed on a device
Active	No	Yes	Yes	No	Profile is applied to a device and device connects to the cloud

magic leap

PROFILES:

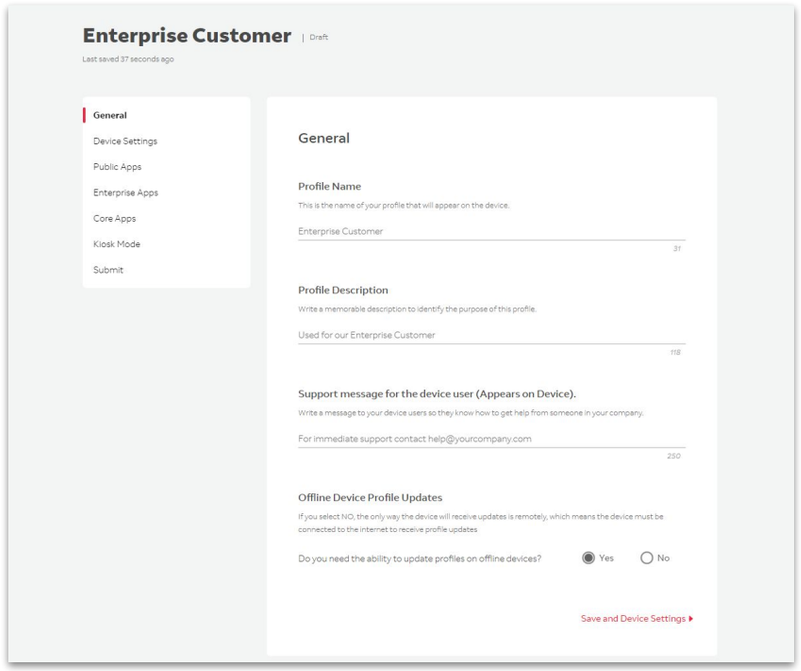
CREATE PROFILE-GENERAL

On the General tab we will begin creating the basic information for the profile.

- **Profile Name**: This is the name of your profile that will appear on the device.
- **Profile Description**: Write a memorable description to identify the purpose of this profile.
- **Support message for the device user (Appears on Device):** Write a message to your device users so they know how to get help from someone in your company.
- **Offline Device Profile Updates: (Choose Yes or No)**

  Note: We recommend **Yes** for this feature to ensure access to the device, if needed. If you select **NO**, the only way the device will receive updates is remotely, which requires internet connectivity.

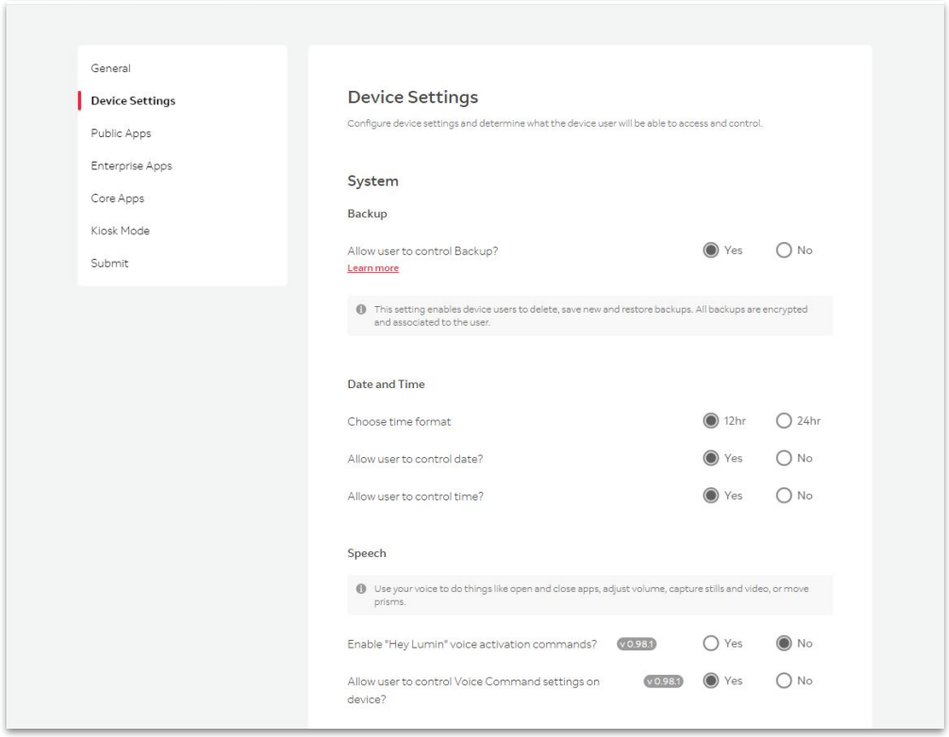
  Once you have entered the general information you can proceed to the next step



magic leap

PROFILES: CREATE PROFILE-DEVICE SETTINGS

On this page you will configure device settings and determine what the device user will be able to access and control while using the device.



System

- **Backup**
    - Allow user to control backup? **(Choose Yes/No)** This gives users the ability to delete, save new and restore backups. All backups are encrypted and associated with the user.

- **Date and Time**
    - Choose Time Format **(Choose 12hr/24hr)**
    - Allow user to control date? **(Choose Yes/No)**
    - Allow user to control time? **(Choose Yes/No**

- **Speech**

  Use your voice to do things like open and close apps, adjust volume, capture stills and video, or move prisms.
    - **Enable "Hey Lumin" voice activation commands?: (Choose Yes/No**) All devices require internet connection during the initial set up to ensure successful profile installation.
    - **Allow user to control Voice Command settings on device? (Choose Yes/No)** If you pre-configure Wifi networks, the device user will only be able to control and connect to those networks.

PROFILES:

CREATE PROFILE-DEVICE SETTINGS

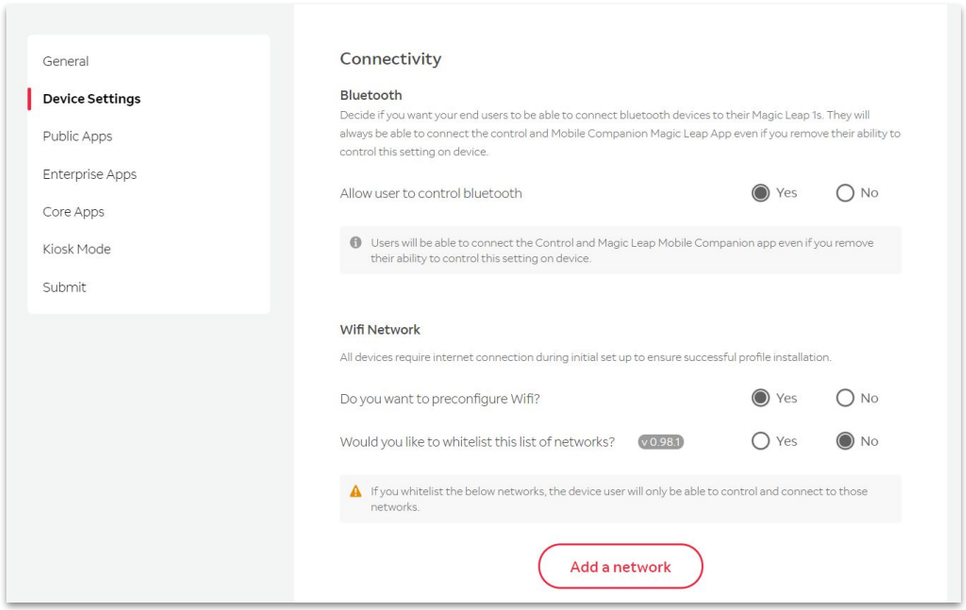
On this page you will configure device settings and determine what the device user will be able to access and control while using the device.

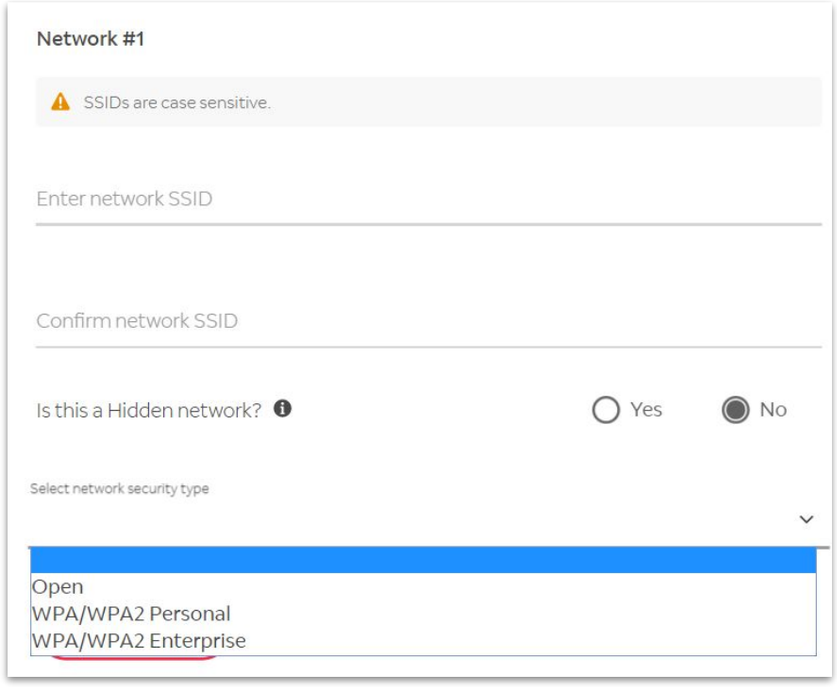
Connectivity

- **Bluetooth**: Device Users will have access to control Bluetooth settings which means they will be able to pair the Control, Magic Leap Mobile Companion App and other Bluetooth devices (**Choose Yes/No)**
- **Wifi Network**: All devices require internet connection during the initial set up to ensure successful profile installation.
- **Do you want to preconfigure Wifi? (Choose Yes/No)**

  To preconfigure Wifi:
  - choose yes to preconfigure Wifi.
  - click ‘add a network’
  - enter the network SSID
  - select the network security type from the drop down menu:
    - Open
    - WPA/WPA2 Personal
    - WPA/WPA2 Enterprise

**Note* for Open, WPA/WPA2 Enterprise PEAP, and WPA/WPA2 Enterprise TTLS networks, the end user will still be required to enter wifi credentials on the device.*





magic leap

PROFILES:

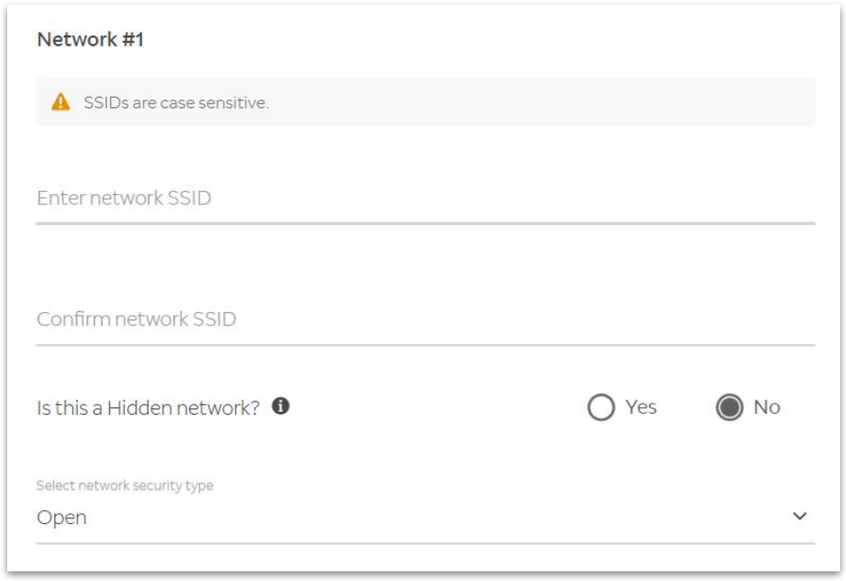
CREATE PROFILE–DEVICE SETTINGS

Connectivity

- **Wifi Network (continued)**

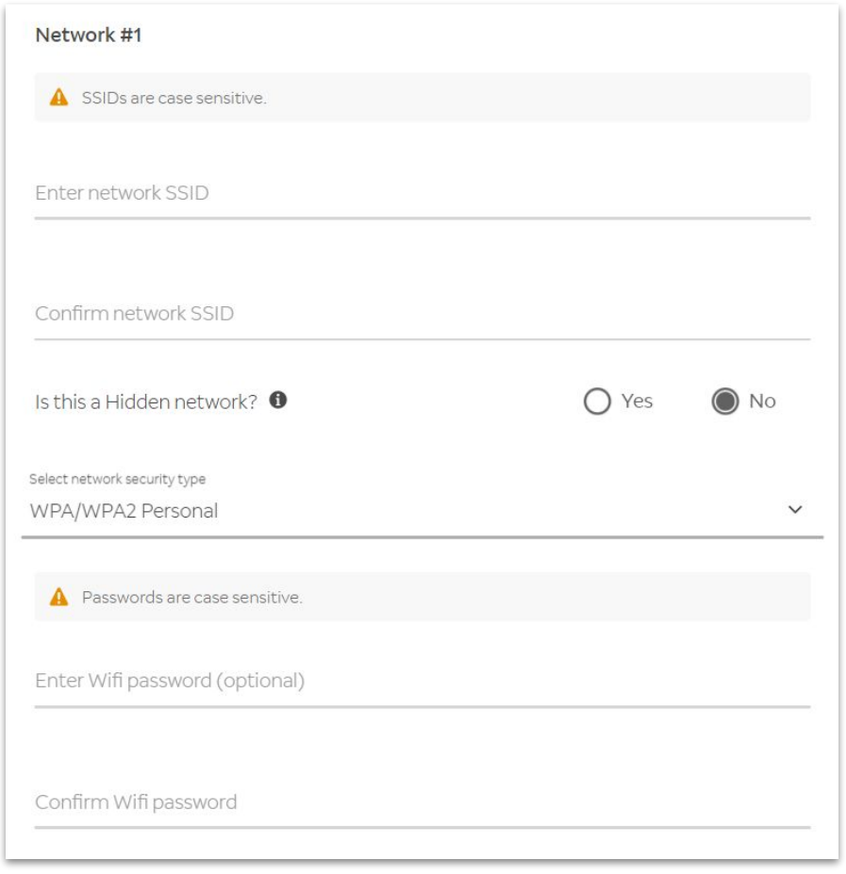
Open network

SSID required



WPA/WPA2 Personal network

SSID & Wifi password required



magic leap

PROFILES:

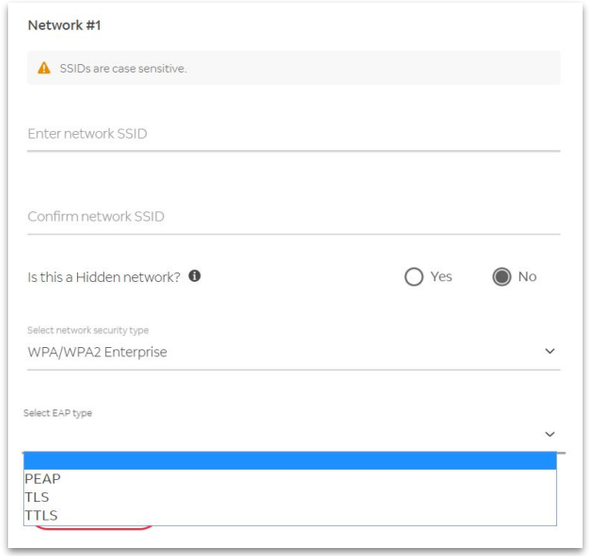
CREATE PROFILE–DEVICE SETTINGS

Connectivity

- **Wifi Network (continued)**

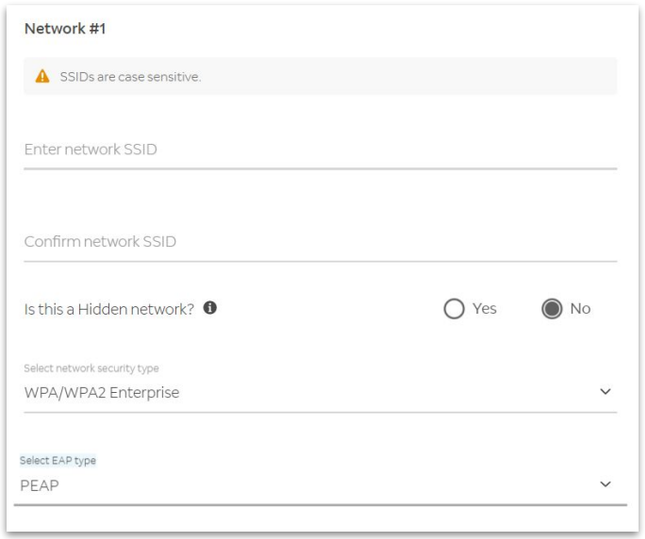
WPA/WPA2 Enterprise network

SSID and, select the EAP type: PEAP, TLS, TTLS



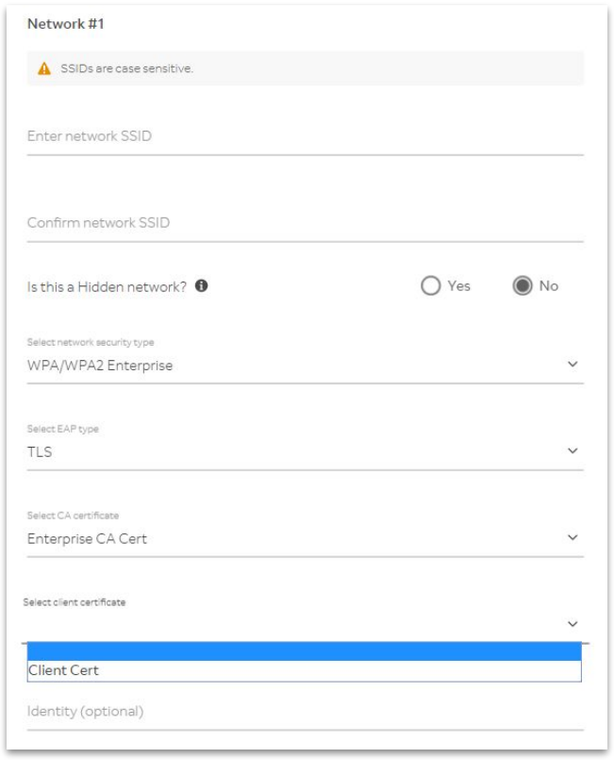
PEAP

no cert required



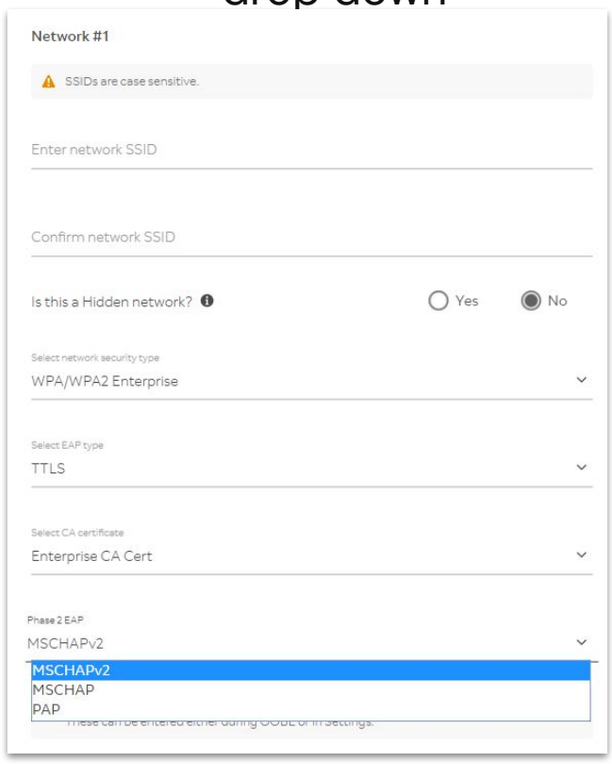
TLS

CA & Client cert required plus optional identity field



TTLS

CA cert required plus specify TTLS type from the drop down



magic leap

PROFILES:

CREATE PROFILE–DEVICE SETTINGS

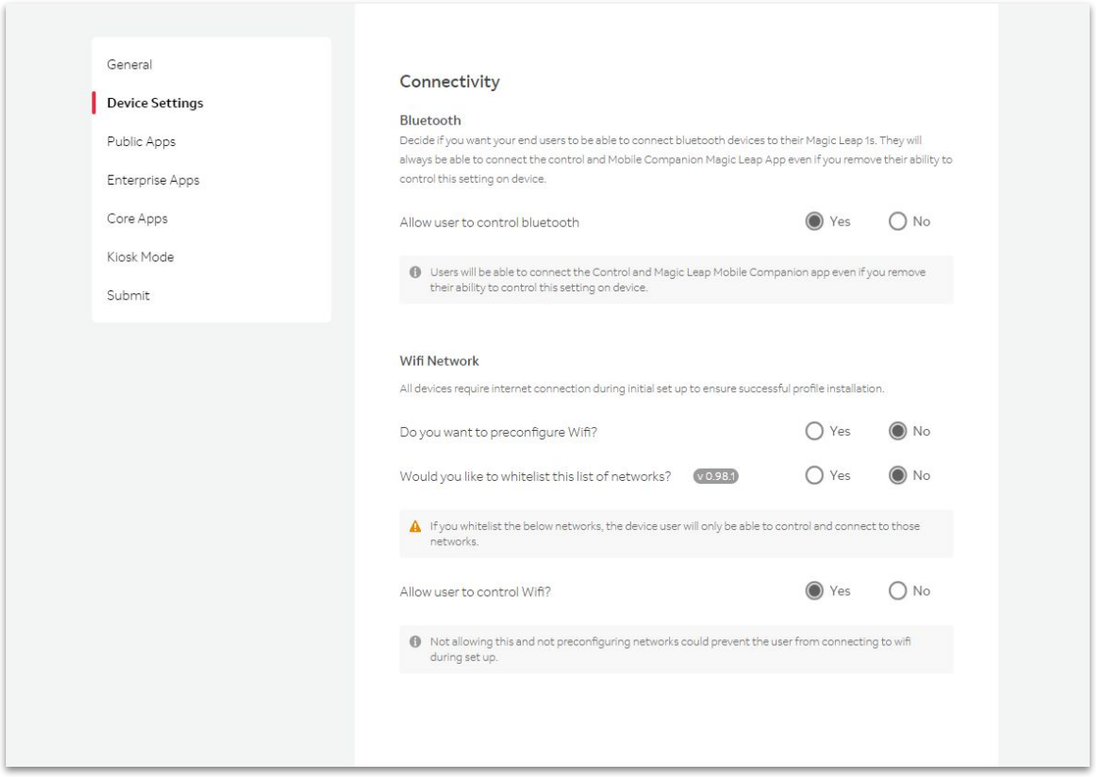
Connectivity

.

- **Would you like to whitelist this list of networks? (Choose Yes/No)** v0.98.10+

  If you whitelist networks, the device user will only be able to control and connect to those networks.

- **Allow users to control Wifi? (Choose Yes/No)** **IMPORTANT Not allowing this and not configuring a network could prevent the user from connecting to wifi during setup. **



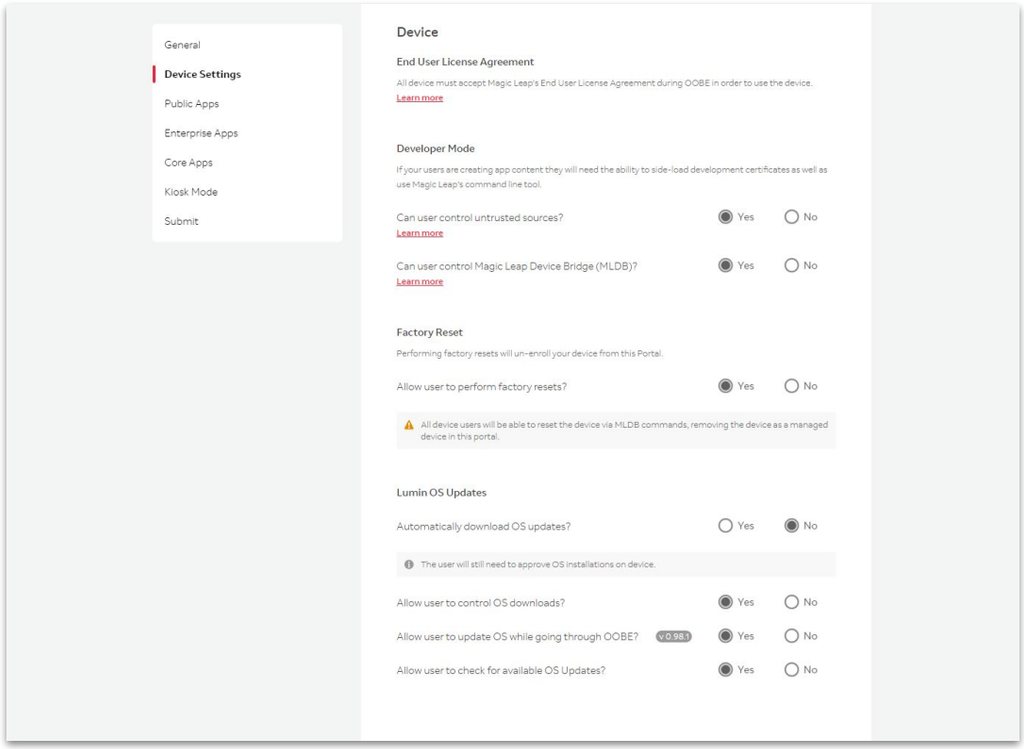
magic leap

PROFILES:

CREATE PROFILE-DEVICE SETTINGS

DEVICE

- **End User License Agreement**: All devices must accept Magic Leap's End User License Agreement during OOBE (Out of Box Experience) in order to use the device.
- **Developer Mode:** If your users are creating app content they will need the ability to side-load development certificates as well as use Magic Leap's command- line tool.
    - Can user control untrusted sources? **(Choose Yes/No)** Learn more
    - Can user control Magic Leap Device Bridge (MLDB)? **(Choose Yes/No)** Learn more
- **Factory Reset:** Performing factory resets will un-enroll your device from the Device Manager.
    - Allow user to perform factory resets? **(Choose Yes/No)** **Note**: Allowing this will provide users with the ability to remove the device from the Device Manager



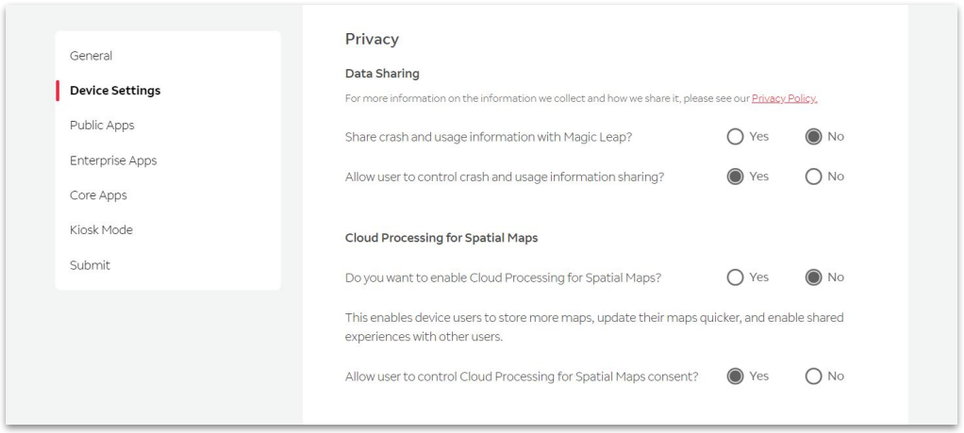
- **Lumin OS updates**
    - Automatically download OS updates? **(Choose Yes/No)** **The user will still need to approve OS installations on device**. Learn More
    - Allow user to control OS downloads? **(Choose Yes/No)**
    - Allow user to update OS while going through OOBE? **(Choose Yes/No)** v0.98.10+
    - Allow user to check for available OS Updates? **(Choose Yes/No)**

PROFILES:

CREATE PROFILE-DEVICE SETTINGS

On this page you will configure device settings and determine what the device user will be able to access and control while using the device.

PRIVACY



- **Data Sharing**: For more information on the information we collect and how we share it, please see our Privacy Policy.
  - Share crash and usage information with Magic Leap? **(Choose Yes/No)**
  - Allow user to control crash and usage information sharing? **(Choose Yes/No)**

- **Cloud Processing for Spatial Maps**
  - Do you want to enable Cloud Processing for Spatial Maps? **(Choose Yes/No)**
    Note: Cloud Processing enables cloud storage of spatial maps created from your device rather than relying solely on maps stored on your device.
  - Allow user to control Cloud Processing for Spatial Maps consent? **(Choose Yes/No)**
    Note: This would allow users the ability to disable this feature.

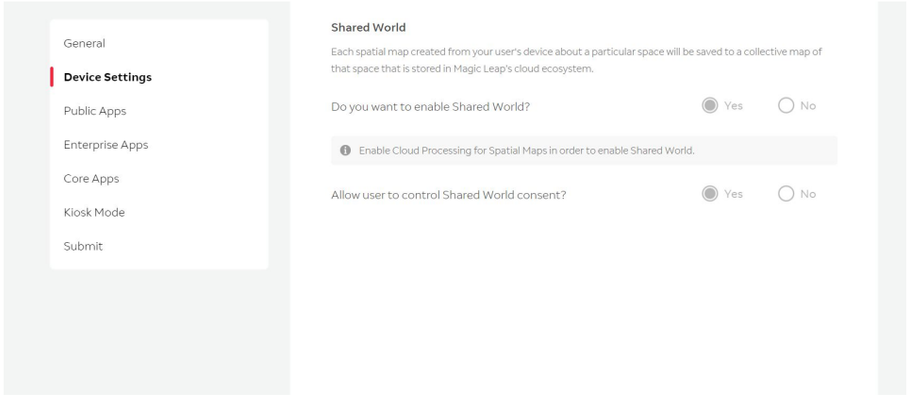
PROFILES:

CREATE PROFILE-DEVICE SETTINGS

On this page you will configure device settings and determine what the device user will be able to access and control while using the device.

PRIVACY (con't)

- **Shared World:** Each spatial map created from your user's device about a particular space will be saved to a collective map of that space that is stored in Magic Leap's cloud ecosystem.
    - Do you want to enable Shared World? **(Choose Yes/No)** Enable Cloud Processing for Spatial Maps in order to enable Shared World.
- Allow user to control Shared World consent? **(Choose Yes/No)**



magic leap

PROFILES:

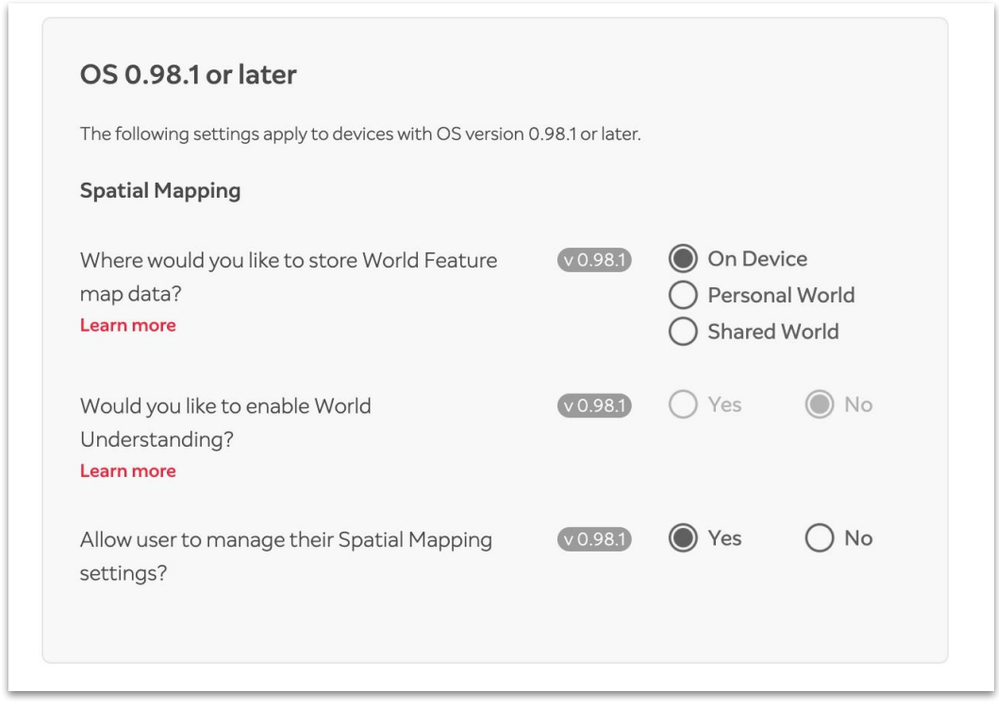
CREATE PROFILE-DEVICE SETTINGS

PRIVACY (con't)

- **Spatial Mapping**

  On this page you will configure the Spatial Mapping settings for devices running Lumin OS 0.98.10. Administrators will be able to determine where map data is stored, the enablement of World Understanding and whether users have the ability to control these Spatial Mapping settings on device.

  - Where would you like to store World Feature map data?
    - **On Device**: Stored Locally, this data is only visible to the user and their Magic Leap Device.
    - **Personal World:** Map data is stored in the cloud, but only visible to the user.
    - **Shared World:** Map data is stored in the cloud, but shared with the community to improve experiences.



- Would you like to enable World Understanding (**Choose Yes/No)**
  Allows Magic Leap to apply labels to the world around you, such as nearby walls or displays. It only shares that information with the user.
- Allow user to manage their Spatial Mapping settings? (**Choose Yes/No)**

magic leap

PROFILES:

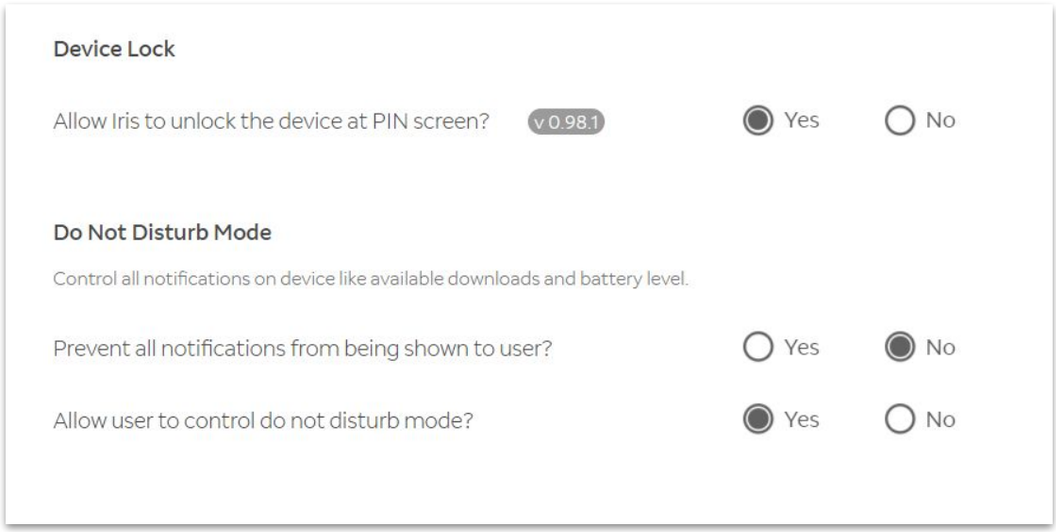
CREATE PROFILE-DEVICE SETTINGS

PRIVACY (con't)

- **Device Lock:**

  Device users will always have the ability to set PIN under the on-device settings menu but as an admin, you may block the user's ability to use Iris scanning at the PIN screen

  - Allow Iris to unlock the device at PIN screen? v0.98.10+ **(Choose Yes/No)**



- **Do Not Disturb Mode:**

  Control all notifications on device like available downloads and battery level.

  - Prevent all notifications from being shown to user? **(Choose Yes/No)**
  - Allow user to control do not disturb mode? **(Choose Yes/No)**

magic leap

PROFILES:

CREATE PROFILE-DEVICE SETTINGS

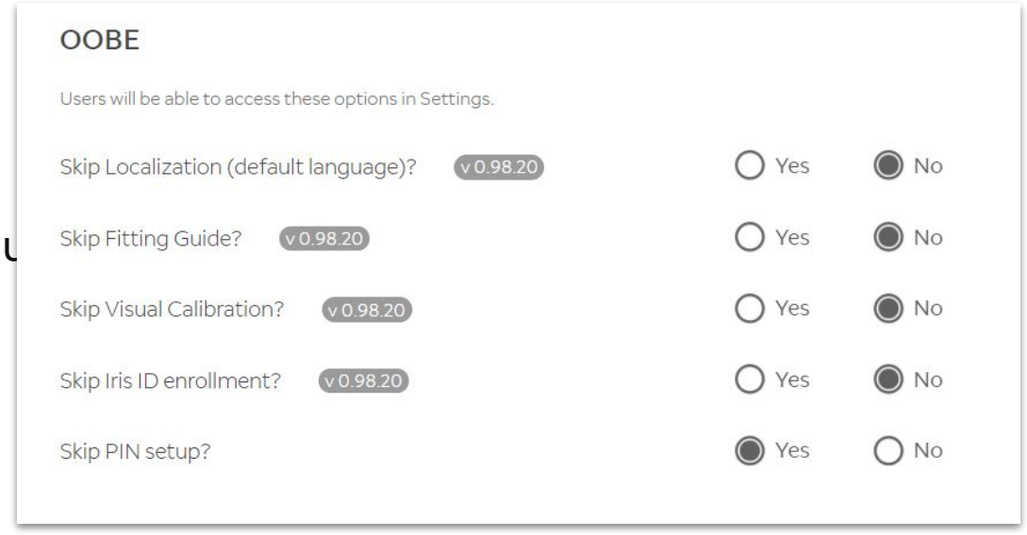
OOBE (end user set up)

OOBE is the Out of Box Experience where the device user performs an on device guided setup.

Selecting 'yes' to skip these steps will bypass them during the setup process but the user will still be able to access these options in the on-device settings menu when needed.

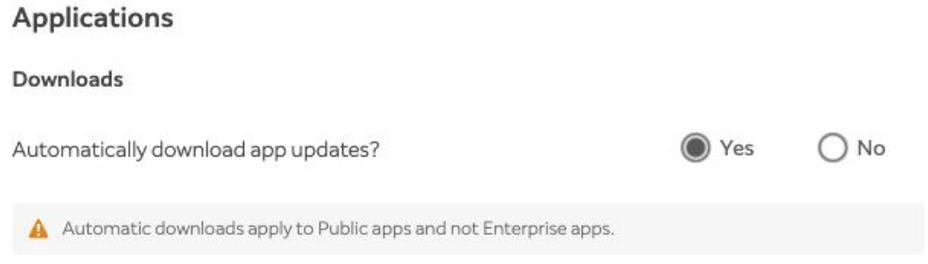
- Skip Localization (default Language)? **(Choose Yes/No)** v0.98.20+

  *Note: if skipped, you will be prompted to select the defau language for the profile
- Skip Fitting Guide? **(Choose Yes/No)** v0.98.20+
- Skip Visual Calibration? **(Choose Yes/No)** v0.98.20+
- Skip Iris enrollment? **(Choose Yes/No)** v0.98.20+
- Skip PIN setup? **(Choose Yes/No)**



APPLICATIONS

- **Downloads**
  - Do you want to enable auto downloads? **(Choose Yes/No)**
    Note: Automatic updates only apply to Public apps, not Enterprise apps



PROFILES:

CREATE PROFILE–PUBLIC APPS

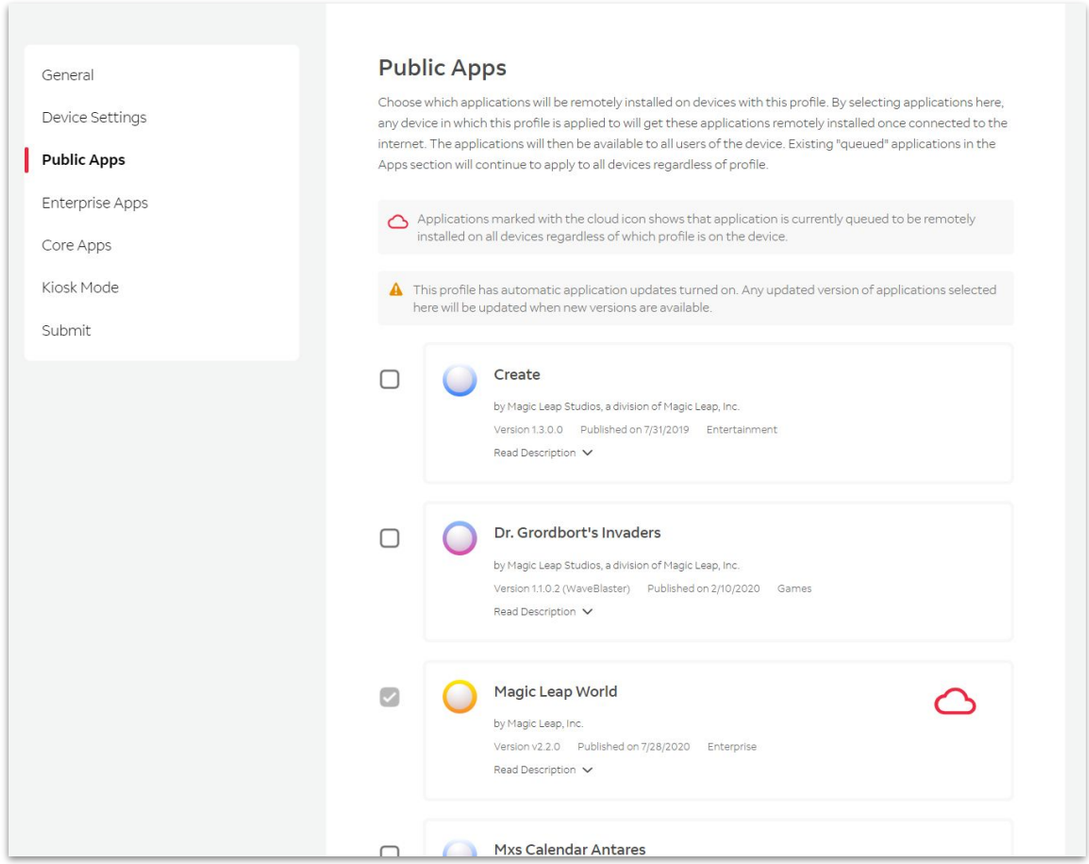
PUBLIC APPS

These apps listed are free, publicly available for download in Magic Leap World in your home country

In this section, an administrator will select which apps to be made available to the end user to download using that profile.

Note

- Apps shared at the org level (installed apps ☁) will be available for the entire organization regardless of profile and cannot be excluded from a specific profile
- Once an app is shared at the org level, it cannot be unshared
- Apps will not install if device memory is full



magic leap

PROFILES:

CREATE PROFILE-ENTERPRISE APPS

ENTERPRISE APPS

These are privately shared apps within your organization.

Administrator will select which apps to be made available to the end user to download using that profile.

Note

- Apps shared at the org level (installed apps ☁) will be available for the entire organization regardless of profile and cannot be excluded from a specific profile
- Once an app is shared at the org level, it cannot be unshared
- Apps will not install if device memory is full

PROFILES:

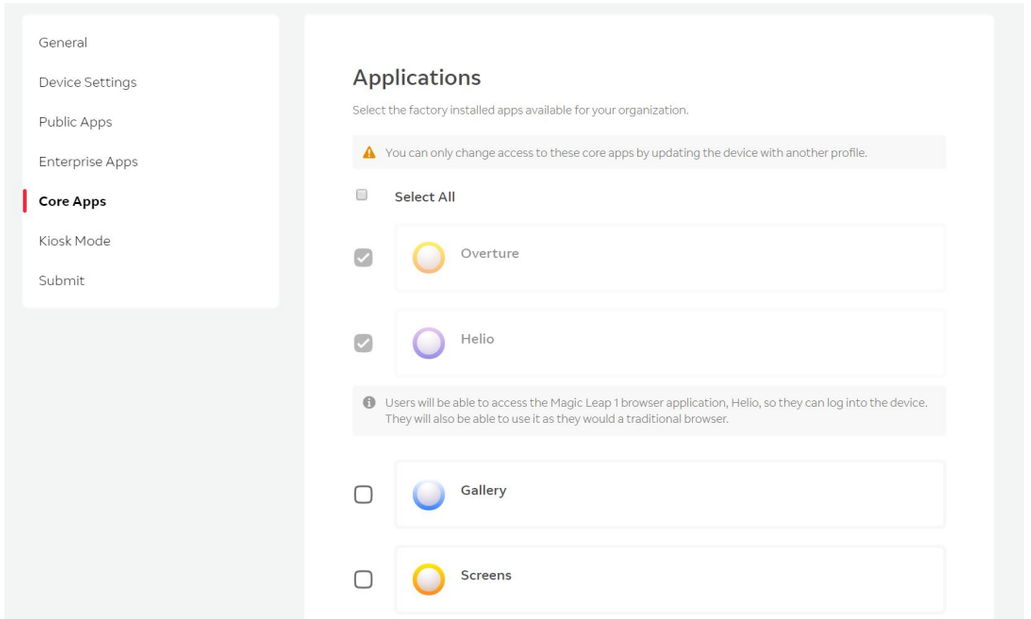
CREATE PROFILE-CORE APPS

In this section, an administrator will select the Factory installed apps that a user can have access to while using their Magic Leap device

Applications

- **Helio**
  Users can access Magic Leap's browser application, Helio, so they can log into the device. They may also use as a traditional browser.

  Description: Helio enables 3D objects to be pulled out of websites and into the physical world, transforming passive web browsing into an interactive spatial experience. With the ability to create true-to-life virtual replicas of anything from recipe cards to living room chairs, the world wide web is ready to bring a new era of accessibility to the world.



- **Gallery**
  Description: Access to our photo and video library application.

- **Overture**
  Description: Overture is an on-device music app for playing your favorite music.

- **Screens**
  Description: Entertainment and News related applications on device. (Must have an active internet connection to access this content)

magic leap

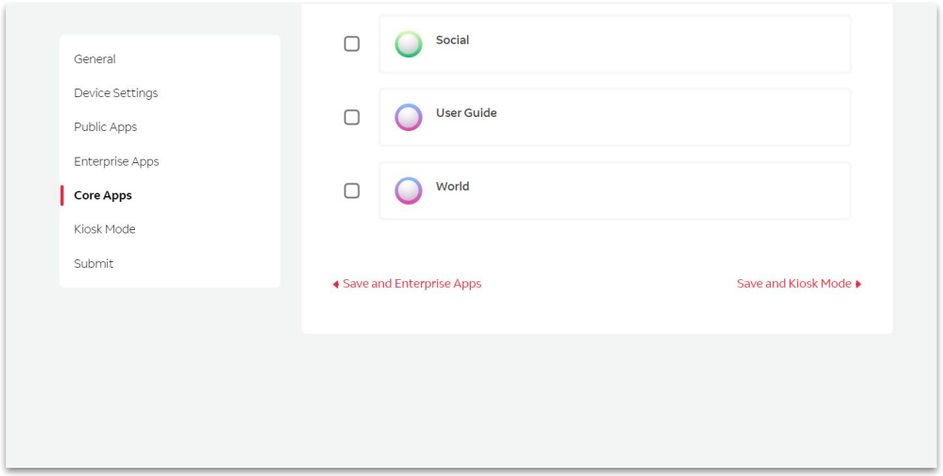
PROFILES:

CREATE PROFILE-CORE APPS

- **Social**
  Description: Share experiences, follow your friends and join other developers to explore this new frontier together. Build, personalize and accessorize your own custom avatars with a suite of creation tools. (Must have an active internet connection to access this feature)

- **User Guide**
  Description: Access to our on-device User guide.

- **World**
  Description: Magic Leap World is our app store, providing access to all of the latest publicly available applications. (Must have an active internet connection to access this content)



magic leap

PROFILES:

CREATE PROFILE-KIOSK MODE

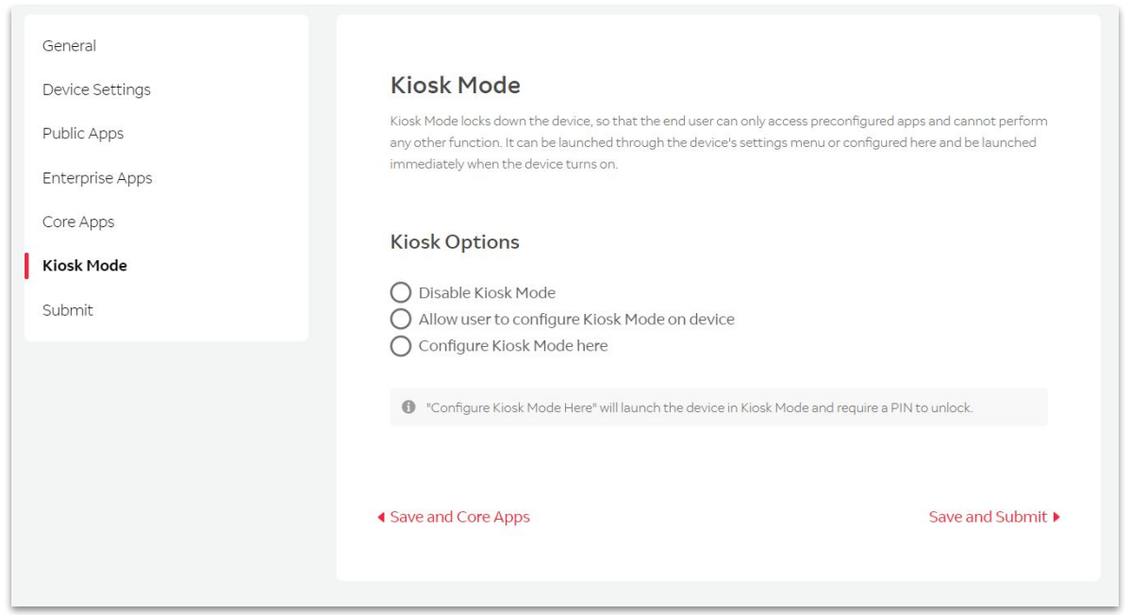
KIOSK MODE

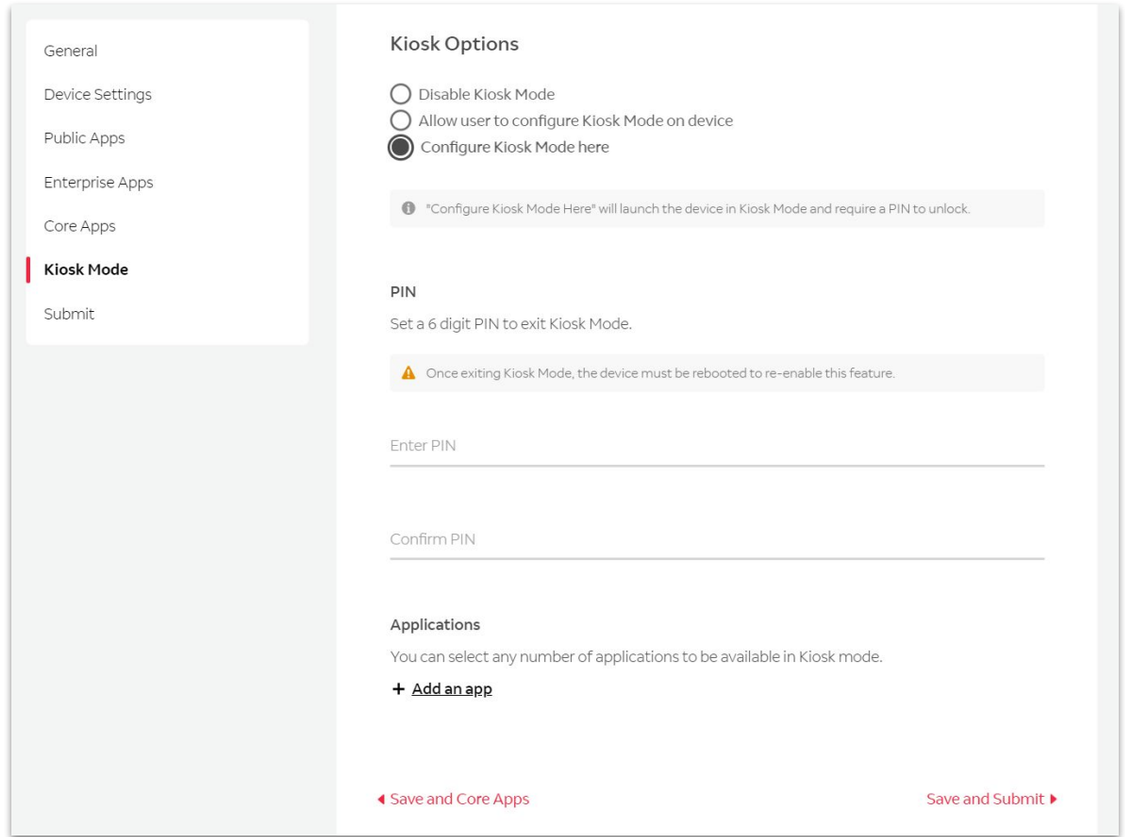
Some organizations require the ability to secure their Magic Leap devices to only allow select applications to be used.

The Device Manager provides this capability using Kiosk mode. Kiosk mode options are:

- Disable Kiosk Mode
- Allow user to configure Kiosk Mode on device
- Configure Kiosk Mode here

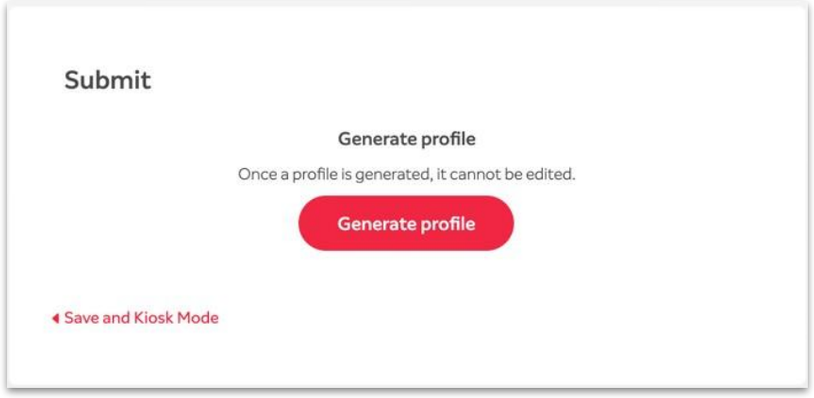
To pre-configure Kiosk Mode for multiple apps, select ‘Configure Kiosk Mode here’, set the **pin** , click **+Add an app** and select app from the drop down menu. Repeat to add more apps.





PROFILES:

CREATE PROFILE–GENERATE PROFILE



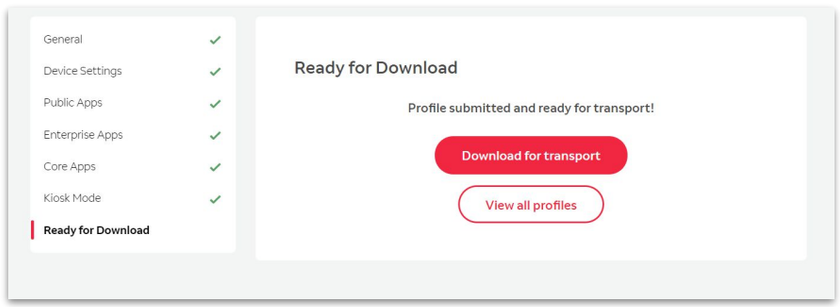
SUBMIT

- **Generate Profile**
  Once you have configured the profile with all of your system requirements, click Generate Profile to create the downloadable key and profile packages.

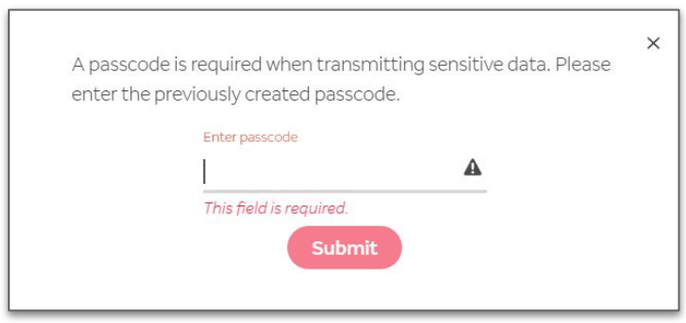
  On the Submit page, click on **Generate Profile**

READY FOR DOWNLOAD

- **Download for transport**
  Once Generate Profile is complete, you will now see a **Download for transport** option. Please click Download for transport.

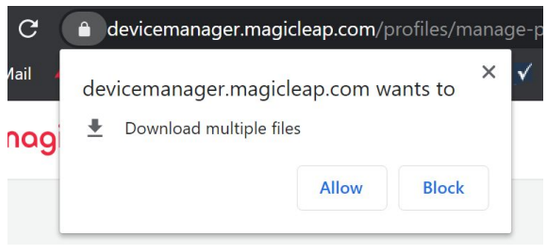


- If you are using wifi certificates and your certificate had a security password when initially uploading to Device Manager>Certificates, you will be required to enter that here as well.



This downloads two files, **profile.zip** and **key**. Document where these files are located or move them to a folder more easily accessible.

Please note you may see a pop up when downloading the second file asking you to allow multiple downloads. Please click “Allow”.



magic leap

PROVISIONING:

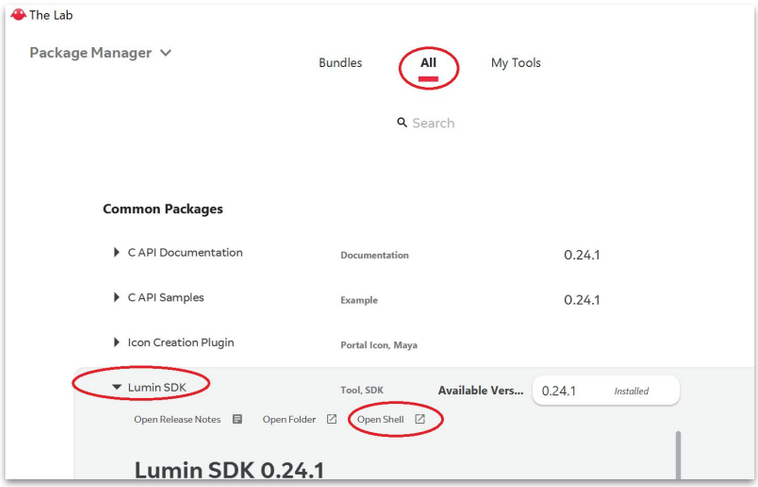
INSTALL FIRST PROFILE ON DEVICE

Profiles can be applied to devices using two different methods, **side loading** or **remote**. Neither method will erase currently installed applications, user information or login status. **The very first profile will require the use of side loading to install the profile**. After the first profile is loaded, all subsequent profile updates can be sent via either method. When a profile is installed, it will require the device to be rebooted for the profile to take effect.

The following pages will detail the two methods and how to apply the profiles to devices.

Before you begin, you will need the following items:

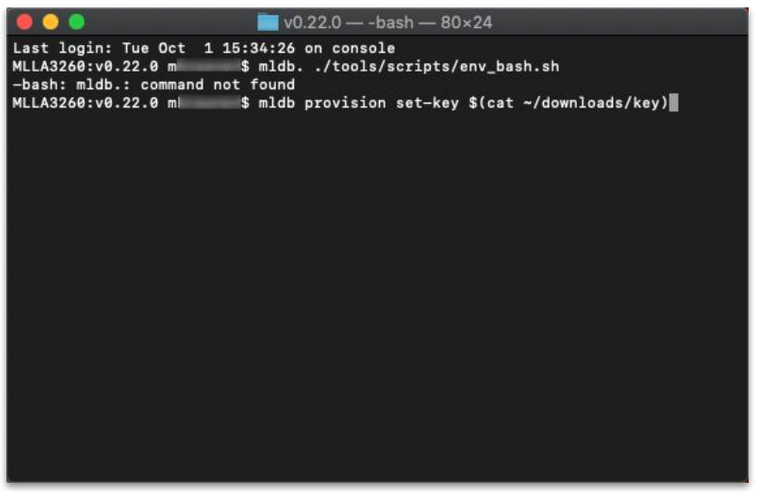
- A computer with an internet connection.
- A copy of Magic Leap's app the Lab installed on your computer
- A Magic Leap device fresh from the factory or one that has been factory reset.
  Note: Do not start the setup of your device, just power it on.
- A USB-C to USB connector (only if you don't have a USB-C port)
- The desired **profile** and **key** downloaded from the Device Manager.



INSTALL PROFILE via SIDE LOADING

First time installation of profiles must be done by side loading. Devices being provisioned must not have gone through on-device setup. This means the device is brand new and never used or that the device has been factory reset.

- Open the Lab and on the top right click on package manager
- Click on All and under common packages, click on Lumin SDK
- Click on Open Shell
- Connect the device to your computer using the USB-C cable (and adapter if you don't have a USB-C port on your computer.
- Run the commands to install the key and profile.zip file downloaded from Device Manager (see next page for install commands)



magic leap

PROVISIONING:

INSTALL FIRST PROFILE ON DEVICE

Install Key and Profile [Windows]

- **Install Key**: The example below shows how to install the decryption **key** for installation. For this example, please **ensure the key you downloaded from device manger is in the downloads folder of your computer.**

```
c:\...> set /p key=<%HOMEPATH%\Downloads\key
c:\...> mldb provision set-key %key%
```

- **Install Profile.zip:** The example below shows how to install the profile.zip file using the MLDB command. For this example, please **ensure the profile.zip file you downloaded from device manger is in the downloads folder of your computer.** You do NOT need to unzip the profile folder.

```
c:\...> mldb provision install %HOMEPATH%\Downloads\profile.zip
Profile installation successful. The profile will be active after  reboot.
```

Install Key and Profile [MAC]

- **Install Key & Profile.zip**: The example below shows how to install the **key** and **profile.zip** file on either a Mac or Linux computer. Again, for this example, we use full paths and assume the key and profile.zip files are in the users Downloads folder.

```
$ mldb provision set-key $(cat ~/Downloads/key)
$ mldb provision install ~/Downloads/profile.zip
Profile installation successful. The profile will be active after reboot.
```

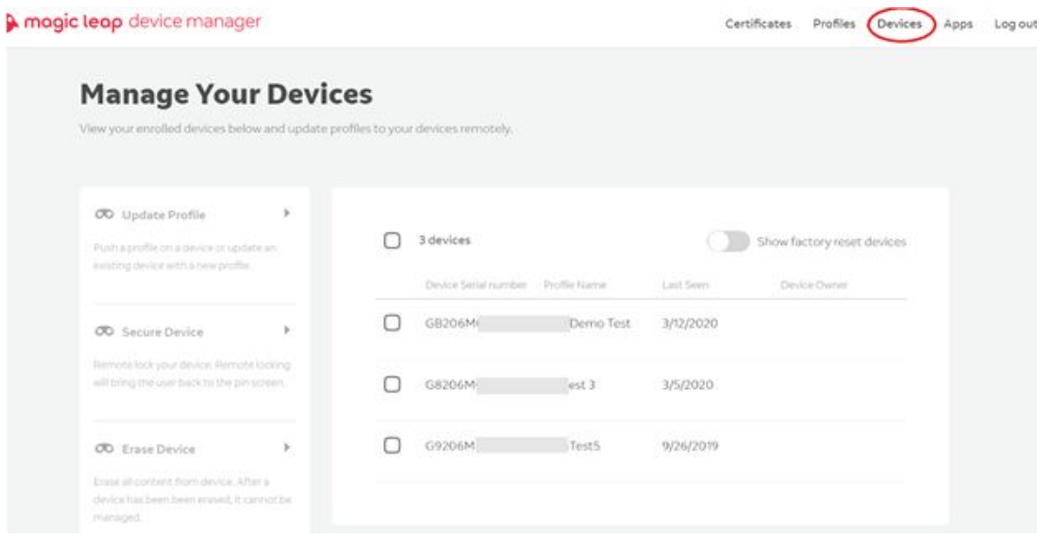
Verify Profile installed correctly (optional)

```
mldb provision show current
```

magic leap

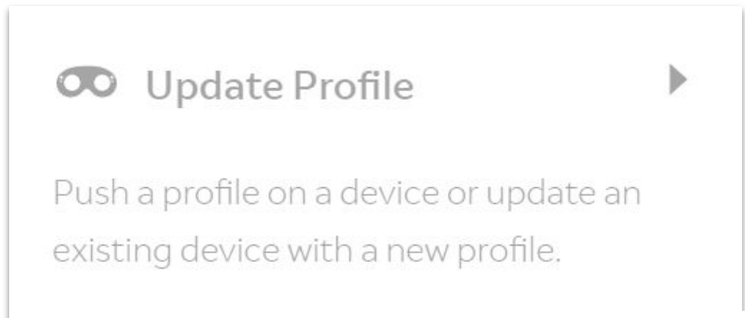
DEVICES:

MANAGE DEVICES-UPDATE PROFILE



Remote Management

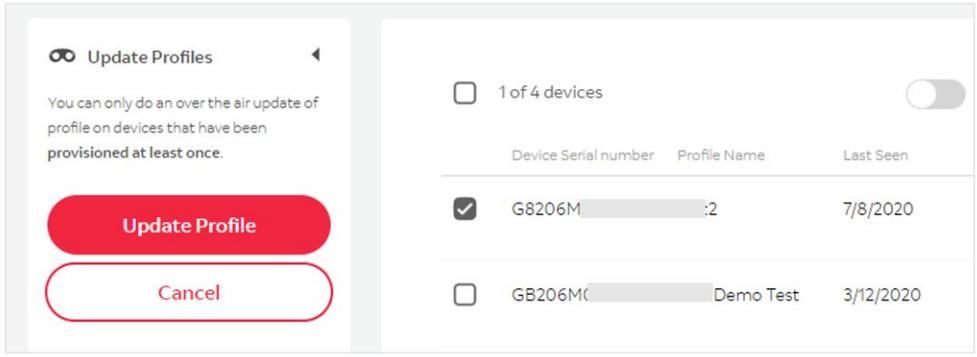
Enterprise administrators can view devices they own and manage them remotely.

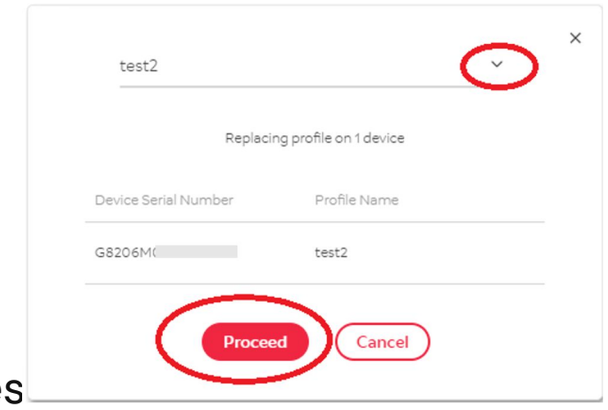


Update Profile Remotely via WiFi

Device Manager Admins can change profiles on select devices by pushing the profile via WiFi. This method will require the device to be connected to the internet for proper deployment of the profile.

- Click on Devices in the header
- Click on the serial number(s) you want to update
- Click Update Profiles from the left hand menu
- Click the red Update Profile button
- Choose the profile you wish to install and click proceed





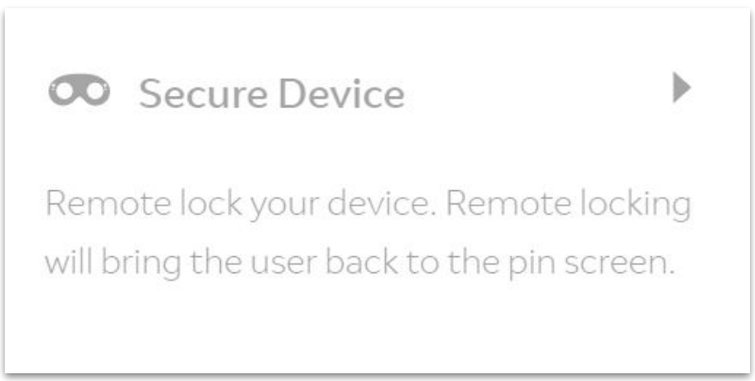
The changes will take effect upon the next device reboot. If the device is not online during the profile update request, it will occur when the device next comes online.

Note: Only devices provisioned and managed via the Device Manager can have profiles applied remotely from within Device Manager.

magic leap

DEVICES:

MANAGE DEVICES–SECURE or ERASE



Secure Device (Remote Lock)

Enterprise administrators can remotely lock a device using Device Manager. This is useful when a device has fallen into the wrong hands and the administrator wants to force the device back to the pin screen. The device user would then be required to enter the pin of the logged in user to unlock the device.

- under Devices, select the device(s) you want to lock
- select Secure Device from the left hand menu.
- select Lock Device and click confirm

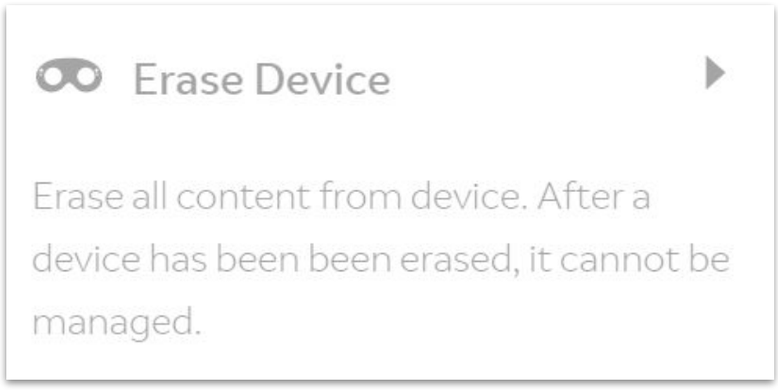
If the device is not online during the lock request, it will occur when the device next comes back online.

Erase Device (Remotely Wipe)

Enterprise administrators can remotely wipe a device using Device Manager. This will remove the existing logged in user as well as remove any user data and provisioning information. The device will need to be provisioned again to be placed back into a managed state.

- under Devices, select the device(s) you want to erase
- click Erase Devices from the left hand menu.
- click the Erase device button and click confirm

If the device is not online during the erase request, it will occur when the device next comes online.



magic leap

APPS:

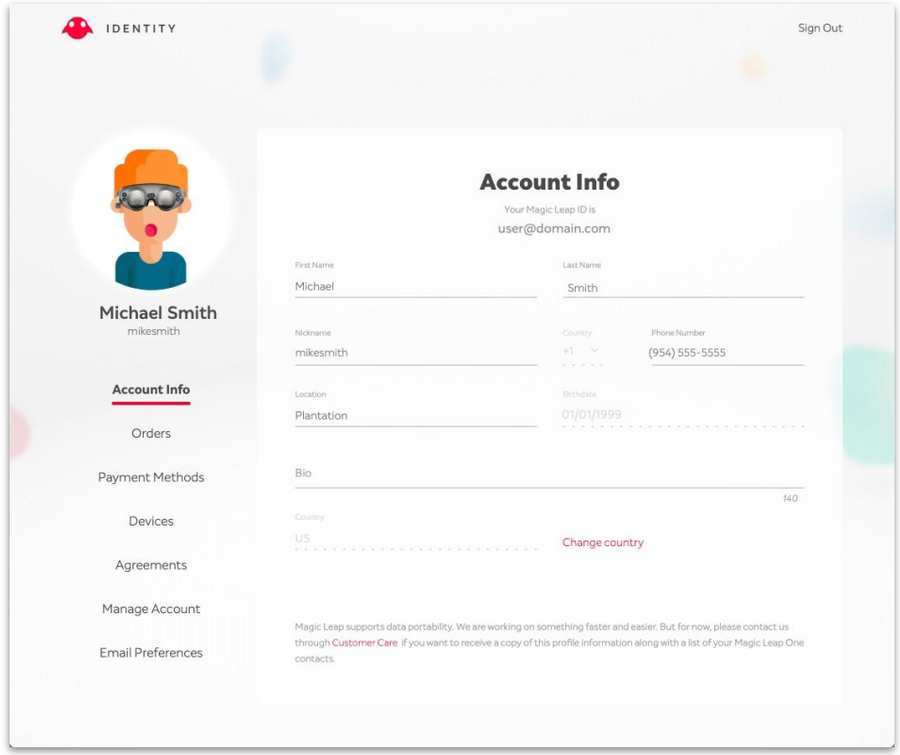
OVERVIEW

Enterprises are able to manage any application that they are entitled to use. Enterprises can develop their own applications and distribute them to their users or purchase applications from third-party developers for use.

Note: At this time, Magic Leap World does not support application subscriptions or the sale of applications outside of its app store.

Magic Leap ID (MLID) Account

If allowing for access to the Magic Leap World app store, users will need to set their Home Country within the Magic Leap Identity portal. For more information, click here.



Creating an Application

To create a custom application as an enterprise, follow the instructions on becoming a developer. Application creation and submission does not change when creating an application for an enterprise. Applications can be submitted as either public or private and both are subject to the normal rules of application submission and approval.

Linking an Application

Once an app has been published on the Developer Portal, the developer can invite the enterprise to use their app using the Enterprise app sharing section of their publisher account.

Important Requirements:

- Apps intended for distribution within an enterprise must be **Published** in Developer Portal.
- Enterprise codes entered for Apps in a **Draft** state will not trigger an email back to the Enterprise to confirm the app link for acceptance.
- Enterprise codes should be entered in the Developer Portal after being published in a Private app mode.

magic leap

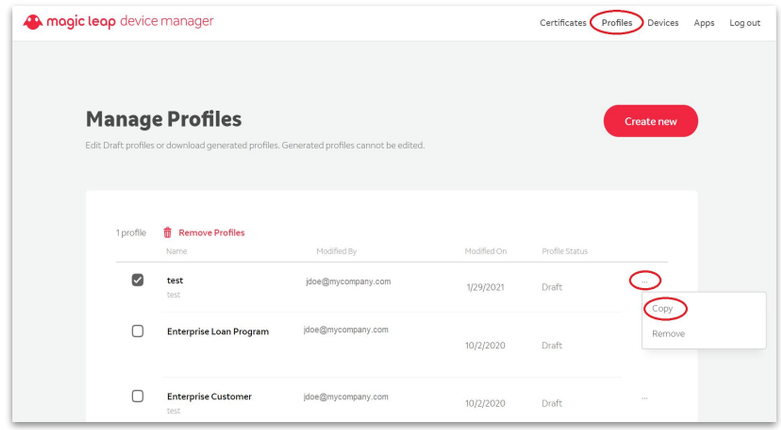
APPS:

INSTALLING APPS – REMOTELY

INSTALLING an APP REMOTELY at the PROFILE LEVEL

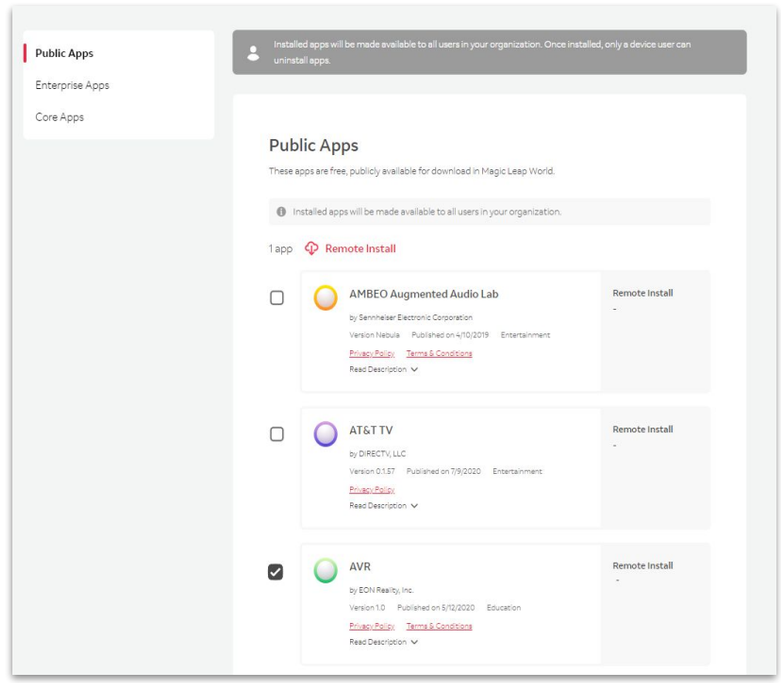
Enterprise Device Manager Admins may wish to install Apps for specific users only. To do this you must create a new profile and push it to those device only;

- Under profiles, **copy** the existing profile and rename it (ex Demo v2) or you may also create a brand new profile
- Select the app from the within the appropriate App section
- Submit
- Follow the steps previously outlined to update profile remotely via wifi



INSTALLING an APP REMOTELY at the ORGANIZATION LEVEL

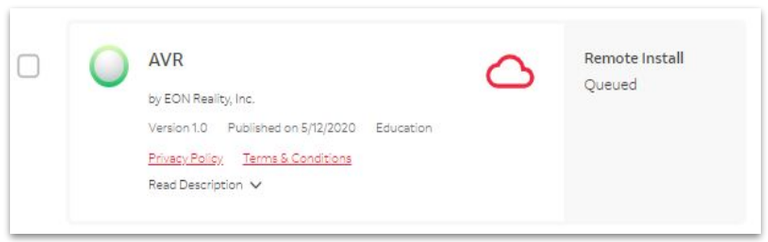
Enterprise Device Manager Admins may choose to install Apps at the organization level instead of at the profile level. The admin can push applications to all of the devices listed under Devices.



- In the APPS section, select the App to install with your entire org
- Click on Remote Install

Note: Once an App is shared at the Org level, it cannot be unshared

These applications will be installed on all managed devices once the device is online. If a device is turned off or not connected to the internet, the application will be installed once the connection has been established. Any new device that is provisioned will also receive the applications that have been queued for installation.



Apps shared at the Org level are denoted with a cloud icon

magic leap

APPS:

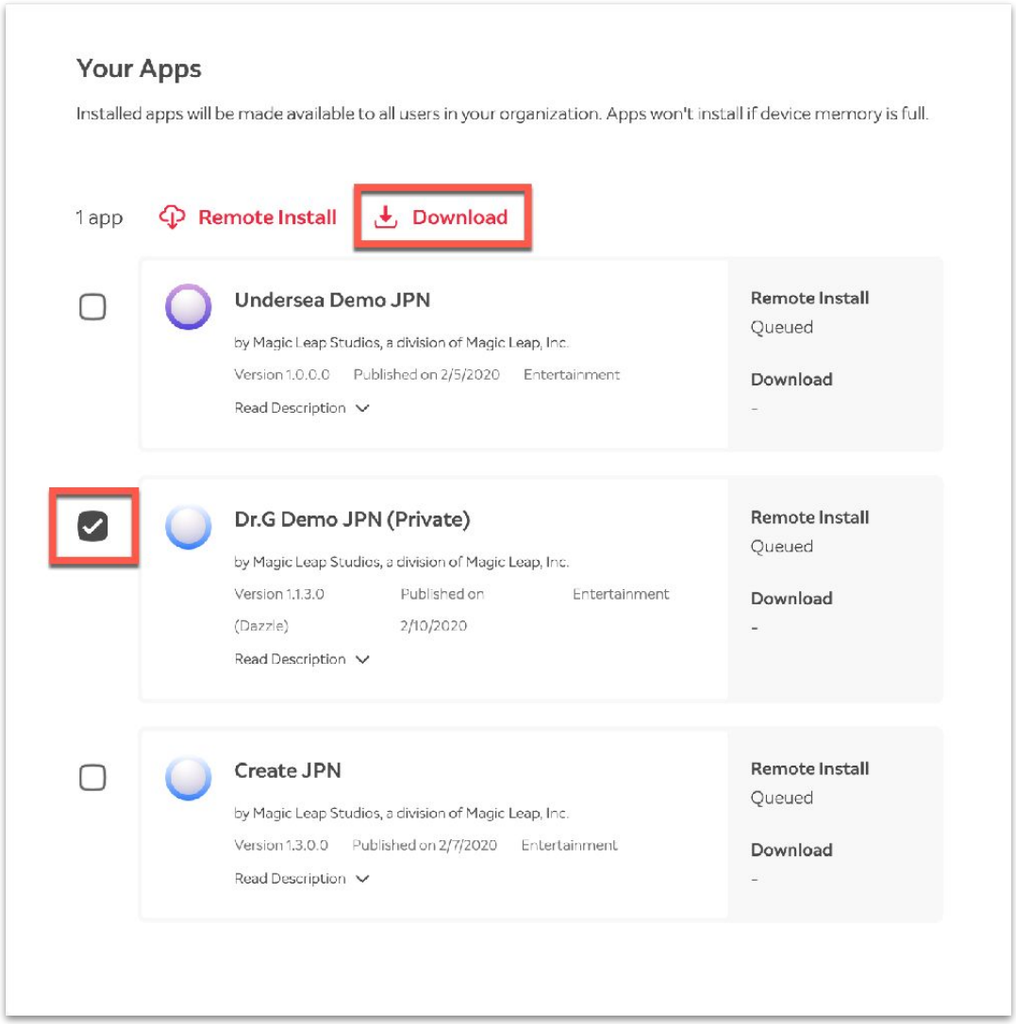
INSTALLING APPS – SIDE LOADING

INSTALLING an APP via SIDE LOADING
In some cases, enterprises will want to install or update an application on their devices while the device is not connected to the internet. In these cases, the administrator can download the application from Device Manager. The application can only be installed on existing managed devices within your enterprise.

It may **NOT** be installed on devices that have not been previously provisioned. The downloaded package is secured via encryption that only devices belonging to that enterprise may decrypt the install packages.

Within Enterprise Device Manager

- Navigate to the Enterprise Apps page.
- Select the apps you wish to download by selecting the checkbox to the left.
- Click on Download, just above the app list, to retrieve the MPK file.



magic leap

APPS:

INSTALLING APPS–SIDE LOADING

To install the Enterprise apps via our Enterprise Managed Side Loading process, you will need to leverage our MLDB protocols located within the Package Manager within the Lab.

To download the Lab, you can visit the Developer Portal Downloads page to download and install.

Installing an Enterprise Application via Side Loading (MLDB)
If you have the .mpk file from the developer, you can install it by side loading utilizing MLDB commands:

- open up the Lab and launch Package Manager in the upper right hand corner.
- open the Shell and enter the following commands with the device on and plugged into the computer:

Command	Description
mldb devices	Displays list of devices
mldb install {AppName}.mpk	For MLDB enabled devices – new app
mldb einstall {AppName}.mpk	For MLDB NOT enabled devices – new app
mldb install [-u] {AppName}.mpk	For MLDB enabled devices – update app
mldb einstall [-u] {AppName}.mpk	For MLDB NOT enabled devices – update app

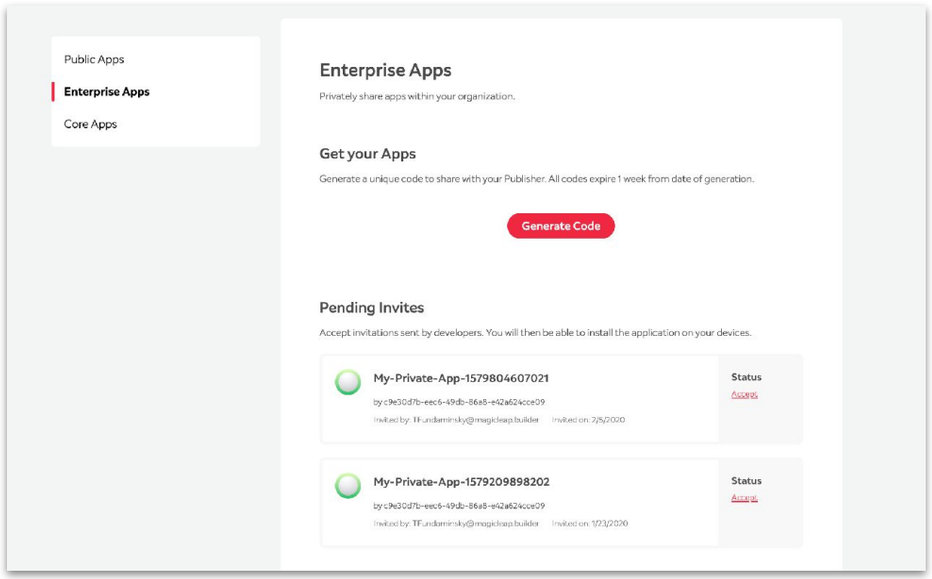
Note: *<mpk-file> is the name of the installable application and is either the full path to that file or the name of the file located in the SDK directory.*

magic leap

APPS:

INSTALLING APPS–ENTERPRISE APP SHARING

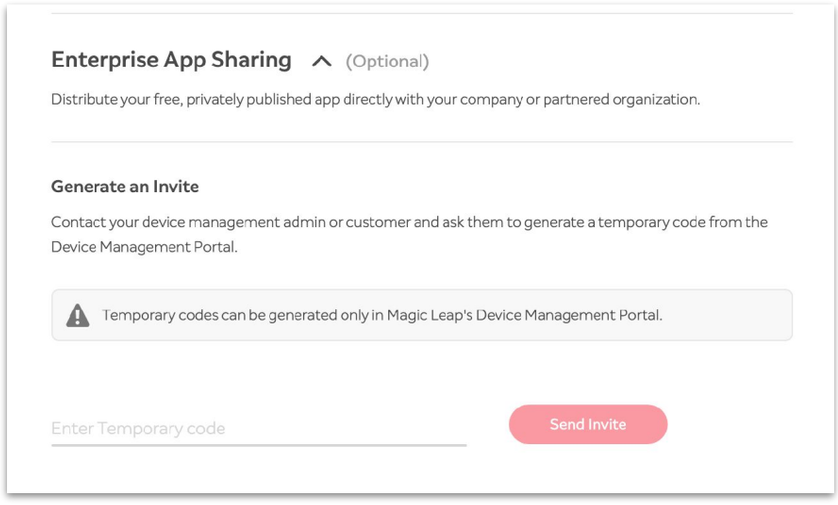
Instead of side loading, Enterprise apps may be shared directly with your company so you can in turn share them with your employees. To get the enterprise app, the developer must share their app with your organization via their publishing account on the Developer Portal.



Getting an Enterprise Application

1. Enterprise Device Manager Customers can click **Generate Code** to generate a unique code in the Enterprise Apps section of Device Manager and share it directly with the developer (via your preferred method of sharing: ex. email)

2. The developer, enters this code in the Enterprise App Sharing section of their publishing account of the Developer Portal and clicks send invite. **Note**: the Enterprise App Sharing section is disabled by default. To enable it, the developer must submit a request to care@magicleap.com



3. Device Manager Admins will receive an email inviting them to accept the app being shared. You will also now receive a notification of “Pending Invites” within the Device Manager Enterprise Apps page.

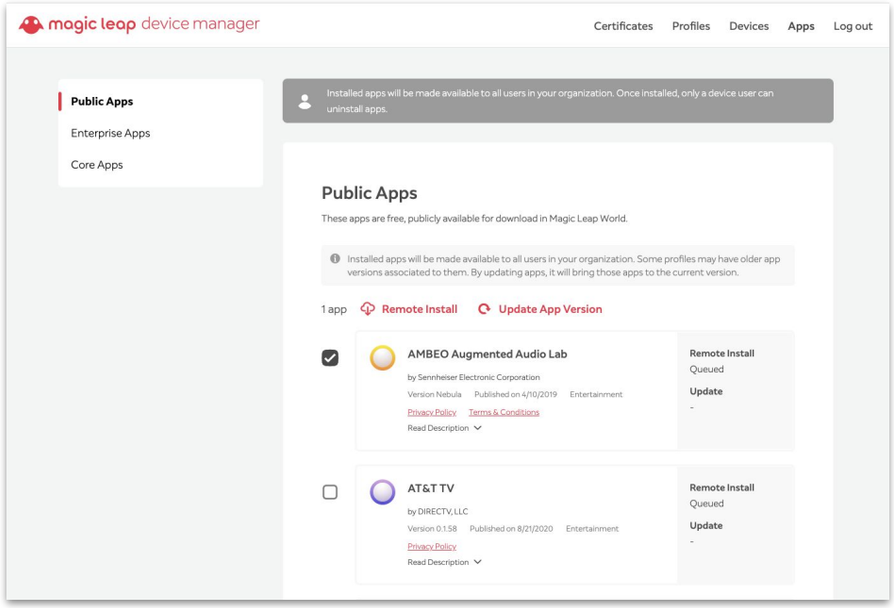
APPS:

UPDATING APP VERSIONS

When a profile is linked to a set of apps, it is linked to specific versions of those apps. When new versions of an app are published, it can leave profiles outdated.

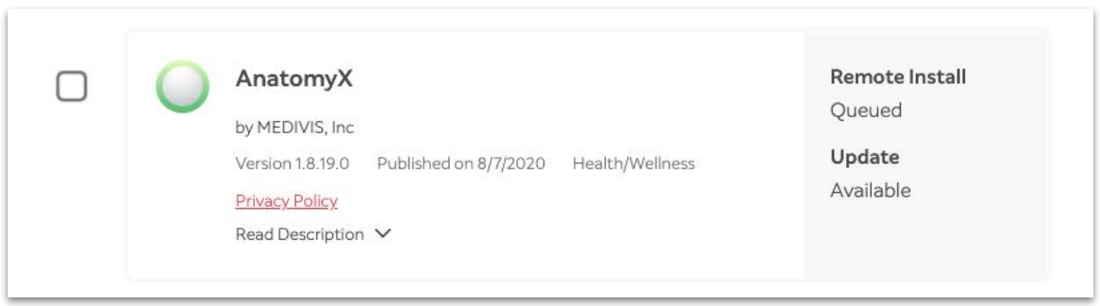
Updating App Versions Across Profiles

1. Enterprise Device Manager Customers can go to the “Apps” tab in the top navigation menu, select one or more apps, and click the red “Update App Version” button.



There is an indicator on the right of each app that shows if there is an update available for that app, however updating an up-to-date application is harmless.

Note: Devices running a profile with an outdated app version will not receive app updates until the device is rebooted.

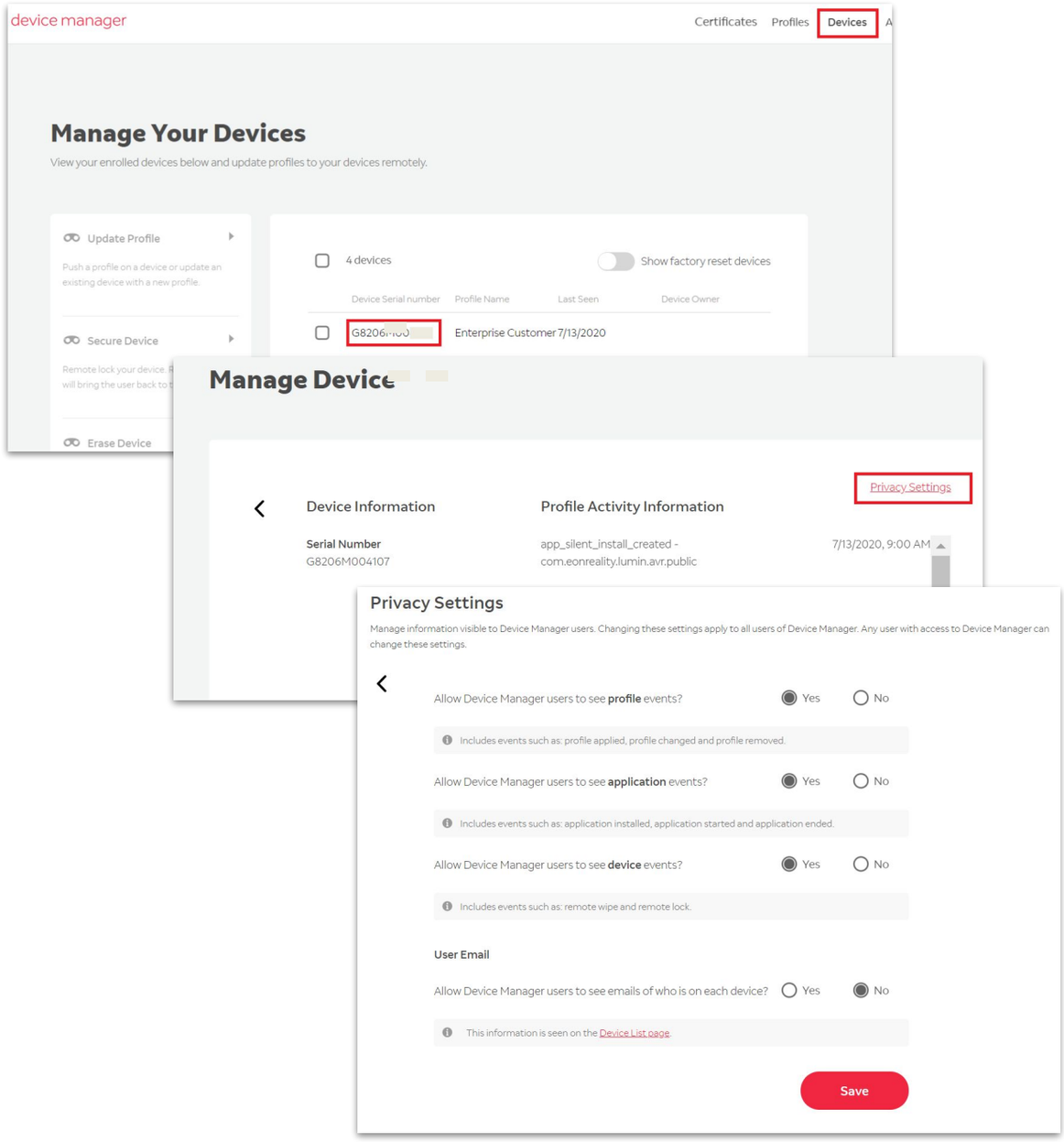


magic leap

MANAGING PRIVACY SETTINGS

Device Manager provides the ability to manage the visibility of Device Events and User Emails associated with all managed Magic Leap devices. To change these settings, you can visit the **Devices page, click any serial number, and then click privacy settings.**

Note: Changing these settings will affect all users. In addition, any user who has access to Device Manager can turn these settings on or off.



DEVICE EVENTS

- Allow Device Manager users to see profile events? **(Choose Yes/No)**
  (Includes events such as: profile applied, profile changed and profile removed)
- Allow Device Manager users to see application events? **(Choose Yes/No)**
  (Includes events such as: application installed, application started and application ended
- Allow Device Manager users to see device events? **(Choose Yes/No)**
  (Includes events such as: remote wipe and remote lock)

USER EMAIL

- Allow Device Manager users to see emails of who is on each device? **(Choose Yes/No)**
  (This information is seen on the Device List page.)

magic leap

DEFINITIONS

TERM	DEFINITION
Cloud Processing	Cloud Processing enables cloud storage of spatial maps created from your device rather than relying solely on maps stored on your device.
Kiosk Mode	Kiosk mode puts a Magic Leap device in a restricted mode where users can only use the apps allowed by the profile.
MLDB (Magic Leap Device Bridge)	Command line language to gather information about devices and deliver profiles
OKTA	Identity management solution used to authenticate users into Device Manager
OOBE (Out of Box Experience)	The initial setup of a device that is used when Device Manager is not in use on a device.
Provisioning Profile	Contains settings that allow the device to be configured with preset values to customize the device to fit their business needs.
Side Loading	To physically connect your Magic Leap device to a computer and install an app or profile directly to the device via MLDB
Silent App Installation	silent App Install allows you to push apps to your devices behind the scenes, without requiring any actions from the user. It can be pushed at once to the entire fleet of devices (INSTALLING an APP REMOTELY at the ORGANIZATION LEVEL), or it can be narrowed down to just a set of devices which have a particular profile (INSTALLING an APP REMOTELY at the PROFILE LEVEL)
World Understanding	World Understanding lets Magic Leap devices recognize certain objects. Requirements: internet connection and Shared World enabled (Settings > Spatial Mapping)

ENTERPRISE SUPPORT

WEB
magicleap.com/support

EMAIL
enterprisecare@magicleap.com

HOURS
see magicleap.com/contactus