Table of Contents:

Configuring CDM Policy
- Standard CDM Configuration
- Configuring USB Device Whitelisting

AgentM for Windows
- Installing AgentM for Windows
- Updating AgentM for Windows
- Configuring Peripheral devices for AgentM on Windows

AgentM for Ubuntu Linux
- Installing AgentM for Ubuntu Linux
- Updating AgentM for Ubuntu Linux

Configuring CDM integration (optional)

Claiming your device

Dashboard
- Landing Page
- Creating Schedules
- Creating a URL Application
- Creating a Google Slide Application
- Creating a Packaged Application

Device
- Changing Device Name
- Setting Operating Schedule
- Setting Reboot Schedule
- Manually Rebooting
- Installing Application
- Configuring Displays
- Configuring Display Schedule
- Configuring Display Options
- Configuring Device Options
- Viewing Device Logs
- Viewing Device Health
- Capturing Screenshots
- Reading Device Properties
- Removing a Device

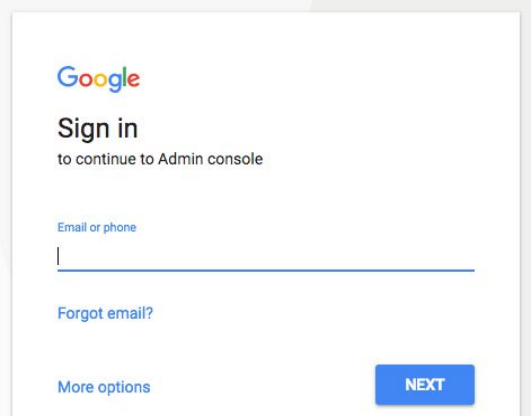
Secure Browser Mode

Troubleshooting MeldCX

Configuring CDM Policy

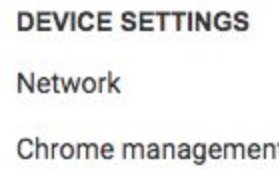
Standard CDM Configuration

1. Sign in to the Google admin console located at https://admin.google.com/

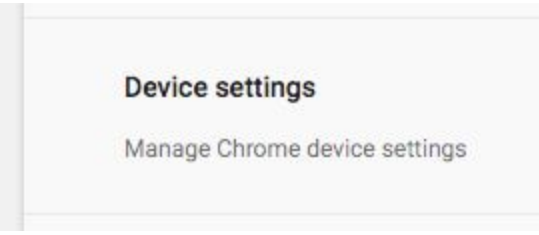


2. On the landing page *click* Device Management

3. From the Device Management page click *Chrome management*

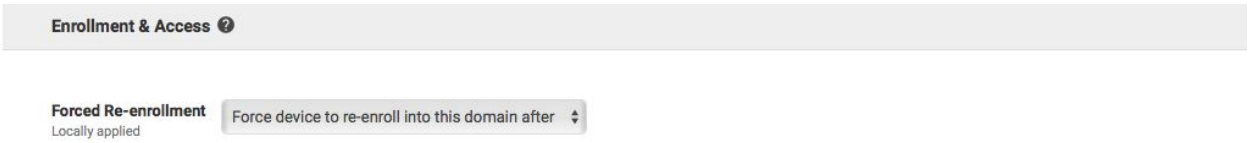


4. From the Menu select *Device settings*



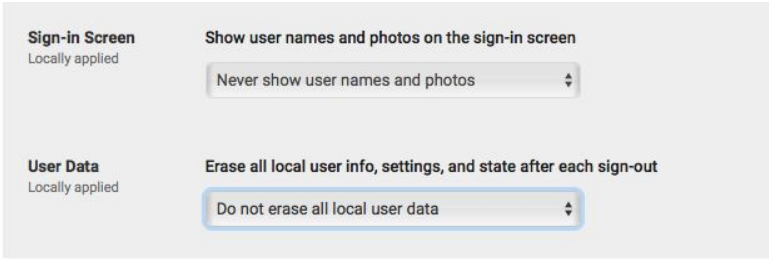
5. Select the OU that your device resides in and that you would like to apply the MeldCX configuration to.

6. From the displayed options, ensure the following settings are configured accordingly:
7. **Forced Re-enrollment:** Force device to re-enroll into this domain...

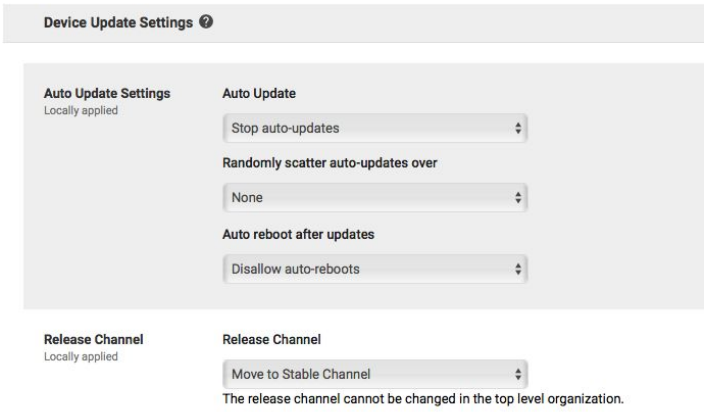


8. **Guest Mode:** Do not allow Guest Mode
9. **Sign-in Restriction:** Do not allow any user to Sign-in

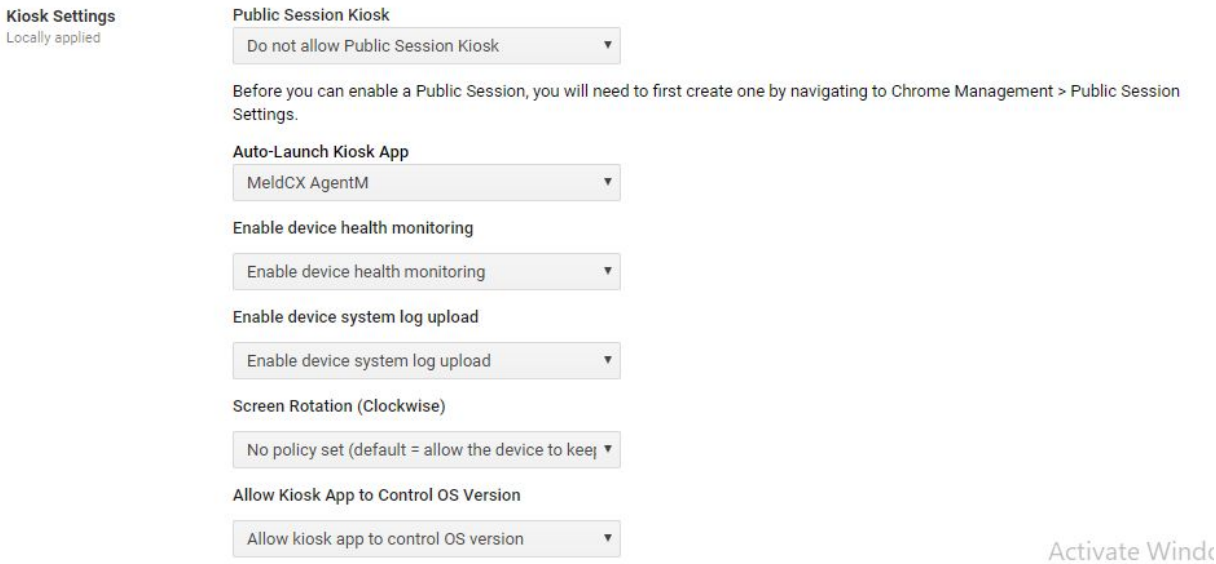
10. **Sign-in Screen:** Never show user names and photos
11. **User Data:** Do not erase all user data



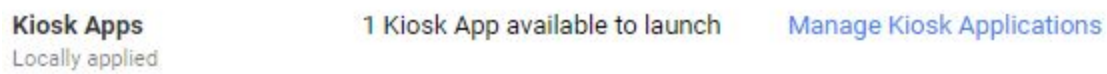
12. **Accessibility Control:** (Ensure checked) Turn off accessibility settings on sign-in screen upon logout
13. **Auto Update Settings:** Stop auto-updates
14. **Auto reboot after updates:** Disallow auto-reboots
15. **Release Channel:** Move to Stable Channel



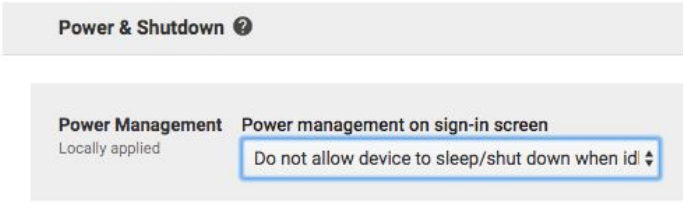
16. **Kiosk Settings:** Do not allow public session kiosk
17. **Auto-Launch Kiosk App:** agentM



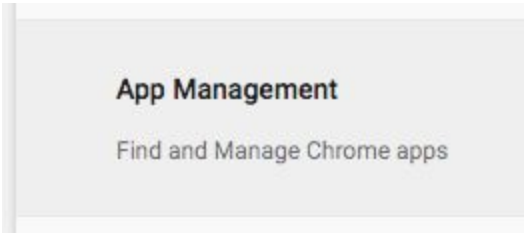
18. **Note:** Please use the chrome webstore link you are provided at time of sign up.
19. **Kiosk App:**
20. *Click* Manage Kiosk Applications



21. *Click* Specify a Custom App
22. Enter the *URL* provided (if you do not have this please email help@meldcx.com)
23. Enter the *ID* provided (this is the random code shown in the URL)
24. *Click* Save
25. **Device Reporting:** Enable device state reporting
26. **Power Management:** Do not allow device to sleep/shutdown when idle….

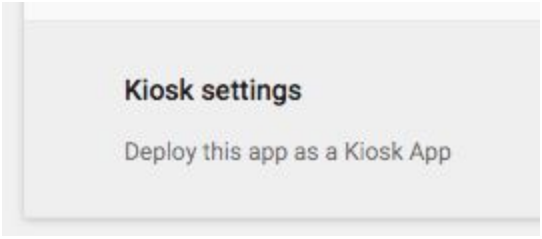


27. Navigate back to the Chrome Management page:
28. *Click* on App Management

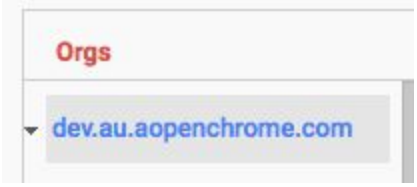


29. *Select* the Kiosk app we provided to you

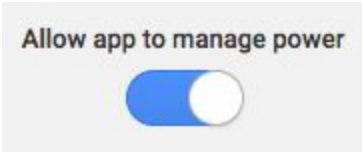
30. *Click* on Kiosk Settings



31. *Select* the Root OU



32. Ensure **Allow app to manage power** is switched on:

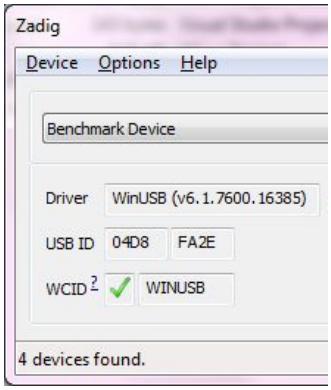


Configuring USB Device Whitelisting

1. Plug in the Device to your computer:

On **Windows**:

a. Use Zadig (found here http://zadig.akeo.ie/) to obtain the USB ID (VID & PID) of the device.



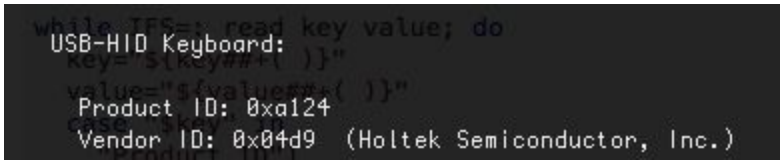
On **MacOS:**

a. Open terminal and type: system_profiler SPUSBDataType

b. Locate the device in the list

c. The VID will be listed next to Vendor ID

d. The PID will be listed next to Product ID

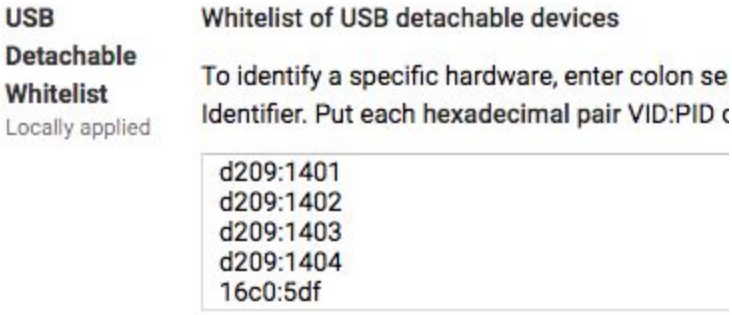


2. Login to your **CDM** account at https://admin.google.com/

Note: If you are using Managed CDM this will need to be done on your behalf.

3. Click **Device Management**
4. Click **Chrome Management**
5. Click **Device settings**
6. Select the Root Organisational Unit

7. Locate the "*USB Detachable Whitelist*"



8. Enter the USB ID you obtained in step 1 into a newline in the text area.
9. Click **Save**
10. Ensure the target device is online and enrolled.
11. It will take up to 15 minutes for the device to receive the updated policy
12. Reboot the device and it should be able to communicate with the USB device

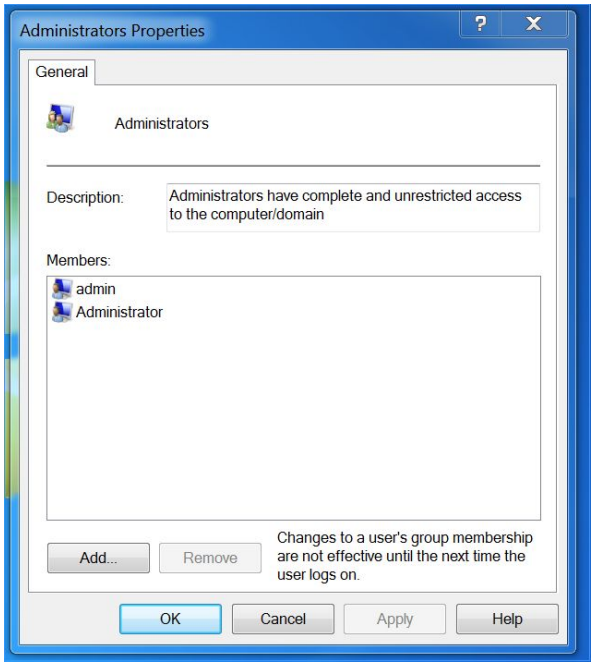
AgentM for Windows

Installing AgentM for Windows

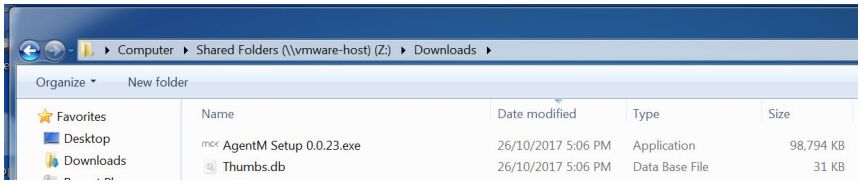
MeldCX AgentM works on any x86 64bit Windows version starting with Windows 7 and up.

1. Using the installer provided. Sign in to the Windows device you want to install AgentM onto.

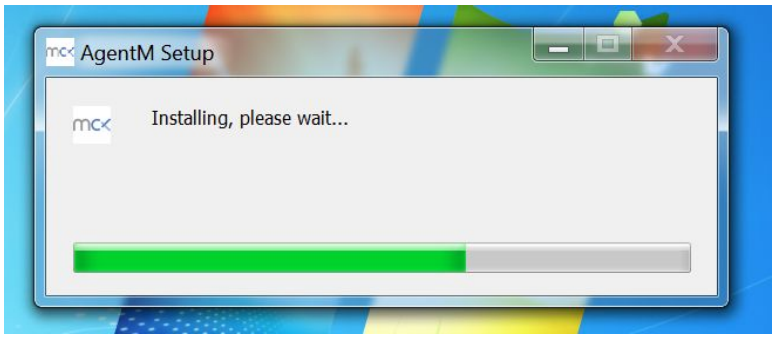
2. Ensure that the user you are signed in as has permission to install applications.



3. Open the AgentM Setup.exe file



4. AgentM will install.



5. Once the install has completed AgentM will open.

6. From there you can register and use AgentM the same as you would AgentM on chromeOS, see here.

Updating AgentM for Windows

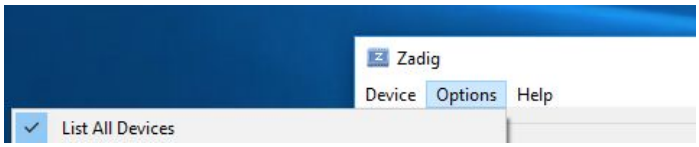
AgentM keeps itself up to date by periodically checking our cloud servers for the latest version of AgentM, if it finds a newer version it will download and install the Agent automatically.

Configuring Peripheral devices for AgentM on Windows

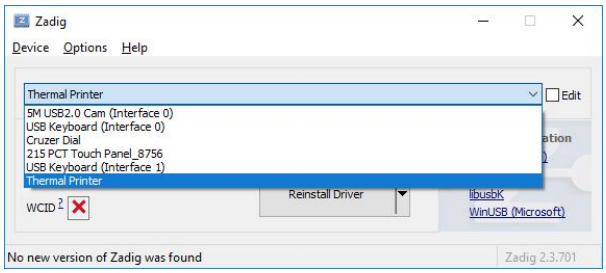
Note:
This process replaces any installed or default os device specific drivers with a standard “libusb” driver.

This is only required for devices support by MeldCX, please confirm with us prior to making any permanent changes to your OS instance if you are unsure, as these changes might not be reversible.

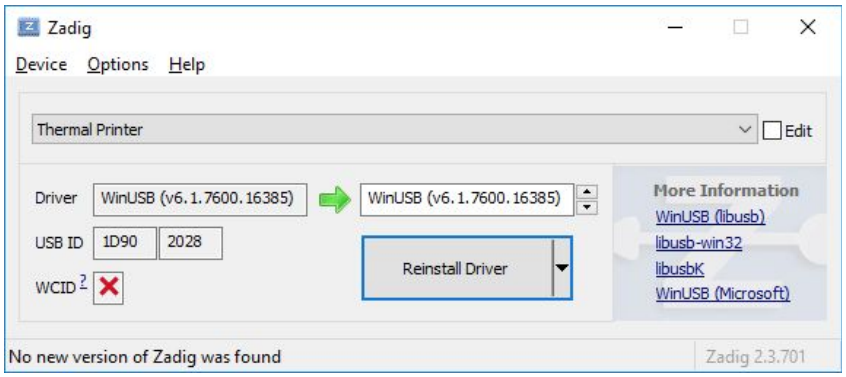
1. Download zadig which can be found here: http://zadig.akeo.ie
2. Once downloaded run zadig.exe
3. From the menu bar click options
4. Click list all devices



5. From the drop down list choose the device you want to use



6. Once you have selected the target device Click Replace Driver



7. Your peripheral device should now be ready for use with AgentM

AgentM for Ubuntu Linux

Installing AgentM for Ubuntu Linux

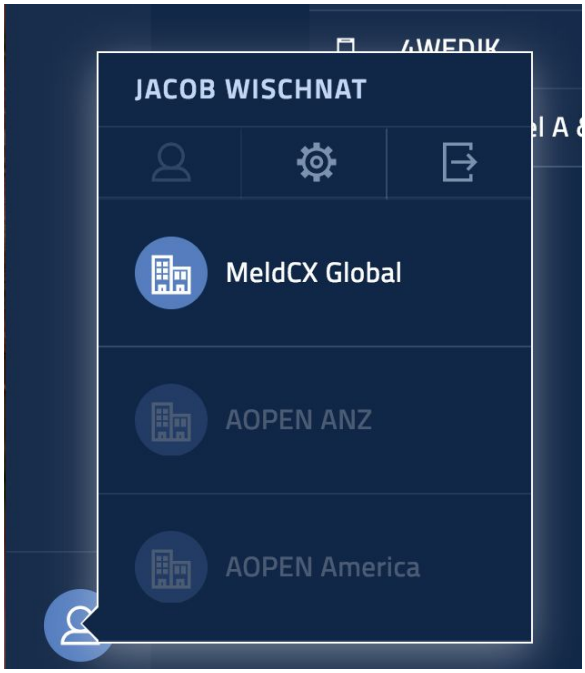
Updating AgentM for Ubuntu Linux

AgentM keeps itself up to date by periodically checking our cloud servers for the latest version of AgentM, if it finds a newer version it will download and install the Agent automatically.

Configuring CDM integration (optional)

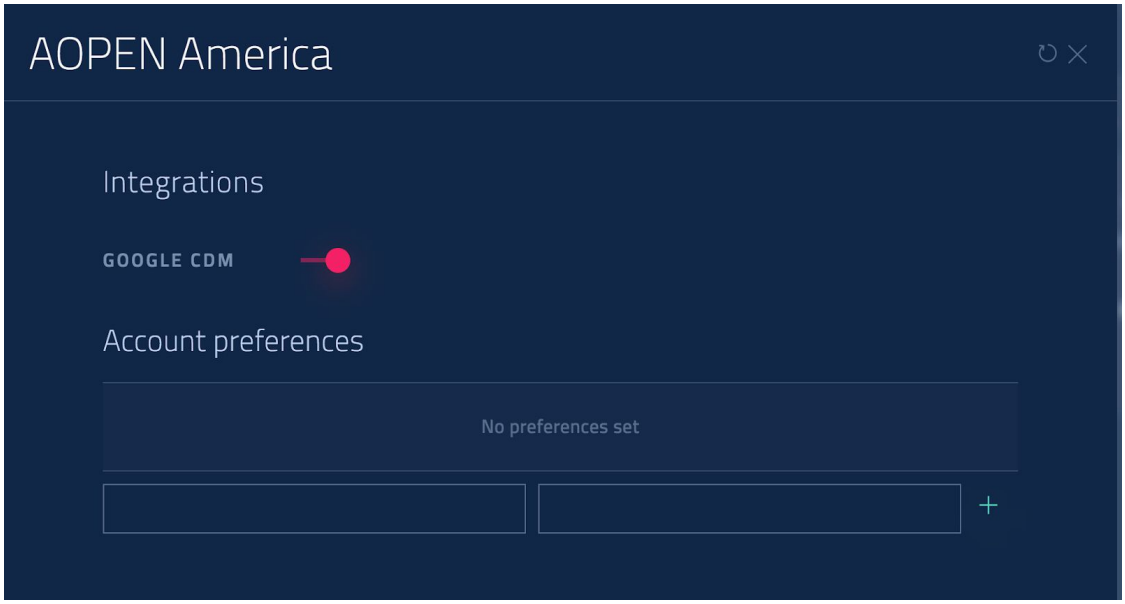
It is possible to configure CDM integration to automate device claiming process (see Claiming your device), view how many active/disabled/deprovisioned devices you have, view additional device properties (like serial number, asset ID, model etc.) and deprovision/disable/re-enable device directly from MeldCX. You can skip this step if you don't need this type of automation.

1. Login to your account in MeldCX
2. Open **User menu** (bottom left corner)



3. Click **Account Settings**

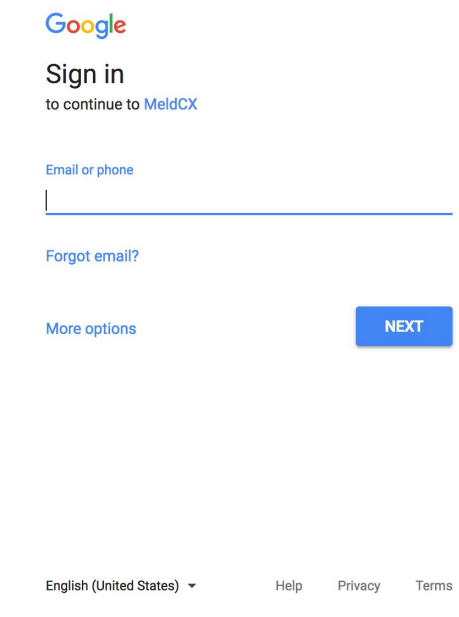
4. You should be able to see the following window.



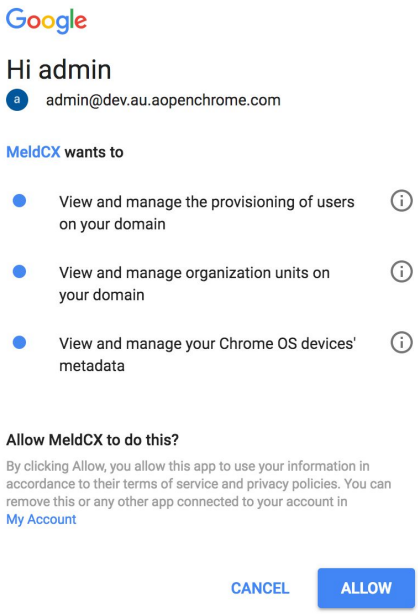
5. Enable CDM integration

by clicking on switch

6. You should be asked for your Google Admin account credentials in the popup window. Please, note that popup windows should be enabled in your browser for https://admin.meld.cx

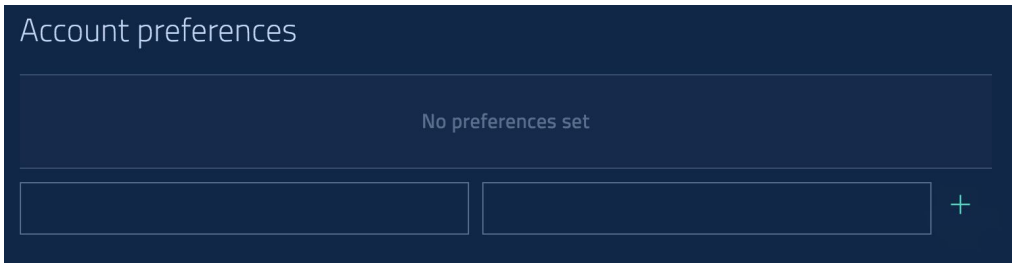


7. Provide your Google Admin account credentials and click **Next**
   You will need to give your consent to MeldCX for using CDM API



8. If everything is OK, you should be able to see the total number of active/disabled/deprovisioned devices in your account

9. You should also configure **OrgUnitPath** account preference if you wish to automate device claiming process and enable better device integration. By default you will see the empty list of the **Account preferences**



10. Enter **OrgUnitPath** in the first field and the **organization unit path** in the second field

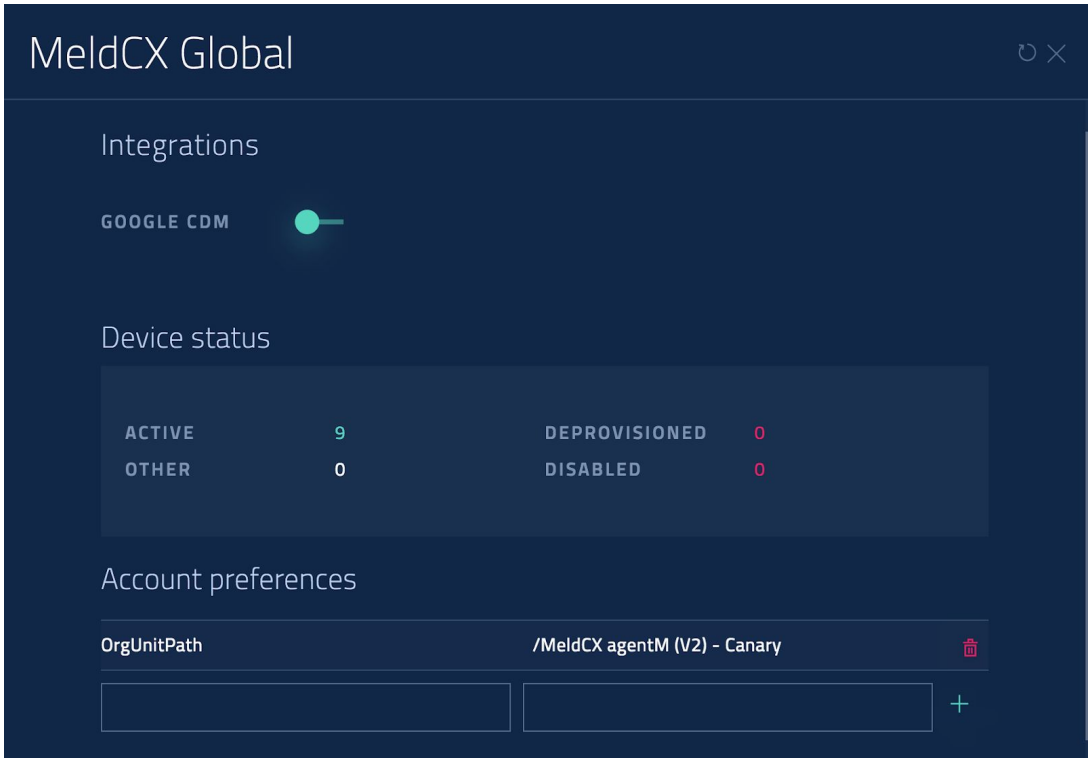
You can find the **organization unit path** in your Google CDM account. By default all the devices in the selected organization unit and in the units down the hierarchy will be synchronized into your MeldCX account. You can use symbol **/** to indicate that you want to synchronize entire hierarchy.

11. Click **Add** button to add **OrgUnitPath** to the list of account preferences

12. You can setup more than one organization unit by using **OrgUnitPath1, OrgUnitPath2,** etc**…**

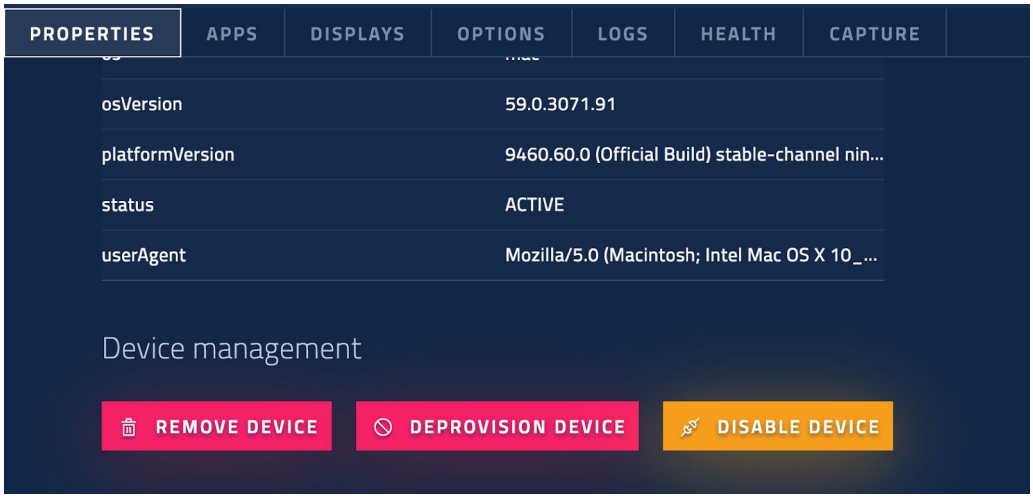
13. It is also possible to exclude the child organization units by preceding the **OrgUnitPath** with symbol **!**

14. Once properly configured your **Account settings** should look like this:



15. With CDM integration enabled you can skip Manual claiming your device and all enrolled devices should automatically appear in your MeldCX account

16. With CDM integration enabled you can manage your devices directly from MeldCX

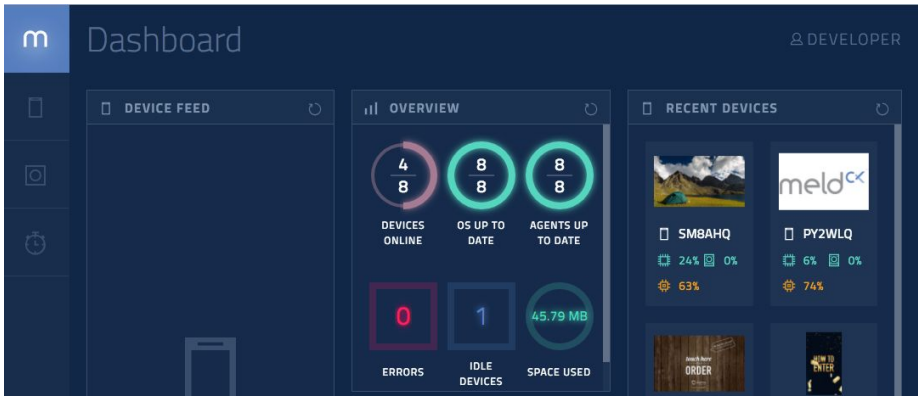


Claiming your device

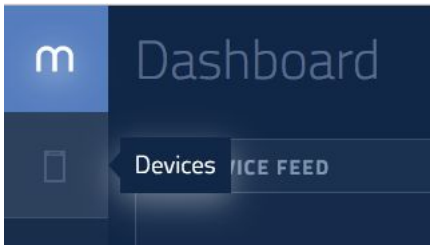
Please note that it is possible to configure CDM integration to automate device claiming process (see Configuring CDM integration)

1. Once you have correctly configured the CDM you should see your Chrome device on the MeldCX AgentM “Idle Screen”

2. In the top left you should see the “Call Home ID” this is an alphanumeric string that uniquely identifies your device. Make note of the ID.
3. Login to the MeldCX Dashboard located at https://admin.meld.cx

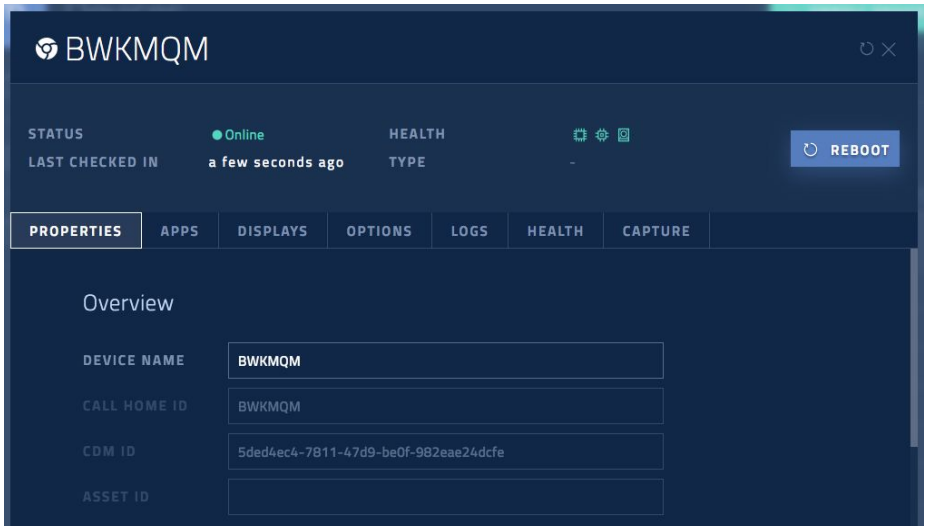


4. *Click* on the **Device icon** in the top left



5. In top right *Click* **Enroll Device**
6. *Enter* the “Call Home ID” you noted earlier.

7. *Click* **Enroll Device**
8. Congratulations, you have successfully claimed your device.



Dashboard

Landing Page

The MeldCX dashboard landing page is designed to provide you with a quick overview of the state of your devices & applications, below is a detailed breakdown of how each component may serve to help you.

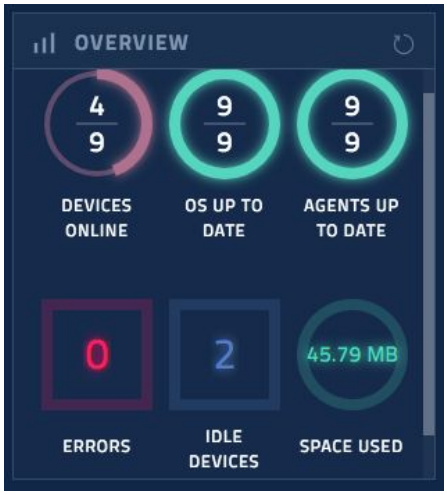
Device Feed

The device feed serves to provide you with a quick overview of the errors being returned by your device. This view shows the devices that have captured an event with a log level of “ERROR”. Here you may click on the device name to quickly navigate to that device and resolve any issues that may be occurring. Errors are sent by using the console.error method in Javascript.

Overview

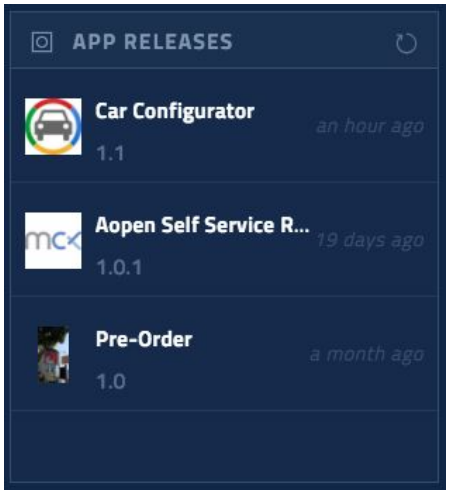
The overview serves to provide you with a snapshot of the following items:

- Devices online out of the total devices
- OS up to date out of the total devices
- Agents up to date out of the total devices
- Errors, the number of errors thrown to date
- The number of idle devices, that is devices with no schedule applications
- The amount of space used to store applications in the MeldCX cloud



App Releases

The app releases component is there to provide you with a quick view of your most recently released applications



Recent Devices

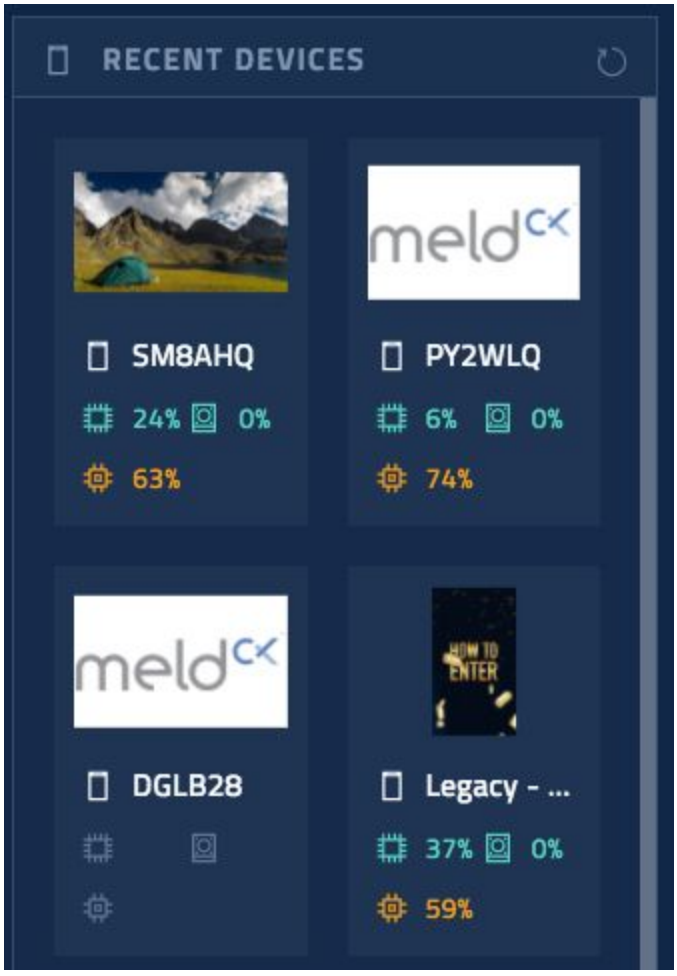
The recent devices component serves to keep you apprised of the state of your recently updated devices. These devices are the devices that you have specifically edited / interacted with.

There is a thumbnail of the most recent capture, the name of the device.

If a screenshot is not available a placeholder image is shown.

Additionally we provide an average of the cpu utilised (across all cores), the amount of disk space utilised and the amount of RAM utilized, all of the amounts provided are shown as a percentage of the total capacity.

From here you can click on the device and quickly navigate to view more device details.



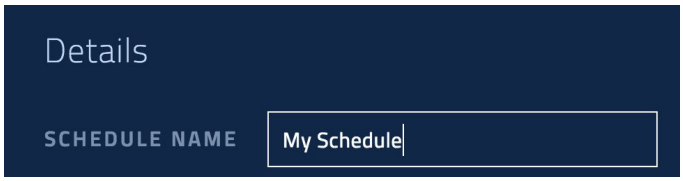
Creating Schedules

Schedules are heavily utilised by MeldCX, they are used to define the time period that an application is running, a time period within which the device is active and the displays are kept on and finally for a scheduled maintenance reboot. Below are instructions on creating a schedule.

1. Click on the Schedule button found on the left hand side menu of the MeldCX Dashboard.

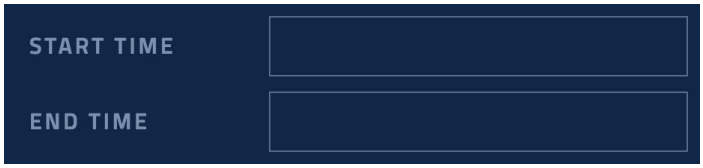
2. In the top right click on Create Schedule

3. Enter a Schedule Name into the Schedule Name text field



4. You may *optionally* choose a start date and end date for the schedule to be active

5. Enter a Start time and End time that this schedule will be active between



6. Select the Days of the week this schedule will be active

Creating a URL Application

A URL application is a simple application to point the MeldCX AgentM webview to a URL on the internet.

1. Click on the Application button found on the left hand side menu of the MeldCX Dashboard

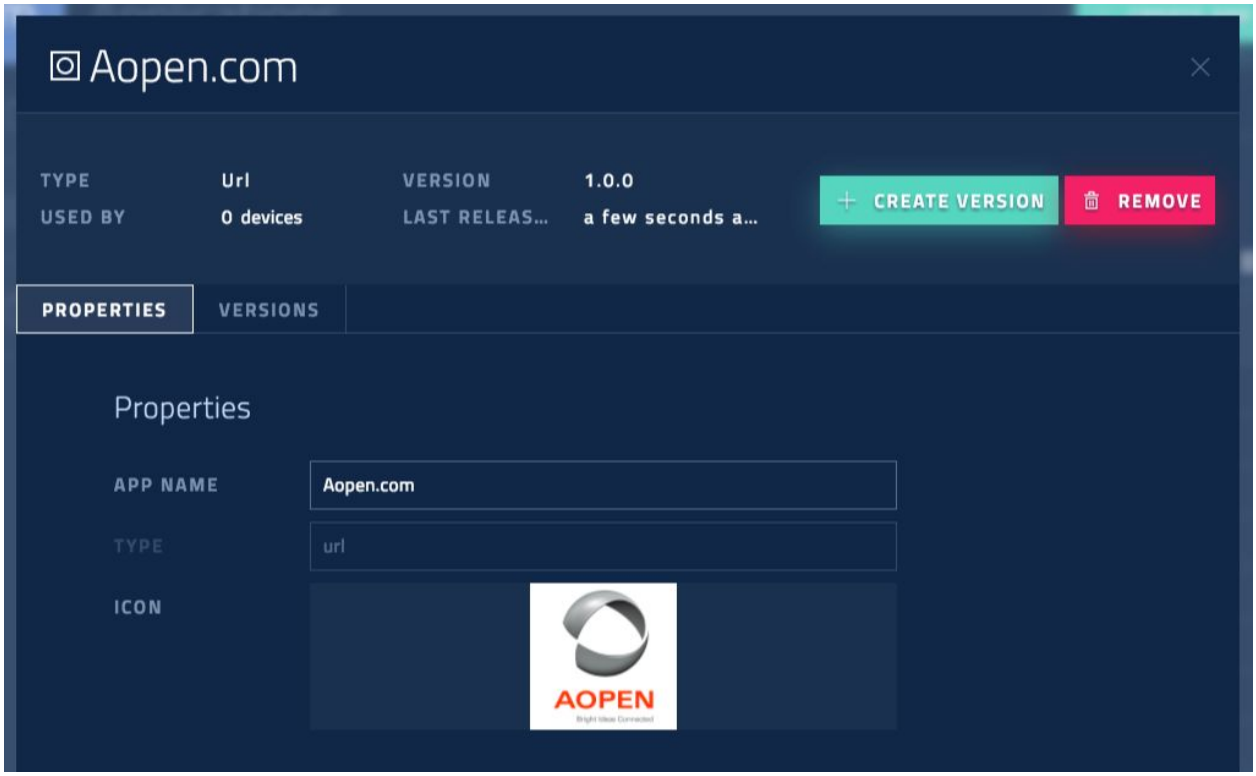
2. In the top right Click on Create App
3. From the Create an app window click Web URL

4. In the App name text field enter a name for this Web URL application

5. Click on the App icon field and choose an image to use as your application icon

6. Click Continue
7. In the Create the first version window enter a version number
8. Choose a channel, this typically will be set to Stable
9. Select an appropriate status:
    a. Pending - This application is not ready to be installed on a device
    b. Published - This application is ready and can be installed on devices.
10. In the URL text field enter the URL you want the webview to show

11. Click Finish
12. The application will upload
13. Congratulations you have created a URL application.



Creating a Google Slide Application

A Google slide application is used to show an Google slide presentation in the MeldCX AgentM webview.

rm=minimal

1. Click on the Application button found on the left hand side menu of the MeldCX Dashboard

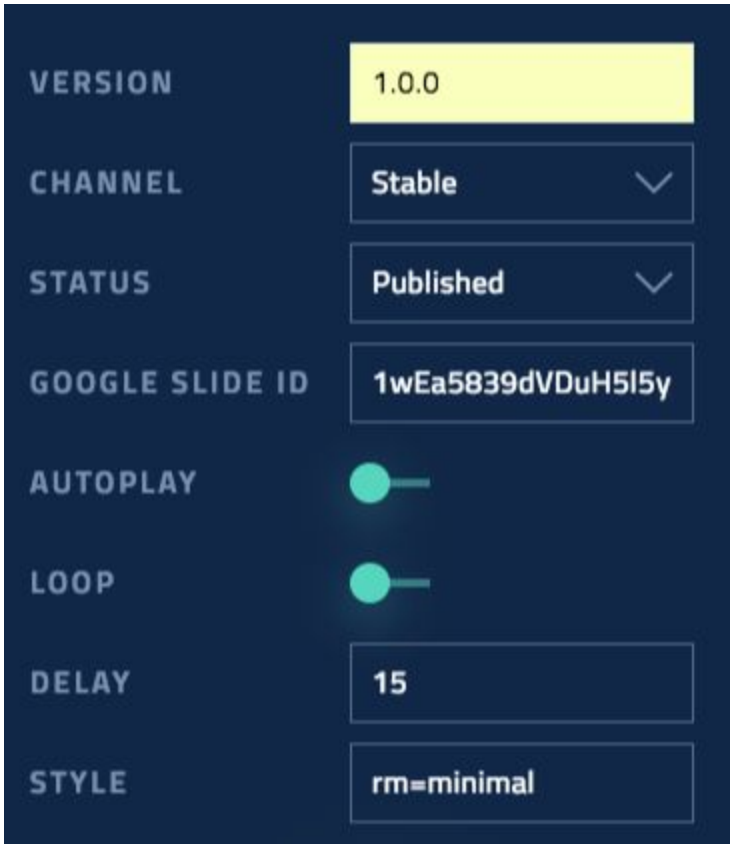
2. In the top right Click on Create App

3. From the create an app window Click Google Slides

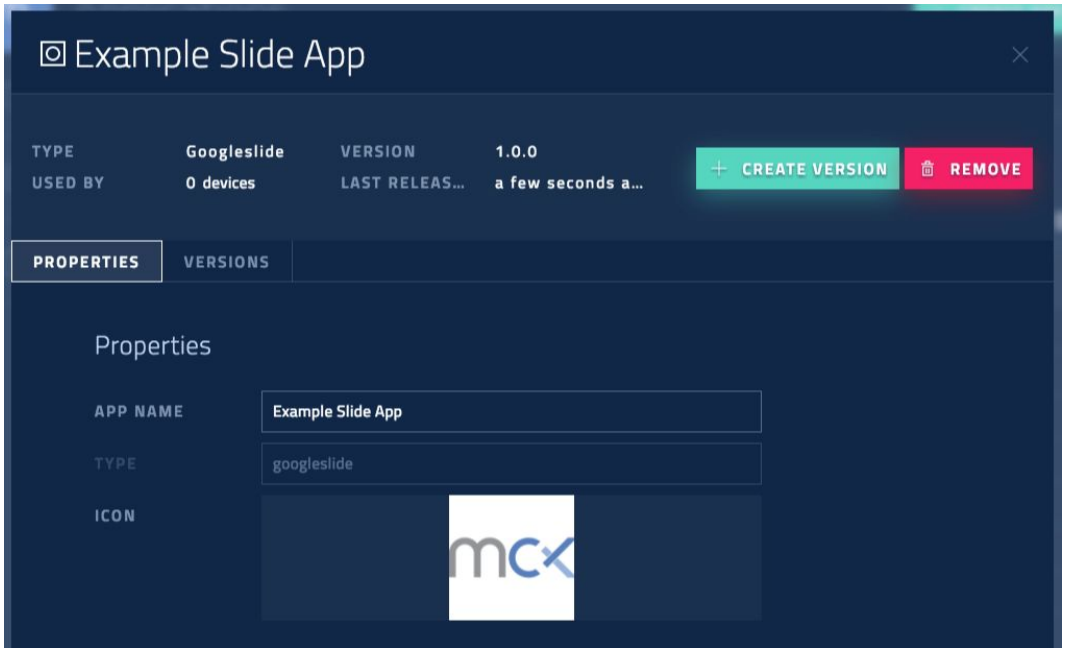
4. In the App name text field enter a name for this Google Slide application
5. Click on the App icon field and choose an image to use as your application icon

6. Click Continue
7. From the Create the first version window enter a version number into the version text field
8. Choose a channel, this typically will be set to Stable
9. Select an appropriate status:
    a. Pending - This application is not ready to be installed on a device
    b. Published - This application is ready and can be installed on devices.
10. In the Google Slide ID text field enter the Google Slide ID
11. If you would like the slide to autoplay turn on the Autoplay switch
12. If you would like the slide to automatically loop turn on the loop switch
13. Set the Delay in seconds that you would like each slide to appear for

14. In the style field enter an optional style, this will typically be set to rm=minimal



15. Click Finish
16. The application will upload
17. Congratulations you have successfully created a Google Slide application



Creating a Packaged Application

A MeldCX packaged application is no different to any other typically web application that is compiled in the browser, the advantage of a packaged application is that it can be stored locally on the device using MeldCX AgentM. The application will be provided to the webview via a built in web server.

1. Click on the Application button found on the left hand side menu of the MeldCX Dashboard

2. In the top right Click on Create App

3. From the create an app window Click Packaged App

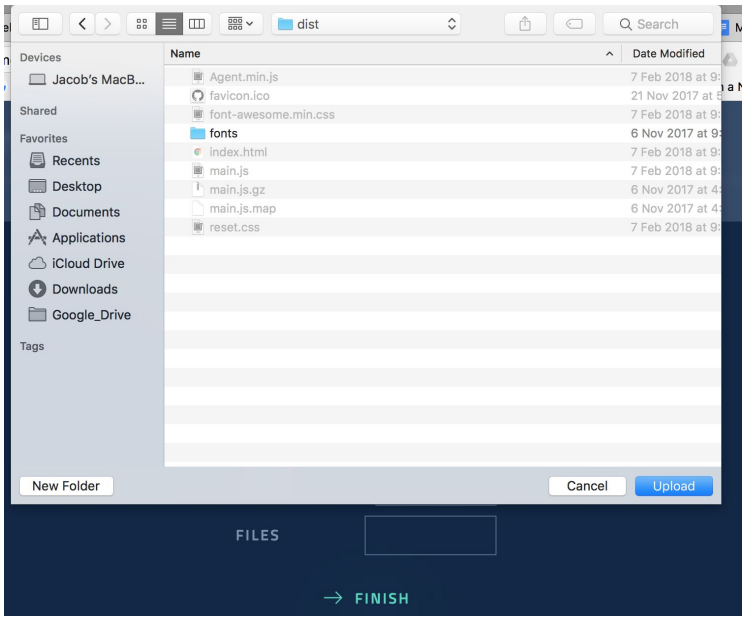
4. In the App name text field enter a name for this Packaged application
5. Click on the App icon field and choose an image to use as your application icon

6. Click Continue
7. From the Create the first version window enter a version number into the version text field

8. Choose a channel, this typically will be set to Stable
9. Select an appropriate status:
    a. Pending - This application is not ready to be installed on a device
    b. Published - This application is ready and can be installed on a device

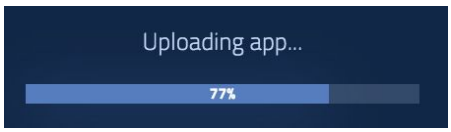
c. Deprecated - The application shouldn't be used any more and will not be downloaded by the device, if it is using this version it will fall back to the next published version.

10. From the files field select the folder which contains your packaged application

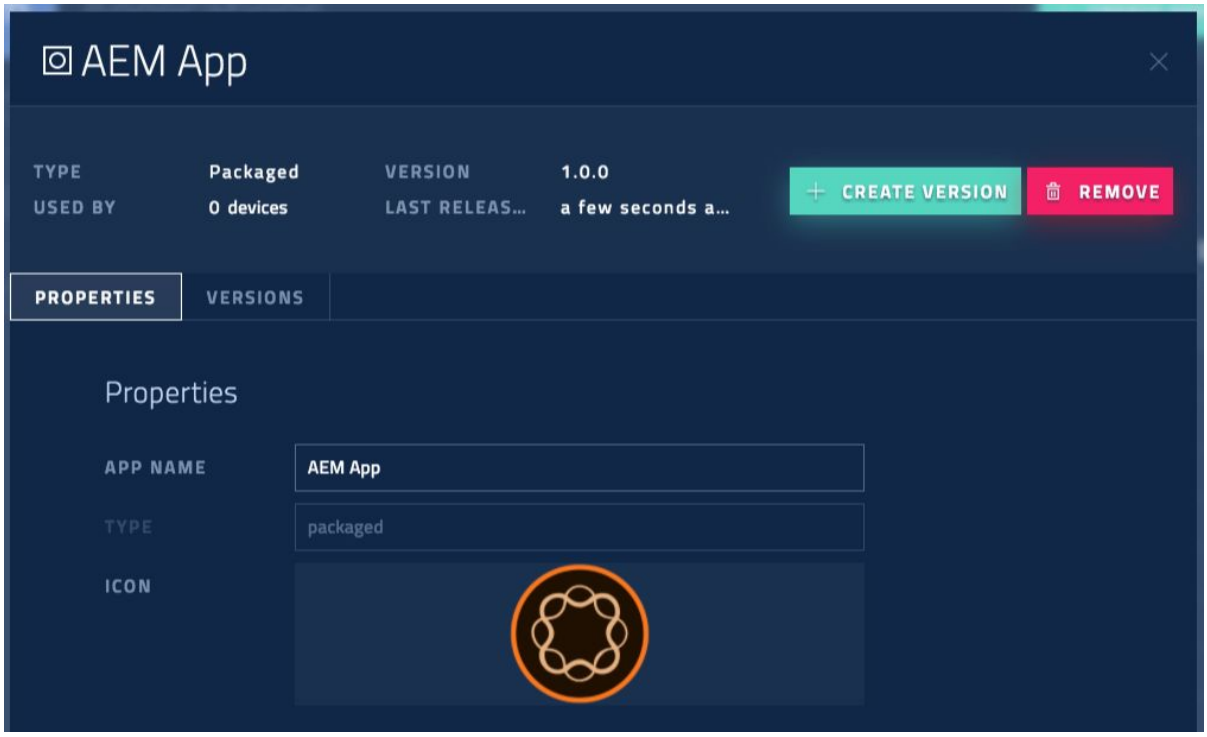


Note: A "Packaged" application is simply the compile and bundled web application, this is the same code that you would upload to a webserver to be presented to a client on a web browser. A packaged app can be written in any web supported language so long as it is compiled such that it is able to be run inside of a web browser.

11. Your application should now upload



12. Congratulations you have created a Packaged Application


AEM App
TYPE
Packaged
VERSION
1.0.0
USED BY
0 devices
LAST RELEAS...
a few seconds a...
CREATE VERSION
REMOVE
PROPERTIES
VERSIONS
Properties
APP NAME
AEM App
TYPE
packaged
ICON

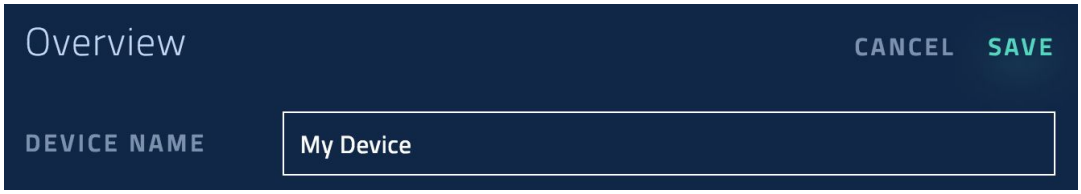
Device

Changing Device Name

1. Select the device from the devices page

2. The device name is located under the Overview section

3. Replace the text located in the Device Name field with the name of the device

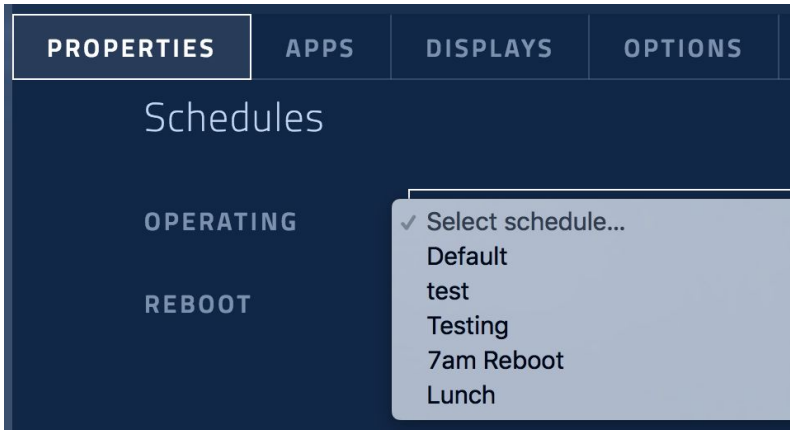


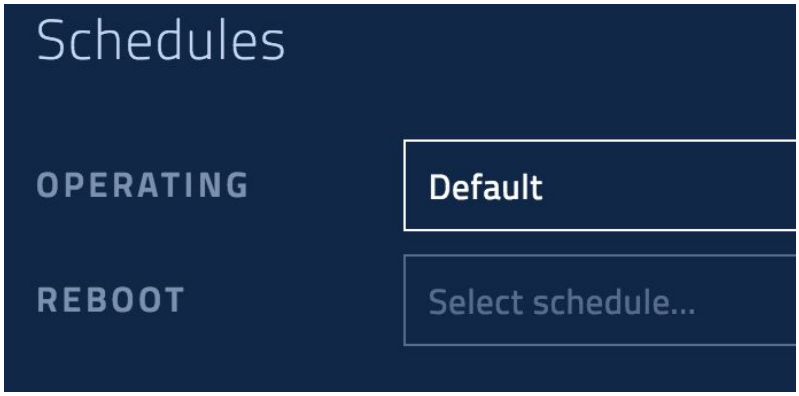
4. Click Save

Setting Operating Schedule

1. Select the device from the device page

2. The operating schedule can be found in the Schedules section
3. Select the schedule you want to use



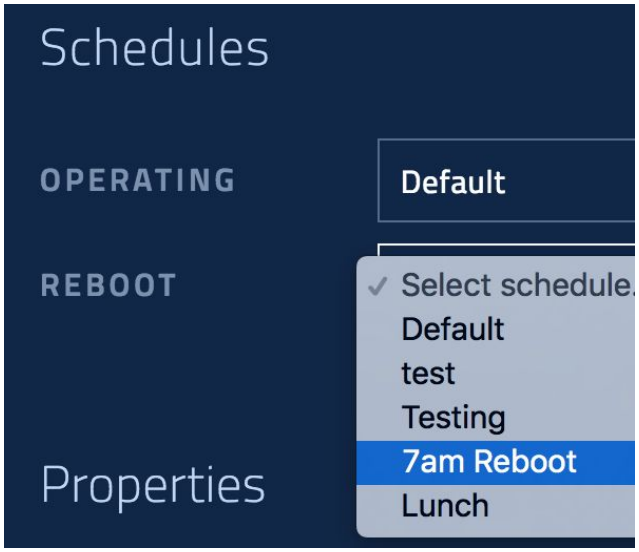


4. Scroll back to the top and click Save

Setting Reboot Schedule

1. Select the device from the device page

2. The reboot schedule can be found in the Schedules section
3. Select the schedule you want to use



4. Scroll back to the top and click Save

Manually Rebooting

1. Select the device from the device page

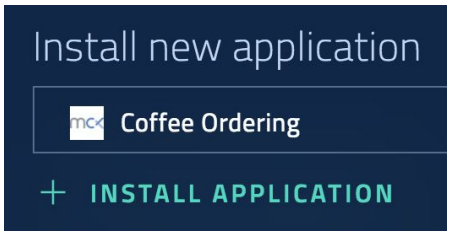
2. Select reboot in the top right over the device modal

Installing Application

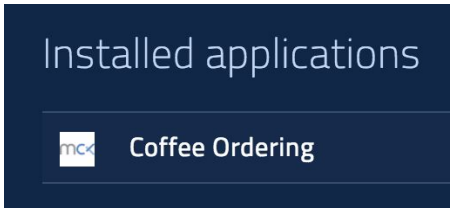
1. Select the device from the device page

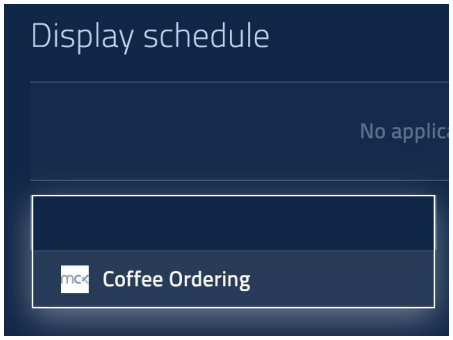
2. Select the apps tab

3. Select the application from the list



4. Click install application
5. Provided there is a valid, installable version available the device will download this application. The application will then be available to schedule in the displays tab.





Configuring Displays

Disable/Enable a display

1. Select the device from the devices page

2. Select the display tab

3. Switch the Enable Display switch to off or on, depending on which state you require

4. Click Save

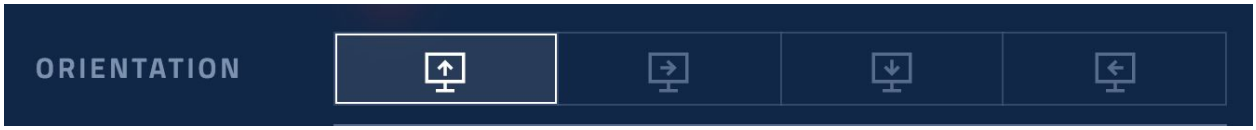
5. The window shown on the particular display will be closed or reopened.

Set the orientation

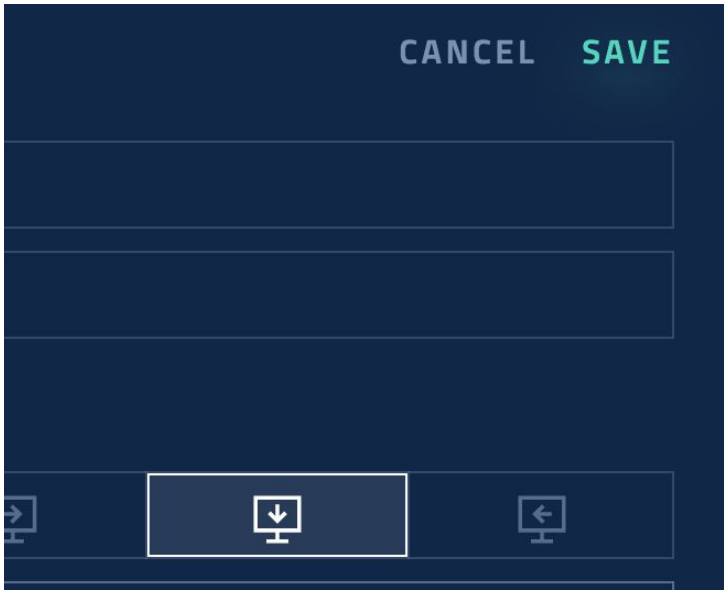
1. Select the device from the devices page

2. Select the display tab

3. Select the appropriate orientation, those being (from left to right)
0 degrees, **90** degrees, **180** degrees and **270** degrees



4. Click Save



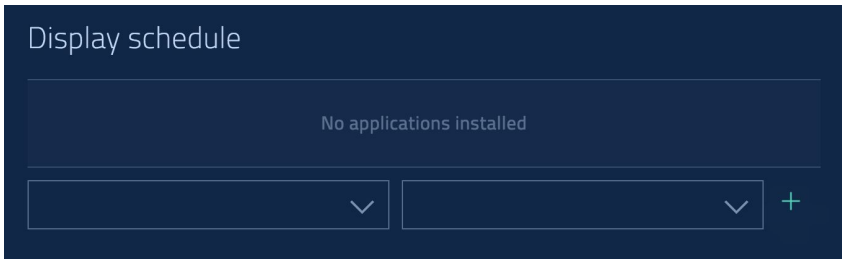
5. The display will then rotate

Configuring Display Schedule

1. Select the device from the devices page

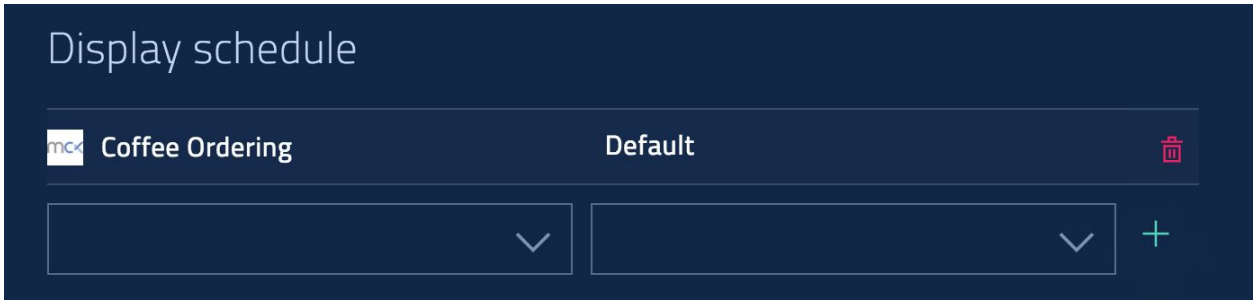
2. Select the displays tab

3. Scroll down to the display schedule section



4. From the left drop down list choose the application
5. From the right drop down list choose the application

6. Click the plus + button to add the application to the display
7. The application will be scheduled and run when the schedule is active



Configuring Display Options

Display options allow you to configure key value pairs that are available to be read by an application. An application can access these properties by utilising the Agent library. The agent library can be found in npm under the following package: @meldcx/matrix-agent-public the documentation for this can be found at https://docs.meld.cx

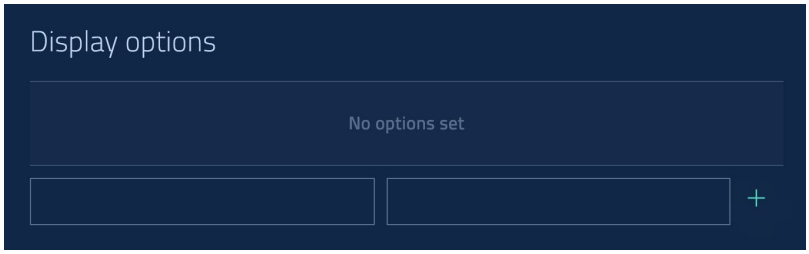
When an application calls for the options via the agent api it will only receive the options that are assigned to that particular display, this means that we are able to use the same “keys” across displays, negating the need for an index on the key.

To set a display option:

1. Select the device from the devices page

2. Select the displays tab

3. Select the display you want to set the options for
4. Scroll down to the display options section



5. Enter the key in the left text field and the value into the right text field.

6. Once you have enter the key and the value click the plus + button

7. The option will now be available in the application scheduled to that display, here is an example of the library usage to access this property.

```
const device = window.Agent.Device;

device.getOptions().then(options => {
    console.log(options);
    // Will return an object that looks like this {mykey: 'myvalue'}
});
```

8. Please see https://docs.meld.cx/ for complete documentation

Configuring Device Options

Device options are similar display options in that they are simple key value pairs that are accessible from the Agent library, however these device options apply to the whole device.

To set a device option

1. Select the device from the devices page

2. Select the options tab

3. Enter the key in the left text field and the value into the right text field

4. Click the plus + button and the option will be added.

Viewing Device Logs

Device logs are immensely useful when troubleshooting and or developing an application. Device logs are transported over an ephemeral and lossy protocol (websockets). This is to ensure that the maximum amount of information can be provided to the end user without producing an overtly large burden on our core database.

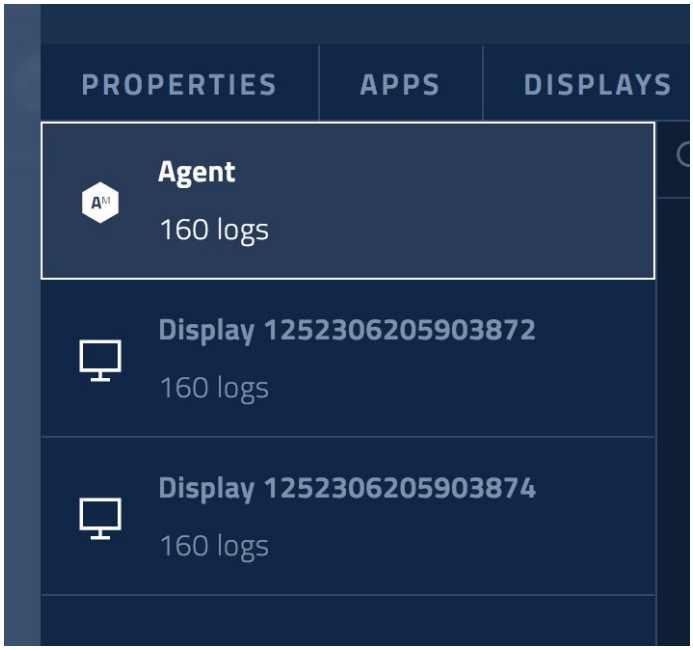
Device logs are captured through aliasing the console log, dir, error, warn and information methods (when the Agent library is installed into your application). There is an alternate set of logs that are captured through the chrome webview if you have not included the Agent library into your app.

Logs are collected in 3 distinct places: MeldCX Agent, Individual Displays and Applications.

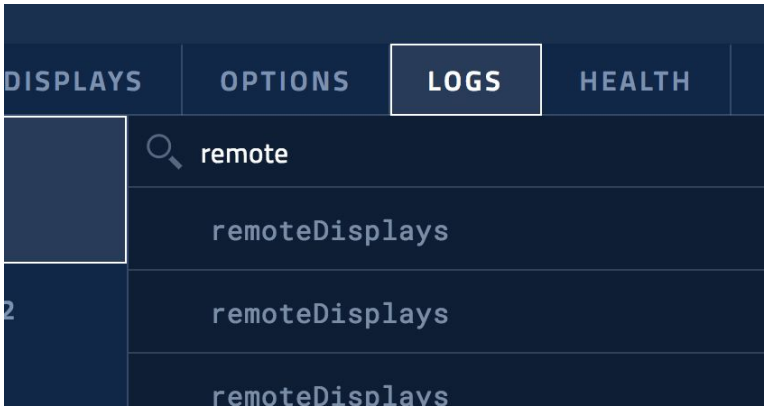
To view your device logs the device must be online and have an active websocket connection to the MeldCX cloud server and the dashboard.

1. Select the device from the devices page

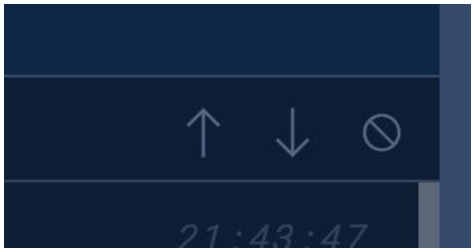
2. Click on the Logs tab
3. On the left you can observe the distinct places that the logged messages are emanating from:



4. There is a search field at the top of the log viewing section to allow you to quickly and easily search the logged messages.



5. You can Snap to top, Snap to bottom and clear the logs using the following buttons in the top right of the log viewing section

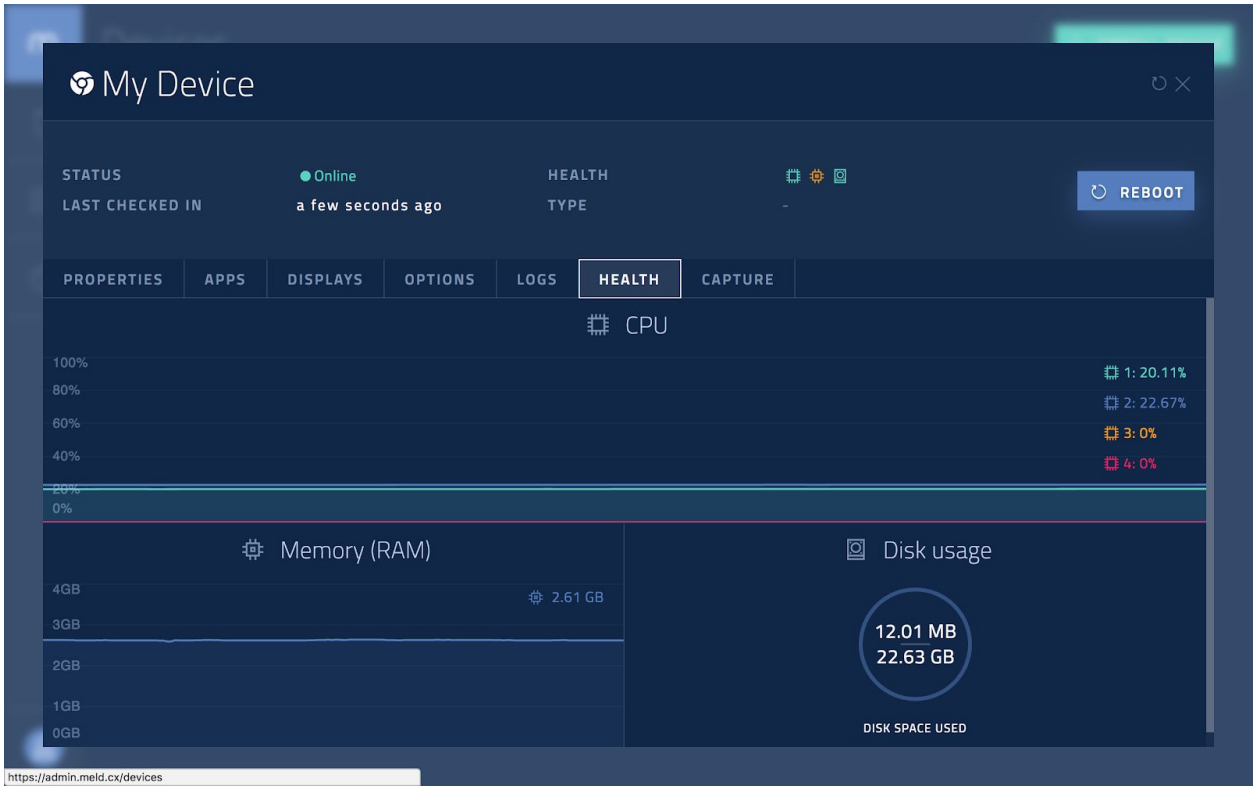


Viewing Device Health

In the device health section we provide you with an overview of the following items:

- Utilisation by percentage of each CPU core in your device.
- Utilisation by amount of RAM out of total available RAM
- Utilisation by amount of Storage out of total available Storage on the devices primary disk.

You can hover over each of the cores to view a highlighted graph

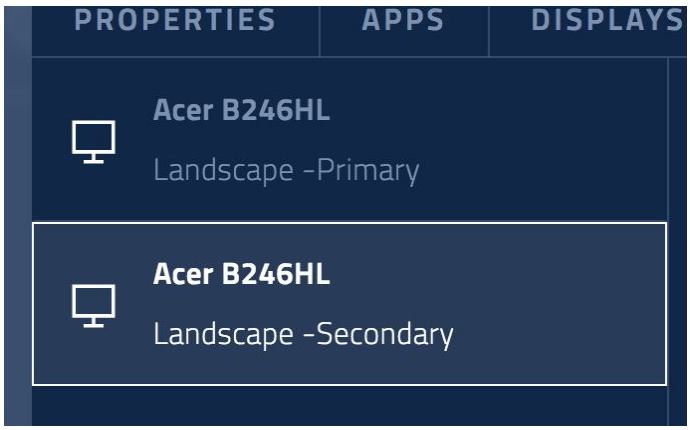


Capturing Screenshots

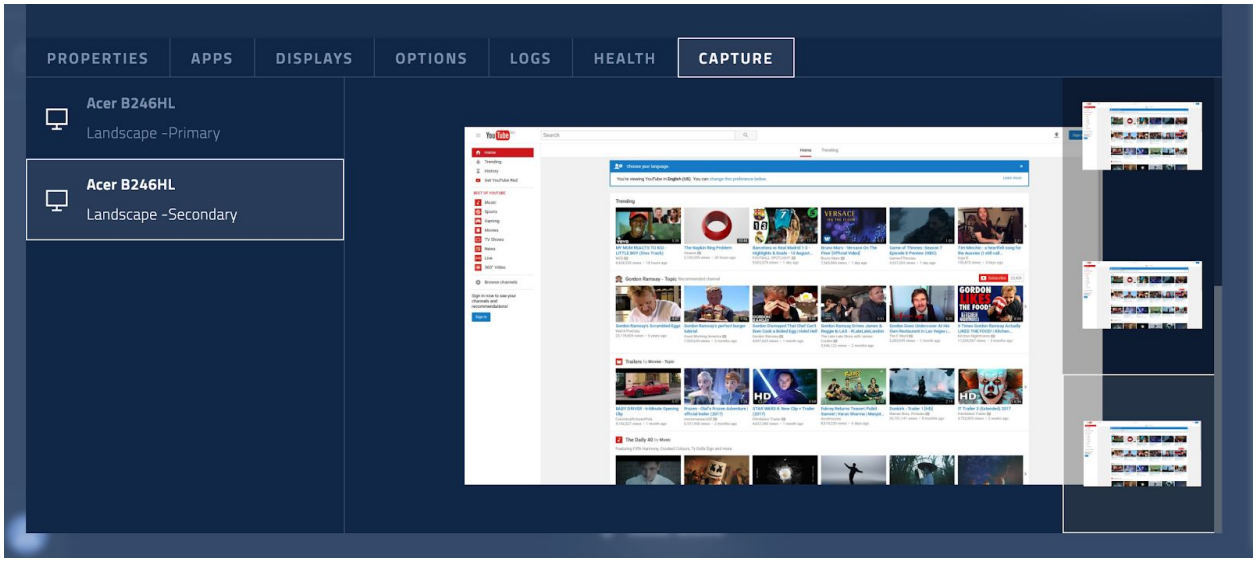
1. Select the device from the devices page

2. Select the capture tab

3. Note: Screenshots can only be taken when an application is scheduled and running on a display. If a device is showing the “idle” screen; then screen capture will not work.
4. Select the display you want to capture



5. Click capture
6. The screenshot will be captured

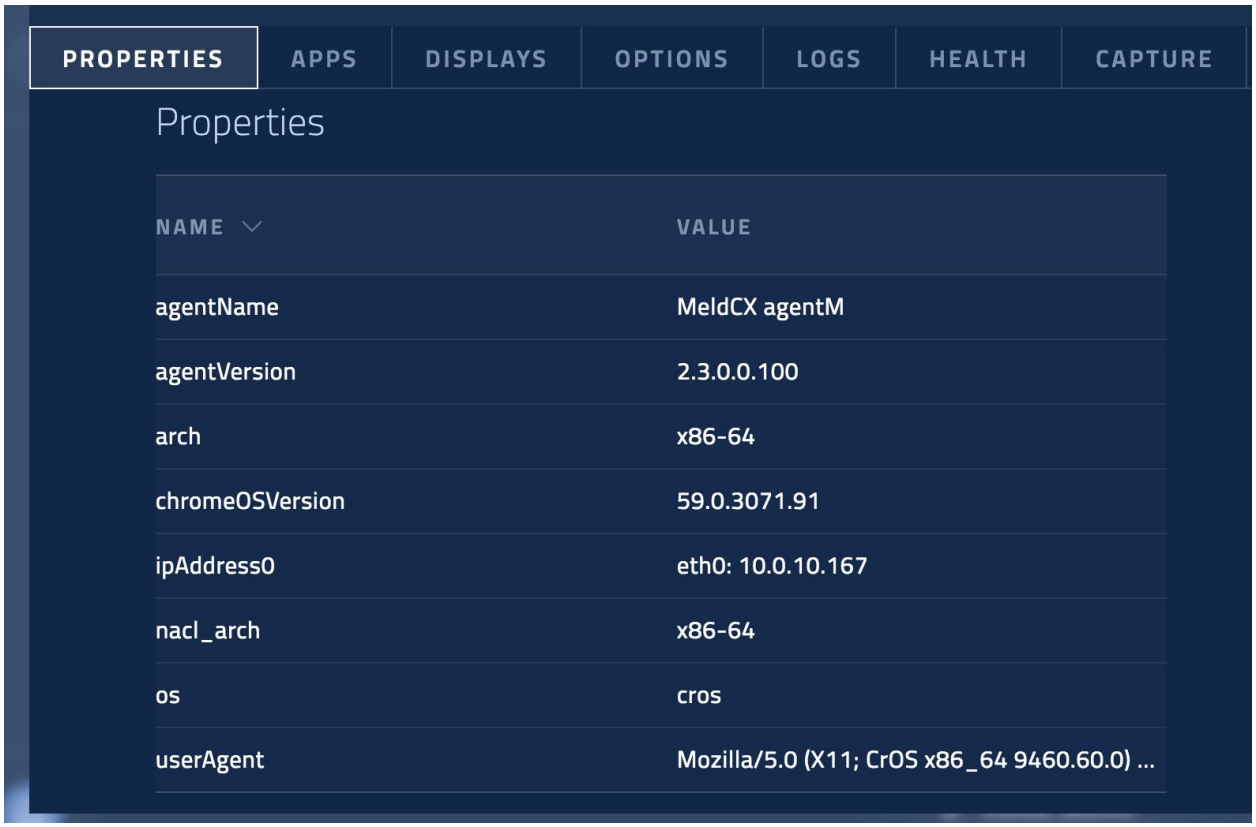


Reading Device Properties

1. Select the device from the devices page

2. Select the properties tab

3. Scroll down to the bottom of the properties tab
4. Here you can see the device properties, some of the items shown are:
    - ChromeOS Version
    - Agent Build Name
    - Agent Version
    - Device CPU Architecture
    - Assigned IP addresses

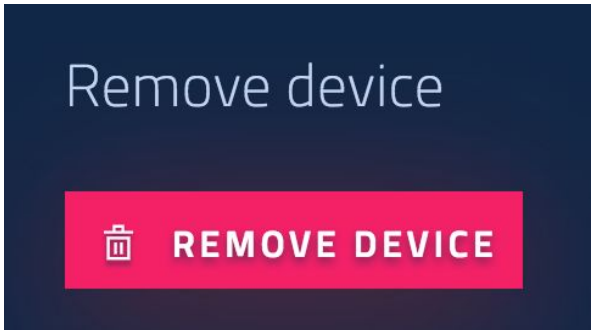


Removing a Device

1. Select the device from the devices page

2. Select the properties tab

3. Scroll down to the bottom of the properties tab
4. Click Remove Device



5. The device will be removed

Secure Browser Mode

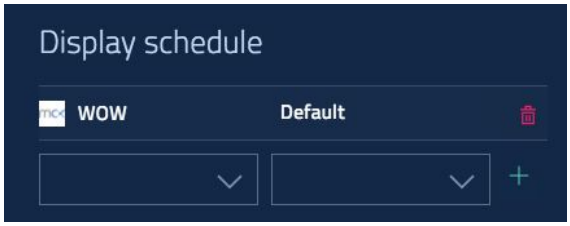
Secure Browser Mode is a feature that extends the existing URL application functionality by providing a navigation bar and user session timeout. The Secure Browser Mode adds the following functionality:

- Navigation Bar:
  - Move Forward in History
  - Move Backward in History
  - Navigate to Homepage (as defined in URL app)
  - Print using built in print functionality of ChromeOS
- User timeout:
  - Clears user cookies after a configurable period of time
  - Clear all data after a configurable period of time.

The timeout is determined by the amount of time since the last interaction i.e. touch, mouse movement.

To configure Secure Browser mode perform the following tasks:

1. Sign In to the MeldCX Dashboard
2. Open the Devices page
3. Select the Device you want to configure
4. Click the Apps tab
5. Install your URL application
6. Open the Displays tab
7. Select the Display you want to schedule your app on
8. Scroll down to the Display Schedule section
9. Schedule the App with an appropriate Schedule



10. Scroll down to the Display Options section
11. Configure the following options:

Key	Value	Default	Type	Description
browserNav	true	none	Required	This will tell AgentM to load the Secure

				Browser Mode. (Boolean)
idleTimeout	15 - 65536	15	Optional	This setting is set to 15 seconds by default, you can configure it to any value you like greater than 14. (Number)
tombstoneTimeout	0 - 65536	15	Optional	This setting is set to 30 seconds by default, you can configure it to any value you like. (Number) If set to 0 then tombstone is disabled.
canPrint	true false	true	Optional	This setting is on by default and add a Print button to the navigation bar. (Boolean)
canGoForward	true fale	true	Optional	Enable Forward Button (Boolean)
canGoBack	true false	true	Optional	Enable Back Button (Boolean)
canGoHome	true false	true	Optional	Enable Home Button (Boolean)
sameOrigin	true false	false	Optional	Don't reset if the origin hasn't changed. (Boolean)

browserNav This option defines whether or not the device is configured to run Secure Browser mode, you can set it to true to enable it or false to disable it.

idleTimeout This option defines the amount of time that the device must be idle before the users browsing session will be cleared, by default this is set to 15 seconds.

tombstoneTimeout This option defines the amount of time that the device must wait after a user session timeout before clearing all of the browser data, by default this is set to 15 seconds.

canPrint This option defines whether or not the Secure Browser Mode will show the print button, by default this will be set to true and the button will be visible.

canGoForward Enabled/Disable the forward button

canGoBack Enable/Disable the back button

canGoHome Enable/Disable the home button

sameOrigin Enable/Disable the origin.

12. Once you have set the relevant settings allow up to 30 seconds for the device to synchronize the configuration.
13. Restart the device.
14. The Secure Browser Mode will be enabled.

Troubleshooting MeldCX

Q: Agent wont load, is stuck showing waiting for application

A: This is typically caused by the ChromeOS version being out of date.

Ensure you device is up to date

1. Reboot your device
2. Press CTRL+ALT+S repeatedly when prompted until your device goes to the sign on screen
3. Login to the device with credentials provided to you (for managed CDM clients)
4. Otherwise use your own CDM credentials to sign in to your device.
5. Navigate to the Settings page
6. Click About ChromeOS
7. Click check for updates (if available)
8. Reboot your device and verify that the Agent loads
9. If your attempt the above process and the Agent still fails to boot please email help@meldcx.com

Q: A prompt is appearing on my screen asking me to permit access.

A: The Agent has been started from a source other than “Pure” “Kiosk Mode”

1. Reboot your device and ensure that the device automatically boots into the MeldCX Agent without user input