



User Manual

Date

2024-Jan

IAdeaCare User Manual 1.6.0

America

20 Fairbanks,
Ste, 170 Irvine, CA 92618
California, U.S.A

Taiwan

114, 3F, No. 21
Ln. 168, Xingshan Rd.
Neihu Dist., Taipei, Taiwan



Table of Contents

1. Overview	3
2. System Requirements.....	4
Minimum system requirements	4
3. Account Setup Process.....	5
4. UI Overview	7
4.1 Main Dashboard	7
Password Change.....	7
4.2 Devices	9
All Devices.....	11
Groups	12
Tag Tab.....	13
Batch Actions.....	17
Home Shortcuts.....	18
Device Dashboard.....	22
IAdeaCare Functions	24
Registration	36
Policy.....	37
4.3 Notifications	42
Alert Setting.....	42
Report.....	48
4.4 Troubleshoot.....	51
Troubleshooting Page.....	51
4.5 License.....	52
Add License	52
Import License.....	54
Reallocate License	56
Advanced Filter	56
5.6 Event Feeds.....	57
Event Log	57
Device Activities.....	59
5.7 Miscellaneous	61



LAN Config Tool.....	61
Access Key.....	62
5.8 Enterprise Account.....	66
Creating Enterprise Account	67
Expiration mechanism of enterprise account.....	68
Domain Change.....	68
Login Portal / SSO.....	68
Admin.....	69
Policy Tab	84
App Management policy (Exclusive to enterprise account).....	85
Certificate Management policy (Exclusive to enterprise account).....	86



1. Overview

Managing your players is no longer a complicated task. With **IAdeaCare**, you are now able to remotely monitor and configure your player's settings from the ease of your internet browser. **IAdeaCare** allows for easy set up and pairing of your players in or outside of your network to connect. Once players are paired with your account, all the remote features, functions, and settings that once required you to physically configure the player are now available remotely.

Player Management made easy with **IAdeaCare**:





2. System Requirements

Minimum system requirements

CPU	<ul style="list-style-type: none">• 2.6 GHz up
Operating System	<ul style="list-style-type: none">• Windows OS• MAC OS
Browser Version	<ul style="list-style-type: none">• Google Chrome: 56• Firefox:38• Microsoft Edge: 20
Firmware Version	<ul style="list-style-type: none">• Available on all model Android 7.1• MBR-1100: 1.2.87.531 or later• XDS-107X: 1.2.86.532 or later• XMP-6250/6400: 1.2.84.533 or later• XMP-7300: 1.0.10.341 or later• WRP-1000: 3.4.0 or later



3. Account Setup Process

- a. Enter <https://care.IAdea.com> to your web browser.
- b. Type in your account email and password to log in.
 - I. If you already have an account, proceed to login with email and password.

- Confirm that IAdeaCare is on the latest Version and Release.
- v1.6.0-67 | Release: 2024/01/XX

- II. If you do not have an account, click on Sign Up to create a new IAdeaCare account.
 - i. Follow the below prompts and fill out the form:

- ii. Once you have your form filled out, click Submit. An email confirmation with an activation code will be sent to your email.



Please input the activation code from your Email to activate your account.

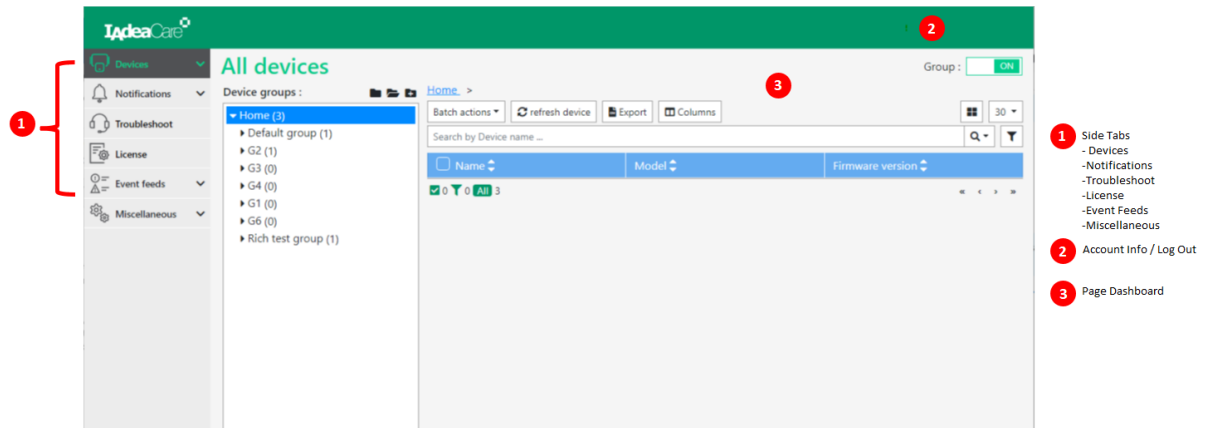
Activation code

[Back to login](#) [Activate](#)

Note: When registering for a new account or using **Forget password** function, an email will be sent from noreply@iadea.com. To avoid these email goes into junk mail, please add it to safety list (e.g., you may want to find some official article link for outlook on how to add contact into safe list). If not, then customer should look for email title **IAdeaCare account activation** or **IAdeaCare password recovery** from junk mail box.

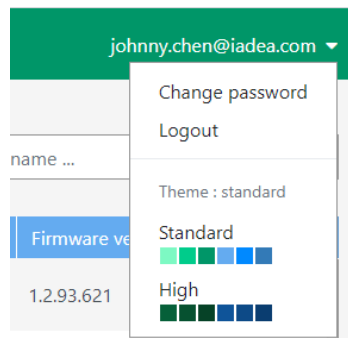
4. UI Overview

4.1 Main Dashboard



1. The main dashboard is composed of side tabs located on the left-hand side that allow you to navigate your IAdeaCare UI.
2. To logout of IAdeaCare, the **Logout** button is located on top right corner.
3. The page **Dashboard UI** will change to display the content for the selected **Page** Tab.

For users that need high contrast color scheme, the **Theme** option is available on the toggle drop down menu next to the account name.



Password Change

To change your password, click on the down arrow next to the account email and select Change password. Enter your old password followed by your new password twice.



johnny.chen@iadea.com ▾

Change password

Logout

Theme : standard

Standard

High

name ...

Firmware version

1.2.93.621

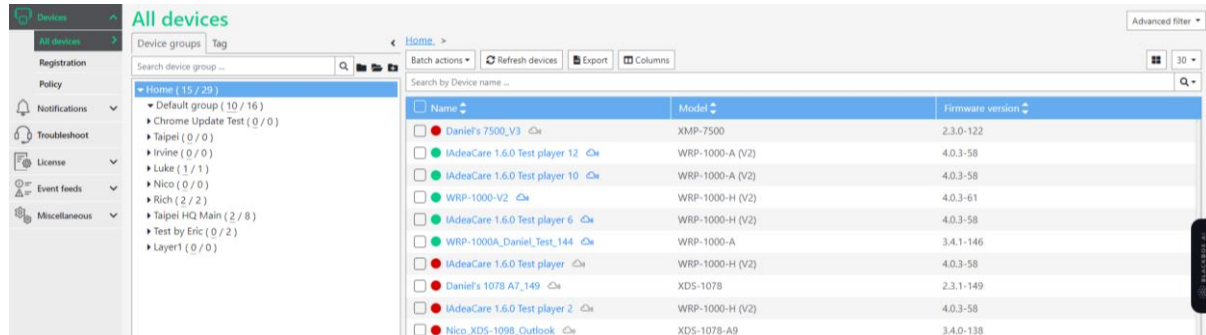
Change password

Old Password

New Password (at least 10 digits)

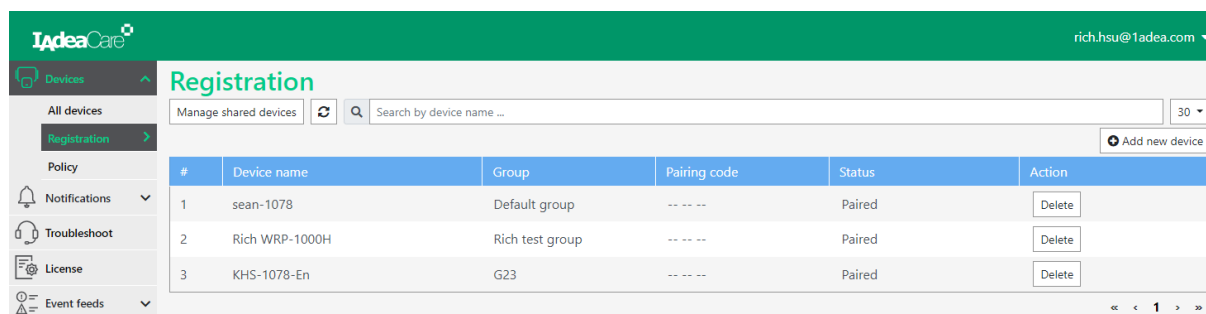
Confirm your new password

4.2 Devices



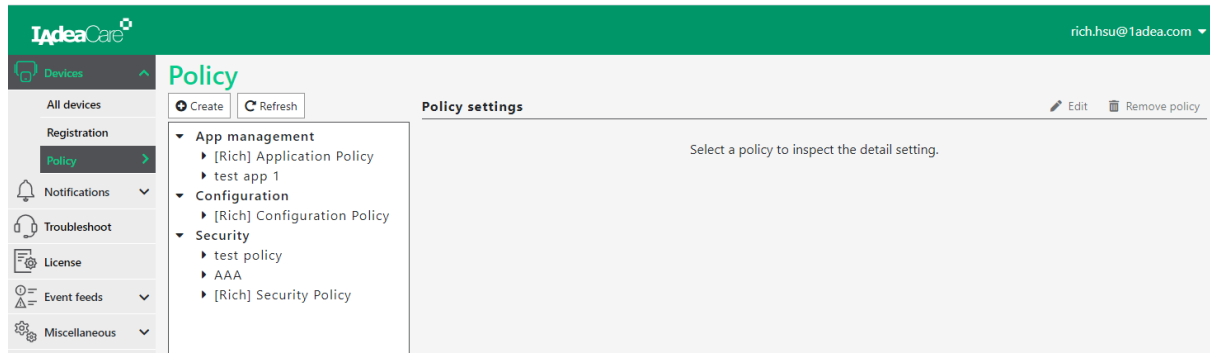
All Devices Elements:

- **Group Function:** Expand, Collapse, New Group
- **Batch Actions:** Basic configuration, Update Password, Update Firmware, Update APK , Reboot, Troubleshoot, Share Player, Clear Cache
- **Refresh icon:** Refresh Players, Change View, Device Activities
- **Export icon:** Export device list.
- **Columns:** Add Device information
- **List View/ Grid View:** Switch between the two views.
- **Sort icon:** Sort by Filters.
- **Search icon:** Search by device name.
- **Information of the paired Players:** The details for the paired devices for management.
- **Search box in Device Group:** Search devices by name within the Device Group.
- **Group by Tag Tab:** The tag tab allows you add labels to devices to create label groups.
- **Advanced Filter:** Advanced filter allows for more advanced parameters to filter your desired device list.



Registration Elements:

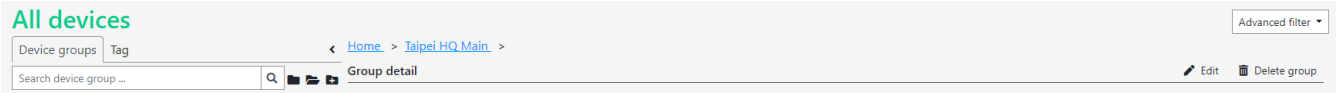
- **Add/remove player:** Add/Remove Paired Player
- **Manage Shared Devices:** More configuration, Password, Firmware, APK, Reboot, Troubleshoot, Share Player
- **Refresh icon:** Refresh Players, Change View, Player Activities
- **Search icon:** Search by Player Name






Policy Elements:

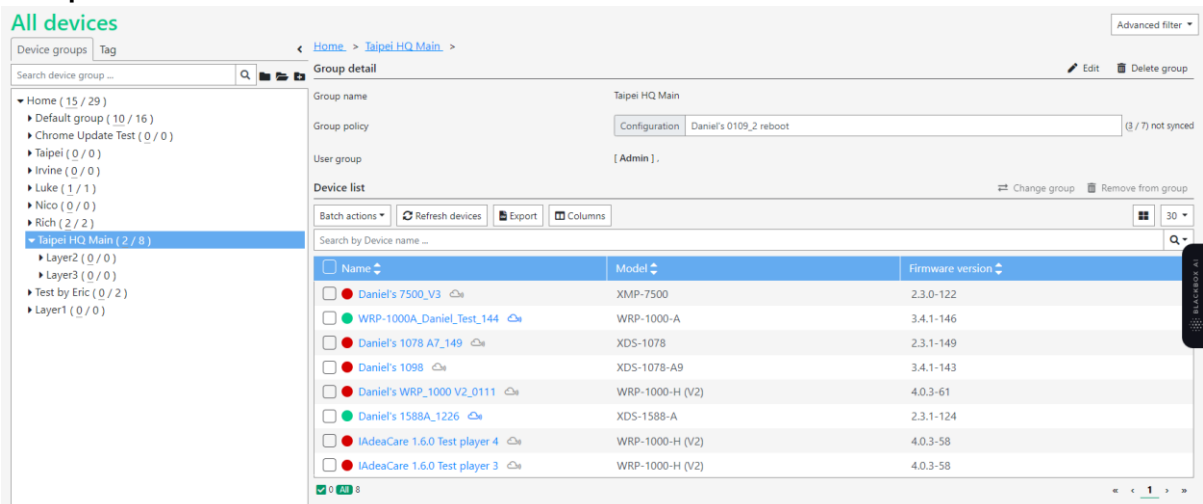
- **Create:** Create a new policy (Configuration, Security, App Management)
- **Refresh:** Refresh the policy list to show changes if policies were edited or devices were added.
- **Edit:** Select an existing policy to edit the policy settings.
- **Remove Policy:** Remove any unwanted policies from the system.

All Devices



Device groups Actions: Collapse Folders , Expand Folders , Create New Group 

Group details:



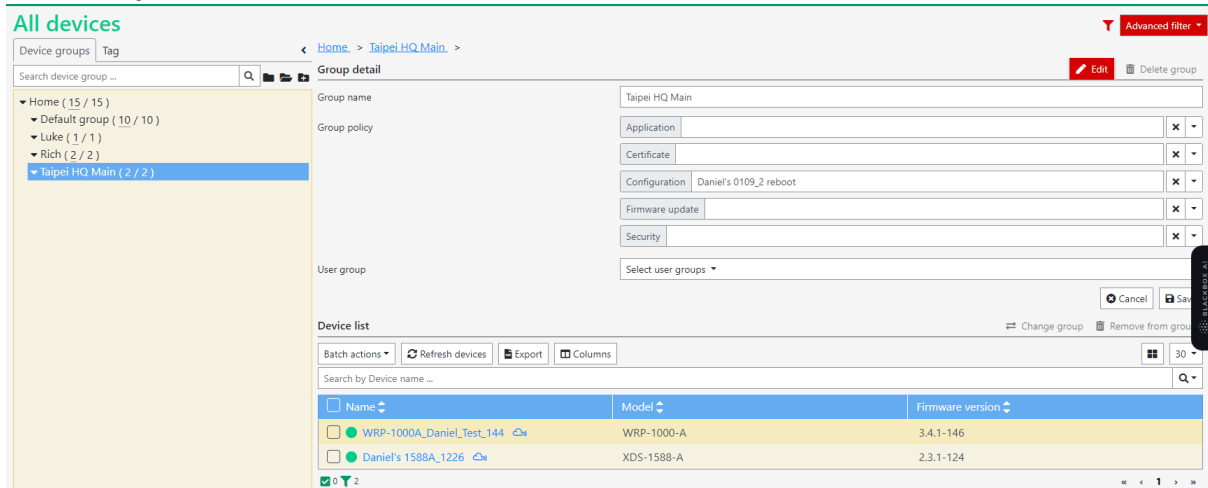
On this page, the dashboard will show Group Name, User Group, and the Device Policy.

****Note: User group** information only exists when under Enterprise account. There is no control button until user click 'Edit'.

Device Groups now show online/total devices for each group.

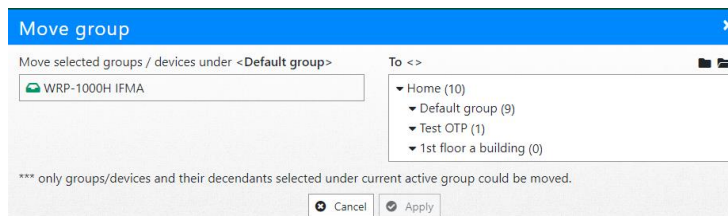
Device Search is applicable to All Device Table and Device Group.

Edit Group:



Click 'Edit' button to expand the editable options.

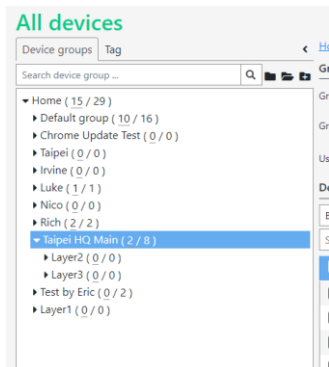
- Edit Group Name.
- Drop down menu to set up group policy
- Drop down menu to set up user group (Enterprise Account)
- Cancel / Save for the above settings.
- Delete Group Button. Once group is deleted, all devices will be moved to default group.
- Change Group: The change group option will only populate once devices are selected. User can change group by drag and drop to the group tree on the left.



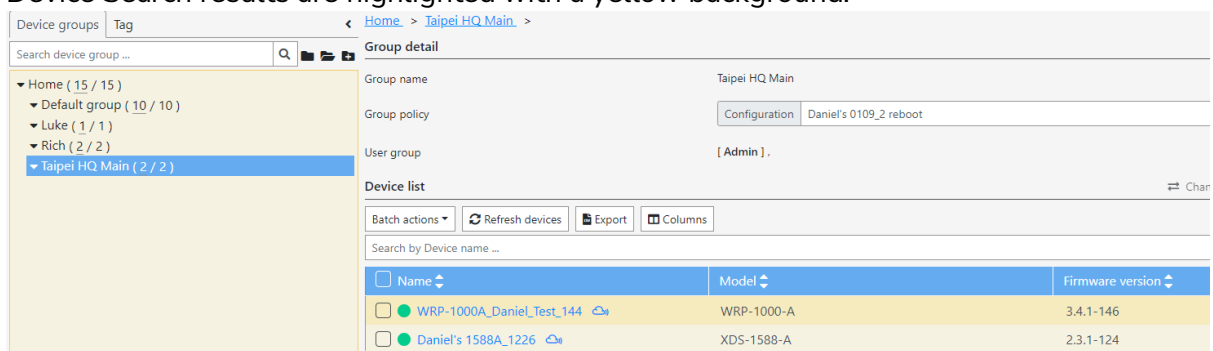
- Remove from Group: This option will only populate when devices have been selected. When Remove Group is selected, a system message will populate to notify user "Are you sure to remove devices from [Group Name] group? Devices will be automatically moved to the Default Group."

Groups

By default, devices that have not been assigned a group will be grouped in the default group. Users will be able to **create groups and sub groups** to organize and filter the devices on your network.

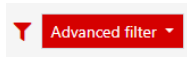


Device Search results are highlighted with a yellow background.

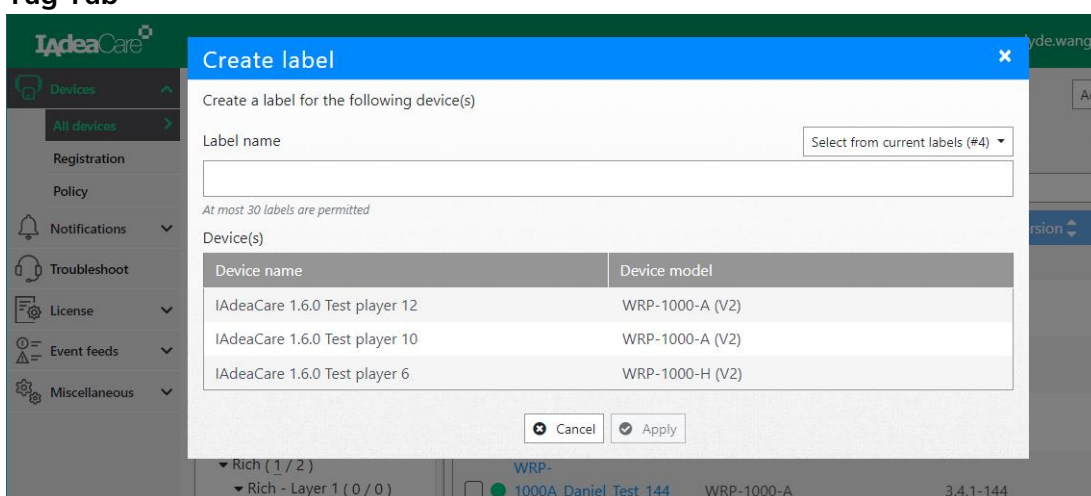


The search will also change the number of devices indicated under the device group.

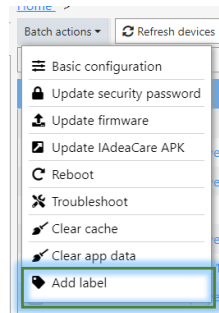
Filtered searches will be indicated by the Red Filter Icon.



Tag Tab

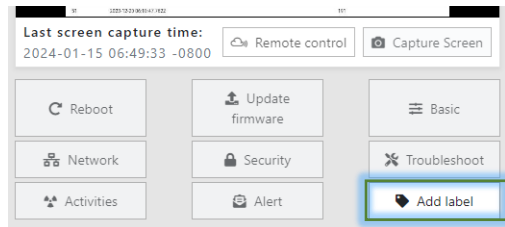


Device Labels can be added to multiple devices through the Batch Action.

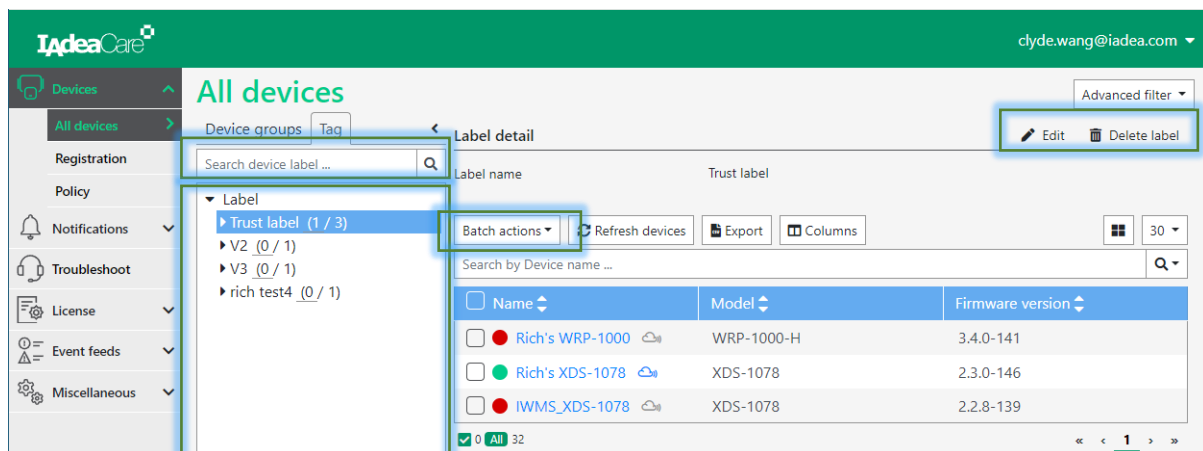


Label can be new or selected from current labels being used.

Device Label can also be added to individual devices through their player dashboard.



Maximum number of labels that can be created is 30.



Users can search label under the Tag Tab.

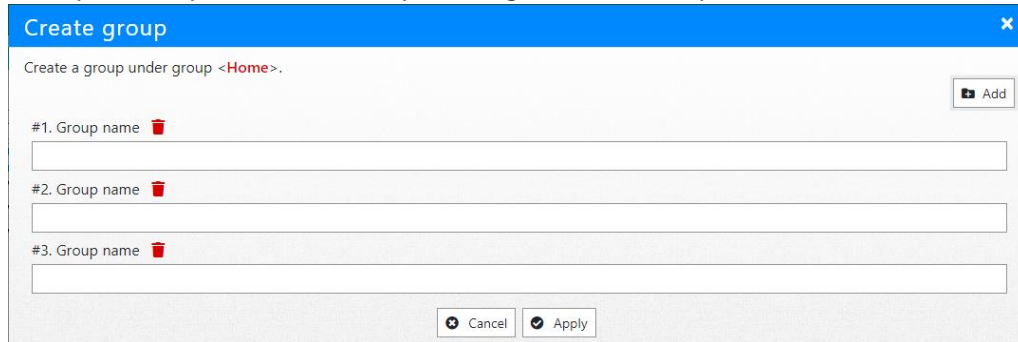
List of search results will show online/total number of devices with label tag.

Users can use Batch Actions for devices under same label. However, Policies do not apply to label groups (Only Device Groups).

Labels can be edited or deleted at any time.


Create Group:


Click Add to add a new group. Input your group name and click apply. You can create multiple Groups at one time by clicking on Add multiple times.




Create group

Create a group under group <Home>.

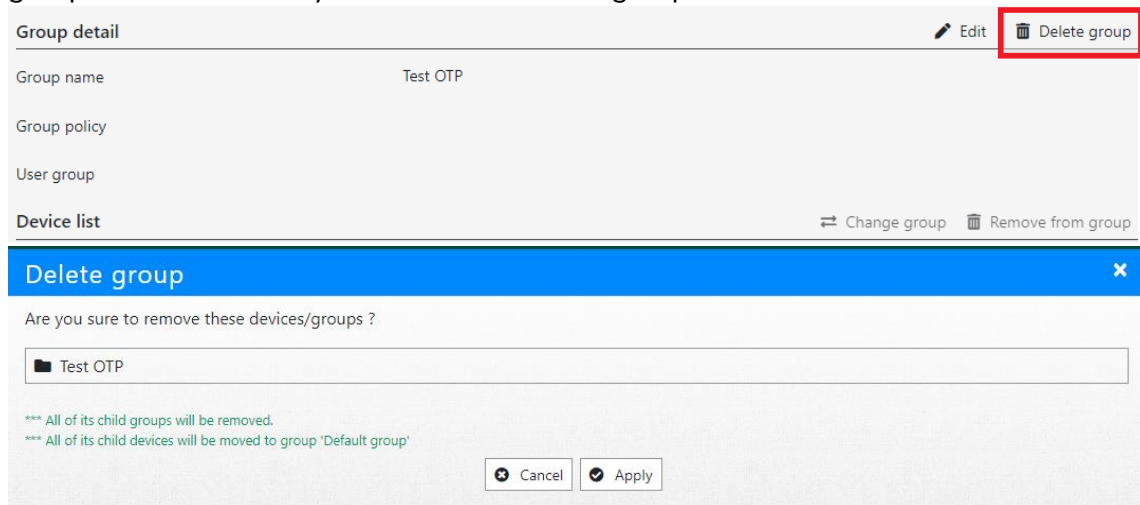
#1. Group name 


#2. Group name 

#3. Group name 

Delete Group:

Select Device or Group from the Group tree to be deleted. Click Delete and confirm. When deleting any group, all subgroups will be deleted as well. Devices belonging to deleted group will automatically be moved to Default group.




Group detail Edit  Delete group

Group name Test OTP


Group policy

User group

Device list Change group  Remove from group

Delete group

Are you sure to remove these devices/groups ?

 Test OTP

*** All of its child groups will be removed.
*** All of its child devices will be moved to group 'Default group'

Move Group:

Select device/group from list and click Move Group. You can also check a group's policy to move along with device/group to another group.

Group detail

Edit

Delete group

Group name

Test OTP

Group policy

User group

Device list

Change group

Remove from group

Move group

Move selected groups / devices under <Default group>

WRP-1000H IFMA

To <>

Home (10)

Default group (9)

Test OTP (1)

1st floor a building (0)

*** only groups/devices and their descendants selected under current active group could be moved.

Cancel

Apply

Edit:

Allow to View and Change Group Policy.

Group detail

Edit

Group name

Test OTP

Group policy

Application

Configuration

Security

User group

Select user groups

Note: When initially pairing devices, users can select the group that the device to belong to

Home

Device overview

Manage shared devices

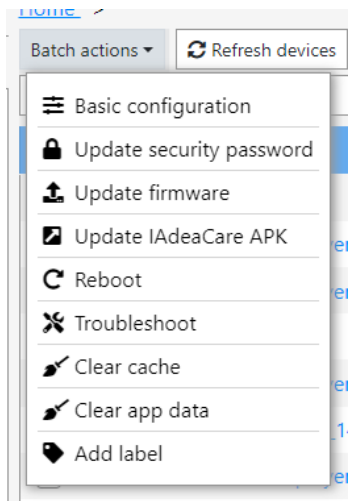
#	Device name	Group	Pairing code	Status
1	XDS-1078-A7	Default group	-- -- --	Paired
2	MBR-1100	Default group	-- -- --	Paired
3		Default group		Not pair

Add new device

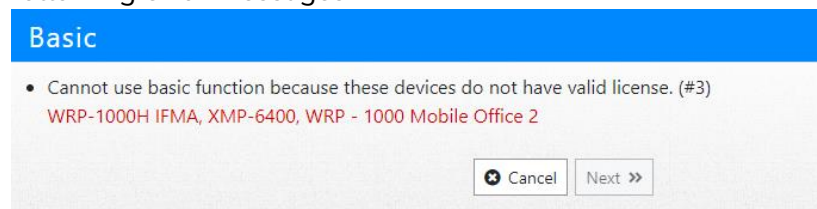
Batch Actions

Under **Batch Actions**, users will be able to:

- **Utilize** the available functions to multiple players at once.
- Accomplish a **batch** function or configuration, click on the empty box next to the desired players to select multiple players. Then select the Batch Actions function you would like to utilize. For most advanced control functions, See [Section 4.2.3](#)



Note: If a selected player does not have a valid license or is offline, you will receive the following error messages.



Update APK – This will update the **IAdeaCare.apk** version on the player. The **IAdeaCare.apk** version should automatically update with each release. However, if there is an issue with the player automatically updating, you may manually update through this function.

Clear cache – This function sends a command to clear the application cache on the player. This will clear any stored cache that may cause the player to malfunction or prevent the player from downloading new content or configurations. Clearing the cache will not reset the player or delete the storage content.


Clear app data – Clear app data on devices to clear both cache and cookies.


Add Label – Add a tag label to devices to create a group.




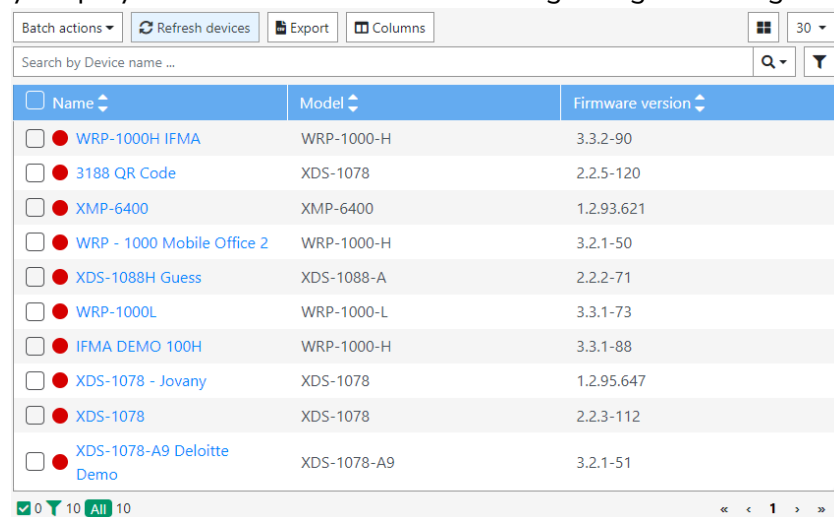
Home Shortcuts




 **Refresh devices** - refresh all content to reflect any changes that you may have submitted. There is a 30 second time restriction between each refresh.

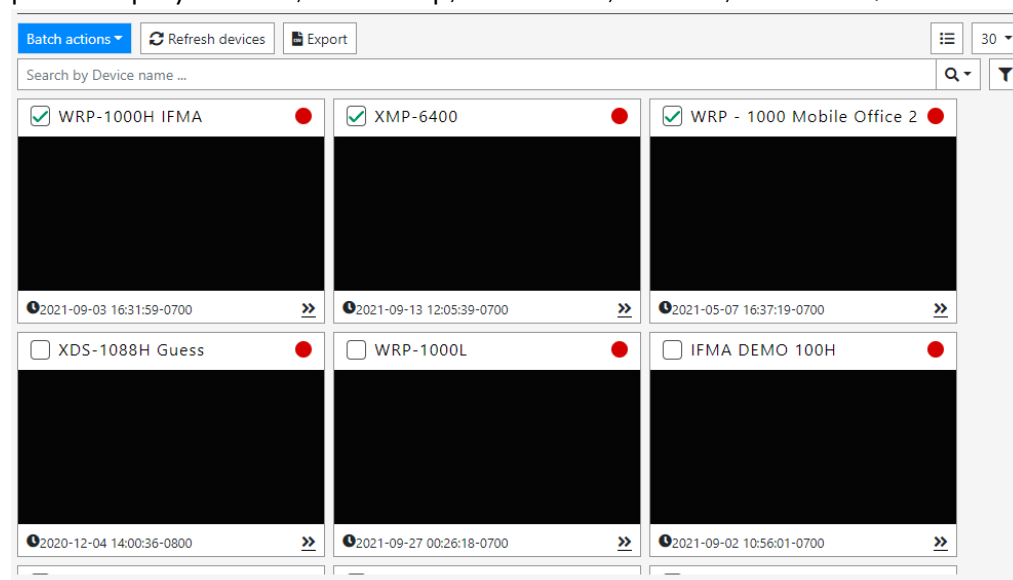
 **Export** - export device information to a .csv file.

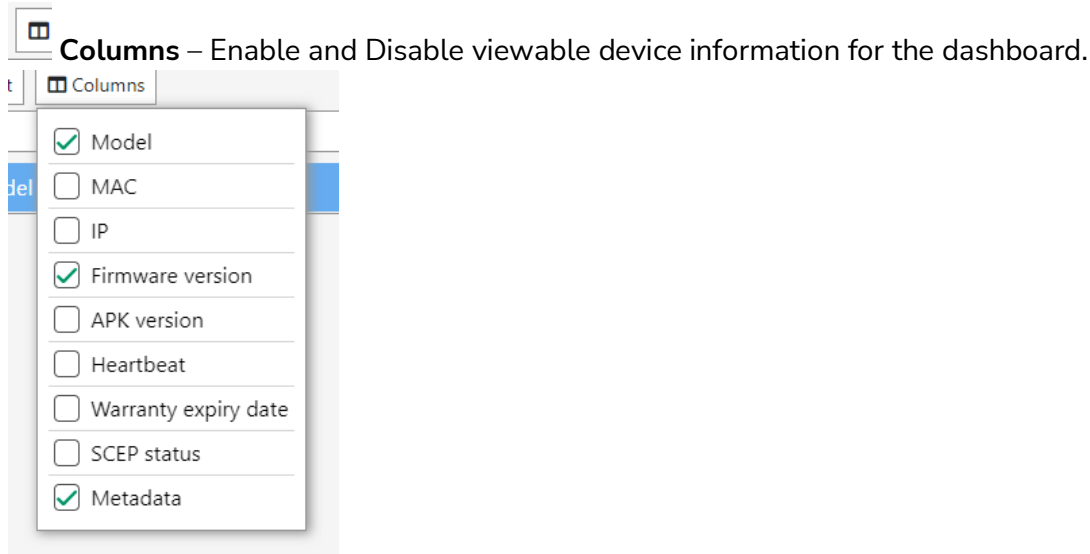
 **Table View** - the default view that will populate, it shows your homepage with all your players with detailed information regarding the configurations of the player.



<input type="checkbox"/>	Name	Model	Firmware version
<input type="checkbox"/>	WRP-1000H IFMA	WRP-1000-H	3.3.2-90
<input type="checkbox"/>	3188 QR Code	XDS-1078	2.2.5-120
<input type="checkbox"/>	XMP-6400	XMP-6400	1.2.93.621
<input type="checkbox"/>	WRP - 1000 Mobile Office 2	WRP-1000-H	3.2.1-50
<input type="checkbox"/>	XDS-1088H Guess	XDS-1088-A	2.2.2-71
<input type="checkbox"/>	WRP-1000L	WRP-1000-L	3.3.1-73
<input type="checkbox"/>	IFMA DEMO 100H	WRP-1000-H	3.3.1-88
<input type="checkbox"/>	XDS-1078 - Jovany	XDS-1078	1.2.95.647
<input type="checkbox"/>	XDS-1078	XDS-1078	2.2.3-112
<input type="checkbox"/>	XDS-1078-A9 Deloitte Demo	XDS-1078-A9	3.2.1-51

 **Grid View** – it shows your homepage with all your players in a **quick view** format that provides player mode, timestamp, screenshot, MAC ID, and online/offline status.





Metadata - IAdeaCare device list can display Metadata

- Metadata key must be “iadeacare:application-feedback” for the value to show in device table
- All customized metadata will only be shown in export csv with both key and key value

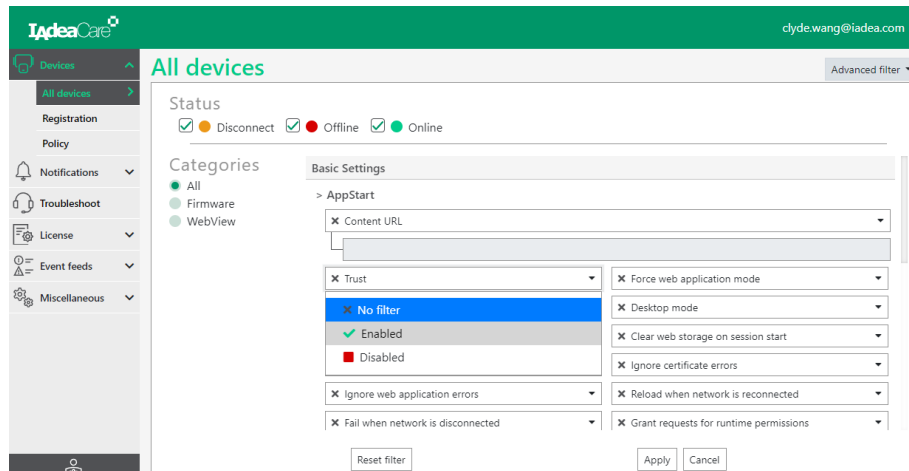


Advanced Filter settings allows user organize and filter player details by the selected settings. Users are able to

- Hide players by their online/offline/disconnect status.
- Configure which settings the filter will use to display desired devices.
 - All Categories include Basic Settings configurations and Schedule configurations.
 - Can also search by Player Model and Firmware Version.
 - Can also search by Player Model and WebView Version.
 - Each filter category has its own filter criteria.
 - No Filter - does not affect filter results.
 - Enabled – show list of devices with filter options enabled.
 - Disabled – show list of devices with filter options disabled.
 - Some fields such as Content URL allows to search the text included or excluded from the setting.



IAdeaCare User Manual



Note: In **Group View**, **Owner** and **Group** will not be available as filters.



Searching by **Name** allows the user to search through and filter their player list by the player's name or tag name.

Search by other Filters allows the user to search and filter players by **Player Name, Model Type, MAC ID address, IP address, or Owner.**


Device Details

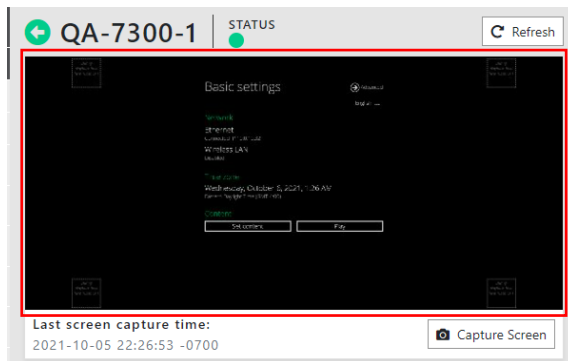
Each device on the home page will show its online/offline status along with the filtered details you have selected to display. To view a specific player individually, click on the player's name to enter the player dashboard.

On **Device page**, some more detail explanation of each device information field (e.g., Player name: user can give a friendlier name to the device. Default name is the primary MAC address.)

Screenshot

A screenshot is provided along with the last screen capture time of what the player is currently playing.

Press the camera icon  to refresh the screenshot (or new screenshot available automatically every 60 seconds).



General

It displays the **General Information** of the selected player.

General


Player name : IAdeaDoor-A (2cc548024861)
Model : XDS-1078
Primary MAC address : 2C:C5:48:02:48:61 (Ethernet)
Content URL : https://
Firmware version : 1.2.91.624
APK version : 1.1.96
Uptime : 00:38:23
Player local time : 2019-11-07 14:34:57 -0800
Heartbeat : 2019-11-07 14:52:04 -0800

Network

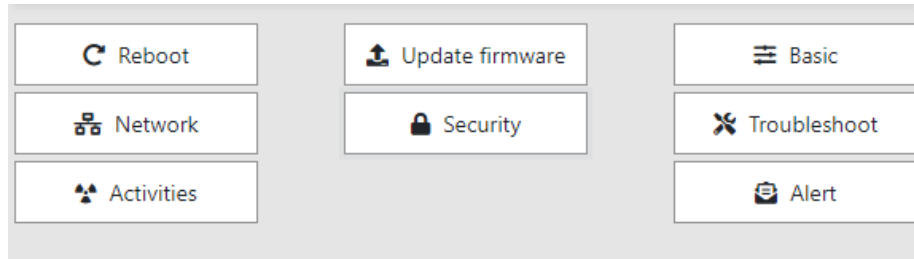
Displays the online/offline status of the player and if it is connected to the network via Ethernet or WIFI.

Provides all IP configuration settings for the player.

Network

Type : Ethernet 
IP address : 192.168.11.145
Gateway : 192.168.11.1
Netmask : 255.255.255.0
DNS 1 : 192.168.11.1
DNS 2 :

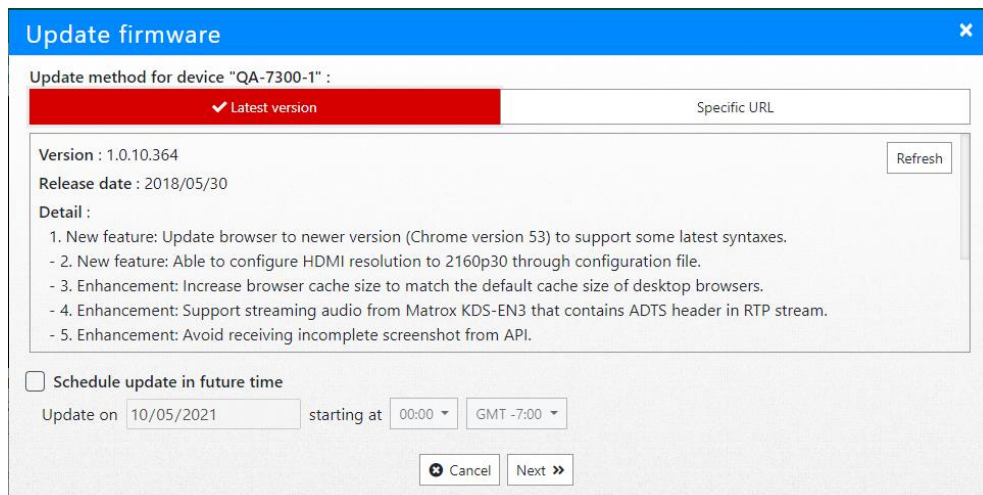
IAdeaCare Functions



Reboot - The reboot function allows the user to remotely reboot the player.

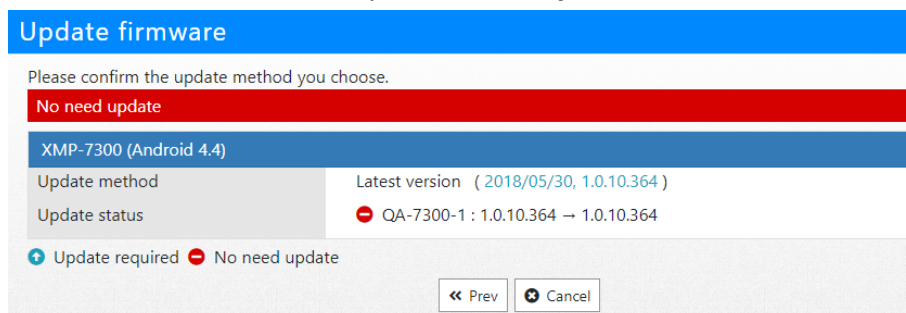
Update Firmware – This function allows the user to remotely update the firmware via IAdeaCare.

- **Latest Version** – Latest Version allows the user to compare the current version with the latest version on our servers. The user will have a chance to compare version and continue the update if you accept the changes.



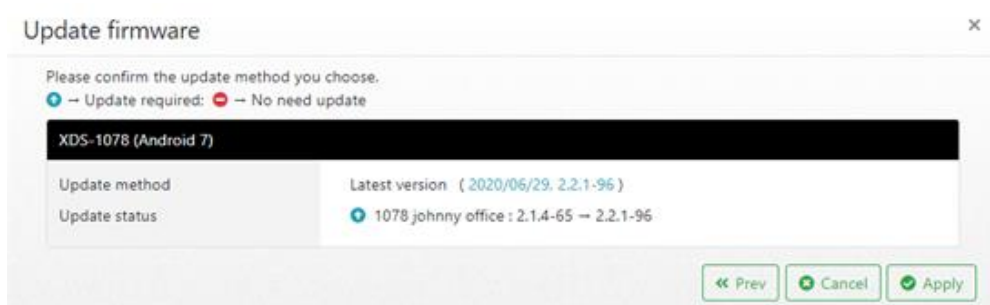
The 'Update firmware' dialog box shows the update method for device "QA-7300-1". The 'Latest version' method is selected. The current version is 1.0.10.364, released on 2018/05/30. The dialog lists five details: 1. New feature: Update browser to newer version (Chrome version 53) to support some latest syntaxes. 2. New feature: Able to configure HDMI resolution to 2160p30 through configuration file. 3. Enhancement: Increase browser cache size to match the default cache size of desktop browsers. 4. Enhancement: Support streaming audio from Matrox KDS-EN3 that contains ADTS header in RTP stream. 5. Enhancement: Avoid receiving incomplete screenshot from API. There is a 'Schedule update in future time' checkbox with fields for 'Update on' (10/05/2021) and 'starting at' (00:00 GMT -7:00). Buttons for 'Cancel' and 'Next >>' are at the bottom.

- The latest version will also provide new **updates / release notes**.



The 'Update firmware' dialog box shows the confirmation screen. It states 'Please confirm the update method you choose.' and 'No need update'. The device is XMP-7300 (Android 4.4). The update method is 'Latest version (2018/05/30, 1.0.10.364)'. The update status is 'QA-7300-1 : 1.0.10.364 → 1.0.10.364'. There is a legend for 'Update required' (blue circle with plus) and 'No need update' (red circle with minus). Buttons for '<< Prev' and 'Cancel' are at the bottom.

- If player is on the latest version, **no need update** will populate.



Update firmware

Please confirm the update method you choose.

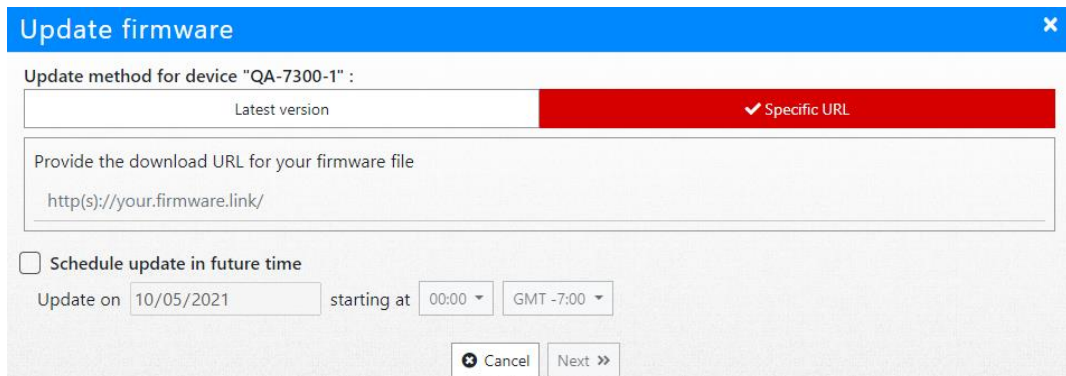
➕ → Update required: ➖ → No need update

XDS-1078 (Android 7)

Update method	Latest version (2020/06/29, 2.2.1-96)
Update status	➕ 1078 johnny office : 2.1.4-65 → 2.2.1-96

⏪ Prev ⚙ Cancel ⏩ Apply

- If player is not on latest version, the system will populate update needed along with current version with the latest version.
- **Specific URL** – This method allows you to update the player using your specific firmware by linking the URL for the firmware. This method is useful if the user wants to roll back firmware versions or has a customized firmware.



Update firmware

Update method for device "QA-7300-1" :

Latest version	✓ Specific URL
----------------	----------------

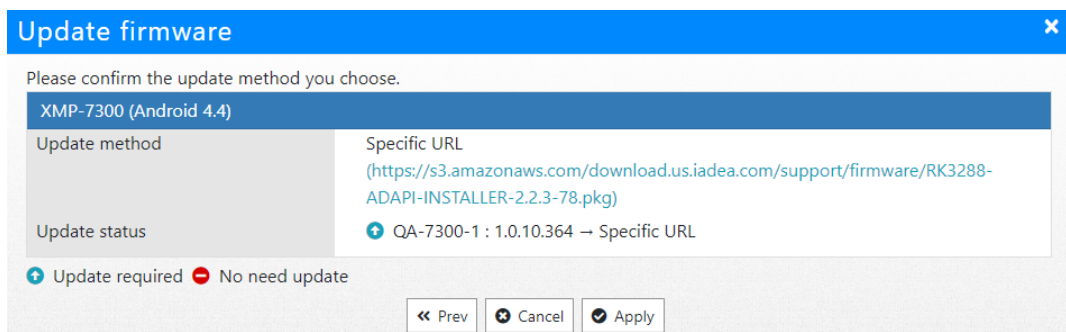
Provide the download URL for your firmware file

[http\(s\)://your.firmware.link/](http(s)://your.firmware.link/)

☐ Schedule update in future time

Update on starting at GMT -7:00

⚙ Cancel Next ⏩



Update firmware

Please confirm the update method you choose.

XMP-7300 (Android 4.4)

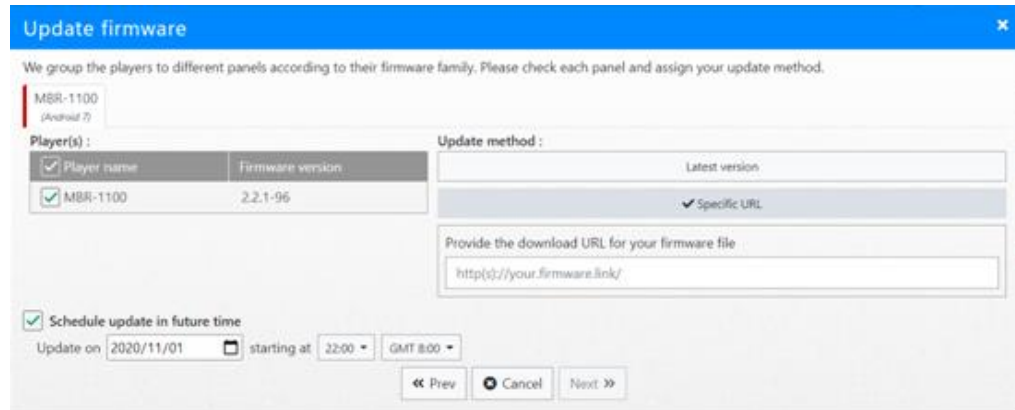
Update method	Specific URL (https://s3.amazonaws.com/download.us.iaidea.com/support/firmware/RK3288-ADAPI-INSTALLER-2.2.3-78.pkg)
Update status	➕ QA-7300-1 : 1.0.10.364 → Specific URL

➕ Update required ➖ No need update

⏪ Prev ⚙ Cancel ⏩ Apply

- **Schedule Firmware Updates** – User is able to schedule a future firmware update at a future date. Along with date, user will also be able to choose the update time and update method. The time will be scheduled on the user's

computer's time zone.



Update firmware

We group the players to different panels according to their firmware family. Please check each panel and assign your update method.

Player(s):

Player name	Firmware version
<input checked="" type="checkbox"/> MBR-1100	2.2.1-96

Update method:

☐ Latest version

☒ Specific URL

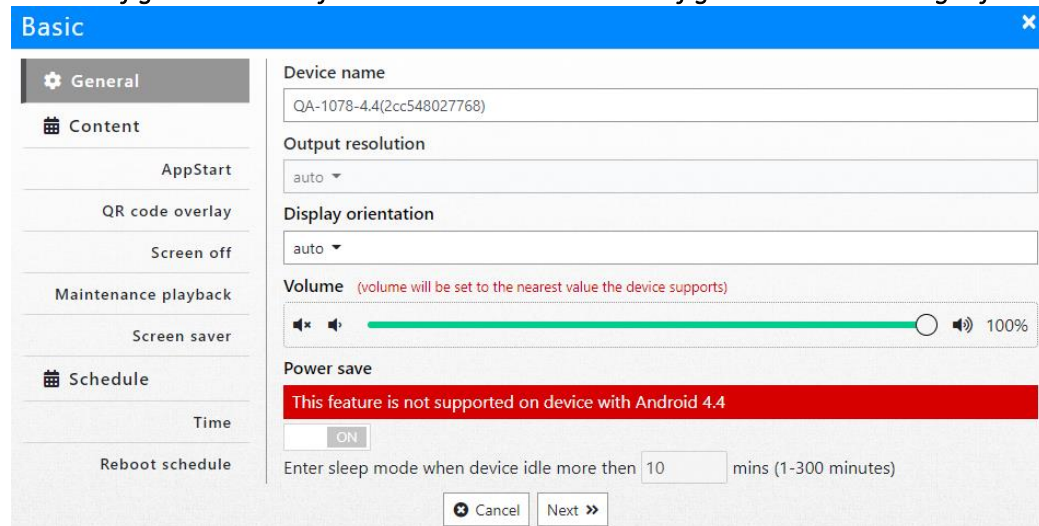
Provide the download URL for your firmware file

☒ Schedule update in future time

Update on 2020/11/01 starting at 22:00 GMT 8:00

« Prev Cancel Next »

Basic Configuration – This function allows the user to configure the Basic Settings of the player.



Basic

General

Content

AppStart

QR code overlay

Screen off

Maintenance playback

Screen saver

Schedule

Time

Reboot schedule

Device name

QA-1078-4.4(2cc548027768)

Output resolution

auto

Display orientation

auto

Volume (volume will be set to the nearest value the device supports)

100%

Power save

This feature is not supported on device with Android 4.4

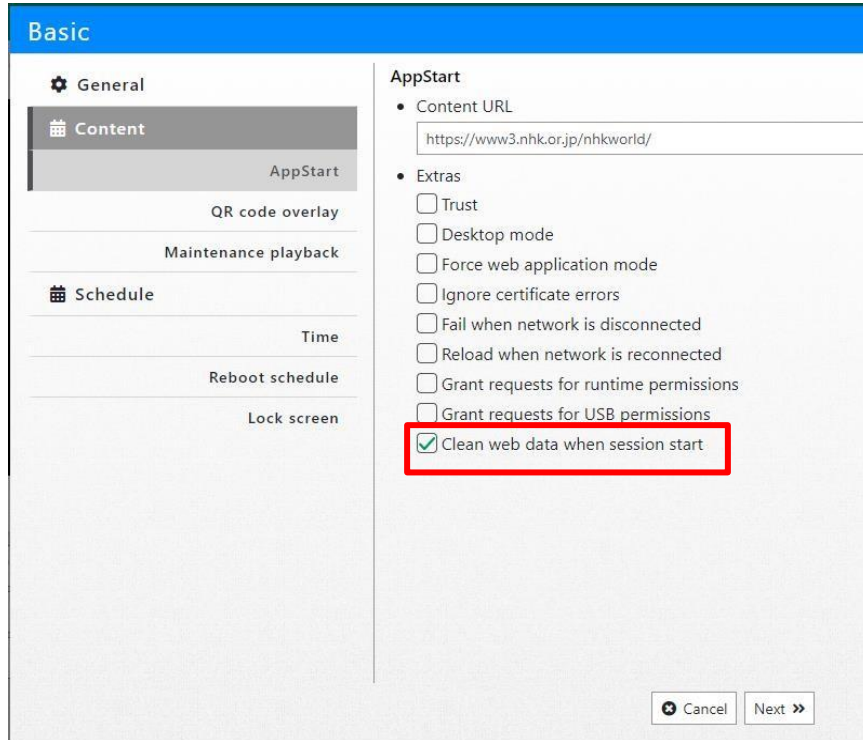
ON

Enter sleep mode when device idle more than 10 mins (1-300 minutes)

Cancel Next »

- **General:**
 - **Device Name (Tag Name)** – Player name within the Basic Configuration is the name given to the player when it is first paired. This name is considered a tag name or a method to filter or group the players to make it easier to organize.
 - **Output resolution** – Select your device output resolution. Can select Auto or a Static Resolution (1080p)
 - **Display orientation** – Select your device display orientation. Can select Auto or Fixed (0,90,180,270)
 - **Volume** – Set the desired volume for the device if playing content with sound.
 - **Power saves** – This feature allows the device to enter Sleep mode if no content is playing after the device is idle for more than the set time.

- Content
- Appstart



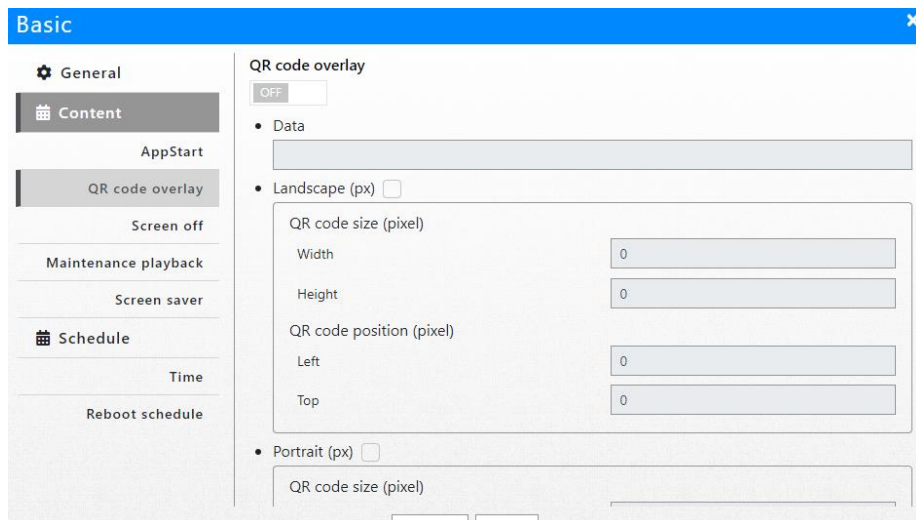
Content URL – The feature allows the user to enter a Web URL to play a website or a HTML5 based software.

****Content URL Advanced options** is used for 3rd-party App configuration only.

Advanced:

- **Trust:** Switch to Enabled to set by-pass authentication verification for REST API calls in HTML application which must be launched by AppStart.
- **Force web application mode:** Switch to Enabled to disable HTTP status code verification to bypass some cookie related issues. It will ignore HTTP ERROR STATUS.
- **Desktop mode:** Switch to Enabled to force player to load content in Desktop mode instead of Tablet mode. Please note: not all the contents are created for Desktop mode, please ask your content provider for details.
- **Ignore certificate errors:** Switch to Enabled to ignore certificate errors to allow visiting Web Pages that do not have valid certificate. It will ignore UNTRUSTED ERROR. When disabled; if there is a certificate on HTML5 content, it will cause a playback error.
- **Trigger failover when network is disconnected:** Switch to Enabled to load failover content when network is disconnected.

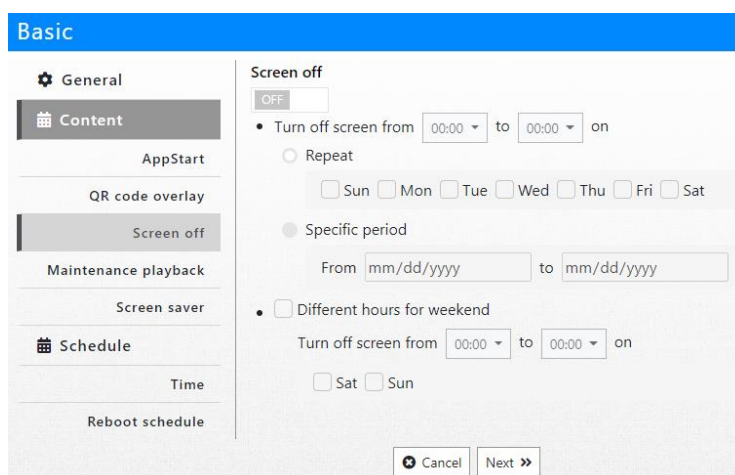
- **Reload when network is reconnected:** Switch to Enabled to reload web page as soon as network connection becomes available.
- **Clean web data when session start:** Device will start the webpage from a clean slate, similar to incognito mode.
- **Overlay (QR Code)** – User may now overlay a QR code on your device. Provide QR Link and configure your QR code placement.



QR can be data to be converted to a QR code or an URL to QR code.

- **Screen Off:** Schedule the time period for the screen to turn off. Default screen off is set to be repeated daily. User can configure specific days of the week, screen off for a specific period, and different screen off schedule for the weekend.

Note: **Screen Off Schedule** has highest priority over other content related function such as Content Source URL and Maintenance Mode.

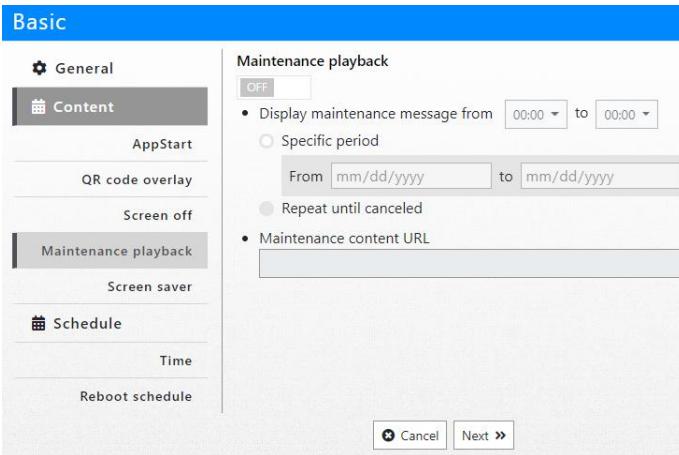


Devices that are not on a compatible firmware will get below message.

Screen off

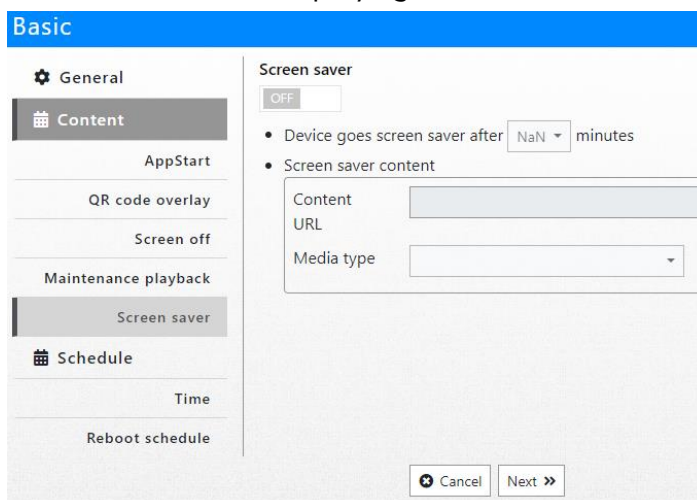
This feature is not supported on the device. Please confirm if your firmware version is up-to-date.

- **Maintenance Mode:** User can schedule to display a **maintenance message** set for a specific time period or display until manually cancelled. The **Maintenance content URL** can be set to an image with a direct URL or an html webpage.



Note: Both **Screen off** and **Maintenance Mode** only work when Content is playing. Will not work if **AutoStart** play is cancelled and player remains on **Basic Settings Page**.

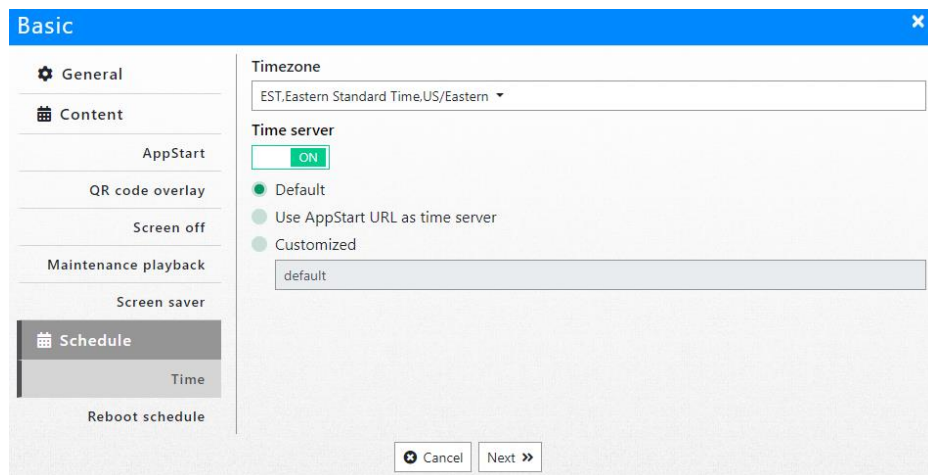
- **Screen Saver:** User can schedule a screen saver to display if device is idle for a set amount of time not playing content.



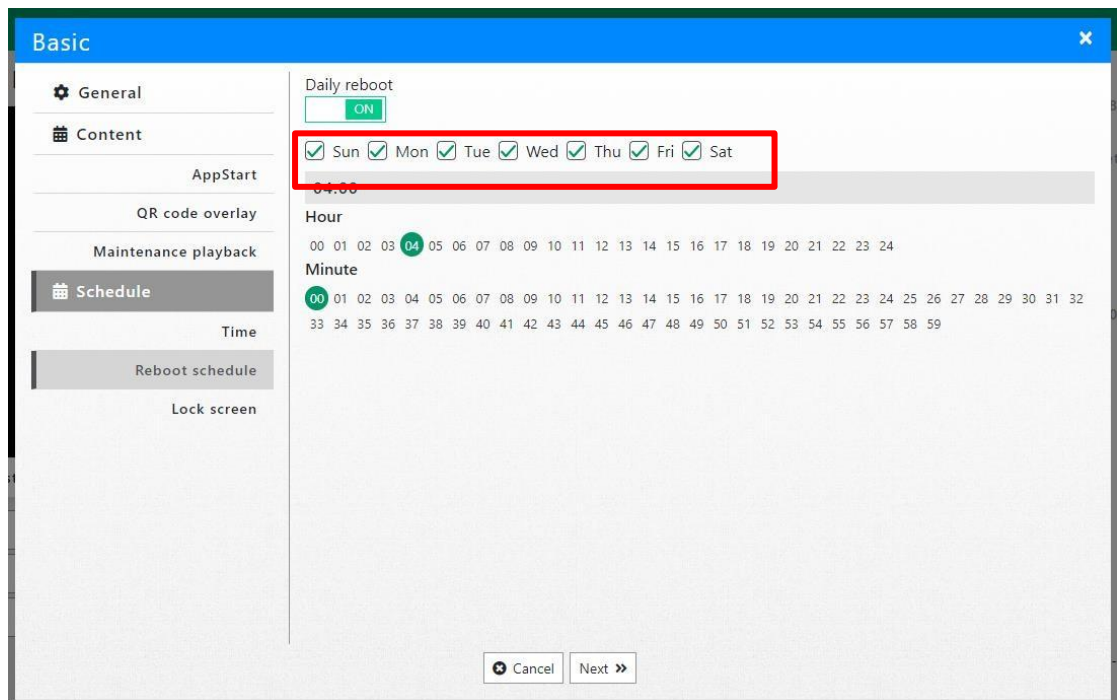
Media Type: .jpg or .png

- **Schedule:**

- **Time Zone:** Select the Time Zone closest to the area where the player is operating.
- **Timer Server:** Enable Time server to sync the player's clock with the server clock.
 - *Default: ntp.pool.org*
 - *Use AppStart: Syncs the player's clock with the server's clock that the URL (Content URL or AppStart setting) is hosted on*



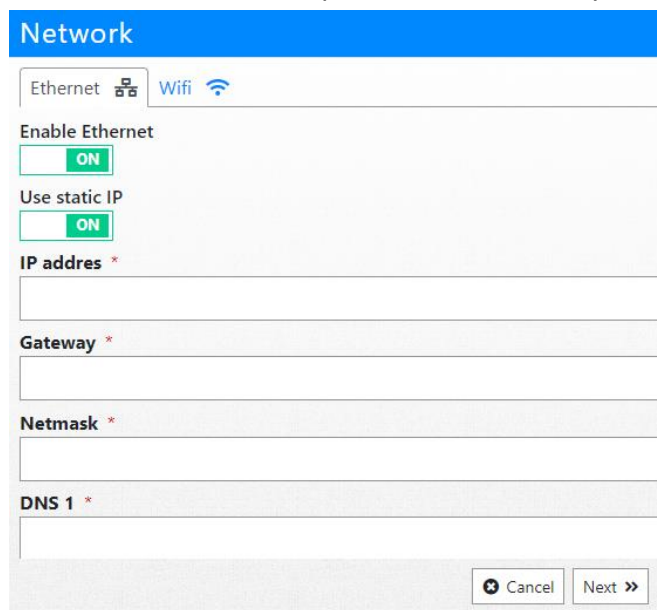
- **Enable daily reboot:** Enable or disable the daily reboot of the player. User can also configure the reboot time.



- Users can now choose which day of week they would like device to reboot itself.

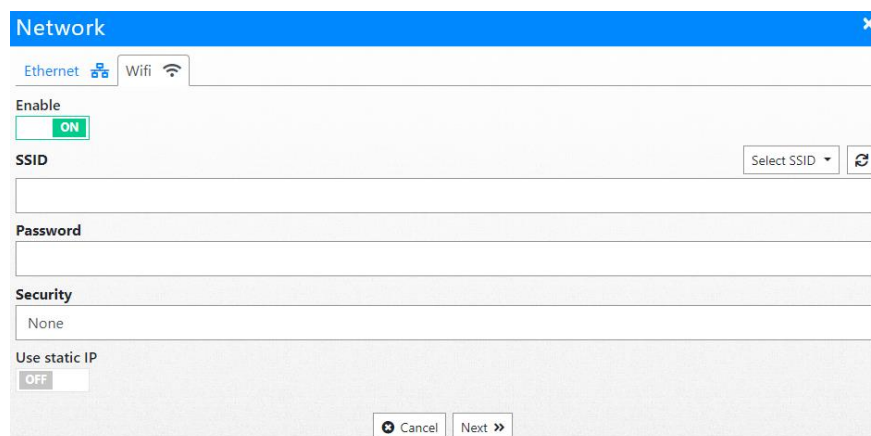
Network Configuration – This function allows the user to configure the network settings of the player.
Note: If player is disconnected from the network remotely, User will need to physically enable Wi-Fi or Ethernet on the player to reconnect.

- **Ethernet** – Configure the network settings via Ethernet.
 Enable Static IP to set up Static IP address by filling out all parameters.



The screenshot shows the 'Network' configuration window with the 'Ethernet' tab selected. The 'Enable Ethernet' toggle is set to 'ON'. The 'Use static IP' toggle is also set to 'ON'. Below these, there are input fields for 'IP address', 'Gateway', 'Netmask', and 'DNS 1', each followed by an asterisk indicating they are required. At the bottom right, there are 'Cancel' and 'Next >>' buttons.

- **Wi-Fi** - Configure the network settings via Wi-Fi.
 - Manually enter SSID or choose SSID from drop down menu.
 Proceed with password and Wi-Fi security type.
 - Enable Static IP to set up Static IP address by filling out all parameters.



The screenshot shows the 'Network' configuration window with the 'Wifi' tab selected. The 'Enable' toggle is set to 'ON'. There is a 'Select SSID' dropdown menu with a refresh icon. Below this are input fields for 'Password' and 'Security' (currently set to 'None'). At the bottom, the 'Use static IP' toggle is set to 'OFF'. At the bottom right, there are 'Cancel' and 'Next >>' buttons.



Security – Enable a password to access the device. For OTP (One-Time Password) See Policy.

Update security password

New password

Device name	MAC
TPE-WRP-1000-A	2C:C5:48:05:BE:A6

Cancel

Next >>

Troubleshoot - Remotely collect a DEBUG via IAdeaCare. The system will collect the DEBUG log and allow you to send to 5 recipients or attach the DEBUG log along with your support ticket and automatically email to IAdea Support.

Troubleshoot

Obtain device logs

Contact IAdea support

Cancel

Next >>

- **Obtain device logs:** This option will allow you to send the DEBUG logs to 5 different recipients via email.

Troubleshoot

Obtain device logs

1. Recipients (Up to 5 recipients)

+ Add recipient

Recipient #1

qa-admin@1adea.com

Recipient #2

Recipient #3

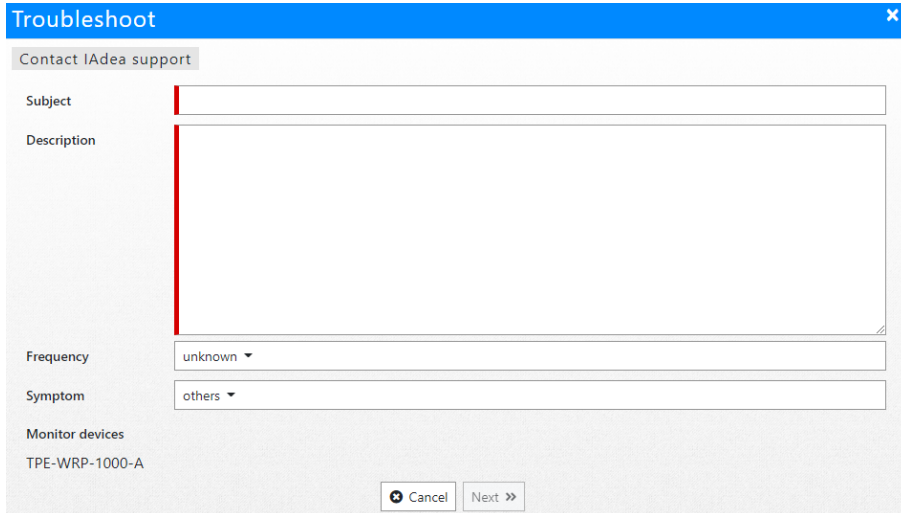
2. Monitor devices

TPE-WRP-1000-A

Cancel

Next >>

- **Contact IAdea support:** This option will collect the DEBUG log and create a support ticket and send automatically to IAdea Support.



Troubleshoot [X]

Contact IAdea support

Subject [Red line]

Description [Red line]

Frequency unknown ▾

Symptom others ▾

Monitor devices
TPE-WRP-1000-A

[Cancel] [Next >>]

- **Subject** – Enter quick overview of support needed for troubleshooting ticket.
- **Issue Description** – Provide more in-depth description of the issue.
- **Symptom** – Choose closest symptom from the drop-down menu.
- **Frequency** – Choose how frequent the issue occurs.



Activities – History log of all actions/activities performed on the player.

Activities ×			
Activity	Status	Issue date	Finish date
Reboot	Finish	2021-10-05 02:36:43	2021-10-05 02:38:44
Reload license	Finish	2021-10-04 23:00:14	2021-10-04 23:00:31
Reboot	Finish	2021-10-01 07:05:49	2021-10-01 07:08:18
Reboot	Finish	2021-10-01 06:05:09	2021-10-01 06:06:40
Reboot	Finish	2021-10-01 05:59:39	2021-10-01 06:01:20
Reboot	Finish	2021-10-01 05:56:59	2021-10-01 05:58:51
Reboot	Finish	2021-09-30 23:33:54	2021-09-30 23:35:35
Reboot	Finish	2021-09-30 23:31:49	2021-09-30 23:33:25
Basic configuration	Finish	2021-09-30 21:06:16	2021-09-30 21:06:24
Basic configuration	Finish	2021-09-30 21:03:46	2021-09-30 21:04:24
Basic configuration	Finish	2021-09-30 20:09:46	2021-09-30 20:10:24
Last activity tracking time : 2021-10-05 23:01:57			
Close Refresh			

Click on the Activity to expand detailed information for each activity.

Activity	Status	Issue date	Finish date
Reboot	Finish	2021-10-05 02:36:43	2021-10-05 02:38:44
Reload license			
Activity status : Finish			
Activity ID : 1633413614197-329d4754-21c4-4308-b9c9-d8a2a4b758b0			
Issue date : 2021-10-04 23:00:14			
Start date : 2021-10-04 23:00:31			
Finish date : 2021-10-04 23:00:31			
Reboot	Finish	2021-10-01 07:05:49	2021-10-01 07:08:18

Queued Tasks:

Activity	Status	Issue date	Finish date
Reboot			
Activity status : Pending			
Activity ID : 1633500202268-07536973-1958-4cf1-9ec9-343e839510c9			
Issue date : 2021-10-05 23:03:22			
Start date :			
Finish date :			
Reboot	Finish	2021-10-05 02:36:43	2021-10-05 02:38:44
Reload license	Finish	2021-10-04 23:00:14	2021-10-04 23:00:31

The system will show when activities are pending in queue or in progress of being updated. The log will also record the time stamp for when each activity was issued and when it finished.

Alert

[See 4.3 Alert Settings](#)

- **Share Player** – Share the ability to monitor and configure players with other IAdeaCare users.



Share device

Add collaborators and set their authorities for XDS-1078 Tech Room

Enter shared account...

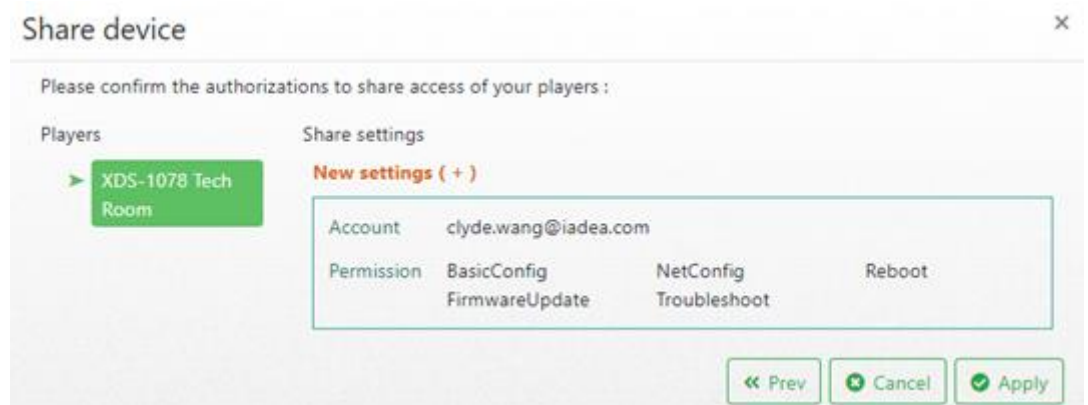
Editor Viewer

Basic config Network config Reboot

Firmware update Troubleshoot

Cancel Next >>

- **Editor** – Enables Full Access to Monitor and Configure Settings.
- **Viewer** – Allows Monitor Access Only. No Ability to Configure Settings.



Share device

Please confirm the authorizations to share access of your players :

Players

XDS-1078 Tech Room

Share settings

New settings (+)

Account clyde.wang@iadea.com

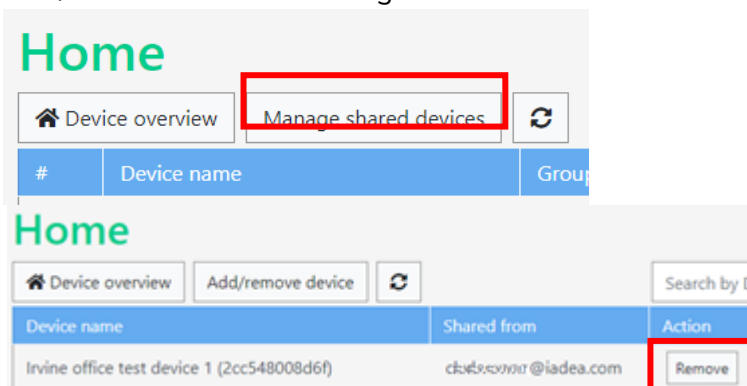
Permission BasicConfig NetConfig Reboot

FirmwareUpdate Troubleshoot

<< Prev Cancel Apply

Confirm authorized accounts and configurations to be shared.

To remove shared devices from account. From the Home Page > Select Add/Remove Device > Manage Shared Devices > Remove.



Home

Device overview Manage shared devices

#	Device name	Group
	Irvine office test device 1 (2cc548008d6f)	ckb@iadea.com

Home

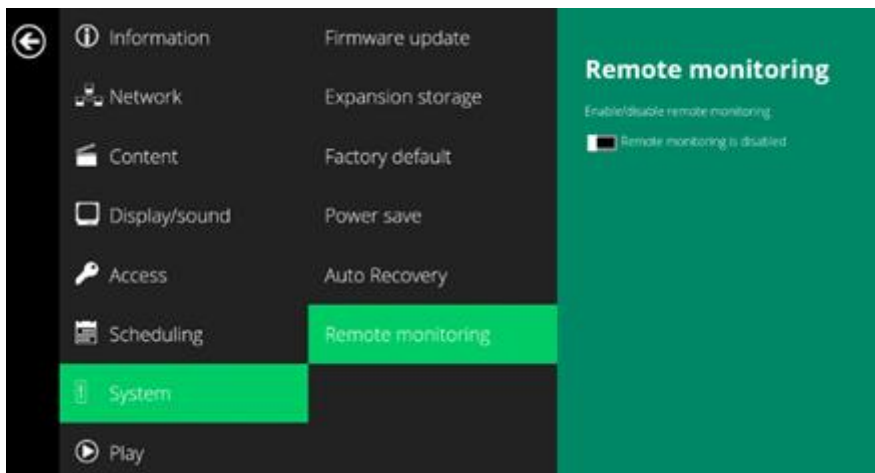
Device overview Add/remove device

Device name	Shared from	Action
Irvine office test device 1 (2cc548008d6f)	ckb@iadea.com	Remove

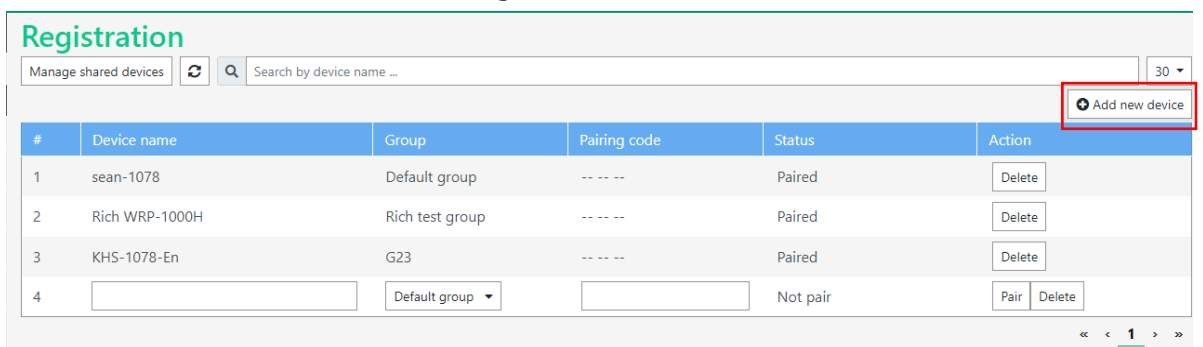
Registration

Add/Remove Player

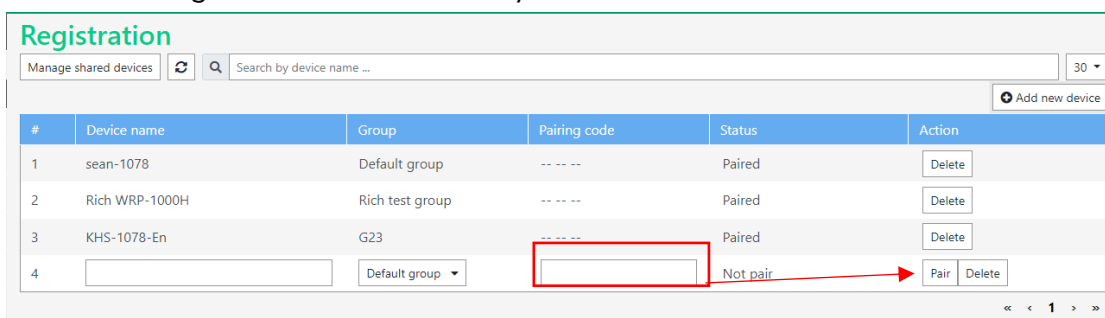
1. From the **Basic Setting** menu on your IAdea device, click on **Advanced Setting** > **System** > **Remote Monitoring**.



2. Toggle to enable **Remote Monitoring**.
3. The **Pairing Code** will populate. This code will be used to pair the player to your account.
4. In **IAdeaCare**, Click on **Devices** -> **Registration** -> **Add new device**.

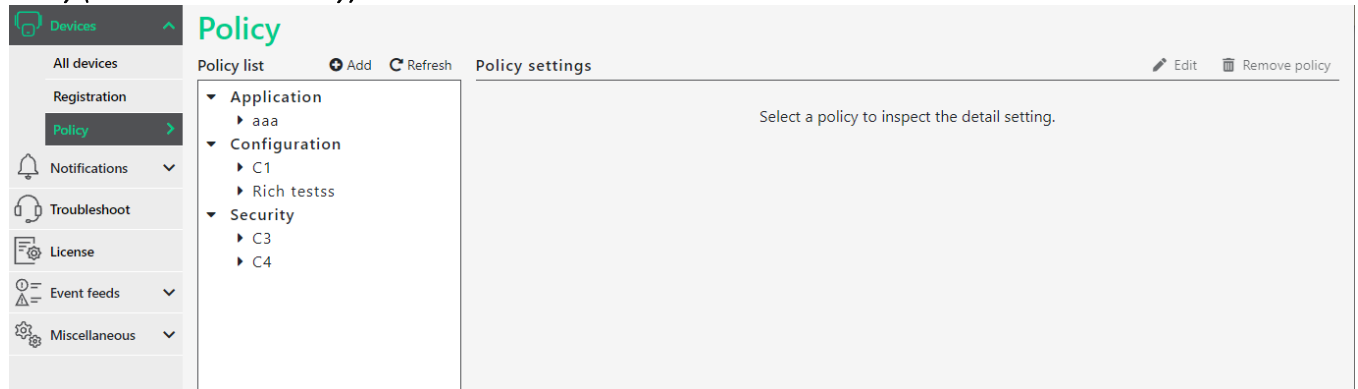


5. Enter in Pairing Code for the select Player and click Pair.



Policy

Policy (Premium License Only)

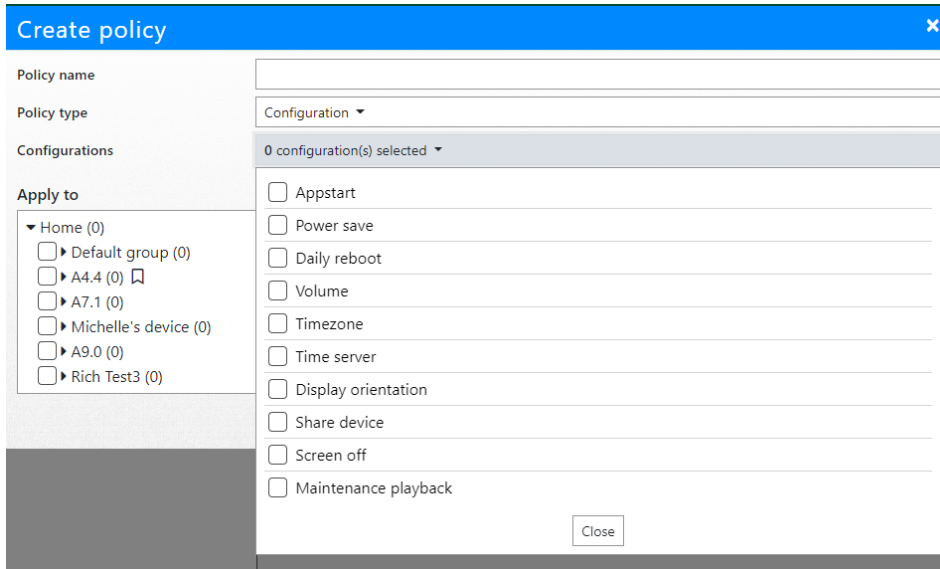


Policies can be assigned to existing groups in this page. Users are able to assign multiple policies of different types but only one policy of the same type to each group. Once a policy is deleted, the policy will be deleted from all assigned groups as well. The policy settings on the player's will not be removed.

If a device was not set up with a group configuration policy during set-up, and the policy was created and attached later on, the policy settings will re-sync to the device within 30 minutes of the device being online.

Create Policy

Configuration Policy



Create policy [X]

Policy name:

Policy type: Configuration ▾

Configurations: 0 configuration(s) selected ▾

Apply to:

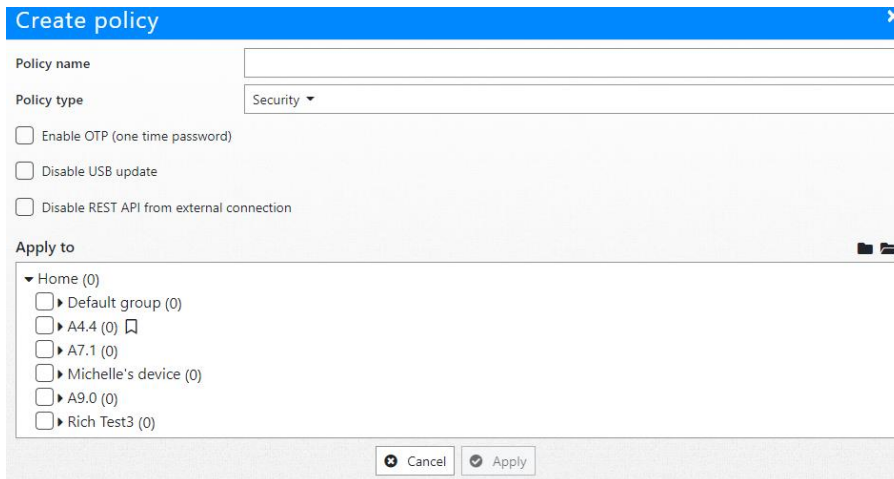
- ▼ Home (0)
 - ☐ Default group (0)
 - ☐ A4.4 (0) [🔖]
 - ☐ A7.1 (0)
 - ☐ Michelle's device (0)
 - ☐ A9.0 (0)
 - ☐ Rich Test3 (0)

☐ Appstart
☐ Power save
☐ Daily reboot
☐ Volume
☐ Timezone
☐ Time server
☐ Display orientation
☐ Share device
☐ Screen off
☐ Maintenance playback

[Close]

Select all device configuration settings that you would like to configure. All devices set to this policy group will inherit all configuration settings.

Security Policy – Create



Create policy [X]

Policy name:

Policy type: Security ▾

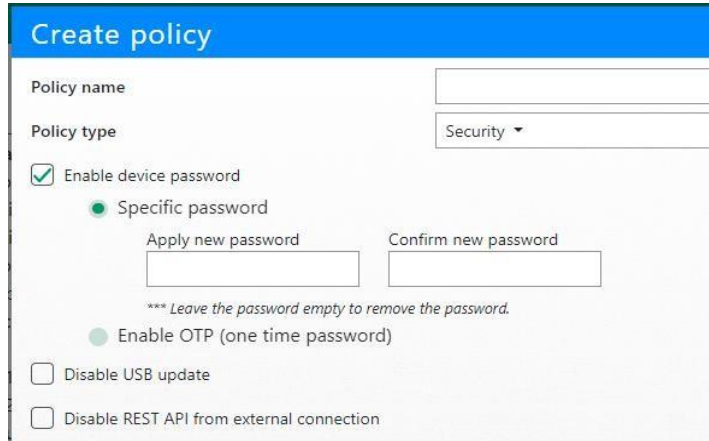
☐ Enable OTP (one time password)
☐ Disable USB update
☐ Disable REST API from external connection

Apply to:

- ▼ Home (0)
 - ☐ Default group (0)
 - ☐ A4.4 (0) [🔖]
 - ☐ A7.1 (0)
 - ☐ Michelle's device (0)
 - ☐ A9.0 (0)
 - ☐ Rich Test3 (0)

[Cancel] [Apply]

- **Specific Password** - Users can create policy to reinforce new password to apply to devices that are newly added to the policy



Create policy

Policy name

Policy type

☒ Enable device password

- ☒ Specific password

Apply new password
 Confirm new password

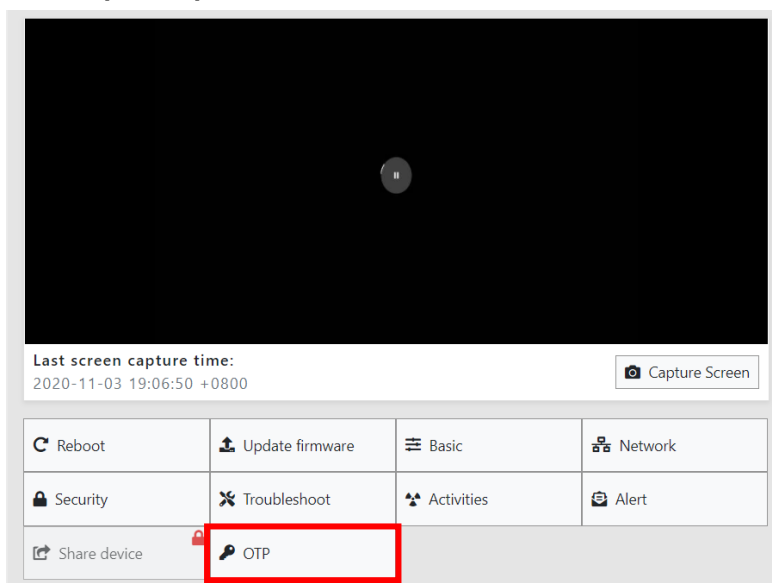
*** Leave the password empty to remove the password.
- ☐ Enable OTP (one time password)

☐ Disable USB update

☐ Disable REST API from external connection

- **OTP** – Time based password that will be changed every day by device.
- **Disable USB update / REST API** – Disable external access to the device.

Security Policy – Get Password





When **OTP** is enabled, user will need to log into Device Dashboard in **IAdeaCare** to receive your **OTP**.

User can request **Today**'s password or a password from a past date. The date for a past password must be manually chosen from the dropdown calendar.

Every password will be available for **30 days**. The player will have a maximum of 30 passwords.

Policy – Change in Device Dashboard Page

General	
Device name	MBR-1100-Nov-release (2cc5480190aa)
Model	MBR-1100 Rev1.1
Primary MAC address	2C:C5:48:01:90:AA (Ethernet)
Content URL	https://bcbsnc.avuity.com/vuspace/booking
Firmware version	2.2.2-108
APK version	1.1.113
Uptime	05:02:45
Device local time	2020-11-12 17:27:58 +0800
Heartbeat	2020-11-12 17:37:50 +0800
Warranty expiry date	
Network	
Type	Ethernet
IP	10.0.10.120
Gateway	10.0.10.254
Netmask	255.255.255.0
DNS 1	168.95.1.1
DNS 2	8.8.8.8
Policy	
Group configuration	Maintenance (TPE) syncd
Security	Password (TPE) syncd

Lists out which policies are currently assigned to the device. If the device inherited a group policy, the group name will appear in parentheses. Clicking on the Policy Name will link the user to the Policy Page.

- Synced Status: Policy Setting is synced to device.
- Pending Status: Device is waiting to sync with server (30 Minute Maximum)

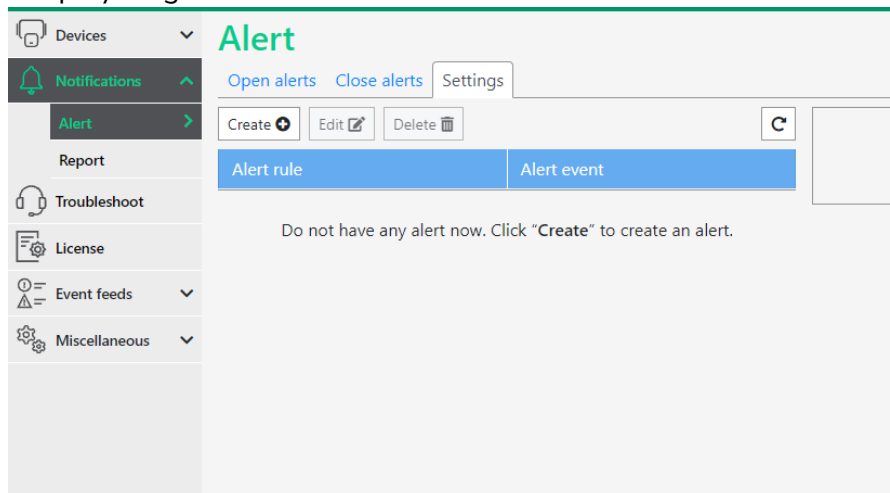
If device does not have a Premium License, it will show **Policy (Nor applicable)**.

Policy (Not applicable)

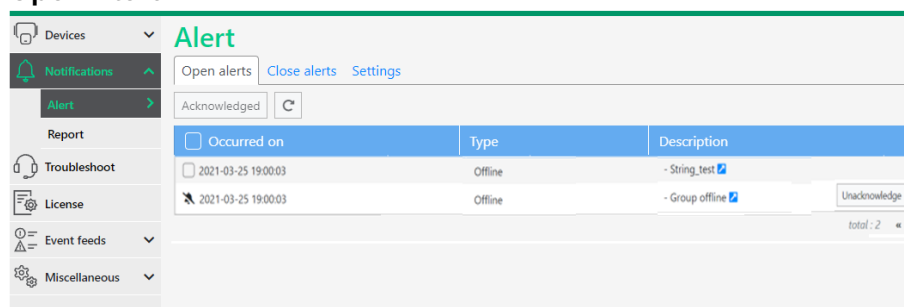
4.3 Notifications

Alert Setting

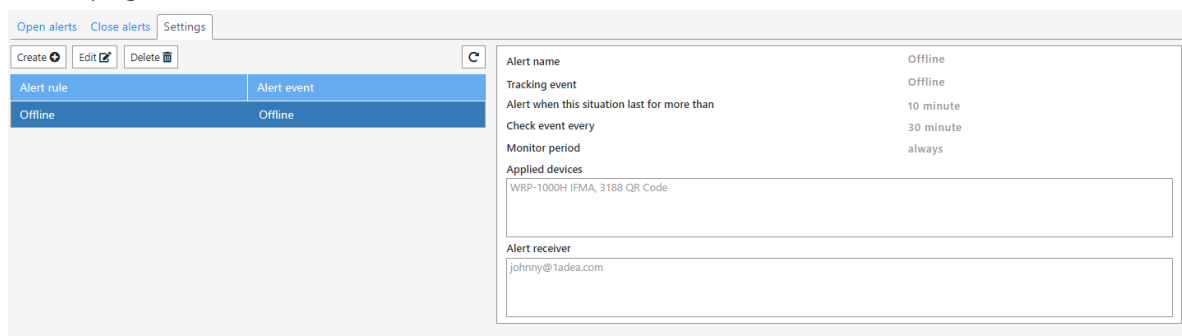
Alert Settings allow the user to create offline alerts to be sent to the account email when the players go offline within the created rules.



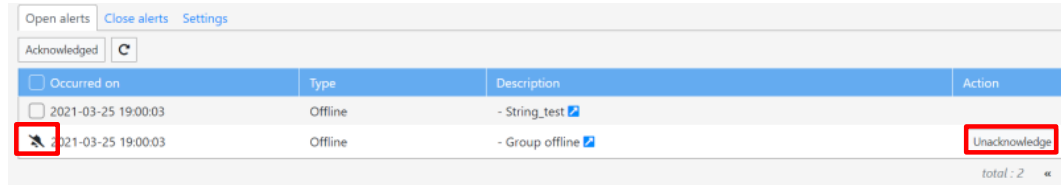
Open Alert



- When an Offline or Device Status alert type occurs, the system will create a new Open alert.
- User is able to acknowledge the alert listed in the table.
- Each alert will have an alert link in Description that will bring you to the alert's setting detail page when clicked.



- When alert is acknowledged, the alert will also show the 'Unacknowledge' button in the action column if the user wants to keep the alert open.

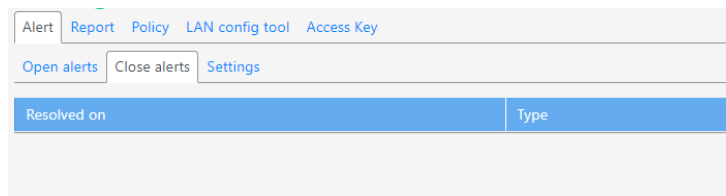


Occurred on	Type	Description	Action
2021-03-25 19:00:03	Offline	- String_test	
2021-03-25 19:00:03	Offline	- Group offline	Unacknowledge

- When the alert has been triggered in the Open Alert but deleted in the settings, the alert will be moved from Open Alert to Close Alerts.
- When the alert has been acknowledged, the server will NOT send the alert email.

Close Alert

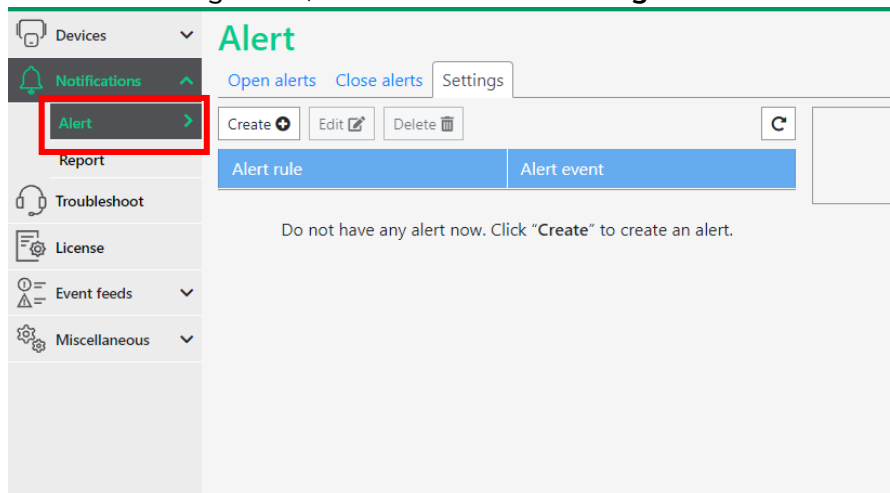
- Once an Open alert has been resolved, the alert will be moved to the Close Alert tab.



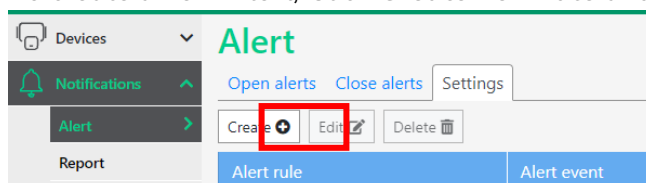
Resolved on	Type
-------------	------

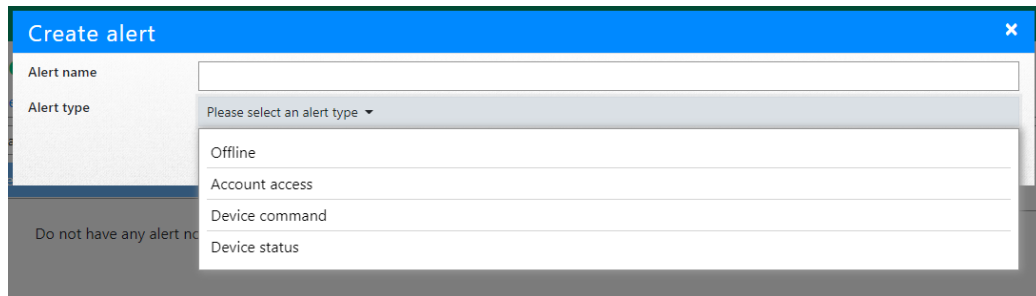
Create Alert

To start creating alerts, click on the **Alert setting** Tab.



To create a new Alert, Click **Create new rule** and select the Alert type.





Create alert

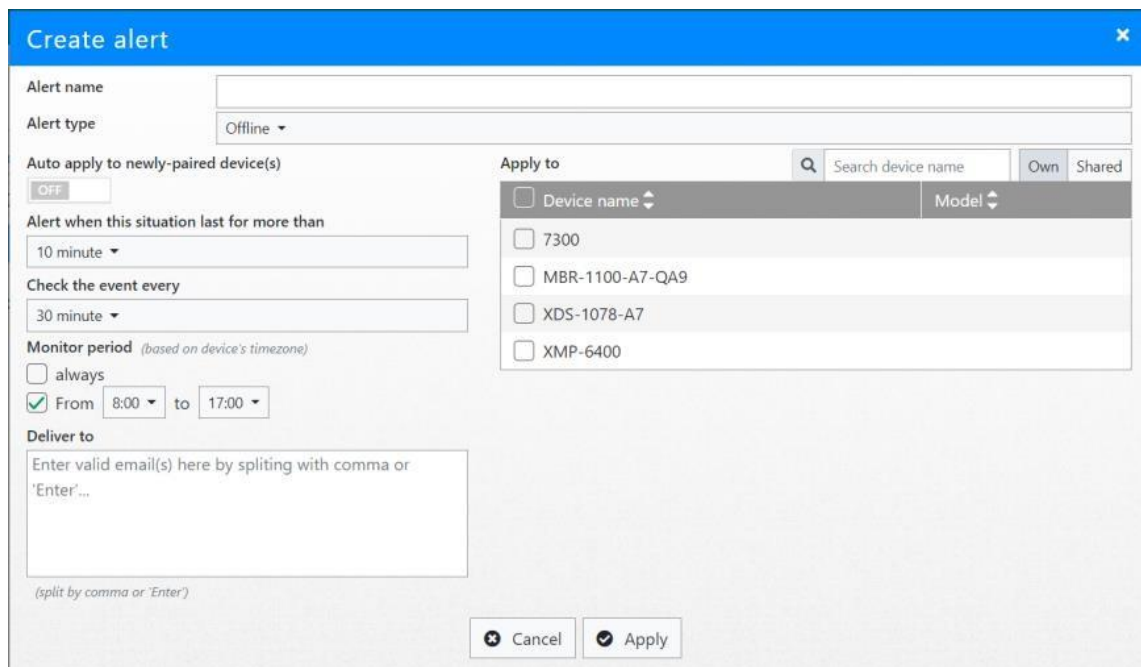
Alert name:

Alert type: Please select an alert type ▼

- Offline
- Account access
- Device command
- Device status

Do not have any alert no

Create - Offline



Create alert

Alert name:

Alert type: Offline ▼

Auto apply to newly-paired device(s): OFF

Alert when this situation last for more than: 10 minute ▼

Check the event every: 30 minute ▼

Monitor period (based on device's timezone):

☐ always

☒ From 8:00 ▼ to 17:00 ▼

Deliver to:

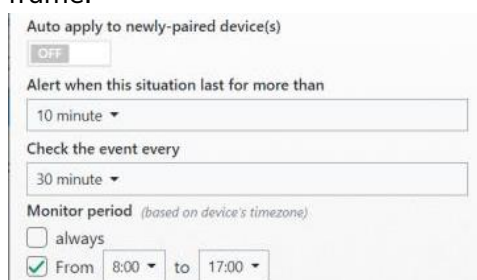
(split by comma or 'Enter')

Apply to: Search device name Own Shared

Device name	Model
<input type="checkbox"/> 7300	
<input type="checkbox"/> MBR-1100-A7-QA9	
<input type="checkbox"/> XDS-1078-A7	
<input type="checkbox"/> XMP-6400	

Cancel Apply

1. **Alert Rule** – You can name your alert rule here.
2. Pick your criteria to recognize the behaviour and the frequency of its reporting. You can choose to enable this alert for all newly-paired players to the account.
3. Decide how long the player must remain offline before the alert rule is enacted.
4. Decide how often to the system will check if the player is offline.
5. Configure the monitoring period. User can set for 24 hours a day or a specific time frame.



Auto apply to newly-paired device(s): OFF

Alert when this situation last for more than: 10 minute ▼

Check the event every: 30 minute ▼

Monitor period (based on device's timezone):

☐ always

☒ From 8:00 ▼ to 17:00 ▼

6. **Deliver to** allows the user to list which email accounts to send the offline email alerts to.



Note: Add 'self account' will add the email address for the IAdeaCare account that is currently logged in.

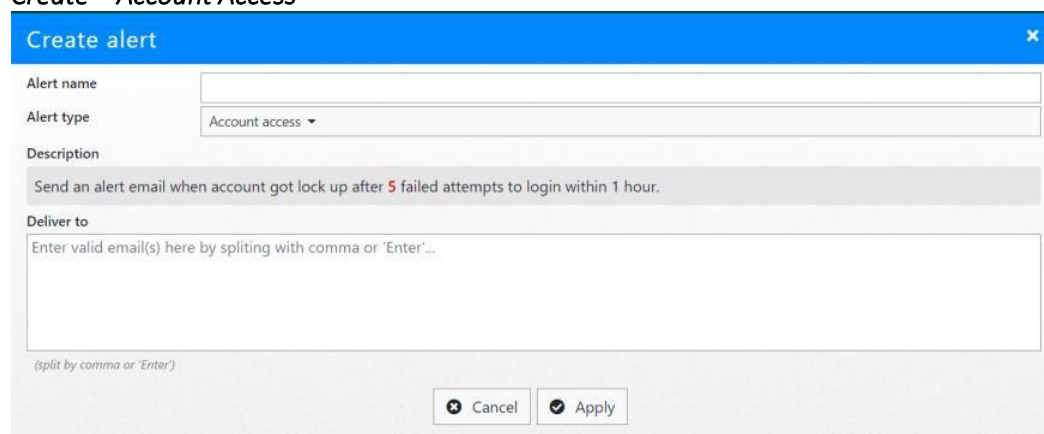
7. Select the players which will adhere to the alert rule.



- **Own** – The current IAdeaCare account is the admin/owner of these players.
- **Shared** – The players in this list are being shared by another owner to be monitored.

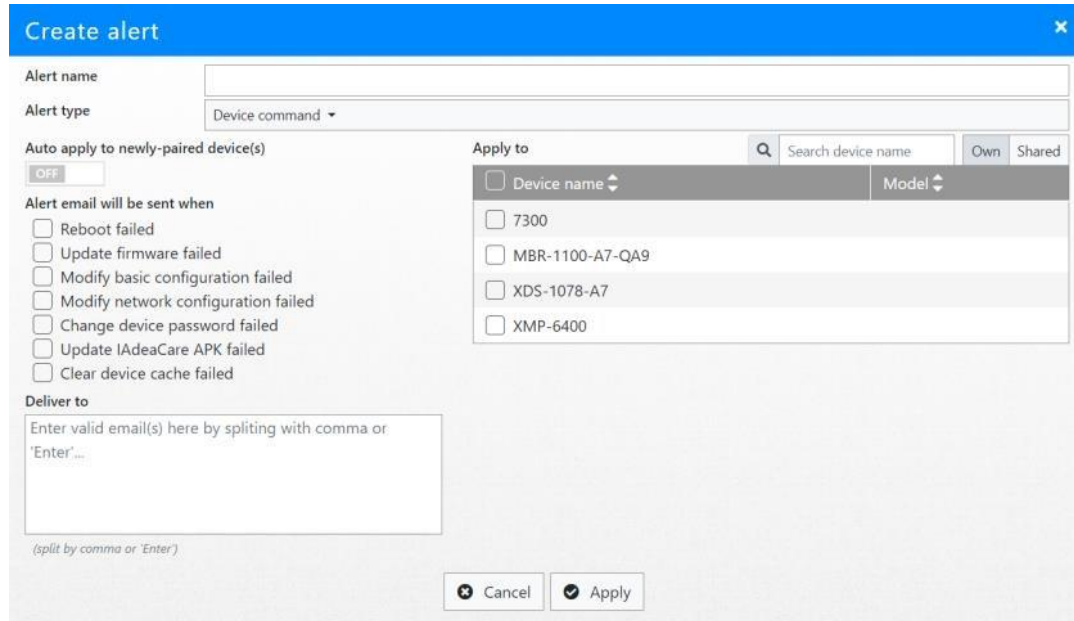
If **Auto apply to newly paired players** is checked, the rule will automatically bind all newly paired players.

Create – Account Access

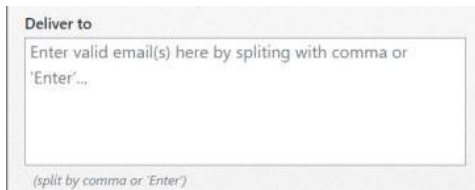


1. Name the Account Access Alert.
2. Fill out the Deliver to with the email addresses you would like to alert in the case the account has 5 failed login attempts within 1 hour.

Create – Device Command



1. **Alert Name** – You can name your alert rule here.
2. Select your device command failure type for the system to alert.
3. **Deliver to** allows the user to list which email accounts to send the offline email alerts to.



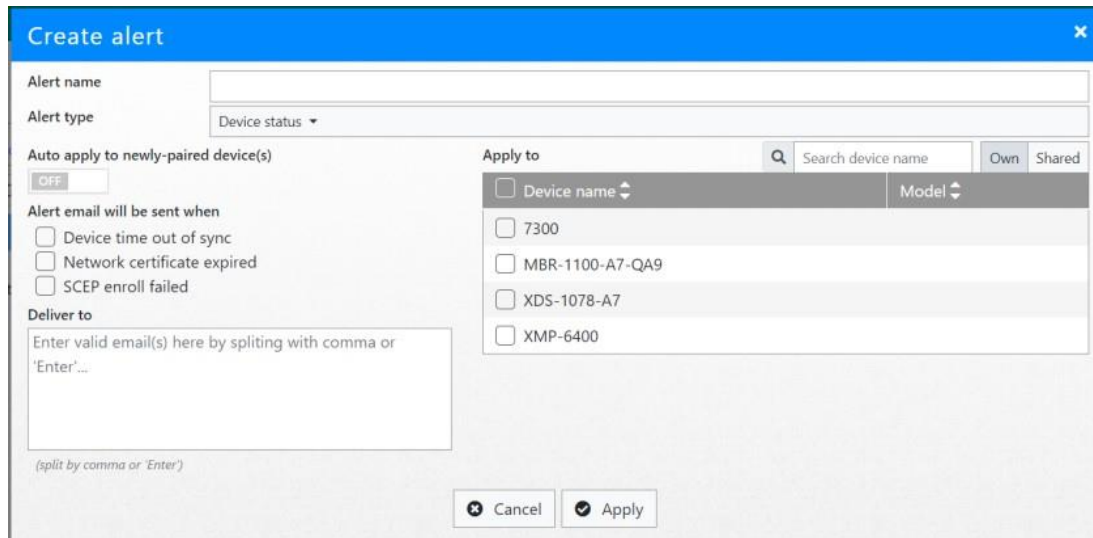
4. Select the players which will adhere to the alert rule.



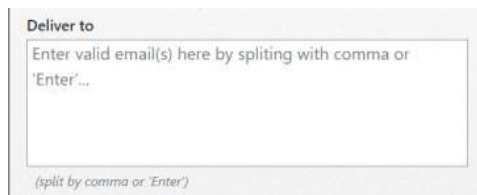
- **Own** – The current IAdeaCare account is the admin/owner of these players.
- **Shared** – The players in this list are being shared by another owner to be monitored.

If **Auto apply to newly paired players** is checked, the rule will automatically bind all newly paired players.

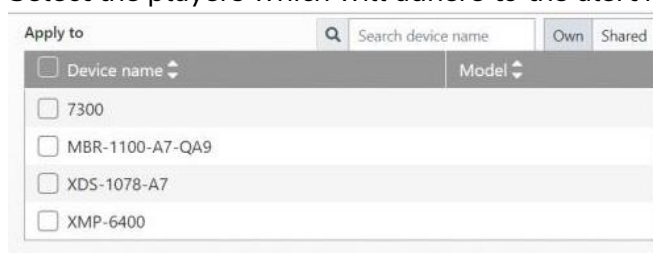
Create – Device Status



1. **Alert Name** – You can name your alert rule here.
2. Select your Device Status error type for the system to alert.
3. **Deliver to** allows the user to list which email accounts to send the offline email alerts to.



4. When alert is triggered, will create the alert in Open alert tab.
5. Server will send the alert e-mail as below twice a day (00:00 & 12:00 UTC+0).
6. Select the players which will adhere to the alert rule.



- **Own** – The current IAdeaCare account is the admin/owner of these players.
- **Shared** – The players in this list are being shared by another owner to be monitored.

If **Auto apply to newly paired players** is checked, the rule will automatically bind all newly paired players.

Report

Devices	Report				
	All reports	Settings			
Report sent on	Network status	Warranty	License	Error	
2021-09-25 21:22:01	Good	Good	Good	0	
2021-09-18 21:22:02	Good	Good	Good	0	
2021-09-11 21:22:01	Warning	Good	Good	0	
2021-09-04 21:22:02	Warning	Good	Good	1	
2021-08-28 21:22:01	Warning	Good	Good	0	
2021-08-21 21:22:01	Good	Good	Good	0	
2021-08-14 21:22:01	Warning	Good	Good	0	

Users can now choose what information to be added to weekly report.

Devices

Notifications

Alert

Report

Troubleshoot

License

Event feeds

Miscellaneous

Admin

Report

All reports

Settings

☒ Subscribe weekly report

Good network evaluation :

☒ 90 % devices uptime is over 90 %

Expiration warning :

☒ Warranty is expiring within 30 days

☒ License is expiring within 30 days

Deliver to : (split by comma)

clyde.wang@iadea.com

Cancel

Apply

All Reports

1. The Report Dashboard will load 50 reports per page.
2. Click on the report icon to view the report.

Report sent on	Network status
2021-09-25 21:22:01	Good
2021-09-18 21:22:02	Good

3. View the selected report.

Report

Date: 2021-03-14 ~ 2021-03-20

Quick Summary

Report items	Status	Evaluation	Suggestion
Overall device network health:	50% devices uptime over 50%	Good	The device network uptime is within or better than threshold value.
Warranty status tracking:	27% need renew soon 9% warranty expired	Warning	Renew warranty before it expired.
License status tracking:	50% license need renew 100% of devices without valid license	Good	There is no device license approaching its expiration date. No action is required.

Errors that need attention

Date	Tasks	Failed devices
2021-03-15	Account lockout	1
2021-03-15	Install software failed	1
2021-03-16	Device offline	23
2021-03-16	Device time out of sync	1

Warning messages

Date	Warning	Affected devices
2021-03-17	Delete alert rule	3
2021-03-17	Delete group policy	1
2021-03-17	Login failed	4
2021-03-20	Approaching expiration (renewable) - warranty	3
2021-03-20	Approaching expiration - license	4

Evaluation / Suggestion in Quick Summary:

1. Overall device network health:

Evaluation: Good

Criteria: Uptime >= User Defined Value

Suggestion: The device network uptime is within or better than threshold value.

Evaluation: Warning

Criteria: Uptime < User Defined Value

Suggestion: The device network uptime is lower than the threshold.

Please check your device network health or adjust notification settings as needed.

2. Warranty status tracking (The '/' in criterion means divided)

Status: % of devices that need warranty renewal soon.

Criteria: approaching expiration warranty per user defined range / total devices

Status: % of devices that warranty has expired.

Criteria: expired warranty / total devices

Evaluation: Good

Criteria: No approaching expiration on any device warranty per user defined range.



AND no expiration happening before next report.

Suggestion: All devices are either under warranty coverage or reach its maximum years of warranty.

No action is required.

Evaluation: Warning

Criteria: Devices approaching expiration date per user defined range AND no expiration happening before next report.

Suggestion: Renew warranty before expiration.

Evaluation: Need Attention

Criteria: Expiration will occur before next report.

Suggestion: Warranties will be expiring this week. **Please renew them before they expired.**

Warranty extension is not eligible after expiration date.

3. License status tracking (The '/' in criterion means divided)

Status: Licenses that require renewal.

Criteria: Licenses approaching expiration per user defined range / All devices (If device has multiple licenses, will use the highest level with latest expiry date)

Status: % of devices without valid license.

Criteria: Devices without valid license / All devices.

Evaluation: Good

Criteria: No approaching expiration on any device license per user defined range.

AND no expiration to occur before next report.

Suggestion: There are no device license approaching expiration.

No action is required.

Evaluation: Warning

Criteria: Approaching expiration date per user defined range AND no expiration happening before next report.

Suggestion: Renew license to avoid discontinuation of the service.

Evaluation: Need Attention

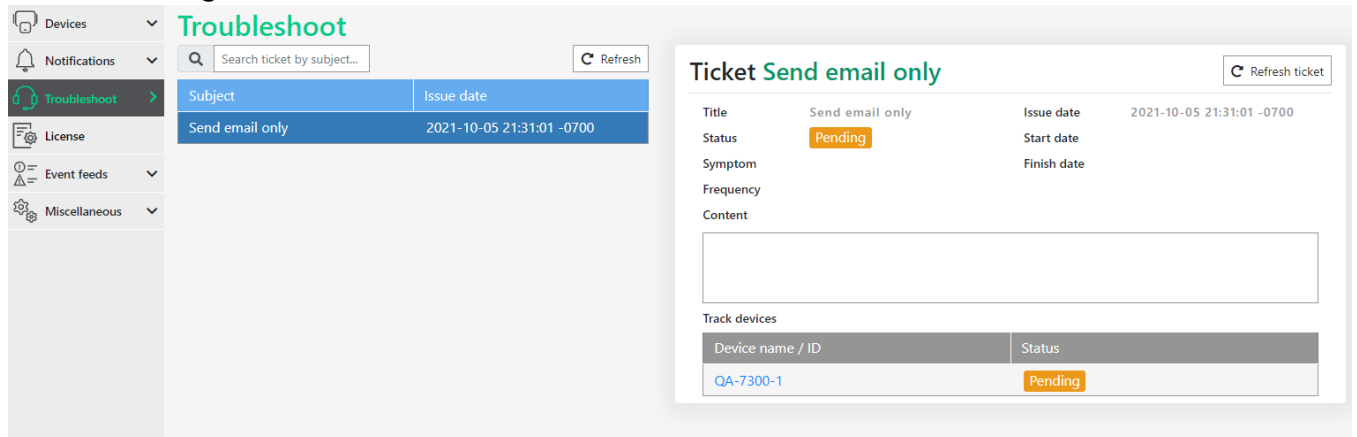
Criteria: Device License will hit expiration before next report.

Suggestion: Some device licenses will be expiring this week. **Please renew them to avoid discontinuation of the service.**

4.4 Troubleshoot

Troubleshooting Page

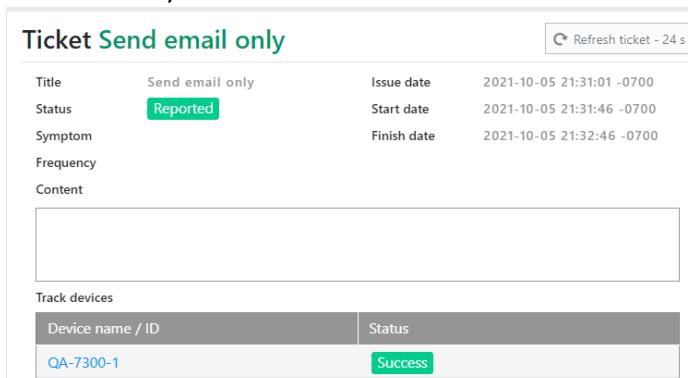
The troubleshooting page allows the user to track the status of their submitted troubleshooting tickets.



The screenshot shows the IAdeaCare interface. On the left is a sidebar with navigation options: Devices, Notifications, Troubleshoot (selected), License, Event feeds, and Miscellaneous. The main area is titled 'Troubleshoot' and contains a search bar 'Search ticket by subject...' and a 'Refresh' button. Below the search bar is a table with two columns: 'Subject' and 'Issue date'. The table contains one row: 'Send email only' with the date '2021-10-05 21:31:01 -0700'. To the right of this table is a detailed view of the selected ticket, titled 'Ticket Send email only' with a 'Refresh ticket' button. The ticket details include: Title (Send email only), Issue date (2021-10-05 21:31:01 -0700), Status (Pending), Start date, Symptom, Finish date, Frequency, and Content. Below the content field is a 'Track devices' section with a table showing 'Device name / ID' (QA-7300-1) and 'Status' (Pending).

1. **Ticket Search** – User is able to search for their troubleshooting ticket by the entered subject title in the module located on the left-hand side to view submitted ticket.

Ticket Information – This is the information that was reported when the ticket was submitted by user.




The screenshot shows the 'Ticket Send email only' page with a 'Refresh ticket - 24 s' button. The ticket details are: Title (Send email only), Issue date (2021-10-05 21:31:01 -0700), Status (Reported), Start date (2021-10-05 21:31:46 -0700), Symptom, Finish date (2021-10-05 21:32:46 -0700), Frequency, and Content. Below the content field is a 'Track devices' section with a table showing 'Device name / ID' (QA-7300-1) and 'Status' (Success).

2. **Ticket Tracking** – Allows the user to track the status of the ticket.
3. **Track Players** - Shows if IAdeaCare is able to connect to the player.

4.5 License

The License Page allows the user to manage their licenses. In this page they will be able to add license, import batch license files, and reallocate license. The License dashboard will also display each player along with their warranty or license type and expiration date.

Devices	License	MAC	Warranty	IAdeaCare license	Miscellaneous
<div> <div>Devices</div> <div>Notifications</div> <div>Troubleshoot</div> <div>License</div> <div>Event feeds</div> <div>Miscellaneous</div> </div>	<div> <div>+ Add license</div> <div>Import license</div> <div>Reallocate license</div> <div>Advanced filter *</div> </div> <div> <div>Search by device name ...</div> <div>Export</div> </div>				
	<div> <div>Device name</div> <div>QA-1000H</div> </div>	2C:C5:48:05:BF:72	2022-10-28	Type: premium Expiration date: 2022-09-29	
	<div> <div>Device name</div> <div>QA-1078-4.4</div> </div>	2C:C5:48:02:77:68	2022-10-28	Type: premium Expiration date: 2022-09-29	
	<div> <div>Device name</div> <div>QA-1078-7.1</div> </div>	2C:C5:48:02:77:8C	2022-10-28	Type: premium Expiration date: 2022-09-29	

1. **Add License** – Click here to manually add your IAdeaCare or SignApps Cloud License.
Import License – Use this feature to upload batch licenses (.csv file).
Reallocate License – This feature allows the user to move licenses from one player to another.
Advanced Filter – Filter results by Type of License and Expiry time range.
2. If the account contains multiple players, the search function allows the user to filter players by name or tag name.
3. The main dashboard shows the player's name along with the license type and expiration date of the warranty or license.
4. The License Page also allows user to configure how many players show up on the dashboard at once.
5. **Export** -  Export button will export license information to a .csv file.

Add License

Select your players and click on **Add License**.

Devices	License	MAC	Warranty
<div> <div>Devices</div> <div>Notifications</div> <div>Troubleshoot</div> <div>License</div> <div>Event feeds</div> <div>Miscellaneous</div> </div>	<div> <div>+ Add license</div> <div>Import license</div> <div>Reallocate license</div> <div>Advanced filter *</div> </div> <div> <div>Search by device name ...</div> </div>		
	<div> <div>Device name</div> <div>QA-1000H</div> </div>	2C:C5:48:05:BF:72	2022-10-28
	<div> <div>Device name</div> <div>QA-1078-4.4</div> </div>	2C:C5:48:02:77:68	2022-10-28

The add license prompt will populate for you to add the corresponding **IAdeaCare** or **SignApps** Cloud license code.

Add License

Device name	License code
QA-1000H	ICARE-D4887-BA405-7F485-WD454
QA-1078-4.4	ICARE-9456E-26484-EF54A-125WEQ

separate your license code by comma

Cancel
Next >>

Licenses can be added to the player individually or in batches. To batch players, select multiple players before clicking on Add License. User can also add more than one license (SignApps Cloud, IAdeaCare) at a time to each player by separating with a comma.

Import License

Import License allows for the importation of multiple licenses into **IAdeaCare**. The licenses will need to be in a in the below format and saved as an **.csv** file. Each license will have its own row. This file may be provided by the **IAdea** Sales team when multiple licenses are purchased.

	A	B
1	ICARE-DDB2F-BB864-523B9-78019	
2	ICARE-280E2-EB133-4C314-AD00F	
3	ICARE-44D7E-1B9A8-04F06-14658	
4	ICARE-36A21-C8669-FD00F-3B0F2	
5		
6		

Select all players that need a license to be imported.

License

+

 Add license

📄

 Import license

🔄

 Reallocate license

⌵

 Advanced filter

🔍

 Search by device name ...

<input type="checkbox"/>	Device name	MAC	Warranty	IAc
<input checked="" type="checkbox"/>	QA-1000H	2C:C5:48:05:BF:72	2022-10-28	Type Expir 2-09
<input checked="" type="checkbox"/>	QA-1078-4.4	2C:C5:48:02:77:68	2022-10-28	Type Expir 2-09
<input checked="" type="checkbox"/>	QA-1078-7.1	2C:C5:48:02:77:8C	2022-10-28	Type Expir 2-09
<input checked="" type="checkbox"/>	QA-1078A9	2C:C5:48:05:D1:84	2022-10-28	Type Expir 2-10

Select **Browse Files** and choose your **.csv** file. The UI will display how many licenses are in the imported file and how many licenses have been distributed.

Import License

Choose your license file and we will help allocate the license to each player.

📄

 Browse Files or drag file here

File name: license-import.csv

0 license(s) available

7 license(s) distributed

Player name	License code		
IAdeaDoor-A	ICARE-39999-88D9E-4CA34-A1F21	🔄	📄
IAdeaDoor-B	ICARE-5101B-5DC2A-FEE66-C2FAA	🔄	📄
MLB Player	ICARE-90565-F694A-8E37B-2789A	🔄	📄
IAdea Reception Desk	ICARE-CD384-DSAD3-2943C-A258A	🔄	📄
XDS-2288 Office	ICARE-D4887-BAF05-BF233-67504	🔄	📄
Test IAdea Player	ICARE-EA396-70535-6E087-510AD	🔄	📄

Cancel

Next >>

If the file does not show up, you will need to change the file type to All Files.


⌵




All Files (*.*)

⌵

Open

Cancel

If there are extra licenses, they will be displayed as distributable licenses if you click on  button. This will allow you to switch or replace licenses.




Player name	License code
IAdeaDoor-A	ICARE-39999-8BD9E-4CA34-A1F21 
Distributable license(s) : <div>ICARE-FB733-5A63B-D6B8B-122AB </div> <div>ICARE-FF3DA-CA05F-C6B69-90B12 </div>	

Once the appropriate license are applied, Click **Apply** to Confirm.

Import License ×

Click 'OK' if you want to apply, or 'Back' to modify again.

Player name	Applied license(s)
IAdeaDoor-A	ICARE-39999-8BD9E-4CA34-A1F21
IAdeaDoor-B	ICARE-5101B-5DC2A-FEE66-C2FAA
IAdea Reception Desk	ICARE-90565-F694A-8E37B-2789A
XDS-2288 Office	ICARE-CD384-D9AD3-2943C-A258A
Test IAdea Player	ICARE-D4887-BAF05-8F233-67504

 Prev
  Cancel
  Apply

Note: If the license has been used, an **Error** message will populate.

Import License ×

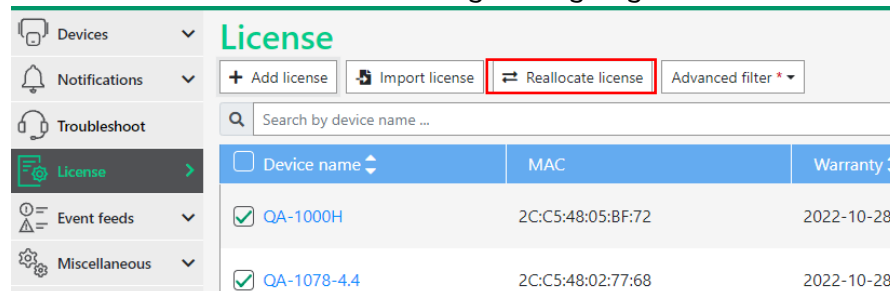
Some settings are failed.

Player : IAdeaDoor-A
Error :
 ICARE-39999-8BD9E-4CA34-A1F21 : The license key has been imported

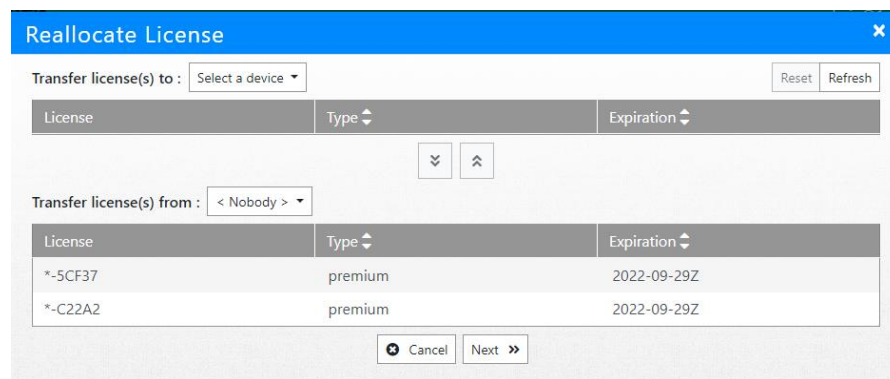
Reallocate License

Reallocation License allows users reassign licenses between the paired players on your IAdeaCare account.

Click on **Reallocate license** to being reassigning licenses.



Device name	MAC	Warranty
<input checked="" type="checkbox"/> QA-1000H	2C:C5:48:05:BF:72	2022-10-28
<input checked="" type="checkbox"/> QA-1078-4.4	2C:C5:48:02:77:68	2022-10-28



Transfer license(s) to:

Reset Refresh

License	Type	Expiration
*-5CF37	premium	2022-09-29Z
*-C22A2	premium	2022-09-29Z

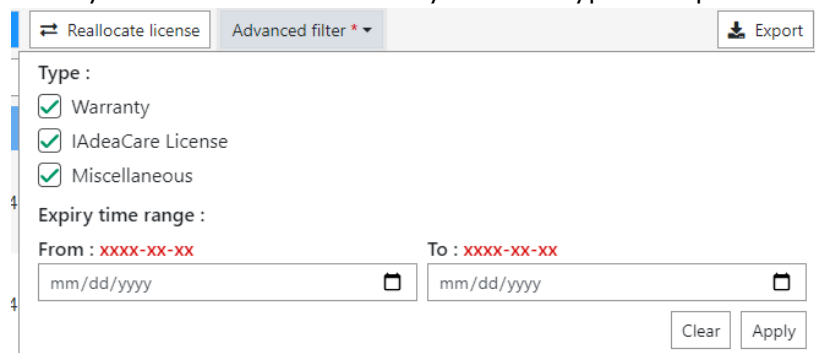
Transfer license(s) from:

Cancel Next >>

1. Select the target player for the player that the license will be assign to.
2. Select the **Currently Assigned to** player that the license is currently assigned. If license is allocated to a player, select **Nobody**.
3. Select the license(s) that will be reassigned in the license table and Click the Up Arrow to apply onto the target player.
4. Click **Next** to apply the change.

Advanced Filter

Filter your License Dashboard by License Type or Expiration Time Range.



Reallocate license Advanced filter * Export

Type :

☒ Warranty

☒ IAdeaCare License

☒ Miscellaneous

Expiry time range :

From : **XXXX-XX-XX** To : **XXXX-XX-XX**

mm/dd/yyyy mm/dd/yyyy

Clear Apply

5.6 Event Feeds

Event Log

Users are able to

- Have an overview look into the status of all account events.
- Filter by event type, by period of time, and severity.
- Sort by occurrence date/time, category, event, or subject.
- Events will load 50 logs at a time and be sorted by time.
- After applying filters, the log will show 100 results per page.
- Events in device task category will have a link to the activity's detail page.

IAdeaCare

johnny.chen@iadea.com

Devices

Notifications

Troubleshoot

License

Event feeds

Event log

Device activity

Miscellaneous

Event log

Filter by events

Time range : 2021-08-02 11:30 ~ 2021-10-04 11:30

Severity : All

Search in subject ...

Search

Occurance time	Category	Event	Subject
2021-09-25 21:33:26	Notification management	Send weekly report	Send weekly report - 2021-09-26
2021-09-18 21:32:48	Notification management	Send weekly report	Send weekly report - 2021-09-19
2021-09-15 11:16:58	Account access	Login	johnny.chen@iadea.com login
2021-09-11 21:32:44	Notification management	Send weekly report	Send weekly report - 2021-09-12
2021-09-07 10:16:10	Account access	Login	johnny.chen@iadea.com login
2021-09-04 21:33:11	Notification management	Send weekly report	Send weekly report - 2021-09-05

Info

Warning

Error

total : 6

<<

<

1

>

>>

Filter & Search

By Event

1. User is able to search even by keyword and cross category.
2. When a category is checked, all events under checked category will also be checked.

- If clear keyword is in search bar, the system will list all category and events and keep the already selected events checked as well.

Filter by event(s)

☐ Select all categories and events

CATEGORIES	EVENTS		
<input checked="" type="checkbox"/> Account access <input checked="" type="checkbox"/> Device activity <input type="checkbox"/> Device management <input type="checkbox"/> Device registration <input type="checkbox"/> Device task <input type="checkbox"/> Enterprise SCEP management <input type="checkbox"/> Enterprise customization <input type="checkbox"/> Enterprise user management <input type="checkbox"/> License management <input type="checkbox"/> Notification management <input type="checkbox"/> System admin activity	Account access <input checked="" type="checkbox"/> Login <input checked="" type="checkbox"/> Login failed <input checked="" type="checkbox"/> Account lockout <input checked="" type="checkbox"/> Change account password <input checked="" type="checkbox"/> Request forget password <input checked="" type="checkbox"/> Password reset	Device activity <input checked="" type="checkbox"/> Device time out of sync <input checked="" type="checkbox"/> SCEP certificate about to expired <input checked="" type="checkbox"/> Network certificate expired <input checked="" type="checkbox"/> SCEP enroll failed <input checked="" type="checkbox"/> SCEP enrolling - wait for approval <input checked="" type="checkbox"/> Screen on and off time <input checked="" type="checkbox"/> Maintenance mode on and off time	Device management <input type="checkbox"/> Create device group <input type="checkbox"/> Modify device group <input type="checkbox"/> Delete device group <input type="checkbox"/> Move device to new group <input type="checkbox"/> Create group policy <input type="checkbox"/> Modify group policy <input type="checkbox"/> Delete group policy <input type="checkbox"/> Sync group policy to device <input type="checkbox"/> Add sharing settings <input type="checkbox"/> Modify sharing settings <input type="checkbox"/> Remove sharing settings
	Device registration <input type="checkbox"/> Pair device <input type="checkbox"/> Unpair device	Device task <input type="checkbox"/> Reload License <input type="checkbox"/> Reload license failed	Enterprise SCEP management <input type="checkbox"/> Add new credential

- Click Apply to filter events. The Filter by Events button will show the number of checked items and send the search date to the server to complete.

Event : 52 events selected ▼

By Time Range

Choose the Date and Time range.

- Pick the date from the Calendar.
- Choose the hour 00-24 (Military) and minute 00 or 30.

Filter by time range : (UTC+0)

From : 2021-08-02 11:30 To : 2021-10-04 11:30

08/02/2021 10/04/2021

Hour	Minute
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24	00 30

- Search up to 90 days in the past.

4. Click Apply Dates to save the settings and return filtered results.
5. The events are searched by server time (UTC +0).

By Severity

1. Choose by severity type.

Filter by severity :

☒ Info

☒ Warn

☒ Error

Apply severity

2. Click Apply Severity to save the settings and return filtered results.

Search Bar

1. Search in subject ... will allow user to search the event log by keyword.

Filter by events ▼ Time range : 2021-08-02 11:30 ~ 2021-10-04 11:30 ▼ Severity : All ▼ ⌂ Export

Search in subject ... Search

2. After keywords are entered, click Search to return results.


Export


1. Export button will export the Event log (with filters if they applied) to a .csv file.


Filter by events ▼ Time range : 2021-08-02 11:30 ~ 2021-10-04 11:30 ▼ Severity : All ▼ ⌂ Export


Search in subject ... Search


Device Activities

Devices

Notifications


Troubleshoot

License

Event feeds

Event log

Device activity

Miscellaneous

Device activity

From

mm/dd/yyyy

to

mm/dd/yyyy

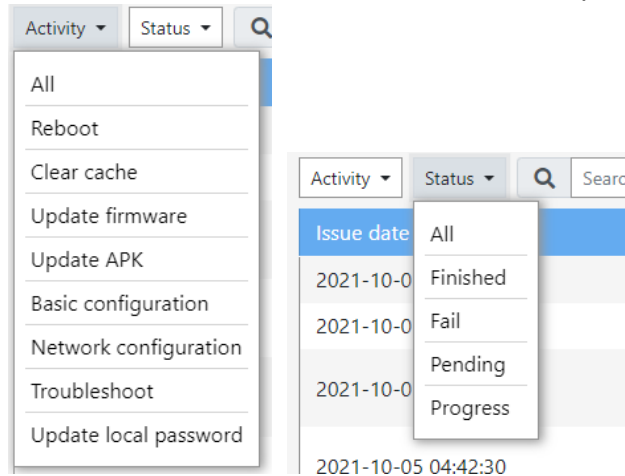
Activity

Status

Search by activity name ...

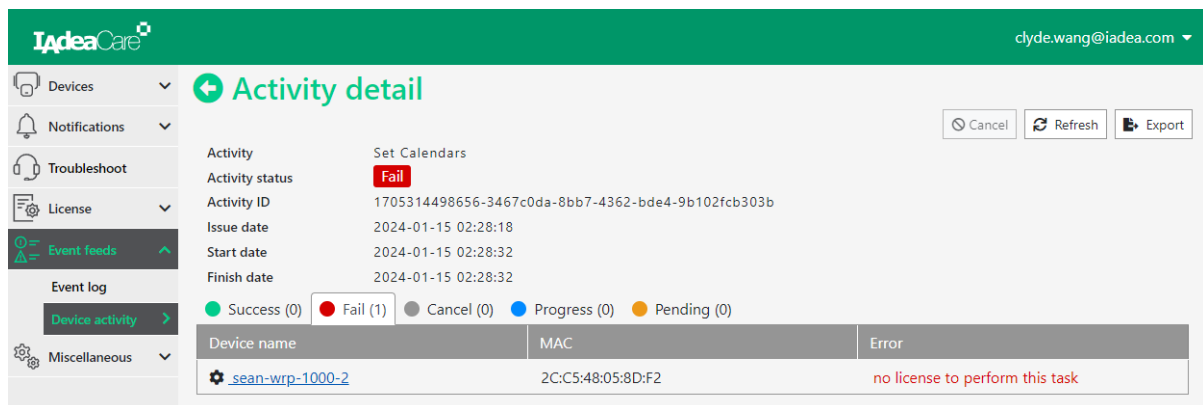
Issue date	Activity	Status
2021-10-05 18:55:15	Update firmware	1 Finished
2021-10-05 18:53:13	Update firmware	1 Finished
2021-10-05 04:43:31	[SignApps] Set ticket for System.Reboot	1 Finished
2021-10-05 04:42:30	[SignApps] Set ticket for System.Config	1 Finished

Search Filters – User can filter device activity results by Activity or Status.



At **Activity**, Users will be able to

- Cancel unfinished or pending tasks.
 - When cancelling the target task, all pending or in progress tasks following after the initial target task will be cancelled as well.
- Export task detail information and refresh statuses.
- See detailed changes before and after applying the activity.
- Device Name now allows Quick Link for easy navigation to player dashboard.



Once **Cancel** is confirmed, the status will show the notification. User will be able to confirm devices that have accept the cancel tasks under the Cancel Tab.



Activity detail

Activity: Update firmware

Activity status: **Fail** (User requested cancel on 2020-11-09 18:07:03)

Activity ID: 1604915275692-b6e1cf7a-d5da-4dfe-95ff-0e9e7cfd0c46

Issue date: 2020-11-09 17:47:55

Schedule date: 2020-11-09 18:00:00

Start date: 2020-11-09 18:10:13

Finish date: 2020-11-09 18:10:13

Configurations:

Setting	Last value	New value
Download link		https://s3.amazonaws.com/IADEACARE/INSTALLER-2.1.3-56.pl

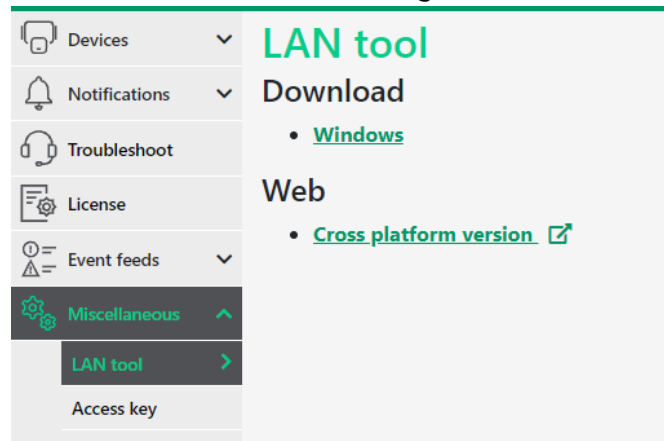
Legend: Success (0) Fail (0) Cancel (1) Progress (0) Pending (0)

Device name	MAC
MBR-1100-Nov-release	2C:C5:48:01:90:AA

5.7 Miscellaneous

LAN Config Tool

See User Manual for LAN config tool.



LAN tool

Download

- [Windows](#)

Web

- [Cross platform version](#)

Access key

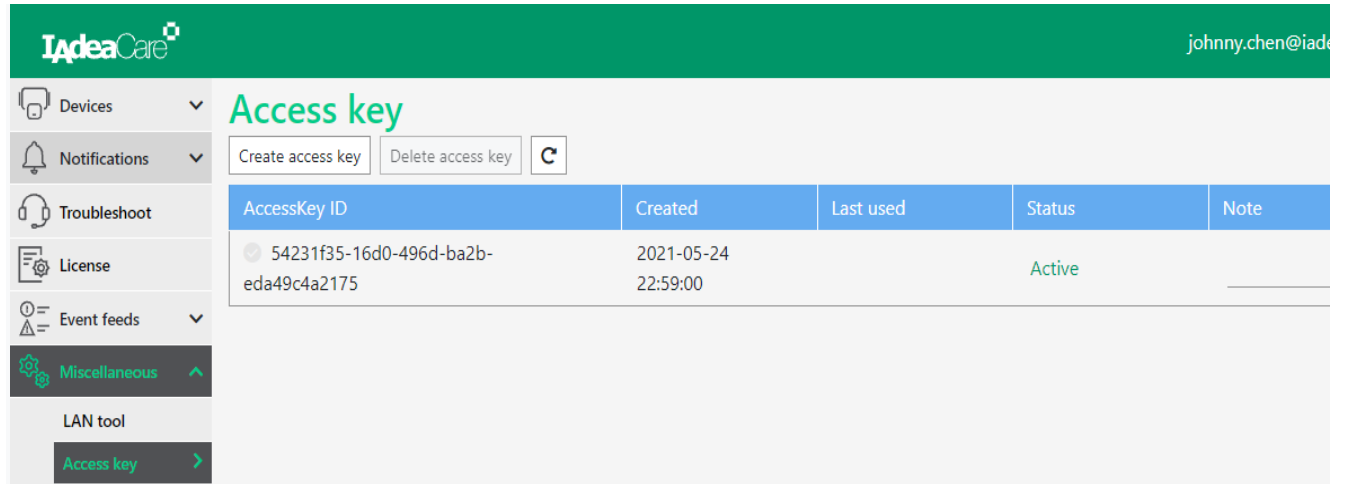
Click on **Windows** to download the **LAN config** tool for Windows OS.
For Mac and Linux OS, click on Cross platform version to open the config tool via default browser.

Note: User can only access cross platform LAN tool through IAdeaCare (cannot access by saving URL).

Access Key

Overview

After entering the Miscellaneous Tab, click on the Access Key tab to enter the overview.

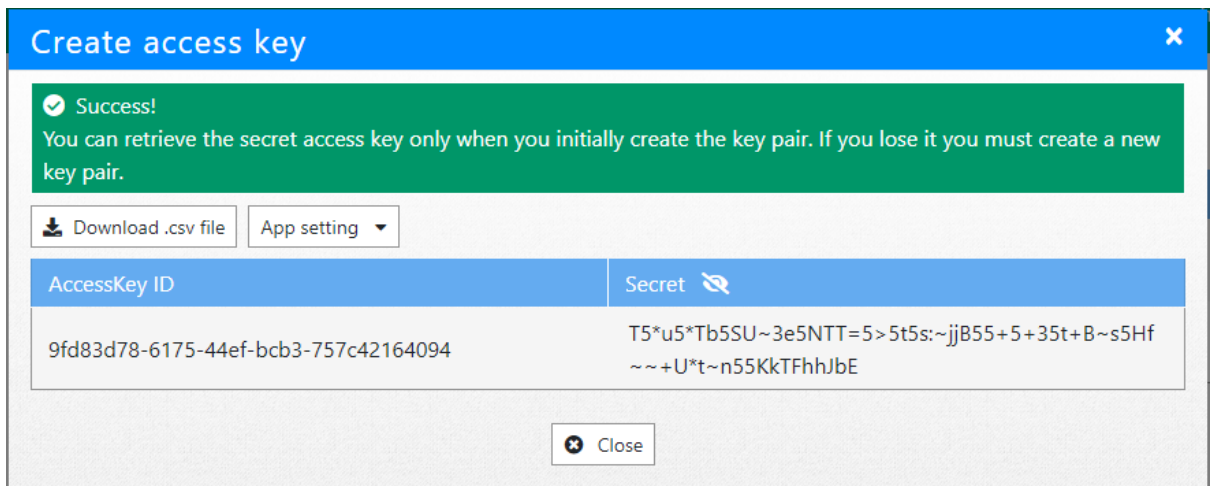


AccessKey ID	Created	Last used	Status	Note
54231f35-16d0-496d-ba2b-eda49c4a2175	2021-05-24 22:59:00		Active	

User will be able to Create, Delete, Activate, Inactive, and Edit the Note for each Access Key. Each account will be able to create up to 3 access keys.

Create Access Key

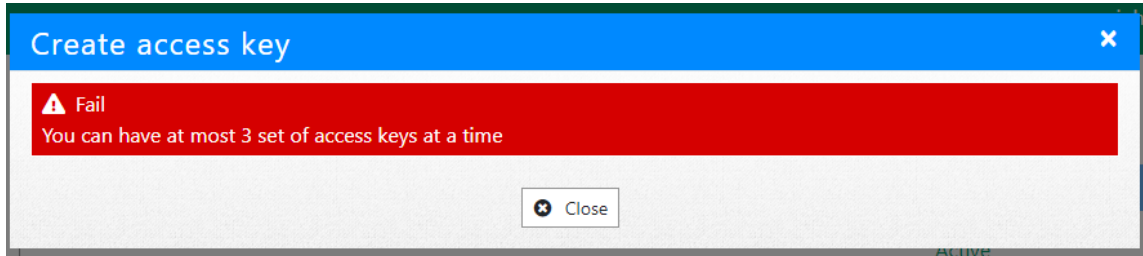
1. Click on Create access key to create a new access key.



AccessKey ID	Secret
9fd83d78-6175-44ef-bcb3-757c42164094	T5*u5*Tb5SU~3e5NTT=5>5t5s:~jjB55+5+35t+B~s5Hf~~~+U*t~n55KkTFhhJbE

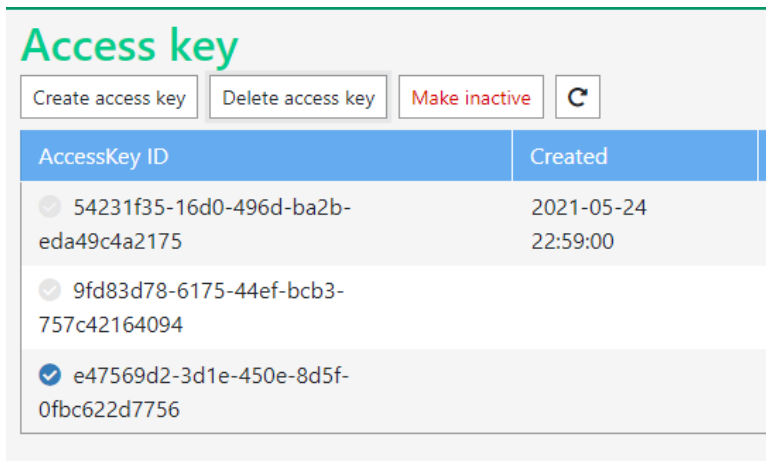
2. Once create access key is successful, you will see a confirmation screen like above.
3. User may click on Download .csv file to download a .csv file name [useraccount]-accesskey.csv that will include the access key and the secret key. User can save this for reference.
4. In the confirmation screen, the secret key will be encoded with *****. User can click on the show (eye) icon to display the secret key.
5. Click on close to view your Access Key dashboard.

- If there are 3 keys under the current account, the system will show an error message when trying to create another access key.

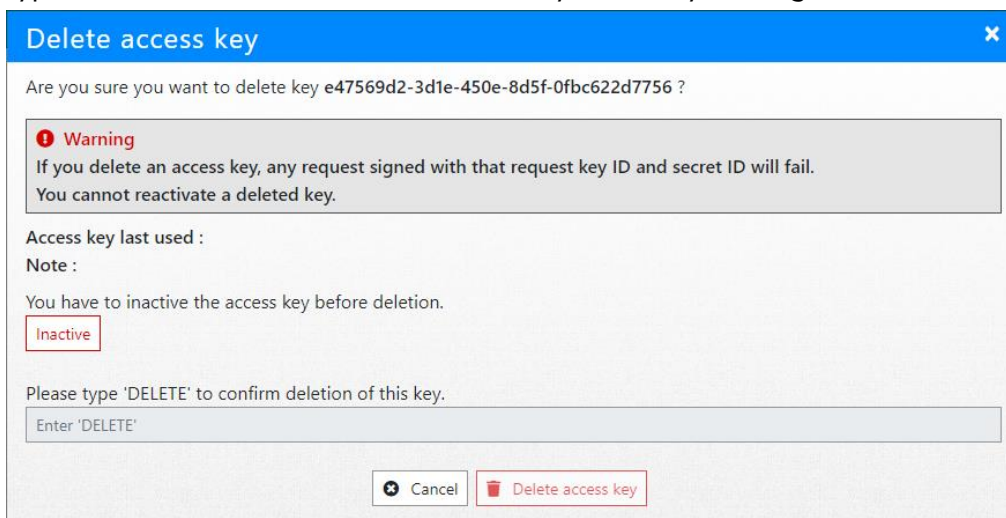


Delete Access Key

- Select the desired access key to delete first and then select Delete access key.



- If the access key is still active, the system will require you to inactive the access key before deletion. You may click on the Inactive Button first, then follow next step and type 'Delete' to confirm deletion of this key. Finish by clicking on Delete access key.



Delete access key

Are you sure you want to delete key e47569d2-3d1e-450e-8d5f-0fbc622d7756 ?

Warning

If you delete an access key, any request signed with that request key ID and secret ID will fail.
You cannot reactivate a deleted key.

Access key last used :

Note :

You have to inactive the access key before deletion.

Access key is deactivated.

Please type 'DELETE' to confirm deletion of this key.

Cancel

Delete access key

Delete access key

Are you sure you want to delete key e47569d2-3d1e-450e-8d5f-0fbc622d7756 ?

Warning

If you delete an access key, any request signed with that request key ID and secret ID will fail.
You cannot reactivate a deleted key.

Access key last used :

Note :

You have to inactive the access key before deletion.

Access key is deactivated.

Please type 'DELETE' to confirm deletion of this key.

Access key is deleted.

Close

- If Access Key is already Inactive, you will only be required to type 'Delete' to confirm.

Delete access key

Are you sure you want to delete key 9fd83d78-6175-44ef-bcb3-757c42164094 ?

Warning

If you delete an access key, any request signed with that request key ID and secret ID will fail.
You cannot reactivate a deleted key.

Access key last used :

Note :

Please type 'DELETE' to confirm deletion of this key.

Cancel

Delete access key

Active / Inactive

1. To inactive a currently active access key, select the desired access key and click Make inactive.

Access key

Create access key
Delete access key
Make inactive
C

AccessKey ID	Created	Last used	Status
54231f35-16d0-496d-ba2b-eda49c4a2175	2021-05-24 22:59:00		Active
9fd83d78-6175-44ef-bcb3-757c42164094			Active

2. When making an access key Inactive, the system will show the follow message to confirm the decision to inactive the access key. The message will show last time the access key was used and any Notes associated with the access key.

Inactive access key

Are you sure you want to inactive key 9fd83d78-6175-44ef-bcb3-757c42164094 ?

Warning

You cannot use inactive access key for API calls to IAdeaCare service but you can active it later.

Access key last used :

Note :

Cancel
Inactive

3. To make active an inactive access key, select the desired access key and click Make active. The access key will turn active without any system message.

Access key

Create access key
Delete access key
Make active
C

AccessKey ID	Created	Last used	Status
54231f35-16d0-496d-ba2b-eda49c4a2175	2021-05-24 22:59:00		Active
9fd83d78-6175-44ef-bcb3-757c42164094			Inactive

Note: Each Access Key allows you to edit a Note to differentiate the difference between multiple access keys. When the Note field shows a check mark, you may input notes in the input field. When the note is complete, click on the check mark to indicate that the note is complete. To edit existing note, click on the pencil and

proceed to edit the note. Click on the check mark to complete your note.

Access key

Create access key

Delete access key

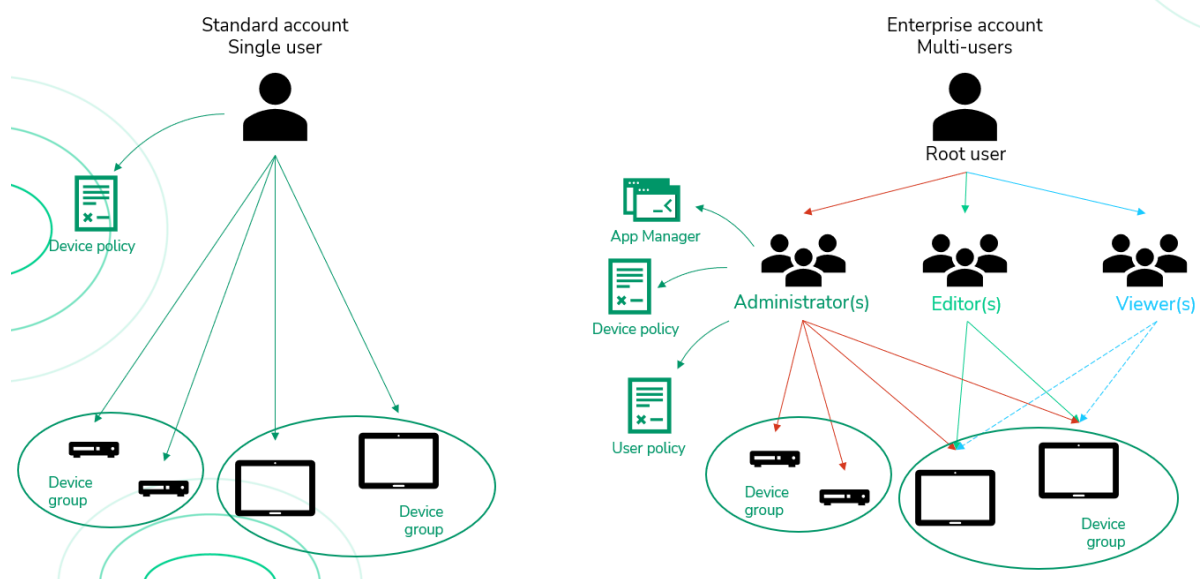
Make inactive

C

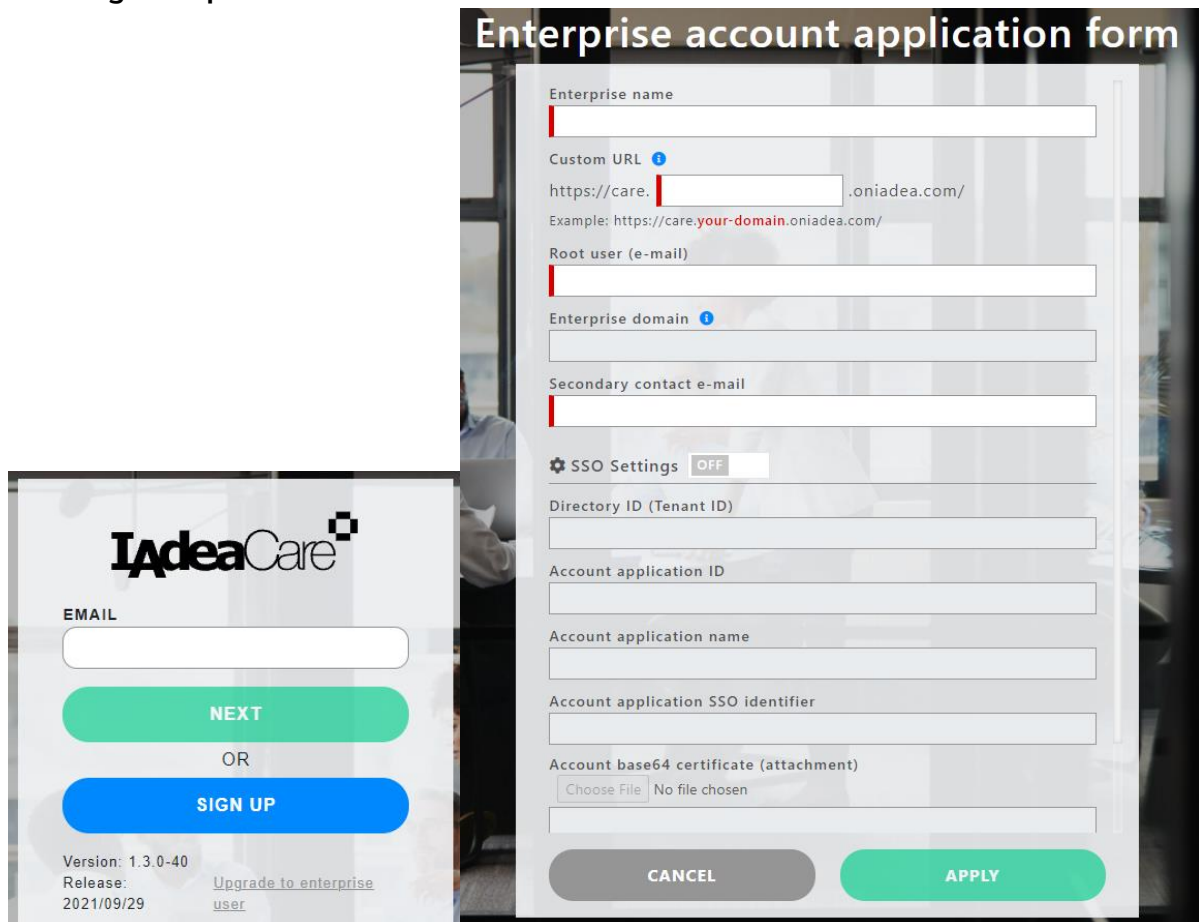
AccessKey ID	Created	Last used	Status	Note
<div>✓</div> <div>54231f35-16d0-496d-ba2b-eda49c4a2175</div>	2021-05-24 22:59:00		Active	<div>note</div> <div></div>
<div>●</div> <div>9fd83d78-6175-44ef-bcb3-757c42164094</div>			Inactive	<div></div> <div></div>

5.8 Enterprise Account

IAdeaCare Enterprise account is designed for corporate to manage their device network in a multi-user with different user role environment. Enterprise version now includes administrator, editor, and viewer roles. It allows multiple administrators to easily manage a large device network. Administrators can design and automate device management with device groups and policies. Enterprise also enhances security by only allowing authorized devices to be registered.



Creating Enterprise Account



The image shows two screenshots of the IAdeaCare interface. The left screenshot shows the 'Upgrade to Enterprise' button. The right screenshot shows the 'Enterprise account application form' with the following fields:

- Enterprise name
- Custom URL: <https://care. .oniadea.com/>
Example: <https://care.your-domain.oniadea.com/>
- Root user (e-mail)
- Enterprise domain
- Secondary contact e-mail
- SSO Settings: OFF
- Directory ID (Tenant ID)
- Account application ID
- Account application name
- Account application SSO identifier
- Account base64 certificate (attachment): Choose File | No file chosen
- CANCEL and APPLY buttons

Click on upgrade to Enterprise User and complete form.

Enterprise Name: The name of your company

Custom URL: This is the URL for your IAdeaCare Enterprise portal.

Root User: The first account able to log in (mail address)

Enterprise domain: The domain name of root user. This is the domain which you can log in Enterprise portal.

Secondary contact e-mail: The backup contact just in case.

SSO settings (optional)

#	Field	Sample Value
1	Directory ID (Tenant ID)	8f84824f-b25c-4dd1-8051-b7b21d2125a1
2	Account Application ID	7744089e-9b78-4897-8082-77178df34f13
3	Account Application Name	IAdeaCare Private SaaS - Account
4	Account Application SSO Identifier	care.iadea.com-account
5	Account Base64 Certificate (attachment)	{{FILE}}

After complete payment, the turnaround time will be 3-5 business days.

Existing personal users will be converted to Enterprise users. When converting personal account to Enterprise account, existing personal account will be deleted and added to the enterprise account.

New user has to receive the invitation mail, click the link and use the password in the mail



to log in. Registration finish!

Expiration mechanism of enterprise account

Before expiration (30 days prior), send e-mail to root account and secondary mail to notify it's expiring soon. If continue subscribe > Contact sales@iadea.com.

If want to unsubscribe > Click Unsubscribe to inform IAdea support team.

If user no longer use Enterprise account > all users will turn into personal user.

(If SSP, members have to use forget password to set up password again for its personal user).

Domain Change

IAdea offers a service to allow the user to add/change the domain of your IAdeaCare enterprise portal.

Login Portal / SSO

Enterprise Users can log in via the Enterprise portal. The log in process will differ depending on how the account is set up.

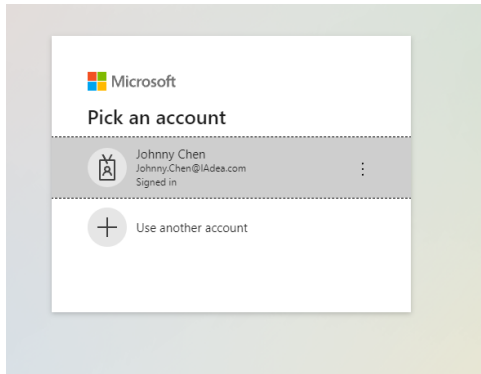
For Enterprise login, the system will verify your login domain. The portal will be redirect to the correct IAdeaCare login.



When logging in via SSO, user is able to log in without an invitation.

Set the user who log in from SSP to Ungrouped user group and as viewer.

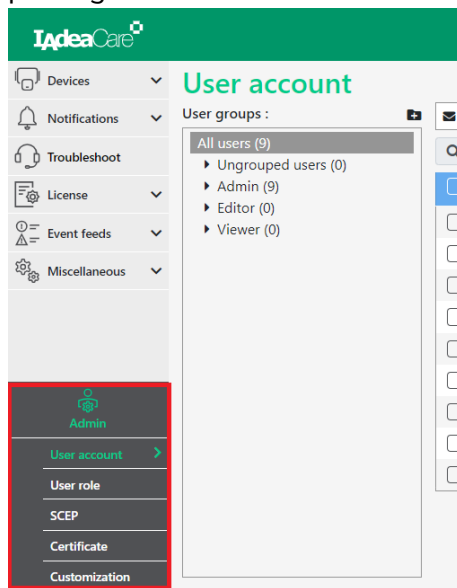
For SSO setup, users will be requested to login using their MS Active Directory account.



Admin

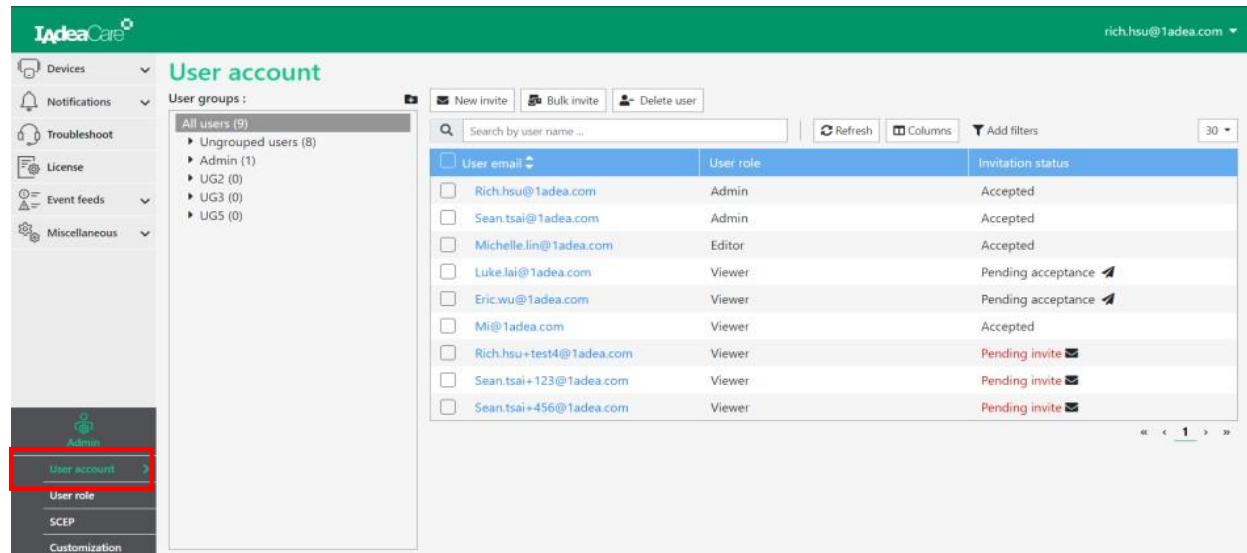
Overview

Administrator Access will show the Admin Icon on the bottom left hand of the screen. This will confirm that the current user that is logged in has administrative privileges.





Click on the Admin Icon to Expand Menu.

User Account

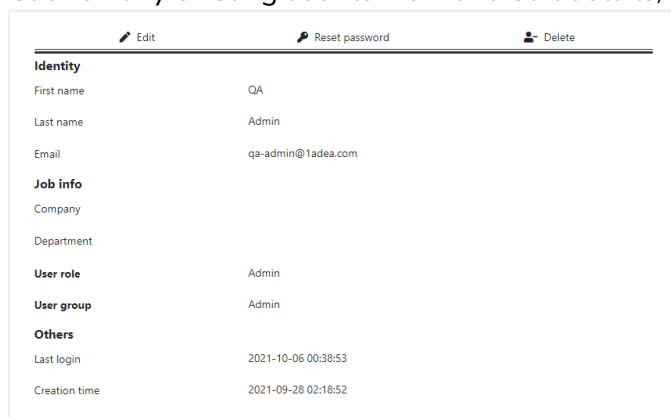


User Account: This allows the Administrator to invite, delete, and delegate user role and groups to sub-users.

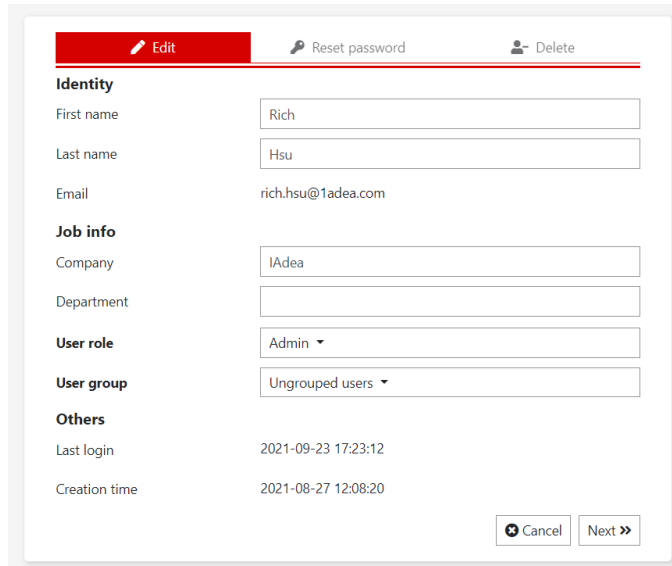
- When All Users is selected; New Invite, Bulk Invite, and Delete User, will be populated for use.
- All Users are shown with their email, user role, and invitation status.
- Invitation status:
 - **Pending acceptance** – Waiting for user to log back into the system.
 - **Accepted** – User received the invitation and completed log in.
 - **Pending invite** – User signed up by itself and is waiting for administrator to send an invitation.
- When the status is **Pending Acceptance**, the admin will have a button  to send the acceptance invitation again.
- When the status is **Pending Invite**, the admin will have a button  to send the new invite invitation again.

User Detail

Click on any existing user to view and edit details, or delete user.



Edit User Detail

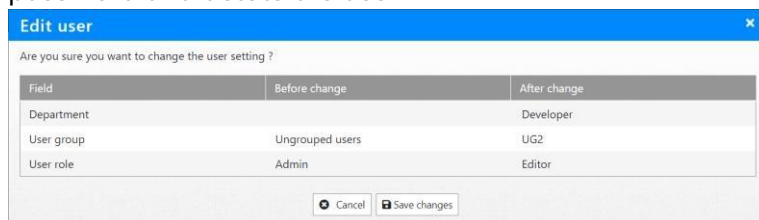


The 'Edit User Detail' form is divided into several sections:

- Identity:** Fields for First name (Rich), Last name (Hsu), and Email (rich.hsu@1adea.com).
- Job info:** Fields for Company (IAdea) and Department.
- User role:** A dropdown menu set to 'Admin'.
- User group:** A dropdown menu set to 'Ungrouped users'.
- Others:** Fields for Last login (2021-09-23 17:23:12) and Creation time (2021-08-27 12:08:20).

At the top, there are buttons for 'Edit' (highlighted in red), 'Reset password', and 'Delete'. At the bottom right, there are 'Cancel' and 'Next >>' buttons.

Admin can edit all user information except for email address. The admin can also reset password and delete the user.



The 'Edit user' dialog box asks 'Are you sure you want to change the user setting?'. It contains a table showing the changes:

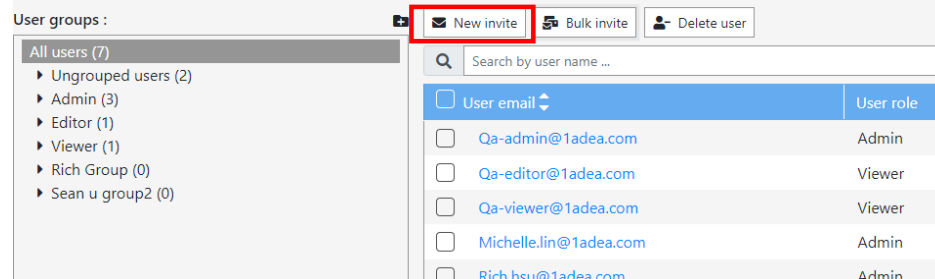
Field	Before change	After change
Department		Developer
User group	Ungrouped users	UG2
User role	Admin	Editor

At the bottom, there are 'Cancel' and 'Save changes' buttons.

Once edit user is complete, click Next to confirm changes.

New Invite

User account



The 'User account' interface shows a list of user groups on the left and a table of users on the right.

User groups:

- All users (7)
 - Ungrouped users (2)
 - Admin (3)
 - Editor (1)
 - Viewer (1)
 - Rich Group (0)
 - Sean u group2 (0)

User actions: New invite (highlighted in red), Bulk invite, Delete user.

User table:

User email	User role
<input type="checkbox"/> Qa-admin@1adea.com	Admin
<input type="checkbox"/> Qa-editor@1adea.com	Viewer
<input type="checkbox"/> Qa-viewer@1adea.com	Viewer
<input type="checkbox"/> Michelle.lin@1adea.com	Admin
<input type="checkbox"/> Rich.hsu@1adea.com	Admin



Click on New invite to invite a new user.

Invite user

Identity

First name *

Last name *

Email * @1adea.com

Job info

Company

Department

User role *

User group *

Messages

Cancel Invite

Fill out new invite form to complete the process.

- If email domain is correct, the system will send a mail with temporary password to user's email address. The system will also create the user in the User Account list with invitation status showing 'Pending acceptance'.
- Invited Users will click the link and go to the IAdeaCare website to log in. The invitation status of User will change to 'Accepted'.

Bulk Invite

User account

User groups :

All users (7)

- ▶ Ungrouped users (2)
- ▶ Admin (3)
- ▶ Editor (1)
- ▶ Viewer (1)
- ▶ Rich Group (0)
- ▶ Sean u group2 (0)

New invite Bulk invite Delete user

Search by user name ...

<input type="checkbox"/> User email	User role
<input type="checkbox"/> Qa-admin@1adea.com	Admin
<input type="checkbox"/> Qa-editor@1adea.com	Viewer
<input type="checkbox"/> Qa-viewer@1adea.com	Viewer
<input type="checkbox"/> Michelle.lin@1adea.com	Admin
<input type="checkbox"/> Rich.hsu@1adea.com	Admin



Bulk Invite allows the user to download an Excel template and upload a bulk user list.

Invite multiple users

1. Download csv template (optional)

Download

2. Edit your csv file

3. Upload your csv file

Choose File

No file chosen

Messages

Cancel

Submit

If the number of editor and administrator exceed the number of user licenses purchased, the below message will populate.



Delete User

User account

User groups :

All users (7)

▶ Ungrouped users (2)

▶ Admin (3)

▶ Editor (1)

▶ Viewer (1)

▶ Rich Group (0)

▶ Sean u.group2 (0)

New invite

Bulk invite

Delete user

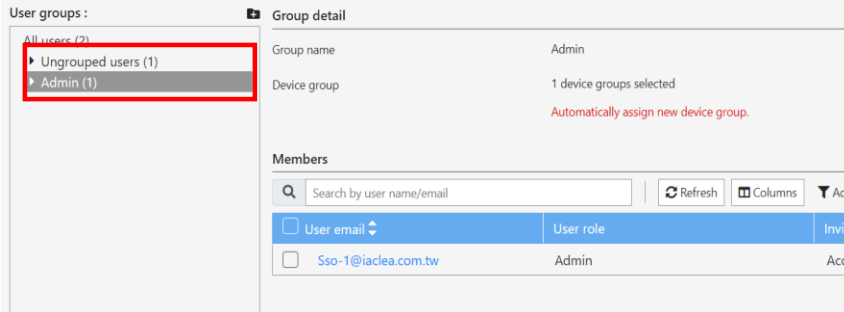
Search by user name ...

User email	User role
<input type="checkbox"/> Qa-admin@1adea.com	Admin
<input type="checkbox"/> Qa-editor@1adea.com	Viewer
<input type="checkbox"/> Qa-viewer@1adea.com	Viewer
<input type="checkbox"/> Michelle.lin@1adea.com	Admin
<input type="checkbox"/> Rich.hsu@1adea.com	Admin

Select desired User and select Delete User. The User will be disabled on the server and will not be able to login.

User Group

User account



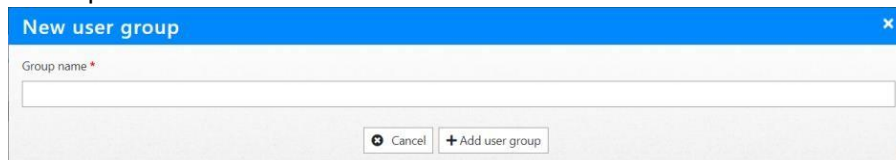
- On the right window, will show the group details and members.
- One user only belongs to one user group.
- There are two pre-defined groups.
 - Ungrouped user** – The users whose user group is deleted or removed from user group. Cannot be deleted.
 - Admin** – The group which pre-check all device groups and automatically assign new device group. Can be edited/deleted by Administrators.

New User Group

User account



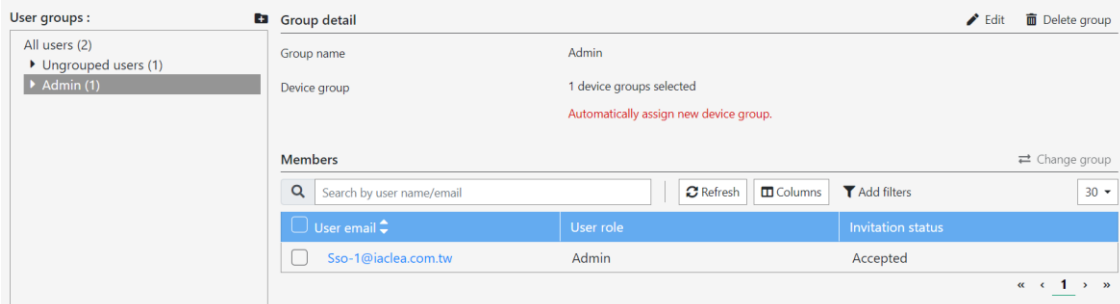
Click on the Add icon to create a new user group. Please confirm that desired group name is unique.



When complete, click +Add user group to confirm and return back to All User page.

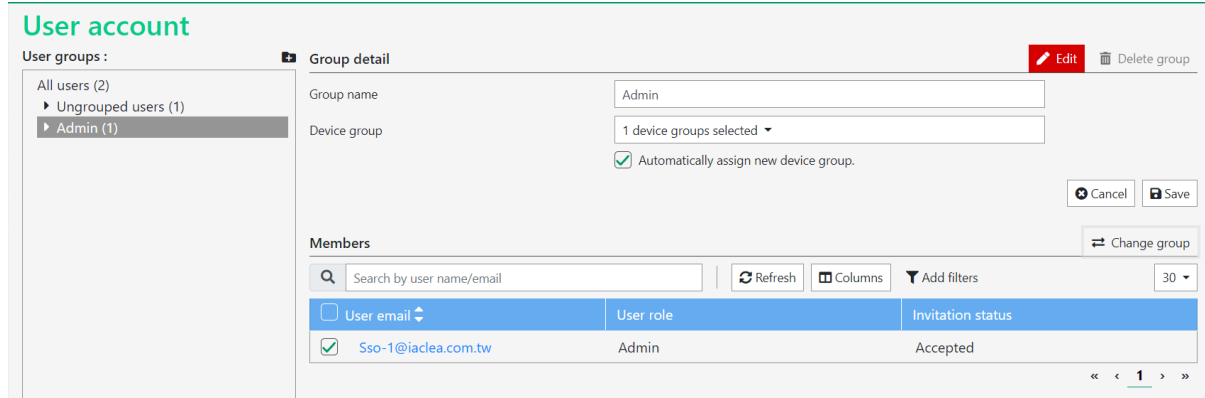
User Group Detail

User account



When User Group is selected, it will populate the Group Detail information.

Edit User Group



User account

User groups :

- All users (2)
 - Ungrouped users (1)
 - Admin (1)

Group detail Edit Delete group

Group name: Admin

Device group: 1 device groups selected

☒ Automatically assign new device group.

Cancel Save

Members Change group

Search by user name/email Refresh Columns Add filters 30

<input type="checkbox"/> User email	User role	Invitation status
<input checked="" type="checkbox"/> Sso-1@iaclea.com.tw	Admin	Accepted

« 1 »

- Group name: The group name should be unique.
- Device group: Assign the device group to this user group. The user in group will be able to view/manage the devices assigned.
- Automatically assign new device group: If selected, the new created device group will be assigned to the user group automatically.
- Save and Cancel button: These two buttons are for Group detail.
- Delete group: Users will be moved to ungrouped group after delete group.
- Change group: Select the user then click button to move user to another group. (Also, able to use drag and drop to change group.)



Change user group ×

Move users from Admin to another user group.

Users under Admin

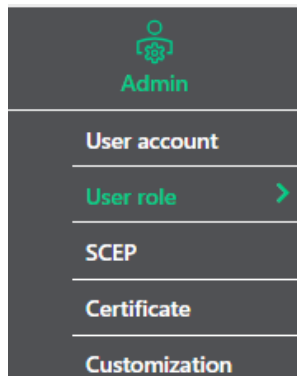
- sso-1@iaclea.com.tw

Move to


- All users (2)
- Ungrouped users (1)
- Admin (1)

Cancel Move

User Role




User role

Role permission		
Name	Description	# of users
Admin	All permissions are enabled	4
Editor	Able to access devices	0
Viewer	View function only	3 

License -> Admin+Editor: 4 / 20, Viewer: 3 / 50

Users with role <Viewer>



Email	User group	Edit policy
qa-editor@1adea.com	Editor	Viewer
qa-viewer@1adea.com	Ungrouped users	Viewer
mark.yang@1adea.com	Viewer	Viewer

User Role will allow the admin to see which users are enrolled into which role. Admin can click on the # of users to populate a user list.

In the Users with role list, admin can edit the roles of the user by clicking on the Edit button



There are 3 predefined User role:

- I. **ADMINISTRATOR** – Able to view/manage ALL user groups/device groups.
- II. **EDITOR** – Able to view/manage the devices groups ADMINISTRATOR assign.
- III. **VIEWER** - Able to view the devices groups ADMINISTRATOR assign.

Permissions Table – To access, click on Role permission.

Role permission			
Permissions	admin	editor	viewer
Batch actions - Basic configuration	✓	✓	✗
Batch actions - Update security password	✓	✓	✗
Batch actions - Update firmware	✓	✓	✗
Batch actions - Update APK	✓	✓	✗
Batch actions - Reboot	✓	✓	✗
Batch actions - Troubleshoot	✓	✓	✗
Batch actions - Clear cache	✓	✓	✗
Create/move/delete/edit/change device group	✓	✗	✗
Create/edit/delete group policy settings	✓	✗	✗
Device status/info display	✓	✓	✓
Device screenshot	✓	✓	✓
Device - Registration	✓	✗	✗
Device - Reboot	✓	✓	✗
Device - Update firmware	✓	✓	✗
Device - Basic configuration	✓	✓	✗
Device - Network	✓	✓	✗
Device - Security	✓	✓	✗
Device - Troubleshoot	✓	✓	✓
Device - Activities	✓	✓	✓
Device - Alert (Create/edit)	✓	✓	✓
Device - Add license	✓	✗	✗
Device - Change policy	✓	✗	✗
Notification - View alert settings	✓	✓	✓
Notification - Create/edit/delete alert settings	✓	✓	✓
Notification - Acknowledged open alerts	✓	✓	✓
Notification - View reports	✓	✓	✓
Notification - Change report setting	✓	✓	✓
Miscellaneous - LAN config tool download links	✓	✓	✗
Miscellaneous - View access key	✓	✓	✓
Miscellaneous - Create/download/delete access key	✓	✓	✓
Troubleshoot - View/search troubleshoot tickets	✓	✓	✓
License - View/refresh/search device licenses	✓	✓	✓
License - Add/import/reallocate license	✓	✗	✗
License - Export device license data	✓	✗	✗
Event feeds - View/search event logs	✓	✓	✓
Event feeds - Export event logs	✓	✓	✓
Event feeds - View/search device activities	✓	✓	✓
Administrative settings - Invite/edit/delete user	✓	✗	✗
Administrative settings - Edit group policy	✓	✗	✗
Administrative settings - Create/edit/delete user group	✓	✗	✗
Administrative settings - Create/edit/delete SCEP server	✓	✗	✗
Administrative settings - Edit logo/background	✓	✗	✗

✕ Close

SCEP

Overview

Devices

Notifications

Troubleshoot

License

Event feeds

Miscellaneous

Admin

User account

User role

SCEP

SCEP

+ Add new credential setting

Alias	Subject	SCEP server	Profile	Action
iadeacare-scep-eap-cert-AAAA				
iadeacare-scep-eap-cert-BBB				
iadeacare-scep-eap-cert-QAtest	OU=IAdea Player	http://52.240.54.88/certsrv/mscep	QA-SCEP-Server2	
iadeacare-scep-eap-cert-T1		http://10.0.10.234/certsrv/mscep/	NDES	
iadeacare-scep-eap-cert-T2		http://10.0.10.206/certsrv/mscep/	NDES2	
iadeacare-scep-eap-cert-T3		http://10.0.10.205/certsrv/mscep/	NDES3	

Add New Credential

Add new credential

Alias

iadeacare-scep-eap-cert-

Subject

Key size

1024

SCEP server

Profile

Usage

APP

Auto renew

120

days before expiration

Cancel

Create

Alias: iadeacare-scep-eap-cert- will be fixed prefix.

Click 'Create' to finish and go back to SCEP page.



Credential Details

Click the Alias hyperlink to view Credential details.

Show the details below with Edit button.

← Credential details

Edit

Alias	iadeacare-scep-eap-cert-AAAA
Subject	
Key size	1024
SCEP server	
Profile	
Usage	APP
Auto renew	120

Device list

↻ Renew SCEP + Add device Export

Search device by name or mac

Refresh devices

No license

Device name	Device group	MAC	Enrollment status	Expiry date
Please wait...				

Edit Credential

Click on the Edit button to edit credentials.

All fields are able to be changed except for Alias.

← Credential details

Edit

Alias	iadeacare-scep-eap-cert-AAAA
Subject	
Key size	1024
SCEP server	
Profile	
Usage	APP
Auto renew	120 days before expiration

Device list

↻ Renew SCEP + Add device Export

Search device by name or mac

Refresh devices

No license

Device name	Device group	MAC	Enrollment status	Expiry date
Please wait...				

Cancel Save

After changes, Click Save and enter authentication info and enable 802.1xEAP.

Update credential

SCEP alias

iadeacare-scep-eap-cert-AAAA

SCEP enrollment settings

Challenge password *

802.1x EAP settings

EAP method

TLS

Domain

Identity *

Device list : 0 device(s) are selected.

Search device by name or mac

Refresh devices

No license

Device name	Device group	MAC	Enrollment status	Expiry date
Please wait...				

Cancel Update

Click Update to complete process and go back to Credential page.

Add Device

To add a device to the SCEP enrolment, click on +Add Device.



rich.hsu@iadea.com

Credential details Edit

Alias: iadeacare-scep-eap-cert-testBySean2

Subject: 1024

Key size: 1024

SCEP server: http://20.106.131.219/certsrv/mscep/

Profile: QA-SCEP-Server2

Usage: EAP-ETHERNET

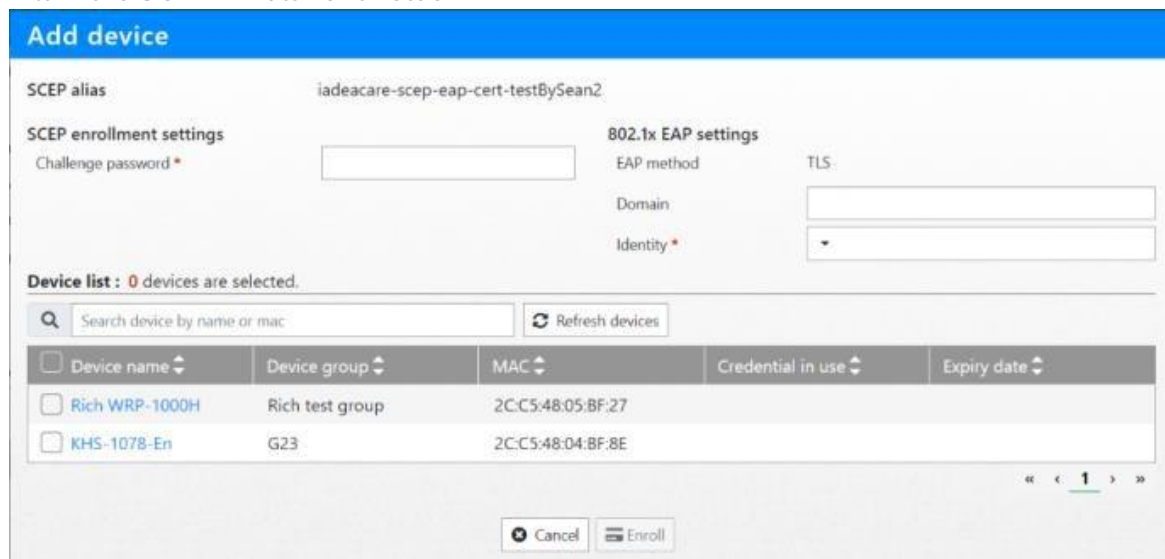
Auto renew: 240

Device list Renew SCEP **+ Add device** Export

Search device by name or mac: Refresh devices

Device name	Device group	MAC	Enrollment status	Expiry date
<input checked="" type="checkbox"/> sean-1078	Default group	2C:C5:48:05:8D:F2	RENEWING	2022-05-10 11:52

Fill in the SCEP Enrollment fields.



Add device

SCEP alias: iadeacare-scep-eap-cert-testBySean2

SCEP enrollment settings

Challenge password:

802.1x EAP settings

EAP method: TLS

Domain:

Identity:

Device list: 0 devices are selected.

Search device by name or mac: Refresh devices

Device name	Device group	MAC	Credential in use	Expiry date
<input type="checkbox"/> Rich WRP-1000H	Rich test group	2C:C5:48:05:BF:27		
<input type="checkbox"/> KHS-1078-En	G23	2C:C5:48:04:BF:8E		

Cancel **Enroll**

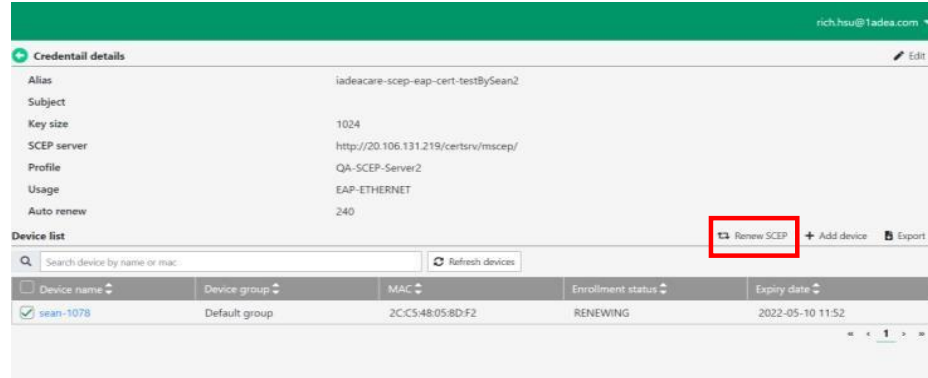
Select desired devices from device list and fill the information below.

- Challenge Password: The password for SCEP server enrolment.
- Identity: Select MAC or Device ID.

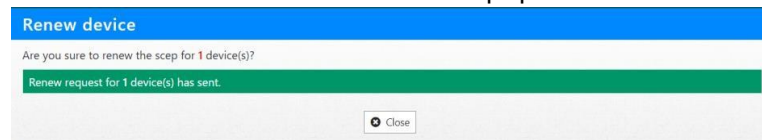
Click **Enroll** to confirm and go back to the Credential detail page.

Renew

When desired device is selected, the option to Renew SCEP will populate.



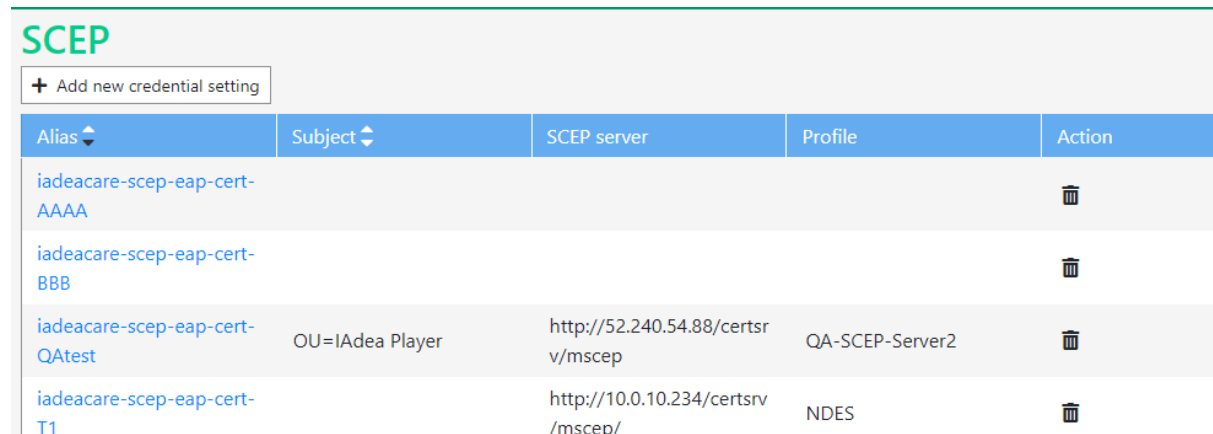
Confirmation for SCEP renewal will populate.




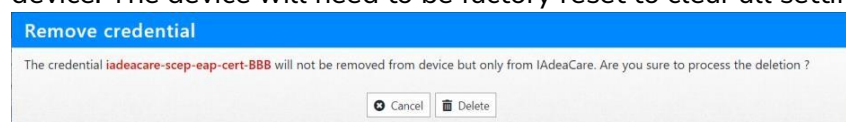
Export

Click on Export  to export the SCEP credentials information to a .csv file.

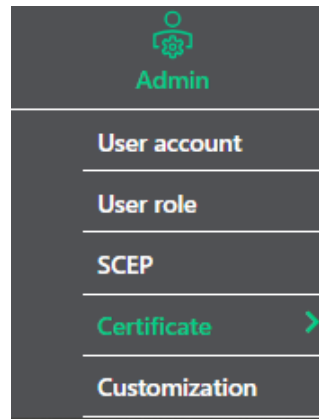
Delete Credential



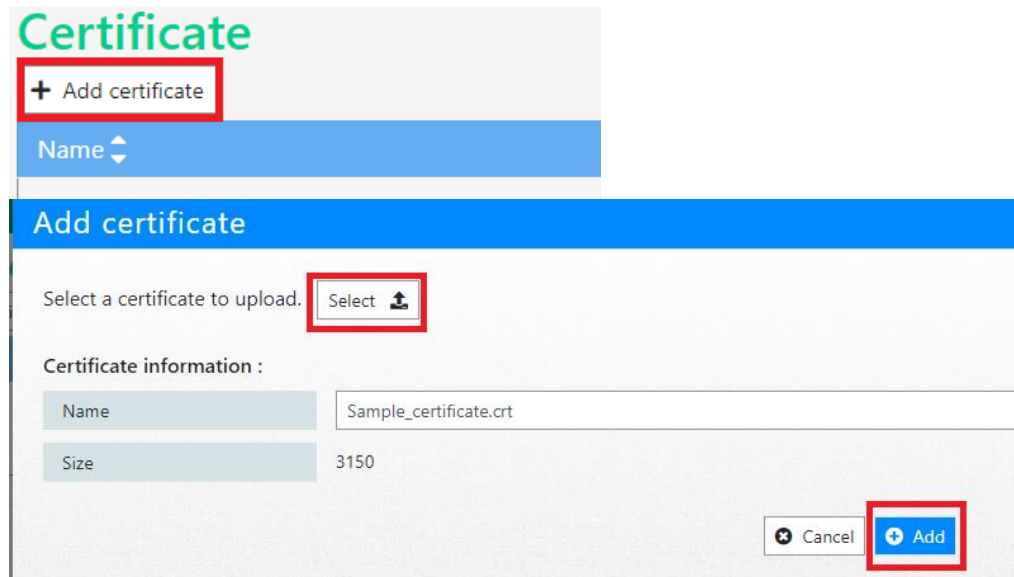
To delete the Credential, click on the  icon to delete. When deleting the credential through IAdeaCare, this will only delete the credential from the server and not from the device. The device will need to be factory reset to clear all settings.



Certificate



To add a certificate, click **+ Add certificate** → 'Select' the certificate you want to upload → click '+ Add'




Certificate

+ Add certificate

Name ▾


Add certificate

Select a certificate to upload. **Select** 

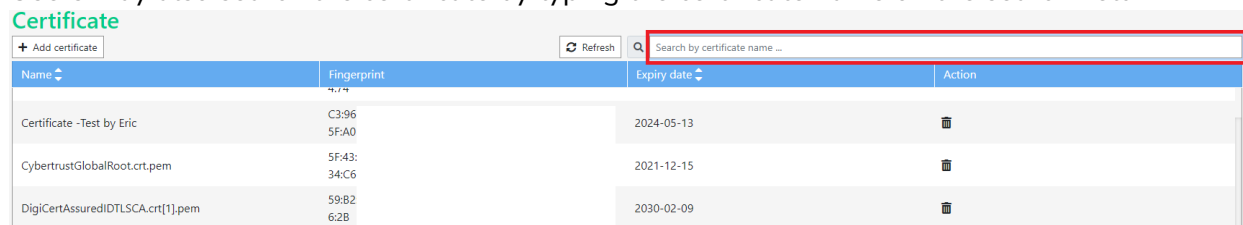
Certificate information :

Name


Size 3150




 Cancel **+ Add**

Users may also search the certificate by typing the certificate name on the search field.



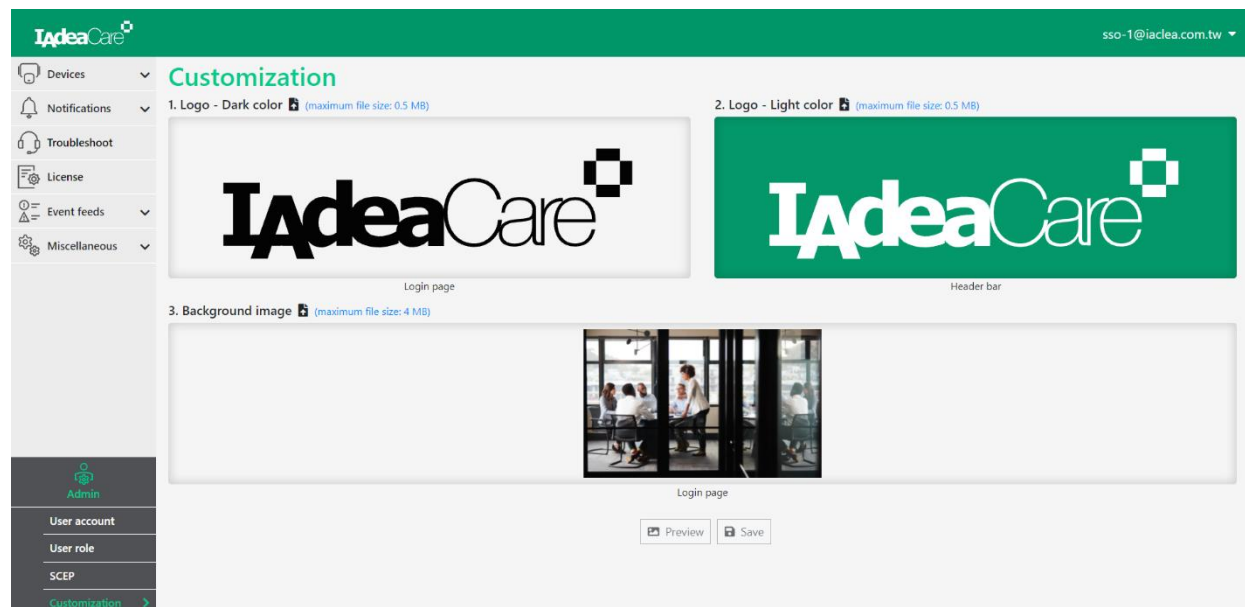
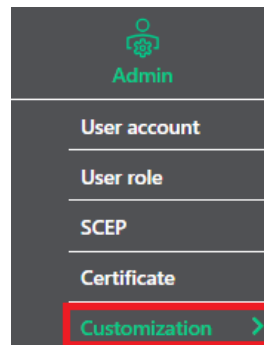
Certificate


+ Add certificate  Refresh

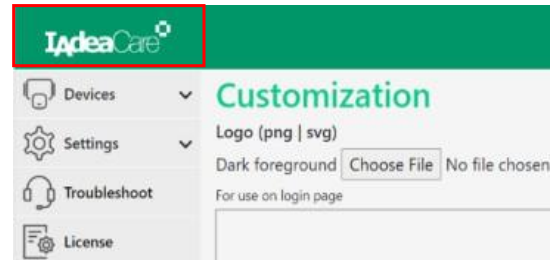
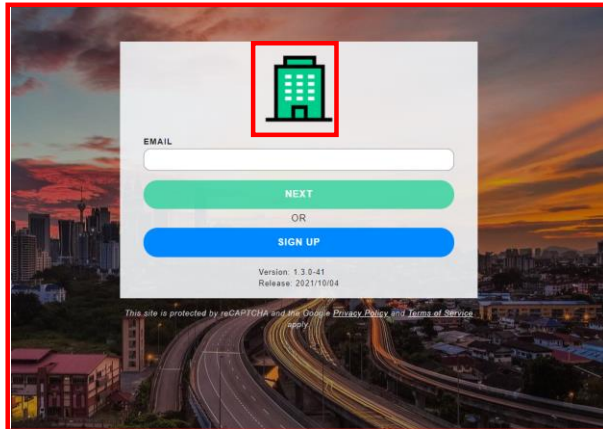
Name ▾	Fingerprint	Expiry date ▾	Action
Certificate -Test by Eric	C3:96 5F:A0	2024-05-13	
CybertrustGlobalRoot.crt.pem	5F:43: 34:C6	2021-12-15	
DigiCertAssuredIDTLSCA.crt[1].pem	59:82 6:2B	2030-02-09	

Customization

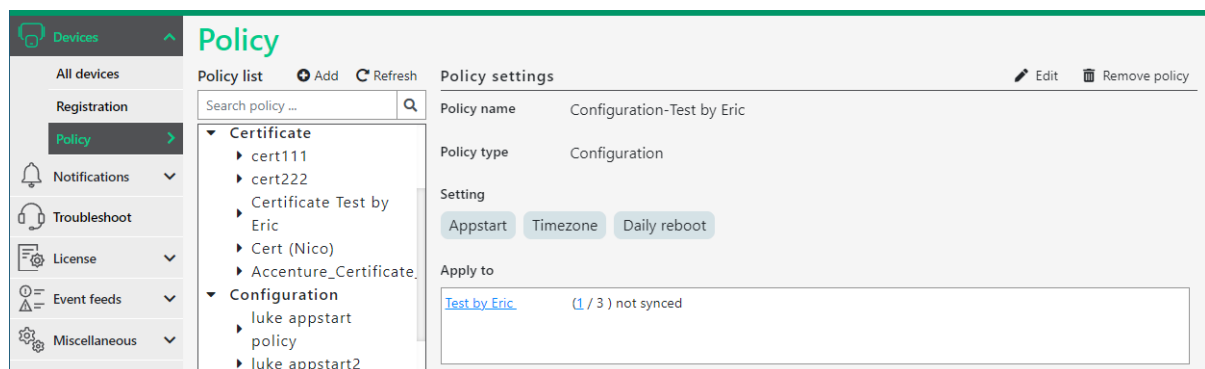
Enterprise allows the user to customize the IAdeaCare login page with branding and background. The logo branding on the top left-hand corner can also be customized.



Click the 'Choose file'  to upload logo and background image.
 Logo maximum file size: 500 KB. Supported format: .svg and .png
 Background maximum file size: 4 MB. Supported format: .jpg and .png



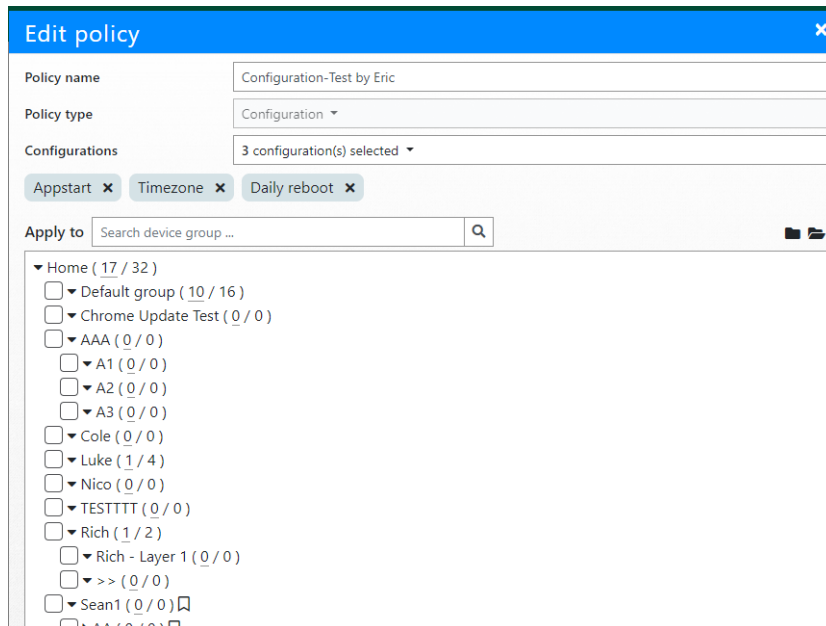
Policy Tab



Policy allows for search by policy name.

Quick Link to the applied Device Group is available for navigation.

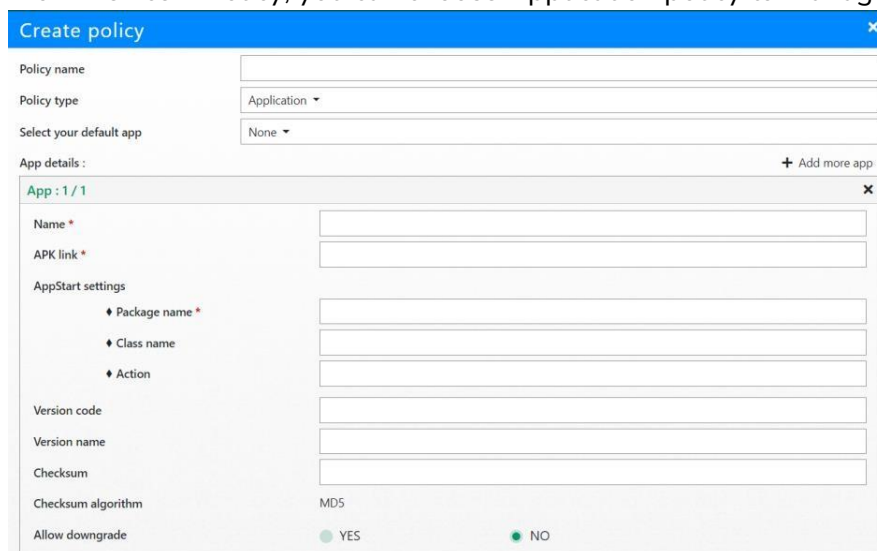
Quick Link and status of device not yet synced to policy is available for navigation.



Search bar is available for searching by group name when editing existing policy.

App Management policy (Exclusive to enterprise account)

From Device > Policy, you can choose Application policy to manage applications.



Click on **+Add more app** to add a new app add-on



APK link: URL where the apk is located.

Package name: Package name of the apk.

Class Name: Class name of the apk.

Action: Action of the apk.

Version code: Version code of the apk.

Version number: Version number of the apk.

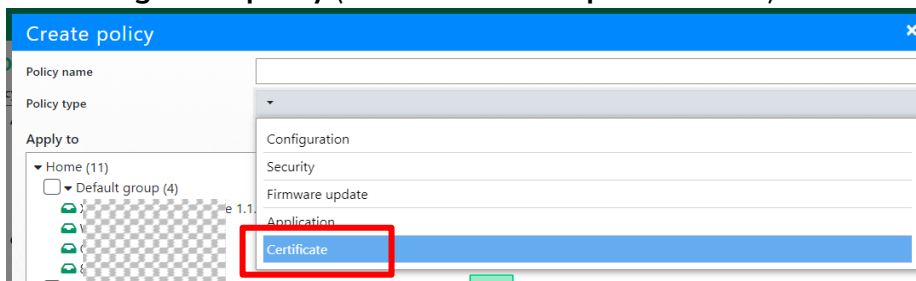
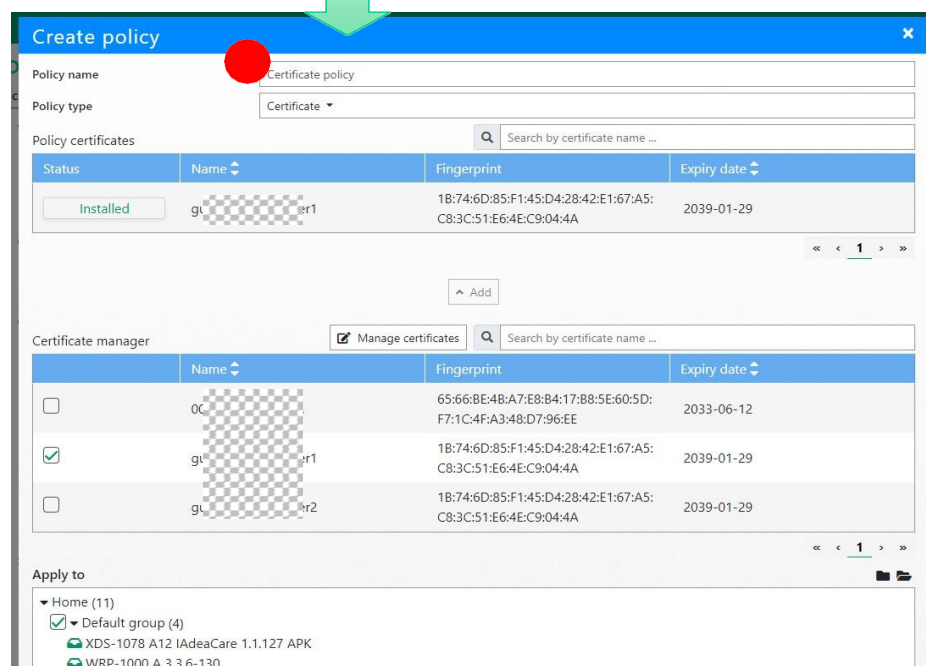
Checksum: The MD5 Checksum of the apk.

Allow downgrade: Allow/ Not allow downgrade to a lower version.

Select your default app: Choose the app for devices to launch automatically.



Certificate Management policy (Exclusive to enterprise account)

Status	Name	Fingerprint	Expiry date
Installed	gl...er1	1B:74:6D:85:F1:45:D4:28:42:E1:67:A5:C8:3C:51:E6:4E:C9:04:4A	2039-01-29

	Name	Fingerprint	Expiry date
<input type="checkbox"/>	OC...	65:66:BE:4B:A7:E8:B4:17:B8:5E:60:5D:F7:1C:4F:A3:48:D7:96:EE	2033-06-12
<input checked="" type="checkbox"/>	gl...er1	1B:74:6D:85:F1:45:D4:28:42:E1:67:A5:C8:3C:51:E6:4E:C9:04:4A	2039-01-29
<input type="checkbox"/>	gl...er2	1B:74:6D:85:F1:45:D4:28:42:E1:67:A5:C8:3C:51:E6:4E:C9:04:4A	2039-01-29

- Certificate option is now available when creating policy
- To apply new certificate to device group
 1. Give policy a name
 2. Select the certificate from the certificate manager. For certificate to be used in policy, it must be added to certificate manager by admin user
 - b. If a certificate is being used in a policy but got removed from the certificate manager, the certificate will become an unmanageable certificate which will be hidden from policy certificate after a new change applied to this policy
 3. Click Add to add certificate to the policy
 - a. For each certificate user can click on installed under status to change certificate status to revoke
 - b. A revoked certificate will be disappeared from the policy certificates after user confirm the change by hitting Apply button
 4. Choose the device group to apply the certificate
 5. Click Apply to create the policy