



ESI eAccess

ESI Access Dashboard User's Guide

This document will guide the Access Dashboard Admin through setting up and managing Access Devices, People, Groups and Schedules.

Overview	3
Configuring the Access Device for the Access Dashboard	4
Creating and Managing Accounts	6
Dashboard Access Login	12
Dashboard	14
People	14
Add Person	15
Delete Person	16
Edit Person Information	16
Import CSV	17
Devices	19
Groups & Schedules	22
Groups	22
Device Profiles (for Groups and Schedules)	24
Creating a Profile	24
Time Plan (aka Door Unlock Schedule)	26
Creating a time plan	26
Daily schedule	27
Weekly schedule	28
Monthly schedule	29
Selecting Inactive Dates	29
Viewing Created Time Plans	30
Image Snapshot	31
Setup	32
Helpful Tips	32

Overview

ESI Access Dashboard (AD) enables you to manage People and Devices associated with premise access for both eSIP Evolution and eCloud Service.

People – managing the access cards associated with people, which can be employees, vendors, etc.

Devices – managing the access devices typically installed at doors.

Who should use Access Dashboard?

Administrators of an office building, school or government building where security is important would find this tool handy and convenient.

There is master admin access for one individual at a site. This individual can create additional admins for the site. These admins can view all access records at a site. They can manage the devices and people along with managing schedules for door access.

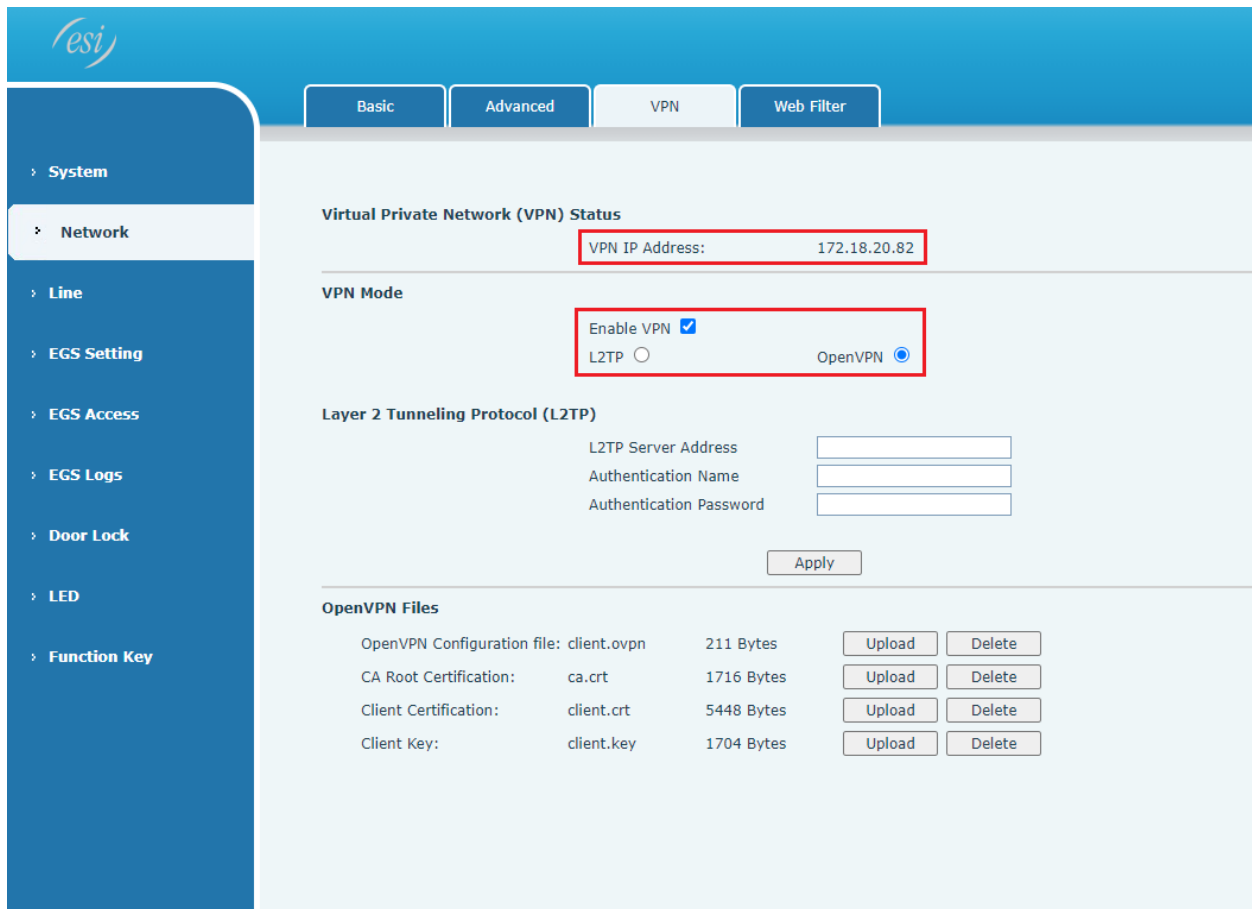
Configuring the Access Device for the Access Dashboard

The Access Device must first be configured to communicate with the ESI Access Dashboard. Please confirm that your device firmware is above 2.6.1.6877 for Cloud systems and 2.6.1.6876 for eSIP systems.

To set up the device for the Access Dashboard, the following steps must be followed,

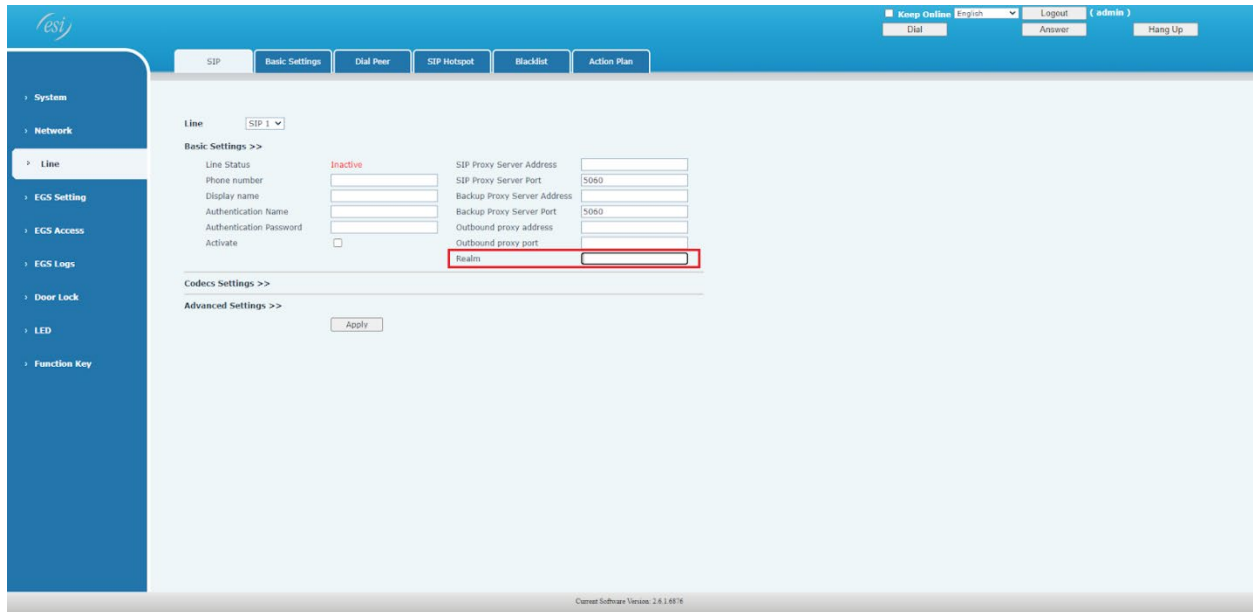
Enable VPN on the Access Devices

- Confirm the OpenVPN Files are loaded on the device.
- Go to Network and select the VPN Tab.
 - Make sure Enable VPN is selected.
 - Make sure OpenVPN is selected.
 - Select Apply
- The VPN IP Address should change to something other than all 0's.



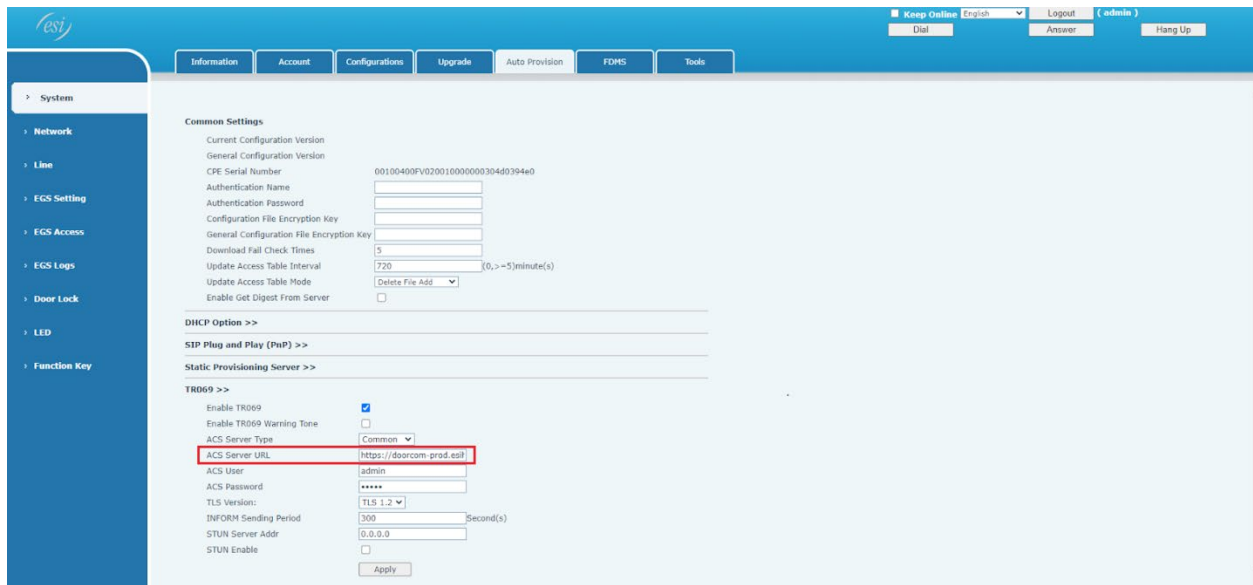
Updating the Realm with Domain name (eSIP Only)

- Navigate to Line>Sip.
 - Modify Realm to match the domain that was created for the account.
 - Select Apply.



Confirm the ACS Server URL


- Navigate to System>Auto Provision.
- Select TRO69.
- Verify that the ACS Server URL is <https://doorcom-prod.esihs.net:7547>.



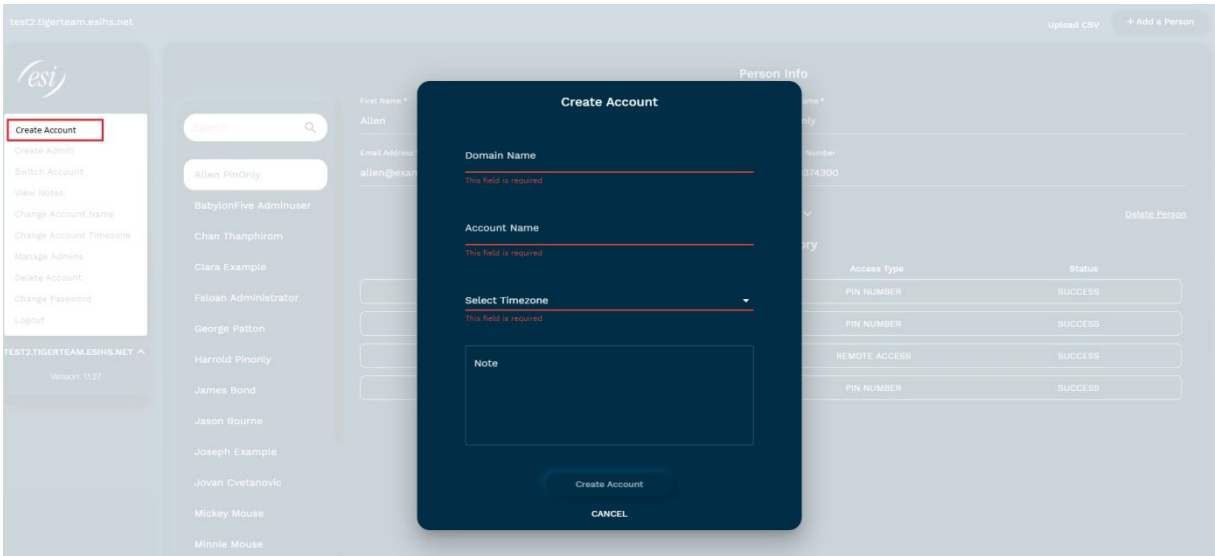
The Access Device should now be able to communicate with the ESI Access Dashboard. You can now set up the Access Dashboard.

Creating and Managing Accounts

Create Account (SuperUser only)

To create an account click the down arrow  on the left side of the screen then select Create Account.

Enter Domain Name, Account Name, Notes that you may want someone to be able to refer back to, select Timezone and select Create Account, or press the Cancel key to exit.



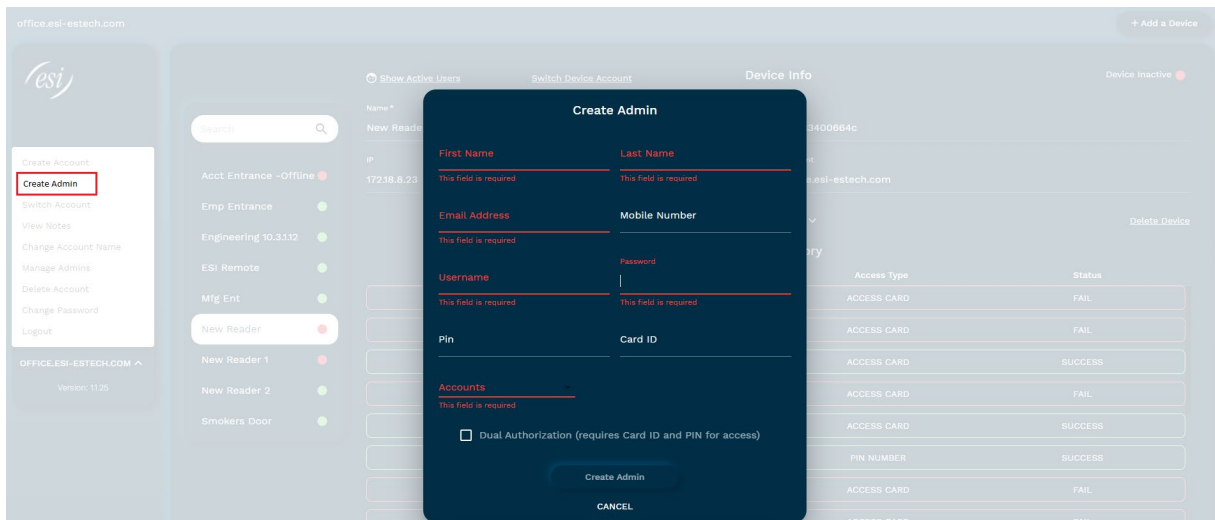
Create Admin (SuperUser Only)

The first Admin for an account can be created by a SuperUser. This admin manages the setup of people, groups and devices as well as can set up additional admins for an account.

To create an account admin select the account on the left hand side of the screen and Select Create Admin.

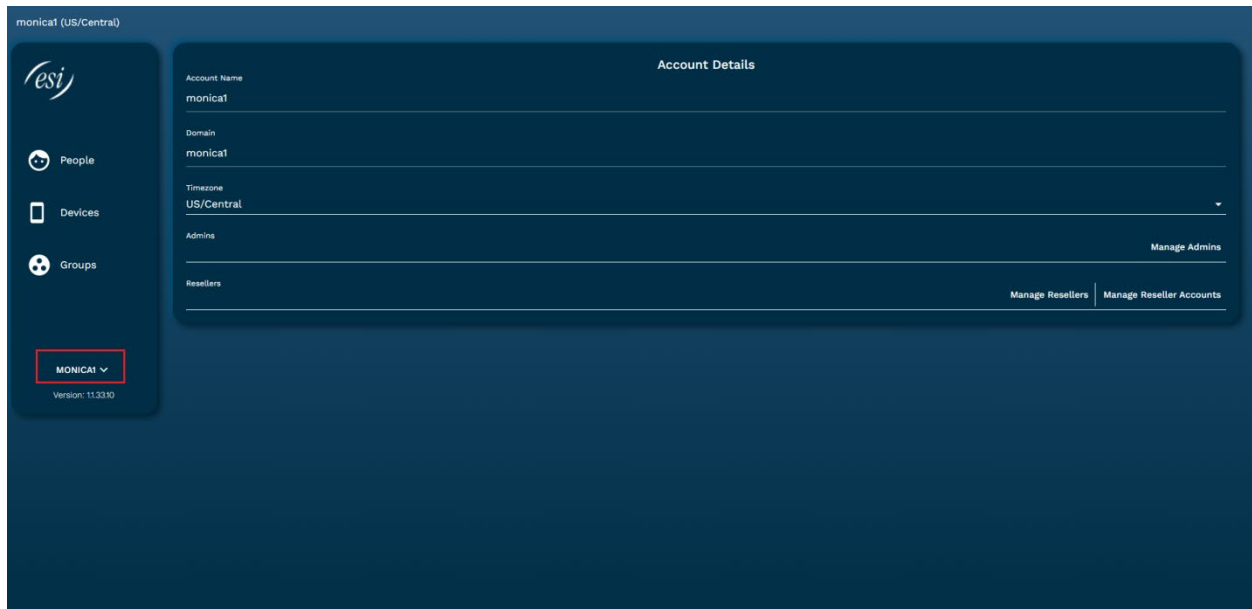
Enter First Name, Last Name, Email Address, Mobile Number (optional), Username, Password, Pin (optional), Card ID (optional), dual Authorization (optional) and select the Account that the user will be authorized to access.

Click Create Admin or press Cancel key to exit.



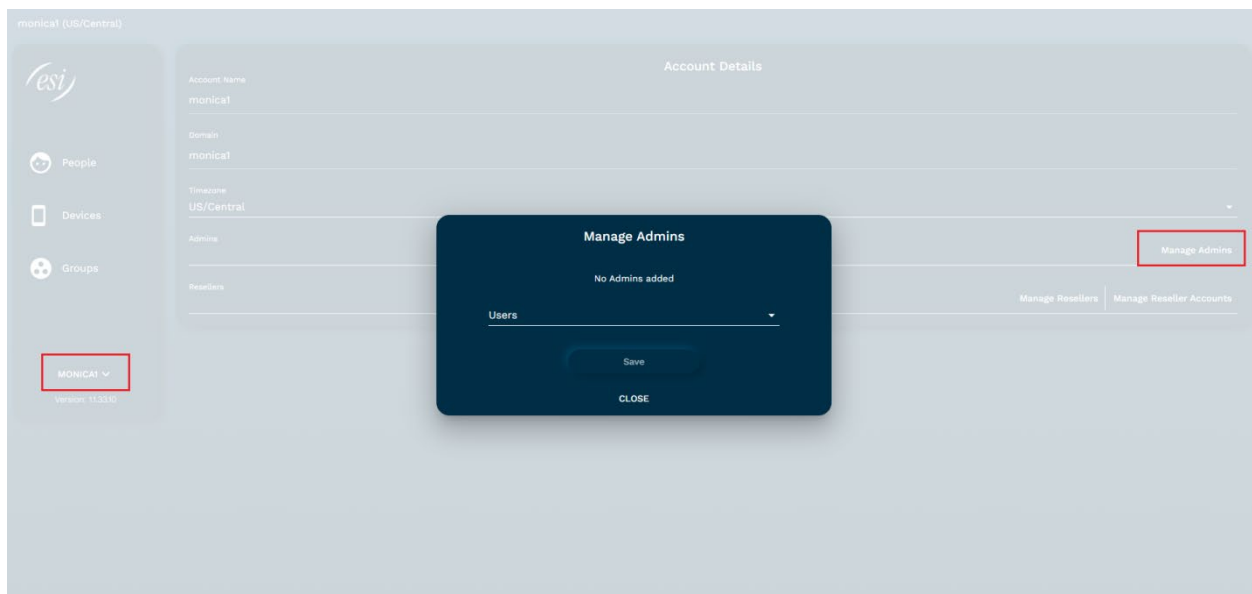
View Account Details

To view, set up or remove admin access for an account select the account on the left hand side of the screen and Select View Account Details.

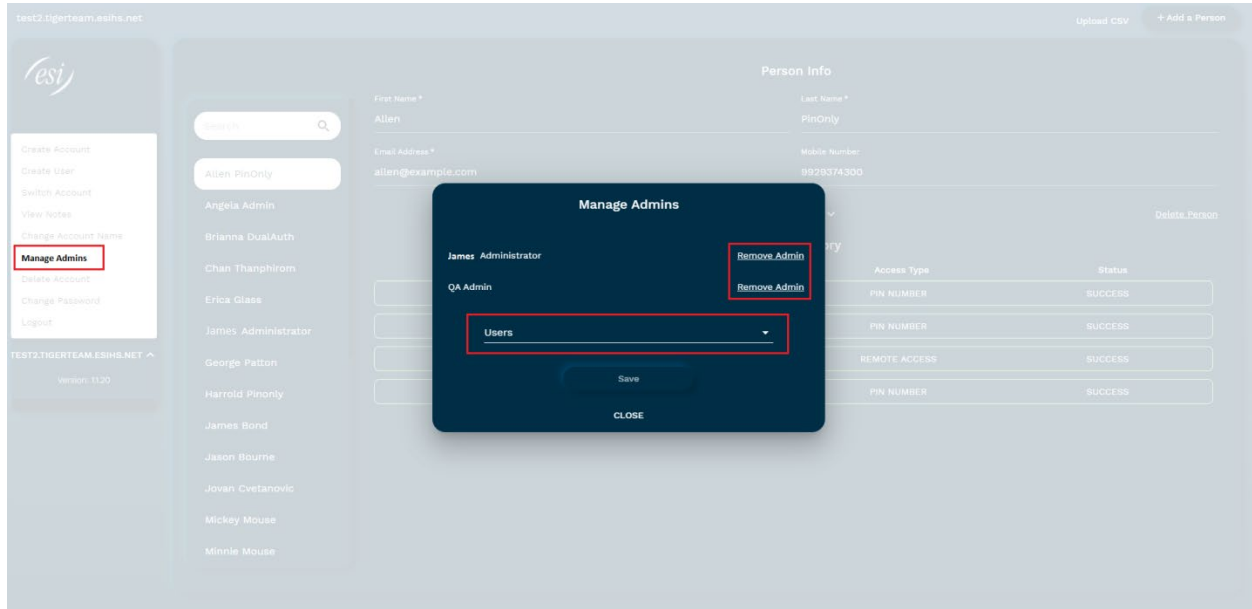


Manage Admins

To set up or remove additional administrators for an account select the account on the left hand side of the screen by clicking the arrow on the left of the screen as shown in the picture below then clicking Switch Account. Once an account has been selected, again select the down arrow on the left, select View Account Details from the list and Select Manage Admins on the right of the screen. To promote an existing person to an admin select the Users dropdown, choose the person to add the ability to have admin functions and select Save. They will be sent an email notifying them they have been made an admin with a link to create a password.

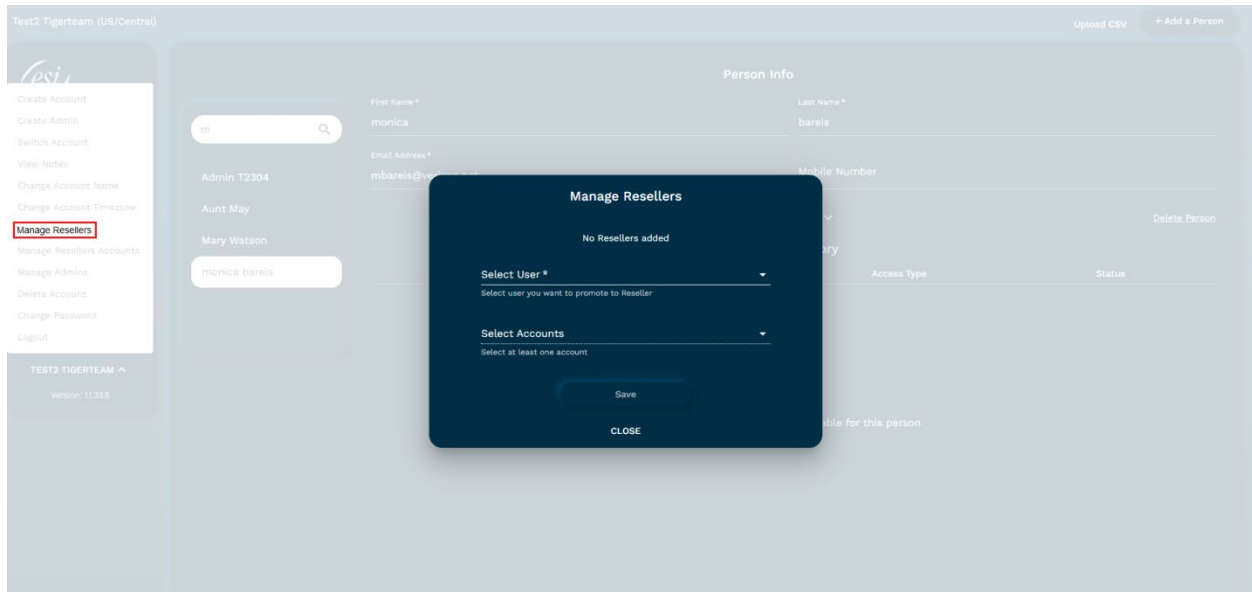


To remove a person from admin capabilities, select Remove Admin next to the name. They will be sent an email notifying them they have been removed from having admin capabilities.



Manage Reseller (SuperUser Only)

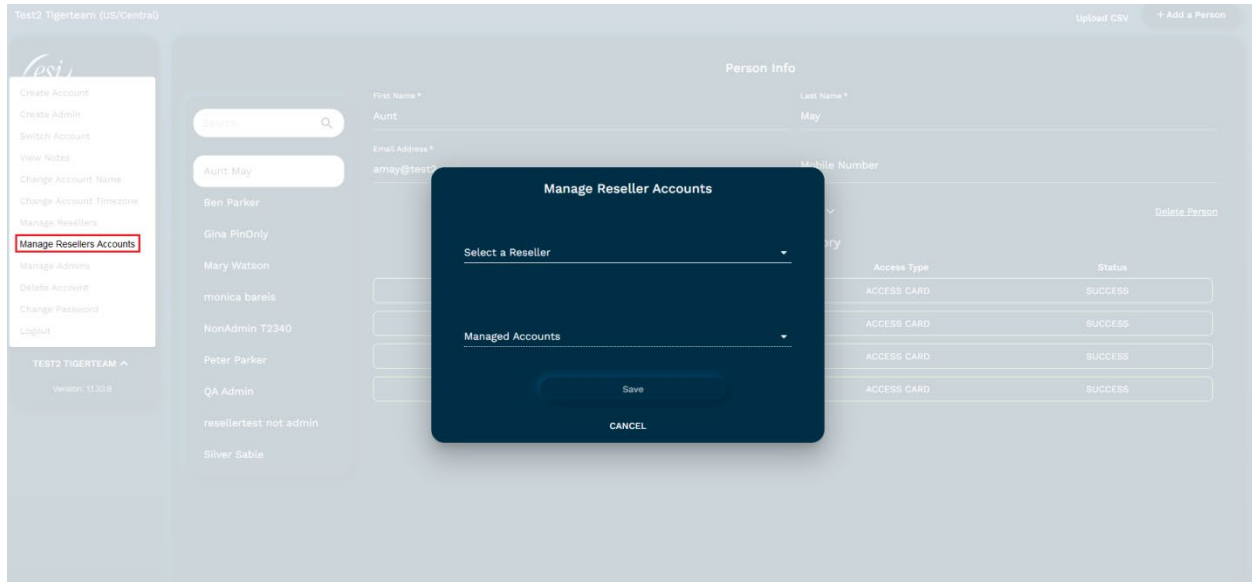
A reseller is a person who is allowed to manage multiple accounts. To promote a user to reseller, go to the account that has the user that you wish to promote to a reseller. Once in that account, Select View account details and Select Manage Resellers. Select the user from the dropdown menu and Select the accounts that the user will be an admin of and select save.



They will be sent a message to create a password. Once they login, it will default to an account which will be displayed in the upper left hand corner.

Manage Reseller Accounts (SuperUser)

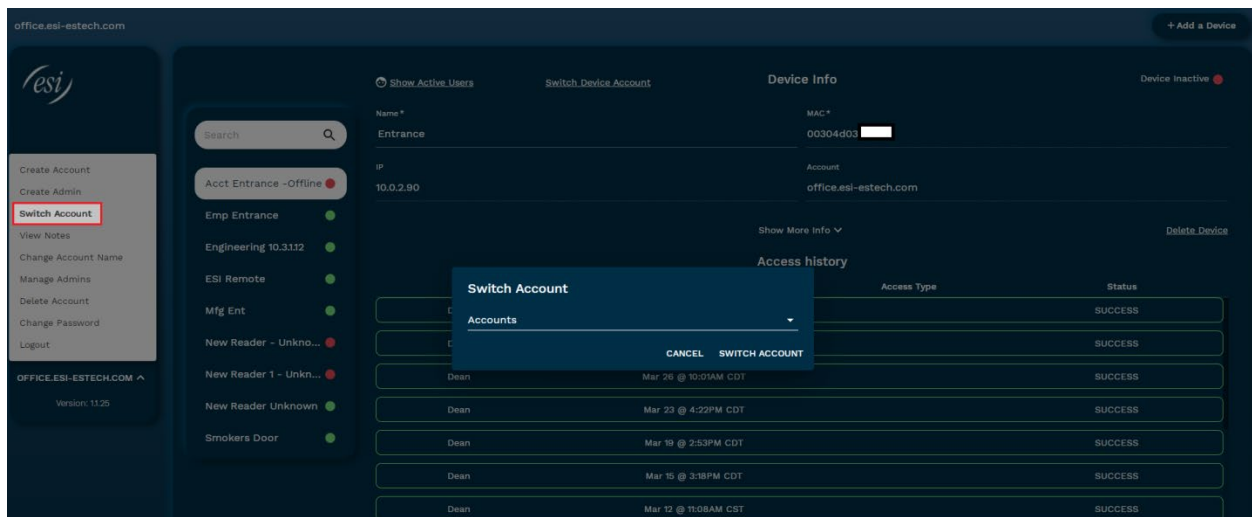
To manage a reseller account for the addition or removal of accounts, select an account that the reseller currently manages. Once in that account, Select View account details and Select Manage Reseller Accounts. Select accounts to add or delete. If an account is deleted, all admin rights for that user for the account will be removed.



Switch Account (SuperUser and Reseller only)

To switch to a different account select the account on the left hand side of the screen and select Switch Account.

Select an account from the drop down menu and click Switch Account.



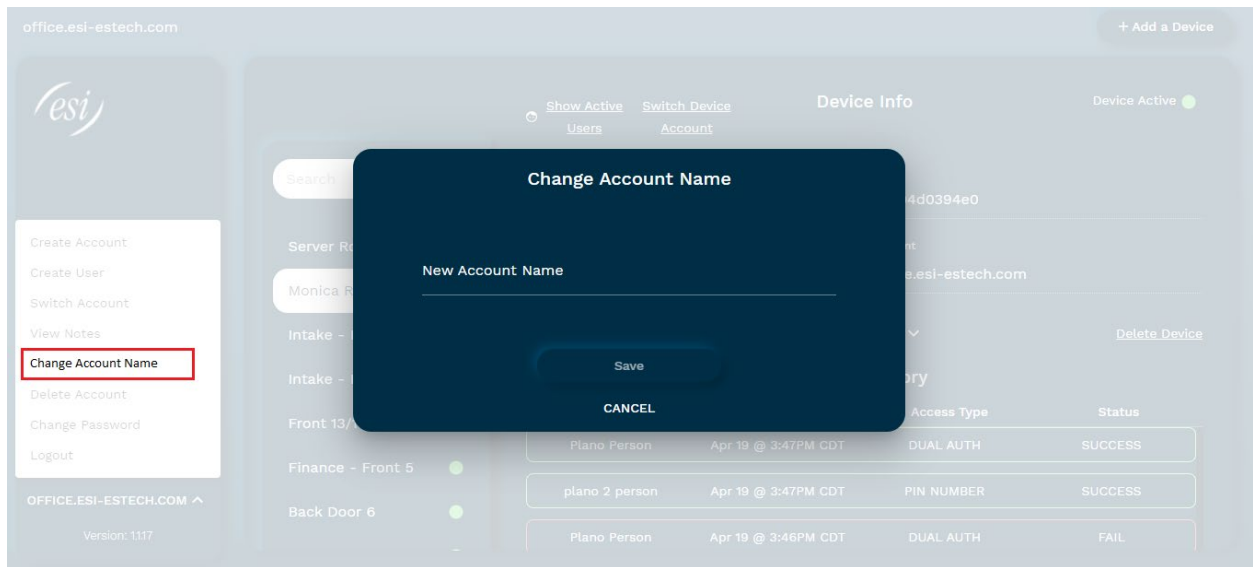
View/Add Notes (SuperUser only)

To view or add any additional Notes on the account select the account on the left hand side of the screen and select View Notes.



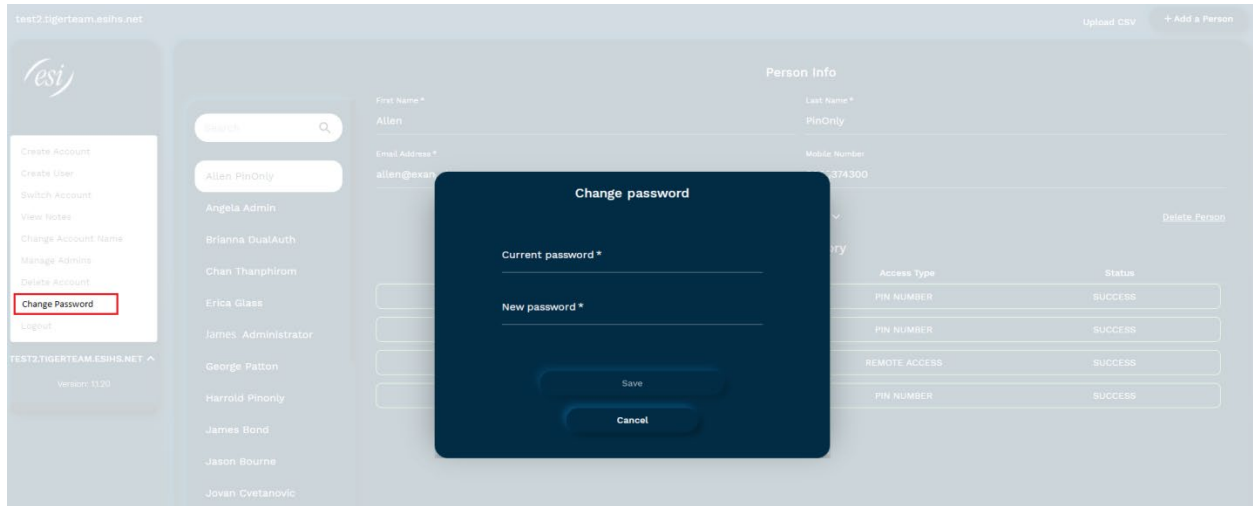
Change Account Name (SuperUser Only)

To change the Account Name, select the account on the left hand side of the screen and select Change Account Name. Note: the Account Name will be modified but the DOMAIN name will remain the same.



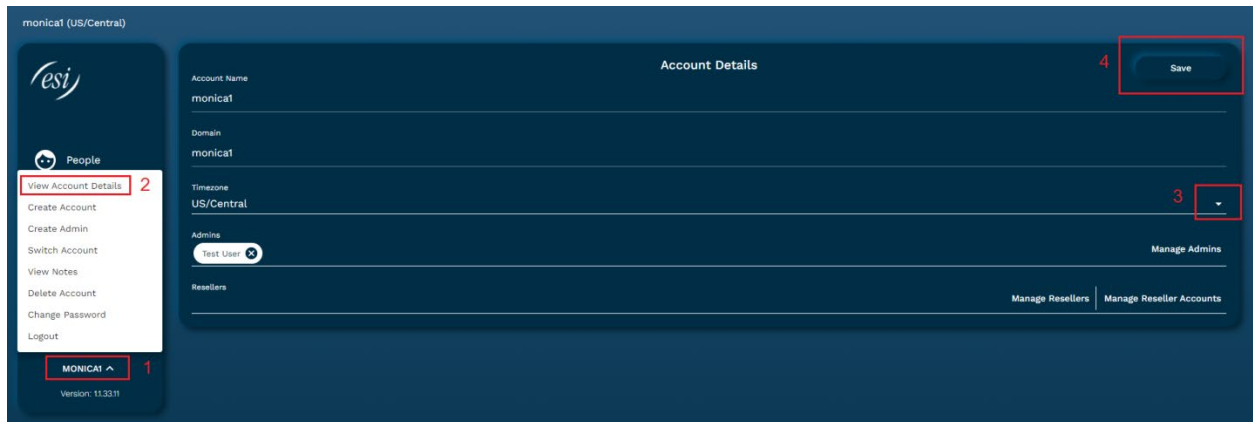
Change password

To change password, click on the account located on the left side of the screen and click Change Password.



Change Account Timezone

To change the account timezone, Select View Account Details from the down arrow on the bottom left, then select the dropdown arrow on the right to change the timezone then select save.



Dashboard Access Login

How do I access the ESI Access Dashboard?

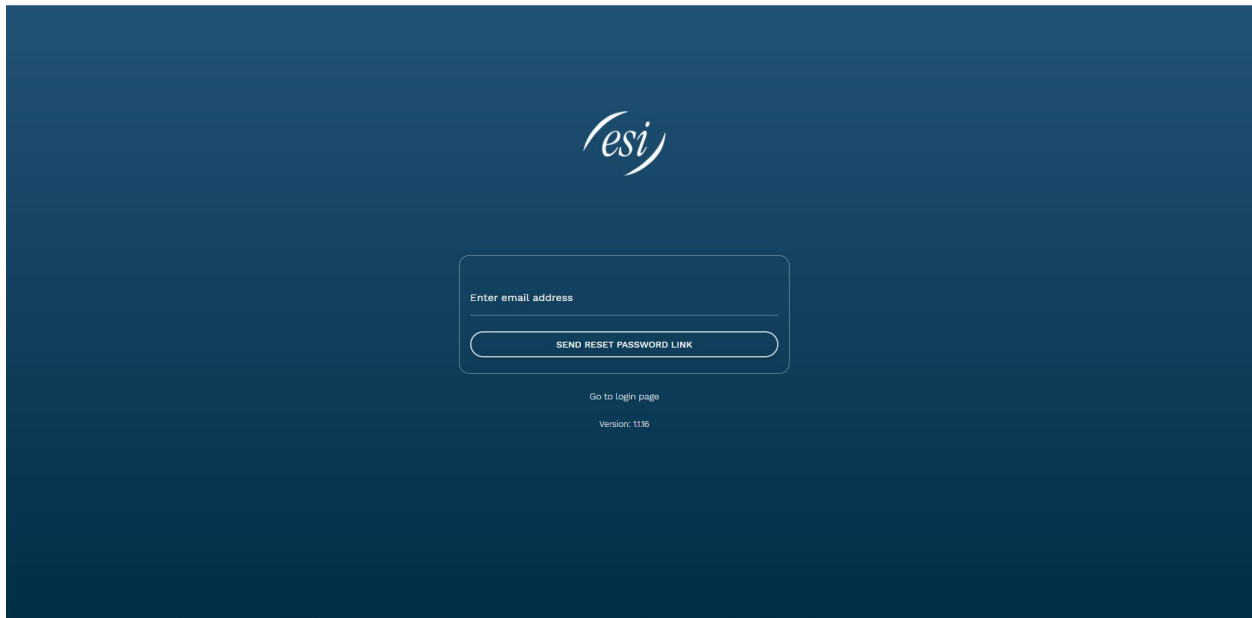
Go to URL <https://esiaccessmanager.com>

The admin will log in with their credentials provided by ESI.



Forgot Password

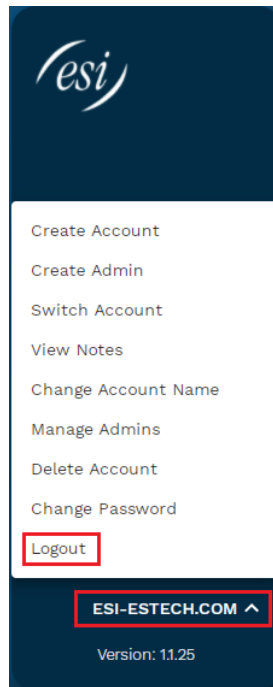
If the admin has forgotten their password, select Forgot password.



Enter in the email address and select Send Reset Password Link. The password reset link will be sent to your email if it matches an account on the system and the screen will be redirected to the login page.

Logout

To log out, click on the account located on the left side of the screen and click Logout.



Dashboard

Dashboard shows the aggregated activity of all the devices in one view. At the top of the screen you will see how many devices are active as well as the number of successful and failed entries for the time period. A graph is displayed followed by a log of all device activity.

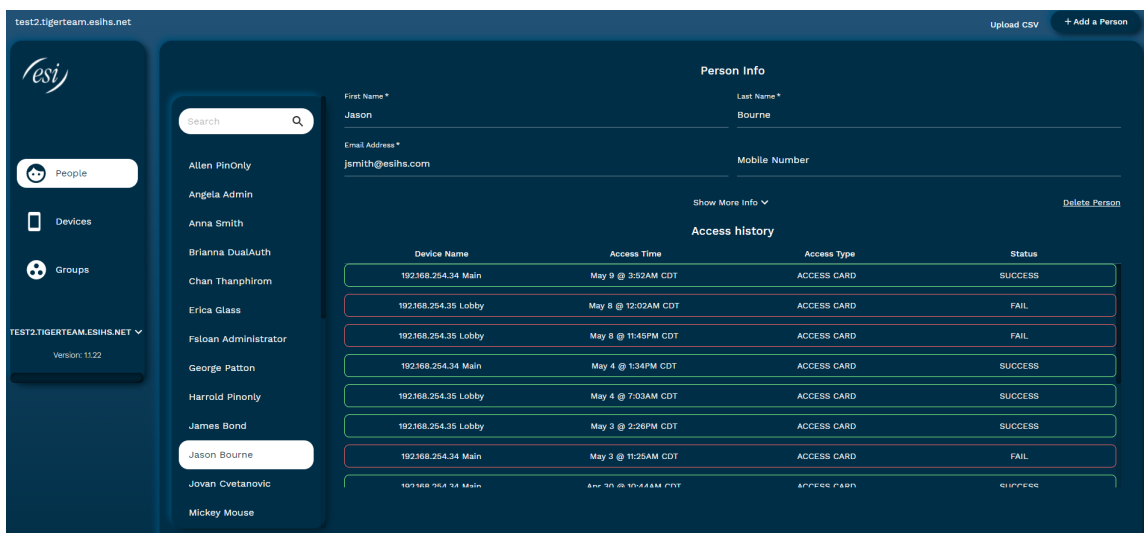


People

People consists of anyone associated with a site that has an access card or pin number. This could be a full time employee, seasonal worker, contractor, vendor, or maintenance staff. A person has a unique card ID that allows for entry and exit at a specified door. A person can belong to one or more groups.

As shown in the screen below the following information associated with each person is displayed: first name, last name, and groups. To display more information for that person, select the **Show More Info** where all of the information associated with that person (first and last name, email, phone number, card ID, pin, dual authorization and groups) will be displayed. The list of People is sorted alphabetically by first name.

When selecting a person a history of their access logs will be presented.



Add Person

To add a person, select People and click on the **+Add a Person** button in the upper right corner. A description of fields is as follows;

First Name – first name of person

Last Name – last name of person

Email Address – email address

Mobile Number – mobile number

Card ID - numeric badge ID

Pin – numeric 4-6 digit

Dual Authorization – select this to enable required card ID and Pin for access

Click **Save and close** when done, or click **Save and add new** to add another person.

The screenshot displays the 'Add Person' modal in the ESI system. The modal is a dark blue box with white text and input fields. It contains the following fields and options:

- First Name *
- Last Name *
- Email Address *
- Mobile Number
- Card ID
- Pin
- Dual Authorization (requires Card ID and PIN for access)

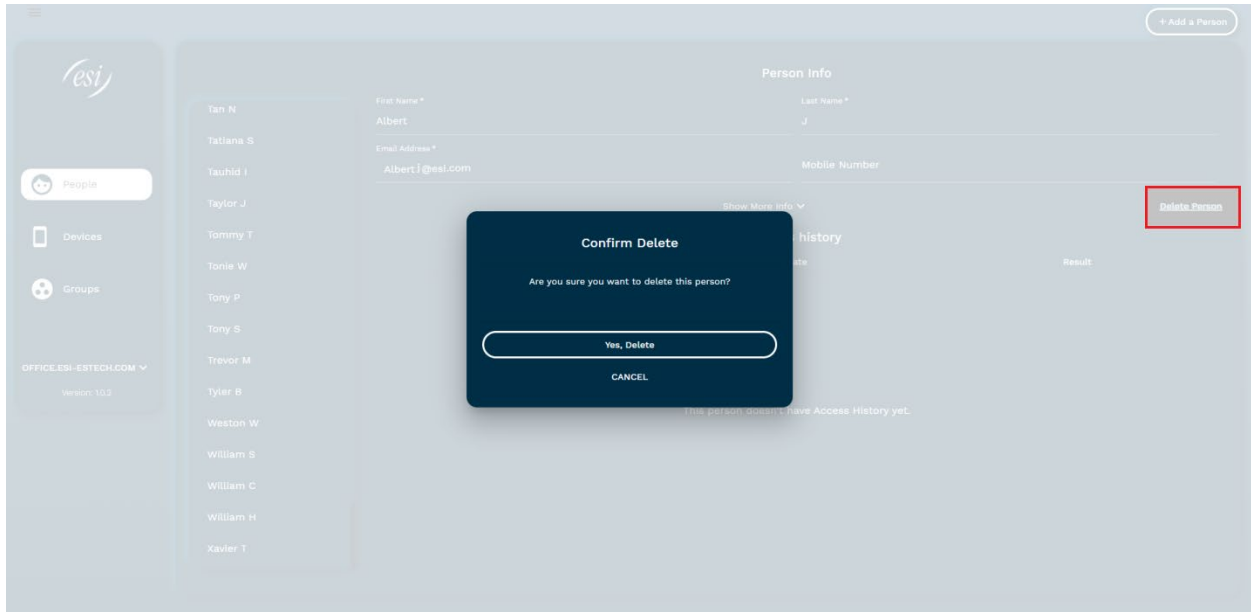
At the bottom of the modal are three buttons: "Save and close", "Save and add new", and "CANCEL".

The background shows the ESI system interface. On the left is a sidebar with the "esi" logo and navigation options: "People", "Devices", and "Groups". The "People" option is selected. Below the sidebar is a search bar and a list of users: Allen PinOnly, Angela Admin, Anna Smith, Brianna DualAuth, Chan Thanphirom, Erica Glass, Fslon Administrator, George Patton, Harrold Pinony, James Bond, Jason Bourne (highlighted), Jovan Cvetanovic, and Mickey Mouse. On the right side of the background, there is a "Person Info" form for Jason Bourne and a table of access logs.

Access Type	Status
ACCESS CARD	SUCCESS
ACCESS CARD	FAIL
ACCESS CARD	FAIL
ACCESS CARD	SUCCESS
ACCESS CARD	SUCCESS
ACCESS CARD	SUCCESS
ACCESS CARD	SUCCESS
ACCESS CARD	FAIL
ACCESS CARD	SUCCESS

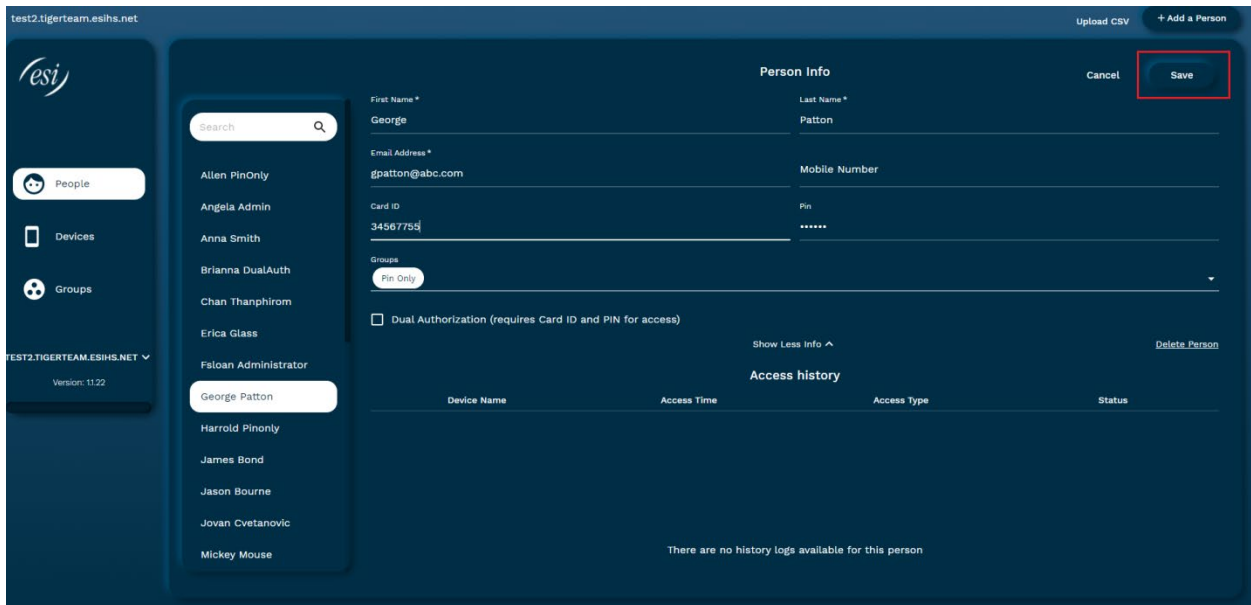
Delete Person

To delete a person, select People, locate the person you would like to delete and select Delete Person located on the right side of the screen. Upon selection you will be asked to confirm delete.



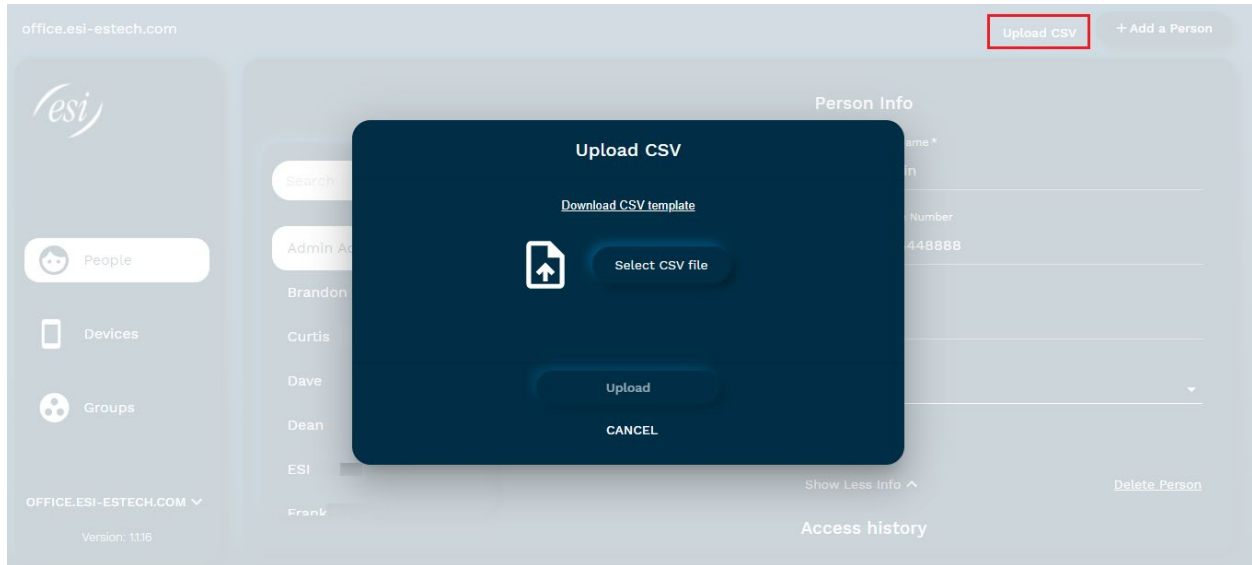
Edit Person Information

To edit people information, select People, locate the person you would like to edit and modify the corresponding field. Upon modification, select the Save button that appears in the top right hand corner.



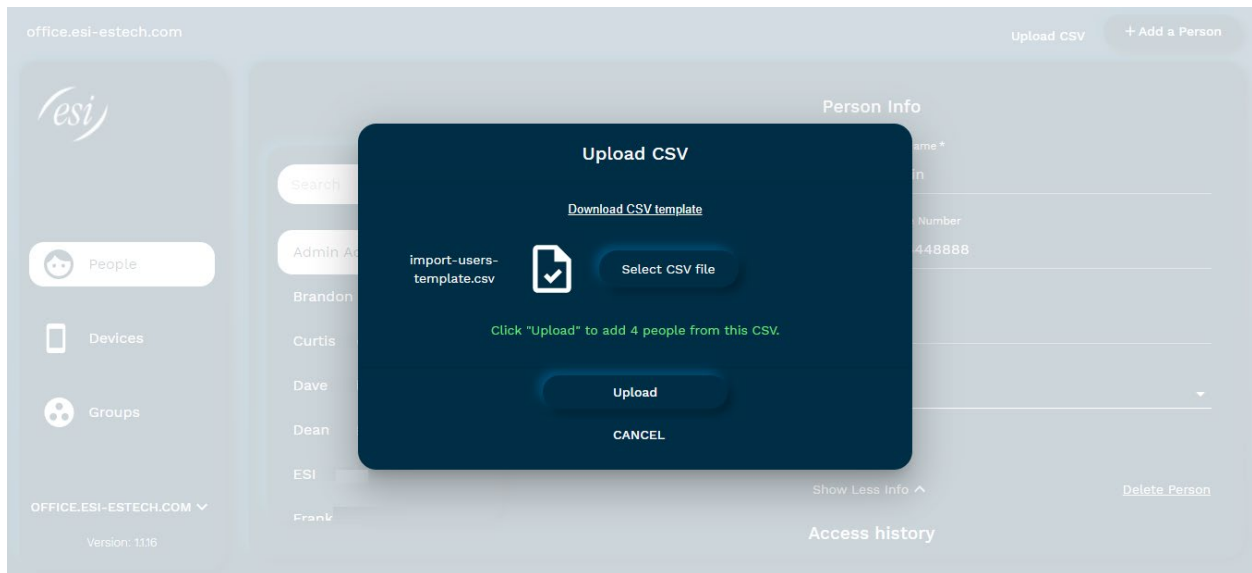
Import CSV

To import a CSV file select Upload CSV from the upper right hand corner of the screen.



Select Download CSV template. Once downloaded, input the information for each column and save as .csv. Select the Select CSV file. The csv file will be displayed to the left of the Select CSV file button. Click Upload to add the people to your dashboard.

Note: if a program such as Google Sheets or Excel is being used to modify the .csv file, the formatting for both Card ID and Pin fields needs to be changed to "Plain Text," in order for leading 0's to be programmed and accepted.



If the import is successful, a banner will display at the top of the screen.

The screenshot shows the ESI user management interface. At the top, a green notification banner states "Successfully imported 4 users from CSV file". The interface includes a sidebar with navigation options: People, Devices, and Groups. The main content area displays the details for a user named "Admin".

Person Info

First Name *	Last Name *
Admin	Admin
Email Address *	Mobile Number
admin@msn.com	8884448888

[Show More Info](#) [Delete Person](#)

Access history

Device Name	Access Time	Access Type	Status
There are no history logs available for this person			

Devices

Supported access devices consist of the following – AC20, AC30v, and AC32v.

As shown in the screenshot below, the information associated with each device is quite simple – Device Name, Model, Device Groups, IP address, MAC address, Account name and Last updated.

Once the devices have been added to the system (eSIP, eCloud) and are online the Access Dashboard will automatically search for these devices when launched. A list of devices that have been added to the system will be displayed when Devices are selected. A green dot next to the device means it has been registered and is active. A red dot means the device is registered and inactive and a yellow dot means the device has not been registered.

The device name will first appear as its IP address. You can rename the device so it is easier to find, such as, “Front Door”, Network Room”, or “Receiving”.

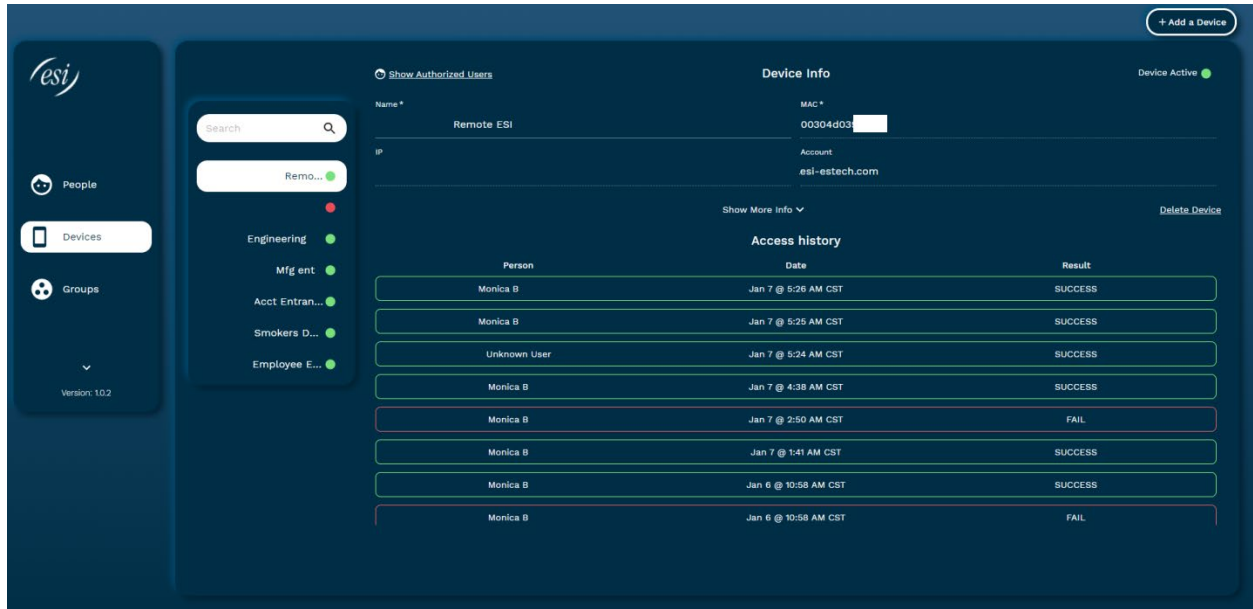
When selecting a device the access history will be presented. It will show the person’s name, access time, Access Type and access Status, whether it was a success or fail.

The screenshot displays the eSIP Access Dashboard interface. On the left is a navigation sidebar with 'People', 'Devices', and 'Groups' options. The main area is titled 'Device Info' and shows details for a device named 'Emp Entrance'. The device is active, indicated by a green dot. The information includes: Name: Emp Entrance, MAC: 00304d03, IP: 10.0.2.76, Account: esi-estech.com, Model: AC30v, and Last Updated At: 2021-05-19T21:49:23.613Z. Below the device info is an 'Access history' table with columns for Person Name, Access Time, Access Type, and Status.

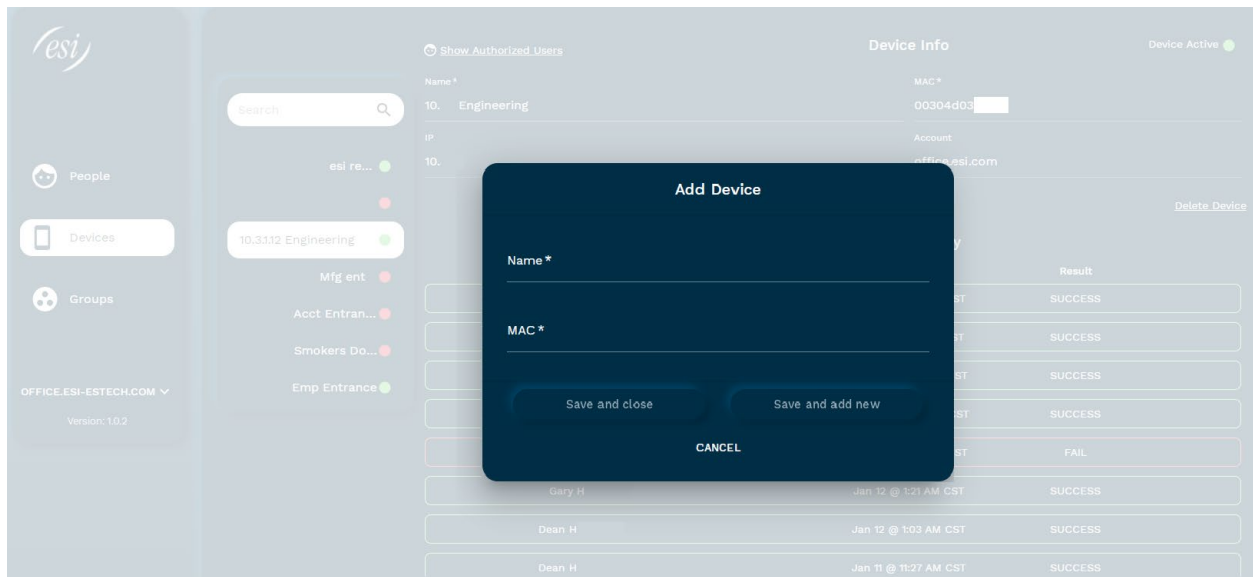
Person Name	Access Time	Access Type	Status
Chuck	May 18 @ 5:50PM CDT	ACCESS CARD	SUCCESS
William	May 18 @ 12:35PM CDT	ACCESS CARD	SUCCESS
Unknown User	May 25 @ 9:59AM CDT	ACCESS CARD	FAIL

Add Device Manually (SuperUser Only)

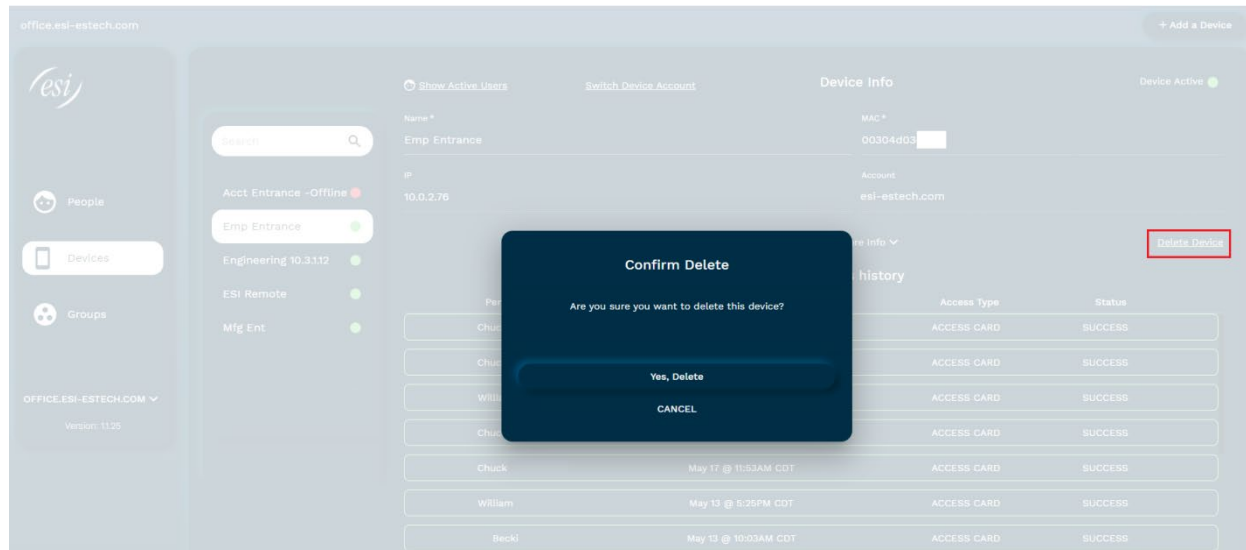
To add a device manually, select the **+Add a Device** button in the upper right corner.



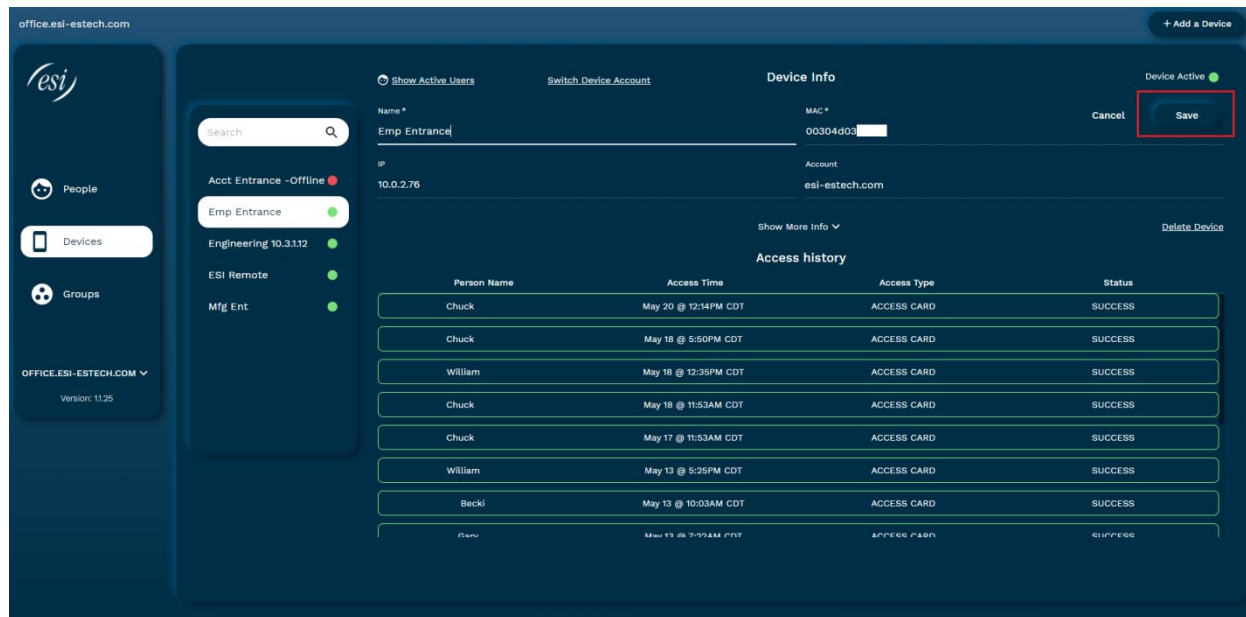
Enter in the Device Name and MAC address and select **Save and close** to exit, or to enter in another device select **Save and add new**. For manual entry, the system does not require the IP address or the model name as those will automatically populate when the devices are found and registered by the system.



To delete a device, select Devices, locate and select the device you would like to delete and select Delete Device located on the right side of the screen. Upon selection you will be asked to confirm delete.



To edit the Name or Group on a device, select Devices, locate and select the device you would like to edit and modify the fields. Upon modification, select the Save button that appears in the top right hand corner. The following fields may not be modified on a device: MAC, IP, Account, Model and Last Updated At.



Groups & Schedules

Schedules can be created to control the time range and People who have access to a specific device. For example you may only want employees to have access to the building between 7am – 6pm. For especially secure rooms that contain sensitive information like a network room, pharmaceutical closet, or file room you may want to restrict access to only approved employees during a specific time range.

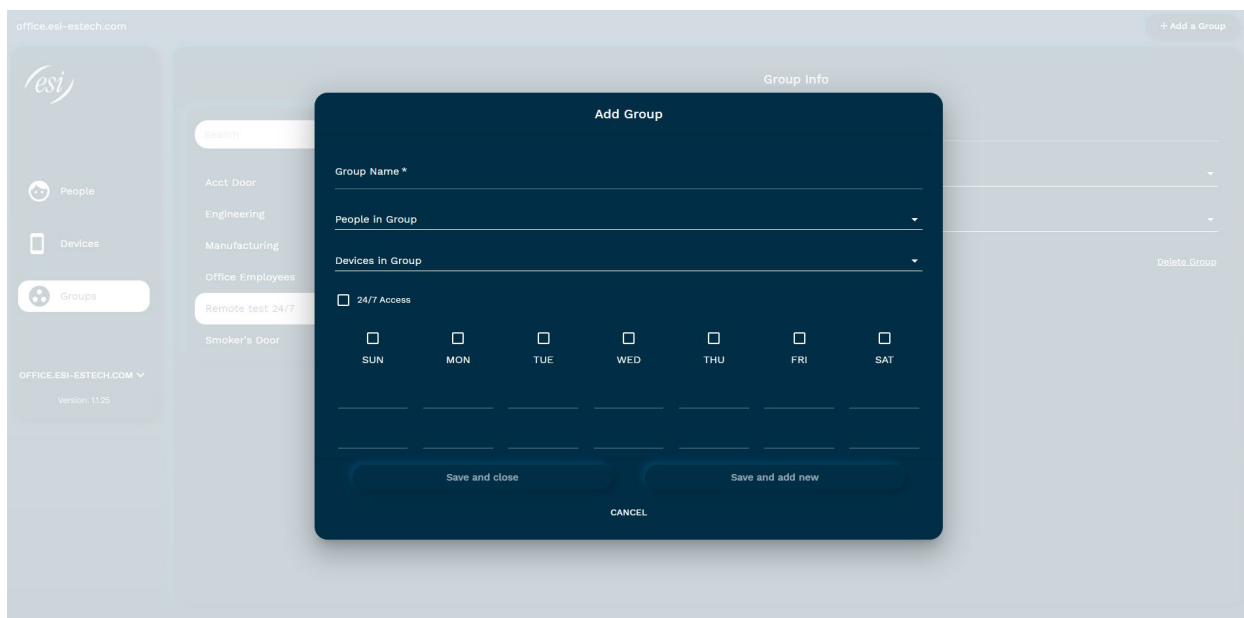
Groups

A group is a collection of specific People based on how they access the building or certain areas. A group should have a descriptive name but may not necessarily be the same groups or departments created on the phone system. For example the phone system may have a department called “Support” consisting of all employees associated with the Support department. However you may not want this same group to have the same access to some or all the devices. The Support department may work in shifts and therefore you will want to create two or more access groups in Access Dashboard to manage when the various Support employees can enter the building. Also consider temporary employees, janitorial staff, and vendors who may need access to your facility.

A person (People) can be added to more than one group. For example the IT manager may be part of the IT group that is created in Access Dashboard but is also one of only a few people who can access the Network Room. Therefore you will want to add them to more than one group within Access Dashboard.

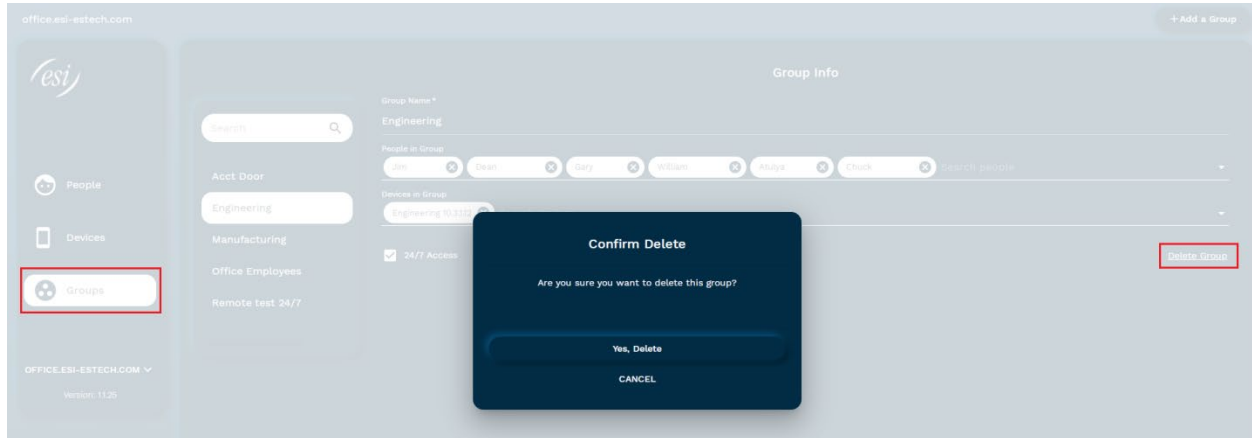
Access privileges are defined at the group level. A person inherits privileges from the group to which they are added. Creating a group

To Create a group select Groups and the **+Add a Group** button.

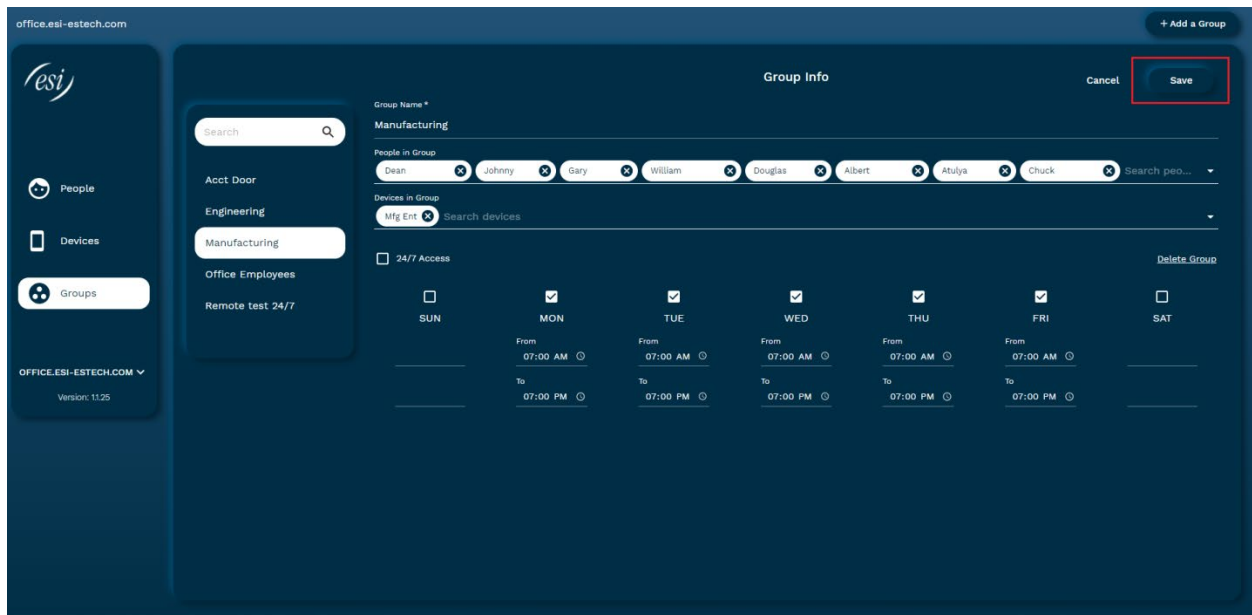


Complete the group's information and schedule and select **Save and Close** to exit. In case of an internet outage, the last schedule sent will be currently retained by the device. For example if a user is scheduled from 8:00 am to 5:00 pm, and the internet goes out at 4:55 pm the user will remain active on the device until such time when internet is restored and the updated schedule is received.

To delete a group and associated schedule, select Groups, locate the group you would like to delete and select Delete Group to the right of the screen. Upon selection you will be asked to confirm delete.



To edit group information or schedule, select Groups, locate the group you would like to edit and modify the corresponding field or schedule. Upon modification, select the Save button in the top right hand corner.



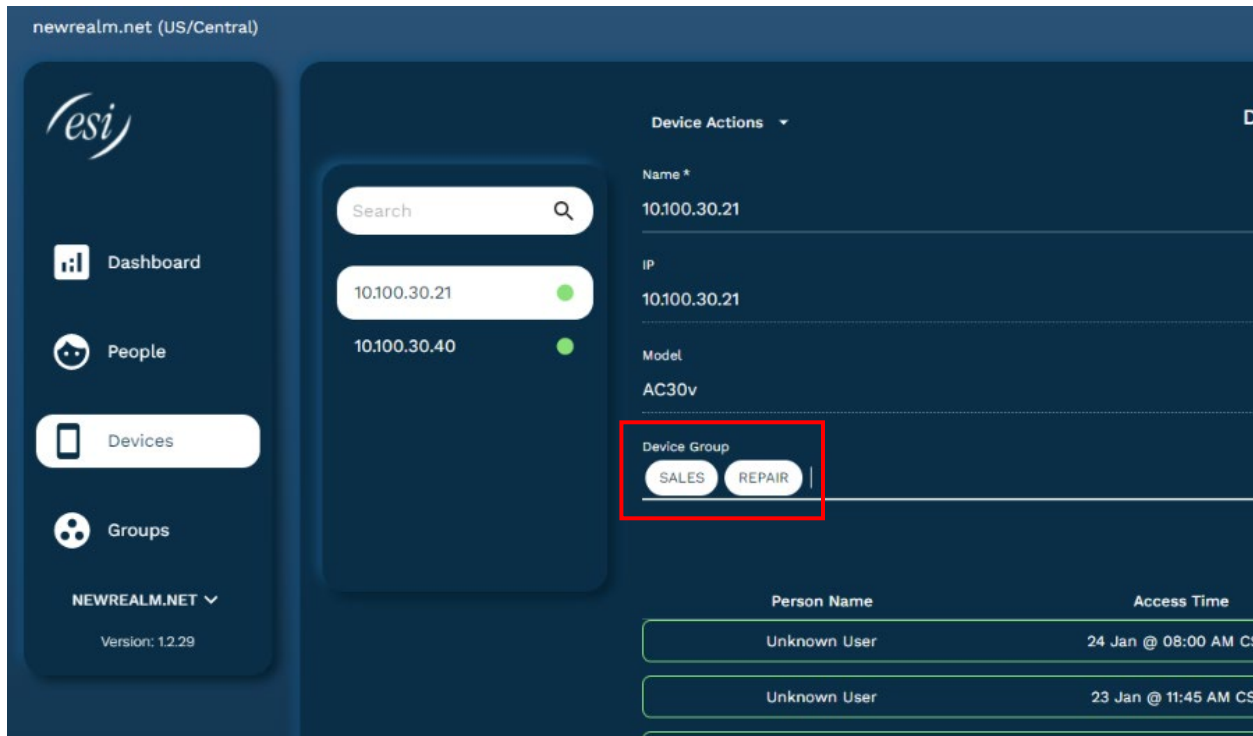
Device Profiles (for Groups and Schedules)

You can add a Group and its schedule to the device as a profile. This will keep the Group and its Schedules on the device. The benefit is that if there is a loss of connection between the reader and the Access database the schedules are still accessible [on the reader].

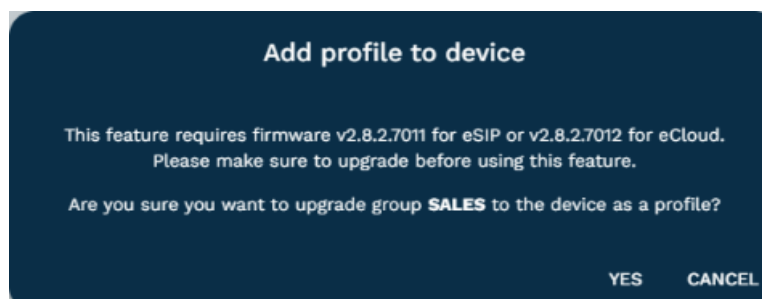
Note: A single reader can support only four profiles, therefore four schedules. You can create more schedules but only four of those can be used for the profile feature.

Creating a Profile

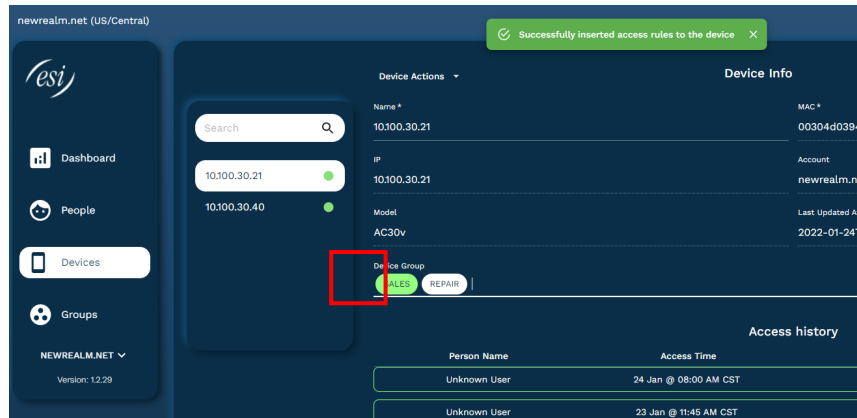
- Go to Device and choose a specific device
- Add a Group under the Device Group, if one is not already listed.
- Click on the desired Group



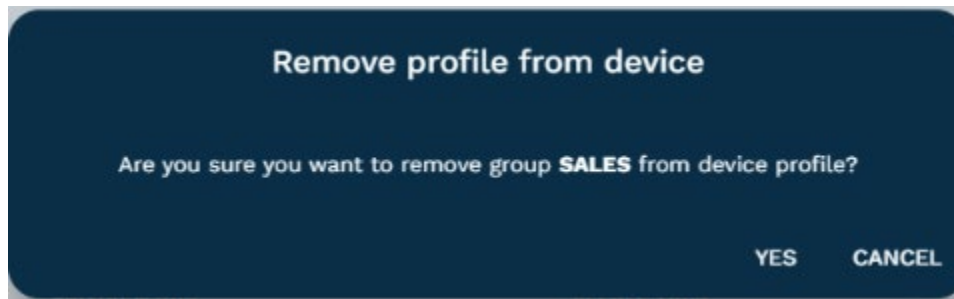
- A popup will appear advising you to ensure the access reader firmware is updated.
 - eSIP Evolution Series – The Certified ESI Partner will load this version through auto-provisioning and then power cycle the Access devices. The new version will then be downloaded to the device.
 - eCloud PBX - The firmware version resides on the eCloud server. You simply need to power cycle the Access device and the new version will be downloaded and applied.
- Click Yes in the same popup to create the profile.



- You'll see a green success notification and the chosen Group (and its schedule) will turn green as well. This way you can tell which Groups are using the Profile feature.



- To remove the Group from the profile click on the green Group name.
- Click Yes to remove the profile.

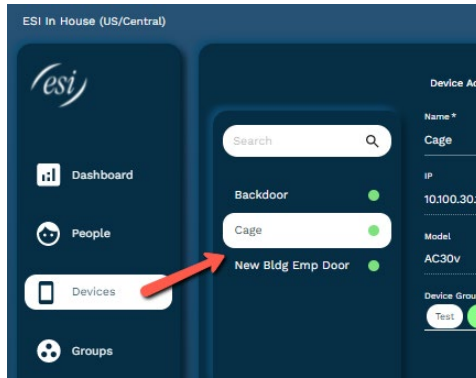


Time Plan (aka Door Unlock Schedule)

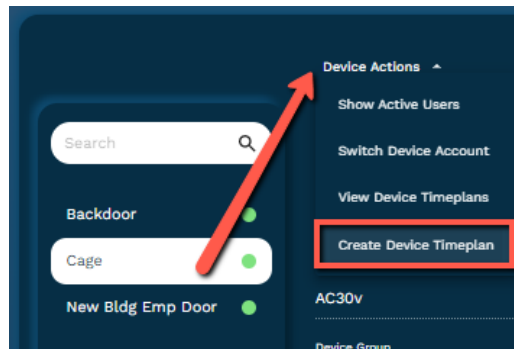
A door unlock schedule is different than a group schedule. Setting a time plan will leave a door unlocked based on a specific date and time. A good example of this is a lobby or customer entrance, where you want the door to remain open during business hours. The same reader can have both a time plan and a group schedule.

Creating a time plan

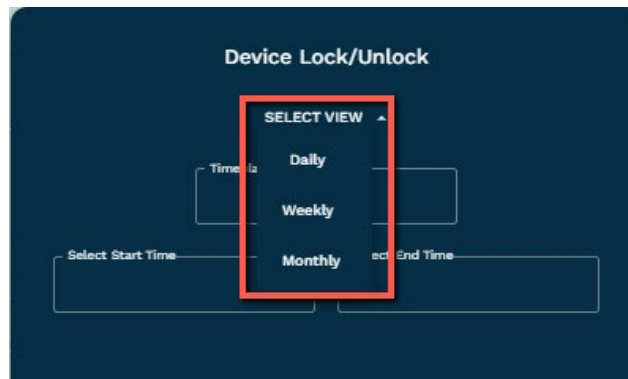
- Click devices on the left, then select the desired device.



- Select Create Device Timeplan from device actions drop down list.



- Select a device lock/unlock schedule from the drop down list. Choose daily, weekly or monthly.



Daily schedule

Using this option means the schedule will take effect every day of the year, except specific inactive dates that you choose.

- Enter the timeplan name and the start and end time.

For instruction on inactive dates see the **Selecting Inactive Dates** section of this document.

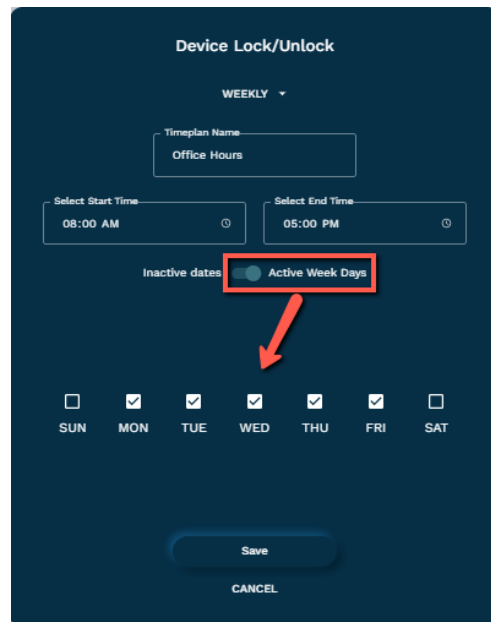
The screenshot displays the 'Device Lock/Unlock' configuration interface. At the top, the title 'Device Lock/Unlock' is centered. Below it, a dropdown menu is set to 'DAILY', which is highlighted with a red box. Underneath, the 'Timeplan Name' field contains 'Office Hours'. Two time selection fields are present: 'Select Start Time' is set to '08:00 AM' and 'Select End Time' is set to '05:00 PM'. Below these, the 'Select inactive dates' section shows a 'Select inactive date' field with '03/16/2022' and a calendar icon. To the right, a list titled 'Selected inactive dates:' contains the following entries: 2022.3.17, 2022.4.17, 2022.5.30, and 2022.7.4. At the bottom of the form, there are two buttons: 'Save' and 'CANCEL'.

Weekly schedule

Using this option means the schedule will take effect for each day of the week and time frame you selected.

- Enter the time plan name.
- Set the start and end times.
- Ensure the slider button is set to Active Week Days. Then choose the days of the week.
 - If the time ranges are different for specific days then you'll need different time plans.

For instruction on inactive dates see the **Selecting Inactive Dates** section of this document.



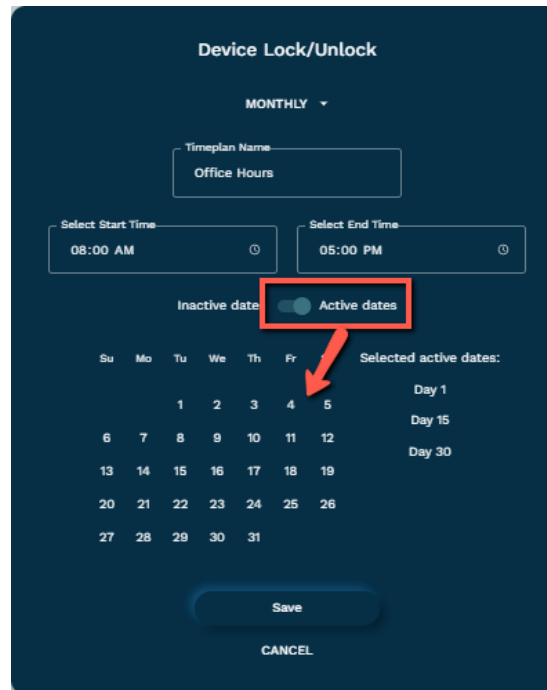
The screenshot displays the 'Device Lock/Unlock' configuration interface. At the top, it is set to 'WEEKLY'. Below this, the 'Timeplan Name' is 'Office Hours'. The 'Select Start Time' is '08:00 AM' and the 'Select End Time' is '05:00 PM'. Under the 'Inactive dates' section, the 'Active Week Days' option is selected and highlighted with a red box. Below this, a row of checkboxes allows for selecting specific days: SUN (unchecked), MON (checked), TUE (checked), WED (checked), THU (checked), FRI (checked), and SAT (unchecked). At the bottom, there are 'Save' and 'CANCEL' buttons.

Monthly schedule

Using this option means the schedule will take effect for the selected day of the month, each month of the year. For example if you choose the 4th day of the month, the schedule will take affect every 4th day of the month.

- Enter the time plan name.
- Set the start and end times.
- Ensure the slider button is set to Active Week Days. Then choose the days of the month.
 - If the time ranges are different for specific days then you'll need different time plans.

For instruction on inactive dates see the **Selecting Inactive Dates** section of this document.



The screenshot shows the 'Device Lock/Unlock' configuration interface. At the top, it is set to 'MONTHLY'. Below this, there is a 'Timeplan Name' field containing 'Office Hours'. Two time selection fields are present: 'Select Start Time' set to '08:00 AM' and 'Select End Time' set to '05:00 PM'. A toggle switch is shown with 'Active dates' selected and highlighted by a red box. Below the toggle is a calendar grid with days of the week (Su to Fr) and dates (1 to 31). A red arrow points to the number '4' in the calendar. To the right of the calendar, there is a 'Selected active dates:' section with 'Day 1', 'Day 15', and 'Day 30' listed. At the bottom, there are 'Save' and 'CANCEL' buttons.

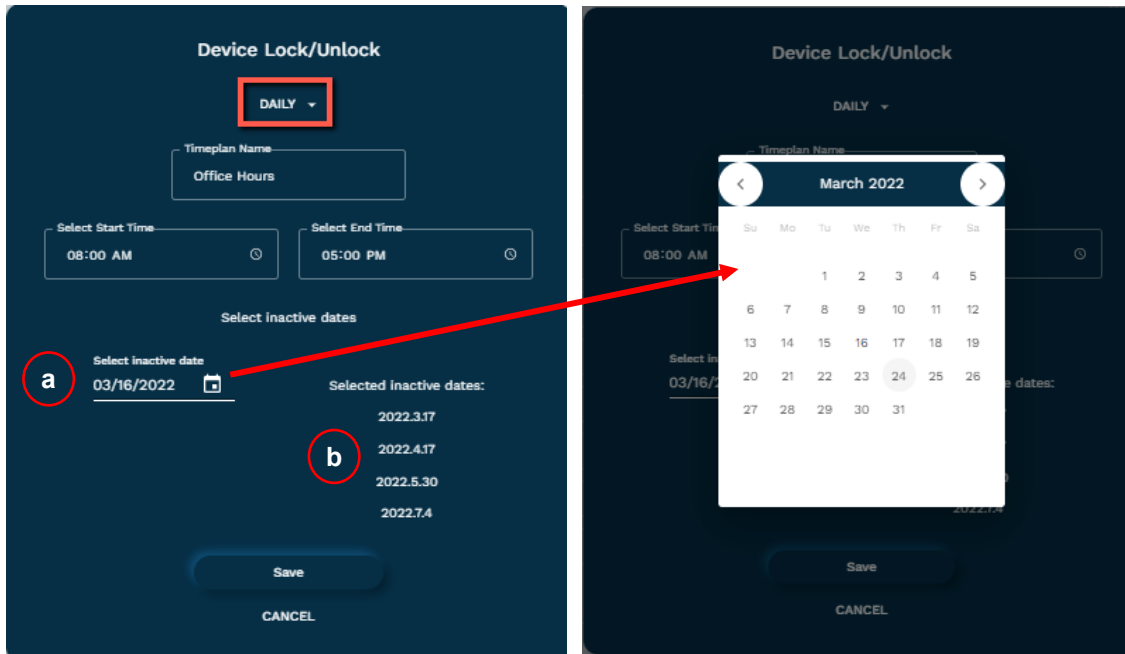
Selecting Inactive Dates

- If there are specific dates where you want the unlock schedule to be ignored or inactive, choose those dates by clicking on the calendar field. The example below is using the Daily schedule. For the Weekly or Monthly schedule simply ensure the button is set for Inactive Dates.

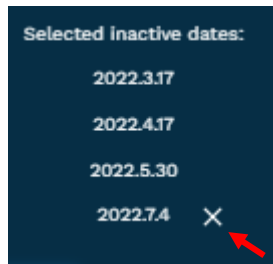


This image is a close-up of the toggle switch. The 'Inactive dates' option is selected, indicated by a white circle next to the text. The 'Active dates' option is unselected. A red box highlights the 'Inactive dates' text and the white circle.

- Once the desired date is chosen it will appear in the Inactive list.




- To remove an inactive date, select that date in the list and click 'X'.



Viewing Created Time Plans

Select View Device Timeplans from the device actions drop down list.

The time plan will show the name, type, start time, end time, repeat dates and invalid dates as shown below.

Click on the trash can  symbol to delete the time plan then click close.

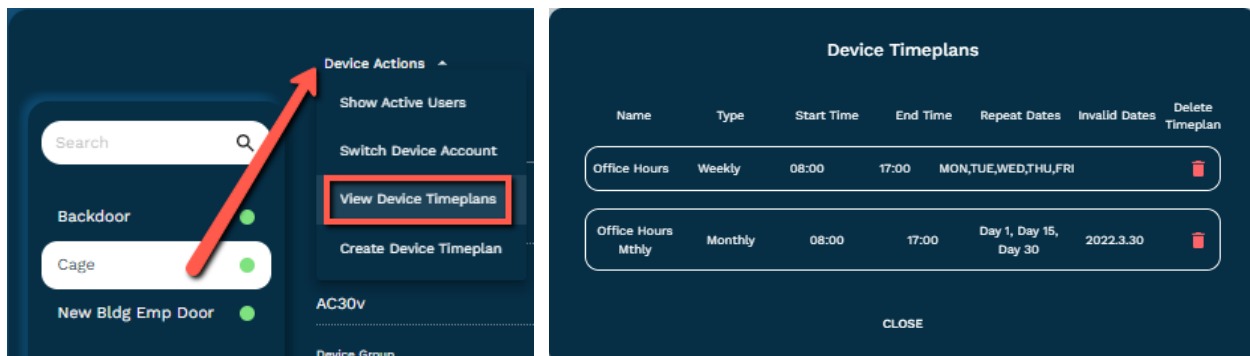





Image Snapshot

Image snapshot provides a static image of who is in front of the access device's camera when a user/visitor is using the access device. The purpose of image snapshot is to allow admins or other Access Dashboard users the ability to verify that the person using their credentials (PIN, RFID card) to gain access into the building is really the correct person.

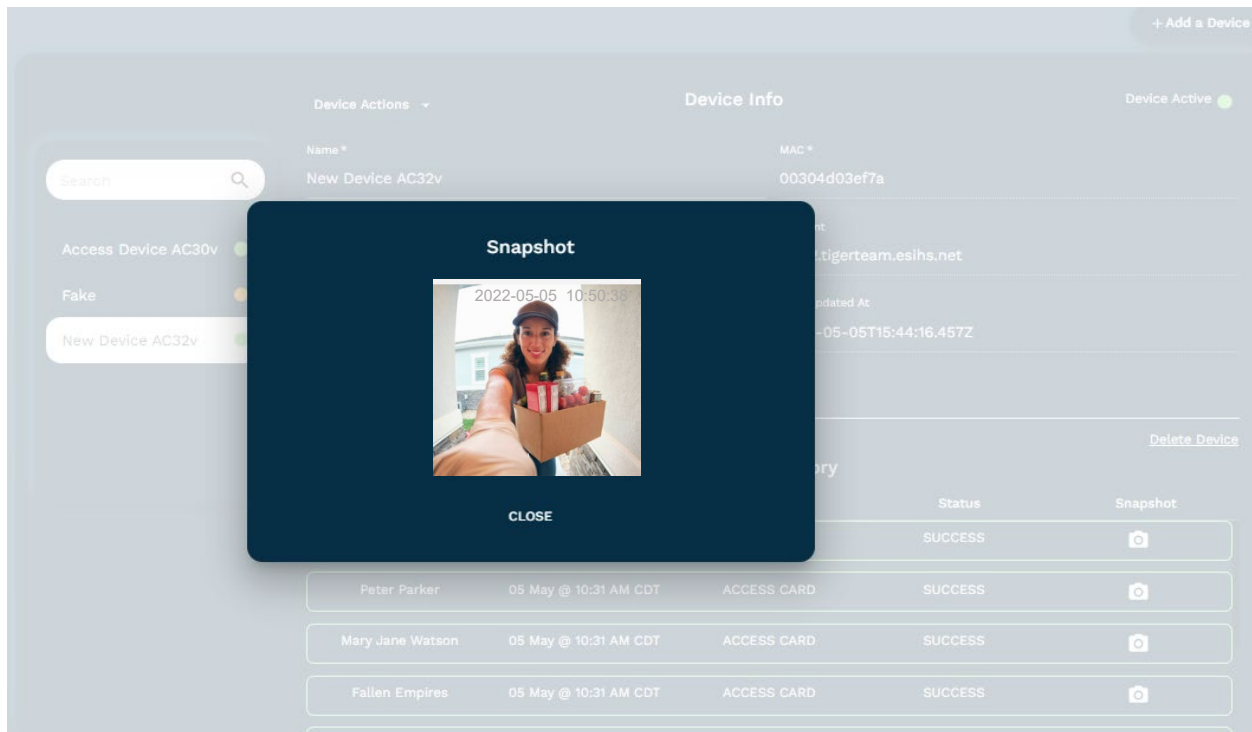
There are three scenarios in which a snapshot is created

- The user enters an access PIN at the reader to gain entry
- The user scans their RFID card at the reader to gain entry
- The employee uses the door unlock code from their phone to unlock the door for a visitor.




To view the image simply login to the Access Dashboard and go to the desired access log entry. Click on the camera icon associated with the log entry.

Access history				
Person Name	Access Time	Access Type	Status	Snapshot
QA ESI Admin	05 May @ 10:32 AM CDT	ACCESS CARD	SUCCESS	
Peter Parker	05 May @ 10:31 AM CDT	ACCESS CARD	SUCCESS	
Mary Jane Watson	05 May @ 10:31 AM CDT	ACCESS CARD	SUCCESS	

The image will appear in a popup window as shown below.

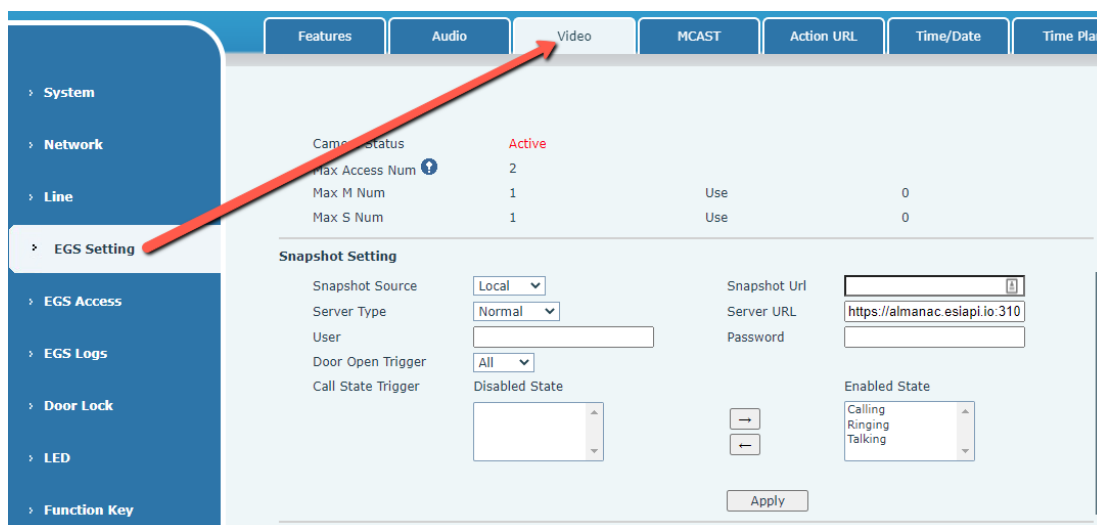


The screenshot shows the 'Device Info' section for 'New Device AC32v' with MAC address 00304d03ef7a. A 'Snapshot' popup window is open, displaying a photo of a woman holding a box of supplies, taken at 2022-05-05 10:50:39. The background shows a table of access history with columns for Person Name, Access Time, Access Type, Status, and Snapshot.

Person Name	Access Time	Access Type	Status	Snapshot
Peter Parker	05 May @ 10:31 AM CDT	ACCESS CARD	SUCCESS	
Mary Jane Watson	05 May @ 10:31 AM CDT	ACCESS CARD	SUCCESS	
Fallen Empires	05 May @ 10:31 AM CDT	ACCESS CARD	SUCCESS	

Setup

1. Login to the Access device via the IP Address.
2. Enter the login credentials
3. Go to the EGS Settings tab on the left
4. Choose the Video tab at the top
5. In the Server URL field enter
https://almanac.esiapi.io:31000/snapshots/snapshots/<MAC address>
where MAC address is that of the reader and contains no colons.
Ex: <https://almanac.esiapi.io:31000/snapshots/snapshots/00304d04ec46>
6. Also be sure the following fields in this tab are set as follows:
 - The Snapshot Source = local
 - The Server Type = normal
 - User = blank
 - The Door Open Trigger = All
 - Call State Trigger: Calling Ringing & Talking states = enabled
7. And don't forget to click Apply.



Helpful Tips

- Be sure the Access Devices run firmware version 2.8.2.705X or higher.
- Images will not appear for events that occurred before the device was updated.
- The camera icon will appear gray for
 - Those events before the upgrade
 - AC20 devices, which don't contain a camera
- The images are never deleted from the server.
- Images cannot be deleted.
- The image contain a date/time stamp in the upper right corner in the following format:
YYYY-MM-DD HH:MM:SS
- The images cannot be downloaded in a bulk file or report but the image can be saved to the PC or LAN if needed by right-clicking on the image and choosing "save image as..."