User Manual

Training Video [https://youtu.be/J1VJxXKZFI0]

Table of Contents

Customer Overview

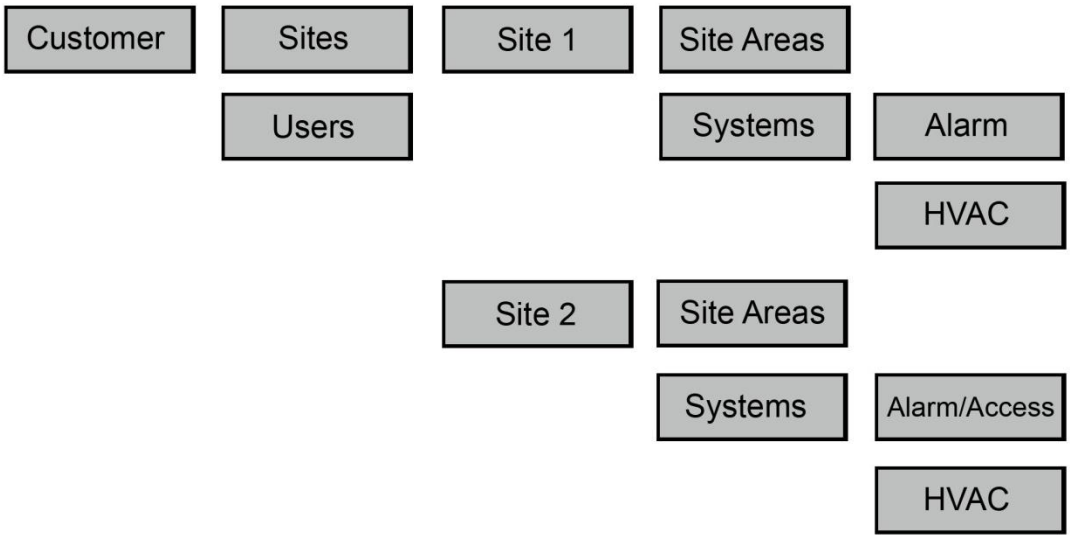


Figure 1: Customer Hierarchy Structure

The top-most level is the Customer. Below the customer are Sites, Systems and Devices.
A site is referred to a postal address or single building.
A system is a grouping of devices.
The users under the customer may have access to any number of sites and systems configured.

Application Overview

Connect ONE ESSENTIAL

- Multi-User Login (Up to 5)
- Full Browser & Mobile Accessible

Application Sections

Monitor – Real-Time Activity – Control Security & Energy Systems – View Video

Reporting – Create Detailed Reports

Interaction – Event Rules (Notifications, HVAC Setbacks)

Users – Manage User Logins (Up to 5) and System Codes

Utilities – System Maintenance

Connect ONE ESSENTIAL+ and PRO

- Multi-User Login
- Full Browser & Mobile Accessible

Application Sections

Monitor – Real-Time Activity – Control Security & Energy Systems – View Video

Reporting – Create Detailed Reports

Interaction – Event Rules (Notifications, HVAC Setbacks), Time Rules (Open/Close Windows) & Task Rules (Command Routines)

Users – Manage User Logins and System Codes

Assets – Manage & Track Assets to Locations and/or Users **(PRO Only)**

Profiles – Manage Login Permissions and System Permissions

Schedules – Manage Alarm, Access, & HVAC Setback Schedules

Cases – Event, Incident, Repair Ticket Tracking & History **(PRO Only)**

Utilities – System Maintenance

Monitor

Each section below may be filtered by clicking the link labeled 'Filter Results'. A menu will appear showing the current Site/Area selected on the right. Click on the particular site heading to filter the results by all areas in that site or click an individual area to view results only in that area. You may click the View All heading to return to the default setting.

Activity - View Recent Events

You may click on any event in the list to pull up the event detail.

The activity will automatically refresh as new events occur, to stop this behavior you may click the link labeled Stop-Refresh . The link will automatically change to Auto-Refresh allowing you to restart the automatic refresh if desired.

If your system has Video Events enabled you may see a camera icon next to the event, this means there is associated video with the event, simply click on the link to view the event detail including the video.

If you have connected cameras you may view cameras on this same screen by clicking the link labeled View Cameras. Multiple camera widows may be opened using this option and may also be popped-out into their own window to be arranged on any monitor.

Arm/Disarm - View Alarm/Access Areas and Arm/Disarm

If your system profile allows you to arm or disarm these options may be selected for each area.

Zones & Sensors - View Zones and Bypass

If your system profile allows you to bypass these options may be selected for each zone.

Doors & Outputs - View Access Doors/Outputs and Lock/Unlock

Open will unlock the door momentarily to allow someone access and then relock. Lock will lock the door indefinitely or until the next scheduled time. Unlock will unlock the door indefinitely or until the next scheduled time.

Cameras - View Live/Playback Video

You can click on a thumbnail image to open a camera window. Multiple camera windows may be open on the same screen.

HVAC - Control Thermostats

You may click on a thermostat to see current values and edit current settings. You may also set each thermostat to use either the Standard Weekly Schedule or an Alternate Weekly Schedule. The standard and alternate schedules are configured in the Schedules section of the website.

Lighting - Control Lighting

You can click on a light to turn it on or off, if the light is a dimmer you can adjust its level of brightness.

Tasks - Activate Automation Tasks

You can choose an option to activate a task or macro key.

Reporting

You may select from predefined reports on the left or choose custom reports saved on the right.

Predefined Reports

Event Activity – List all activity in chronological order.
In/Out by User - List user in and out times for each area and calculate total time in an area.
Exit Exception By User - List users which have logged in but not logged out.
User Codes - List all system codes and authority levels.
Checkpoint by Tour – List checkpoint tours and calculate total time in tour.
Temperature Zones - Display historical temperature data and alarm status.
Thermostats - Display historical temperature data and HVAC status

Custom Reports

Click on a report in the list to create/edit OR Click on 'Create A New Report' to create a new one.

Create/Edit Screen
You must select an Area, a Type, and a User. You may select more than one by holding the 'Ctrl' key while clicking on your selection with your mouse OR you may click on the 'Select All' button below the list to select all.

Event Type
Select the applicable event types to include in the report, Refer to Appendix A for detailed descriptions of each type.

Site / Area
Select the sites / areas you want included in the report.
'[System Events]' - refers to events of which a particular area is not relevant. ex) AC Power Failure

User
Select the user(s) to include. When a user has a * next to their name that indicated that they have been deleted.
'Any' - refers to an event not relevant to any User. ex) Zone Alarm

Specify a Search Keyword List
This will search the location/comment portion of the report.
Search for one or more of these keywords by typing OR between each word.

Example: (To search for either Motion or Door), enter Motion OR Door
To exclude words in your search use the - character before the word, -word.
Example: (To exclude door), enter –door
To include a list of items such as zones, doors, areas, etc
Example: (Include a list of zones), enter Zone:1,4,10,20
Example: (Include a list of doors), enter Door:1,2,5
Example: (Include a list of outputs), enter Output:1,2,501
To search a phrase, surround the phrase in quotes.
Example: (Find Front Door), enter "Front Door”

Specify a time period to search.
'This Week' - refers to the current Sun at 12AM to the next Sat at 11:59:59PM.
'Last Week' - refers to the previous Sun at 12AM to the previous Sat at 11:59:59PM.
'Specify' - allows you to specify any start and end time

Click 'Run Report' and a new window will open with your report. You may print or export the report by clicking on the button at the top.

You may choose to save this report for quick retrieval or to be used as a filter in an interaction rule by:
Report Name - Enter any name to call this report
Sharing - Just Me - This report can only be viewed by you, the creator
or Everyone - Any User on your system will be able to view this report.

Save - This will save the report and return you to the previous screen.
Delete - This will delete the report and return you to the previous screen. You will be prompted to confirm your action and it will not allow you to delete this report if it is currently being used in an interaction rule.

Users

Users are simply a list of people. That being said each person should exist as a user only once, since a user may have an unlimited amount of system codes attached to them. A user is also anyone with any interaction with the onsite systems and/or the application for management control.

Click on a user in the list to edit OR Click on 'Create A New User' to create a new one.
Active/Inactive - Active Users are able to login.
Last Login - Date&Time of the last time this user logged into Connect ONE OR never
Last Activity/Last Area - Date&Time and area of the last time this user performed an action on the system ex) Door Access, Arming, etc., OR never

Create/Edit Screen
Save - This will save the user and return you to the previous screen.
Delete - This will delete the user and return you to the previous screen. You will be prompted to confirm your action and it ask you if you would like to also delete any systems codes for this user.
Active/Inactive - Active Users are able to login. Upon choosing 'Inactive', you will be prompted to automatically mark any alarm codes that are currently active to inactive status as well. Inactive system codes will not work at the keypad.
Name - Specify any name that is not already assigned to another user. The system will prompt you if it is taken.
Custom Fields – You may optionally use up to 5 custom fields, they may be globally named and options set from Utilities->Settings. Selectable options include whether the field is hidden or searchable, and whether or not to have unique values. If searchable then they will appear in the main user list screen and become a field to search when using the search box.
User Profile - Select a Profile from the list. User Profiles are defined in a separate section. A User Profile must be specified to be used as a grouping mechanism for permissions.
OPTIONAL - Login - Specify any login name that is not already assigned to another user. The system will prompt you if it is taken.
Password - Enter a password if you entered a login name. The password must be at least 6 characters. When editing an existing user, you may change the password in this location

Activation/Expiration - User will be inactive until the specified activation date and active until the specified expiration date. These dates must correlate to any system codes applied to the user. Therefore the activation date cannot be set after any system code activation date and the expiration date cannot be set prior to any system code expiration date. If the user has system codes, an option will be shown to update the systems codes with the dates specified. The dates will

be evaluated every 15 minutes therefore it will be acted upon on the next quarter-hour interval from the date specified.

Visitor – Set a guest host to be notified upon visitor self check-in. You may manually set the check-in area, time and check-out time if required or if modification to the dates is necessary.

Upload Image - This will allow you to upload a portrait image of the user. A new window will open allowing you to browse your computer for the file to upload.

Badge – An identification badge can be generated consisting of the user's uploaded image, name, and the first 4 custom fields. The badge design cannot be modified however it can be printed or downloaded. For a custom badge design you may export the user's information and then import the data into badge design software.

Link Account - You may link other user accounts for easy access to switch between them.

Specify the login name, password, and customer number to link; once linked the account can be accessed with an option in the upper right-hand corner.

Contact Information

Phone Number – You may add one phone number to be used as reference only, this is not used for sms, see email below for that feature.
Email Address(s) - You may add up to 5 email addresses per User to be used as for an event notification in an interaction rule.
Push Notifications – Mobile addresses are automatically populated once the App is used for the first time on that device. The name of the mobile address can be modified here for reference in an Event Rule.

System Code(s)

You may apply an unlimited amount of system codes to a User. You may click on a code to edit or delete it.
Active/Inactive - Inactive alarm codes will not work at the keypad or the reader.
Ext# - or External #, this is the number printed on the card of keyfob, this is optional and used for lookup purposes only.
Show Codes - If you have authority a 'Show Codes' link will appear at the upper right of the table allowing you to see the code.

Profiles

User Profiles

User Profiles are used to define which sections of the program users are able to access. It also defines which Sites and Areas they have access to view and control.
Click on a profile in the list to edit OR Click on 'Create A New User Profile' to create a new one.
NOTE: You cannot delete or change the area permissions of the 'admin' profile.

Create/Edit Screen
Save - This will save the profile and return you to the previous screen.
Delete - This will delete the profile and return you to the previous screen. You will be prompted to confirm your action and you will not be able to delete a profile of which has users currently assigned to it.
Active/Inactive - Mark as inactive to prevent any users in this profile from being able to login.

Login Permissions
NOTE: If a user does not have Modify permission in a certain section and they do have Modify permissions for Profiles, they will not be able to set the permissions of a View or View Only section to a higher authority. It will be disabled.
No Permissions - Selecting this will block the entire management section from the user.
View Only - Selecting this will allow the user to view the section but not save or delete.
View & Modify - Selecting this will allow the user to view and modify the section, i.e. All Access

Area Permissions
User Visibility: Setting the user visibility by area means that the users assigned to this profile will be visible only when the logged in user has the same or more areas selected as viewable. Setting the user visibility to all means that the users assigned to this profile will be visible to any logged in user regardless of their selected viewable areas.
This is best explained in an example.
User A has a profile with access to Site A and Site B.
User B has a profile with access to Site A.
Users C ... n have a profile with access to Site A and Site B.
When User A logs in he/she will see user B and users C ... n because their selected viewable areas match or exceed the other users. However when User B logs in he/she will only see themselves because the others users have access to

areas that they do not. This is the default way of handling permissions and is referred to the user visibility option being set to "by area." There is also an option to set the user visibility option to "all." This example continues:

Users C ... n have a profile with access to Site A and Site B, and the user visibility option is set to "all."

When User B logs in, he/she will see Users C … n because those users' profile has the visibility set to all.

Share with Subordinate Profiles (View Only) – This option allows users with less authority to view information about users assigned to this profile, which will include: activity, contact addresses, cases, and assets, exclude: system codes, and restrict modification of the user.

Virtual Anti-Passback: Enabling this option will generate an Access Violation: Anti-Passback event whenever the user, assigned to this profile, is granted access into the same area previously granted access. This will not deny access but will allow a report and/or notification of the violation.

Enable Lockdown Deactivation: Enabling this option will deactivate the users associated with this profile, when lockdown is selected for that system.

Enable System Activity Restriction: Enabling restriction of system activity by the area(s) listed will enable an access violation event to be stored when a user enters an area not authorized in this profile. Please note that it will not prevent the user from entering/accessing the area.

Select Available Areas - These are the areas available to select, when listed in this box they are not viewable by the user of this profile.
Viewable Areas - These are the areas of which a user with this profile may view. To allow a user to view a particular area, select the area(s) from the available areas box and use the right arrows in the center to move them to the viewable areas box. To remove a viewable area, select it from the viewable box and use the left arrows to move it to the available areas box.
NOTE: Hold your 'ctrl' key and click to select or deselect more than one area.

Schedule
Define a timeframe that the users in this profile will be restricted from system activity and/or login.
Enable Login Restriction: Enabling restriction of login by time will not allow any user associated with this profile to login outside of the allowed schedule.
Enable System Activity Restriction: Enabling restriction of system activity by time will enable an access violation event to be stored when a user enters an area outside of the allowed schedule. Please note that it will not prevent the user from entering/accessing the area.

Network
IP Address Filter - Specify a whitelist of IP addresses. Enabling IP address restriction will prevent a user from logging in from disallowed networks.

Auto-Deactivation Inactivity Audit - Enabling the auto-deactivation option will deactivate a user including any system codes after the specified period of login and system inactivity. If no activity has been generated then the user will be deactivated based on the created/modified date.

Login Expiration Timeout Override - Enabling an override will restrict the choices at login for a user, up to the allowed expiration time. For example, if a user selects 24 hours at login but they have an override of 30 minutes set on their profile than 30 minutes will take precedent.

2-Factor Login Authentication - 2-Factor authentication may be enabled for any user individually, setting this option will require assigned users to use 2-Factor authentication rather than it being optional. The user may use an app such as the Google Authenticator App for their 2-Factor credential. Lastly, the 2-factor option may be disabled which prevents a user enabling it on their account.

Safe Passage - Optional: select up to 5 templates. If selected, the assigned user(s) of this profile must be complete the approval process outlined in the template, otherwise their access will result in Access Violation events.

Visitor - Self Check-In is provided via the selected Safe Passage template which may include health and/or legal notices with signature capture as well as the visitor check-in/out instructions and it is sent to the user upon Visitor User creation. Upon user deactivation the visitor will be marked checked out automatically. Setting a profile to a visitor also allows for additional filtering options when viewing user lists to show only visitors with additional options.

Visitor Check-In Area(s) - If only one area is specified the selection will be automatic for the user. If selecting only one area per site then the user will only be shown the site name and not area name.

System Profiles

This section is used to define where, when, and how users are able to use their system code on each particular system.
Click on a profile in the list to edit OR follow the drop-down links to create a new one.
Refer to your Control Panel User Manual for more information about the System Profiles.

System Profile Templates

Permission templates may be configured which can comprise multiple systems.

Once a template is created it can be used to add or modify system codes.

When adding a new code a template may be used which will automatically add the code to all of the systems in the template with the pre-defined permissions. Once a system code is added with the template it is forever linked to the template, unless the dissociate option is selected.

Editing of the template will affect the permissions of all system codes associated with the template. Therefore multiple system codes may be updated at one time just by adjusting the permission template.

The associate option may be used to find potential matching system codes of which were not originally added with the template but you'd like to be able to link them to the template for future modifications.

Schedules

Schedule Types (not all types apply to all systems)
Time Windows – used for setting a window of time that may be applied to System Profiles, Doors, and Outputs.

Shift Schedule - used for Area Shifts which correspond to the System Profiles in the Profiles or Users Section. There are four configurable shifts globally or for each Alarm/Access Area depending on your system configuration.

Door Schedule - used to automatically lock and unlock a door. There are eight independent schedules for each door. Ex) Use door schedule #1 for 8:00am to 12:00pm and schedule #2 for 1:00pm to 5:00pm. This will force the door to be locked during the lunch hour. Door schedules are typically overridden by the armed status of the Alarm/Access Area of which they reside. i.e. If the Alarm/Access Area is armed the schedule will be overridden and the door will lock. Your system may not have any doors to configure.

Output Schedule - used to automatically turn on and off an output. There are eight independent schedules for each output. Your system may not have any outputs to configure.

HVAC Schedule - used to configure setback schedules for each thermostat. There are three independent schedules for each thermostat (In/Out/Away). Once you configure your start times and temperatures, apply the schedules to a standard week. You may also configure an alternate week, you can switch to the alternate week manually via the Monitor section or automatically via an Interaction Rule.

Custom Schedule – used to control start times and timer durations in conjunction with automation rules programmed into the control panel.

Click on a schedule in the list to edit OR Click on 'Create A New Schedule' to create a new one.

Select a Schedule, if no options are listed then you have reached the maximum available schedules of the type selected for that system.

Select a start and end time in 24-Hour format for each day of the week.
Time Window and Shift Schedules also have an ending day selection. If you select a day from the list which is different than the current day, then the schedule will actually end on the day selected. For example, Tuesday: 14:00 - 02:00 Wednesday. This schedule will run through the night until 2am the next day.

Holiday dates are grouped by A,B,or C. For example, group like holidays together, all-day holidays can be set to the A group, half-day holidays can be set to the B group, and so on.
To modify holiday dates click the link titled 'View Dates'.

Interaction

Event Rules

Event Rules are used for user/system interaction based on activity events generated by a User and/or a System. For example, to receive notification about a particular activity you would create an event rule to watch for and act on that event.

Click on an event rule in the list to edit OR Click on 'Create A New Event Rule' to create a new one.

Create/Edit Screen
Name - Enter any name to call this event rule.
Sharing - Just Me - This event rule can only be viewed by you, the creator
or Everyone - Any User on your system will be able to view this rule.

If... Event(s) Matching
Filter Report - when an event occurs it is filtered by this report to determine a match.

(AND) Condition is Present – applies to a particular site or area. The condition options are: Area(s) Armed or Disarmed, Door(s) Locked or Unlocked, or Output(s) On or Off.

(AND) Occurs - Anytime, During, or Not During:

- When Anytime is selected the action will be performed at all times.
- When During is selected the action will be performed only when the event occurs during the selected time frame.
- When Not During is selected the action will be performed only when the event occurs outside of the selected time frame.

Then... Perform Action(s):

Action Options

- Rate Limit - Choose a timeframe to limit quick repeated actions when multiple events occur matching this same rule.
- Last Activity - This option will only send the notification to the specified user(s) when their last activity at the site of which the event occurred is within the timeframe selected.
- Hide System Generated Message - If enabled, show only Notes/Instructions in Notification Message.
- Append Notes/Instructions – optional to add custom notes or instructions to the notification.

- Open/Close will append last device arm/disarm for selected Action. This gives you instant knowledge of when last arm/disarm took place, who performed that action and, if you also select Contact Info, phone number to reach that person.
- Contact Info will include phone number of the user who triggered the action so that you not only know who did it, but have contact information to take immediate action.
- Event Triggered By User – This option will send the notification to the same user which triggered the event.
- Mass Notification – These options will send the notifications to all users of a particular user profile.

Actions

- Email Notification - Select the user to receive an email notification when an event occurs that matches the filter report and the time frame specified. Email addresses are configured in the Users section.
    - Instant refers to the notification being sent as soon as the event occurs. With Instant notification 2 additional options are available:
    - Daily/Weekly/Monthly refers to the notification being sent on a daily, weekly or monthly basis, delivered at midnight, as a report of all the events that occurred during that timeframe. A csv (comma separated value) file is attached to the email and can be opened up in a spreadsheet program.
    - Overnight refers to the Daily report delivered at 7am and comprised of events which occurred from 7am the previous day.
    - Group 1,2,3 or 4 refers to a report delivered at a custom timeframe which is specified via a Time Rule. If no Time Rule exists for the Group then the report will be delivered at midnight. Multiple times of delivery may be specified through the use of multiple Time Rules.
- SMS Notification - Select the user to receive a text message (SMS) notification when an event occurs that matches the filter report and the time frame specified. Phone numbers are configured in the Users section. SMS messages must be added as an additional subscribed service.
- Push Notification - Select the user to receive a push notification when an event occurs that matches the filter report and the time frame specified. Push addresses are automatically added upon App login and are managed in the Users section.
- Onscreen Alert (Audio) - Select the user to receive an onscreen alert when an event occurs that matches the filter report and the time frame specified. Instant refers to the notification being sent as soon as the event occurs. The alert will popup on the users screen when they are logged in and will allow the user to acknowledge the event(s). If you choose with audio, an alarm sound will emit from the computer to bring attention to the screen.
- Record Video – Select the cameras you would like linked to the event triggering this rule. You may select up to 5 cameras that will have a snapshot

recorded at the time of the event. If you choose to record the cameras in the area, the system will choose up to 5 cameras assigned to the same area of which the event occurred. If you also choose to send an email from the event, the email will contain a link to view the camera recording.

- Trigger System Event Push – This action will push the event information to a compatible NVR recorder for bookmarking or logging within that system.
- Trigger Interaction Report - Select the Interaction Rule with a Daily Report Action you would like to be triggered when an event occurs that matches the filter report and the time frame specified. The Interaction Rule must have an Email Daily Report Action to appear in the list. One example may be to generate and email a report of the day's access activity upon an alarm event.
- Activate Task Rule – Select a task rule to be activated automatically when the event matches the selected filter.
- Trigger Lockdown Command – This allows you to have a panic button onsite that when pressed can automatically trigger the lockdown command to be sent to as many control panels as you'd like. Please note that for this to function an active Internet connection is required at the time of the event.
- Set HVAC to (Standard/Alternate) Schedule - Select the thermostat to switch to the standard or alternate weekly schedule when an event occurs that matches the filter report and the time frame specified.
- Create Event Case – This action will automatically create an Event Case for tracking/logging event responses by personnel.
- HTTP(s) Server Push – Send event information to an external server for auxiliary logging. The UserAPI service must be subscribed for this action.

You may choose to remove or deactivate the action by changing the status next to the line item.

Time Rules

Time Rules are timed checks that you'd like to occur. Most common function would be to check that certain areas are armed or disarmed according to the predetermined employee schedule.

Click on a time rule in the list to edit OR Click on 'Create A New Time Rule' to create a new one.

Create/Edit Screen
Select the check from the list, and the time & on which days to perform the check.

An event will be generated when the time check fails for the following triggers:
For Area(s) Armed/Disarmed, Access Occurred, Zone(s) Bypassed, Zone(s) in Exception, Zone(s) Not Active, No User Activity, & Checkpoint checks the event type is "Interaction: Time Violation"
For Door(s) Locked/Unlocked checks the event type is "Status: Output Status"
To receive notification of these events create an event rule with these event types as the filter.

A report trigger will be performed when the time check occurs for the following:
For Trigger Interaction Report: All Event Rules with a matching Group# will be delivered at this time. The report buffer will also be cleared at the time of the report generation. You can specify multiple trigger times to receive the report at multiple times within a day.
For Clear Interaction Report Buffer: All Event Rules with a matching Group# will have their event buffer cleared at this time. This will essentially remove all events from the report which have occurred up until the time specified.

Task Rules

Task Rules are a programmable routine to execute certain commands upon activation. The commands may be acted on any number of systems. Some commands may have a delay parameter to start at some point in the future.

Task Rules can be activated manually from the Monitor section or may also be activated automatically as an action of an Event Rule. This allows for several clever interactions such as, When I disarm my office then disarm all my other buildings, set the thermostats to the standard mode and turn on the lights.

Click on a task rule in the list to edit OR Click on 'Create A New Task Rule' to create a new one.

Create/Edit Screen
Select a name for the Task Rule. This name will appear in the task list from the following pages: Monitor-Activity, Monitor->Cameras, Monitor-Tasks, unless the option is chosen to Disallow Manual Control from the Time Constraint option.

The Task Rule may be scheduled for a one-time future action or recurring action. The recurring options allow for the task rule to automatically activate every week at a particular time and certain days plus every 1st occurrence of a month at a particular time and on certain days or every 2nd, 3rd, 4th, or 5th occurrence of the month. An example would be to set it to activate only on the 2nd Tuesday of the month.

Now you can apply any number of actions to the rule. You can specify the action to be instant or delayed by (15, 30, 45, or 60 minutes, 1, 2, 4, 6, or 8 hours).

An example may be whenever I activate this task I want the Front Door to Unlock Instantly and in 2 hours from now I want the Front Door to Lock. To create this rule, enter one command to Unlock Door – Instant, and another command to Lock Door – 2 hour delay.

These actions may require automated commands to act on a system. A case may occur where the commands cannot process due to a non-responsive system. An event will be logged if the commands fail to process with the Event Type 'Interaction: Warning'. To receive a notification, create an Event Rule with that event type as a filter.

Case Rules

Case Rules allow for notifications to occur when new cases are created. Multiple rules may be configured but only one combination of case type and site are allowed.

The primary contacts will be notified first then backup contacts will be notified between 30 – 60 minutes after the primary contact if none of the primary contacts respond available.

The notification includes a link to respond to the case. All case responses are logged under the case and will also be sent to the contacts in the case rule in a notification update. The first contact which responds available will be assigned to the case.

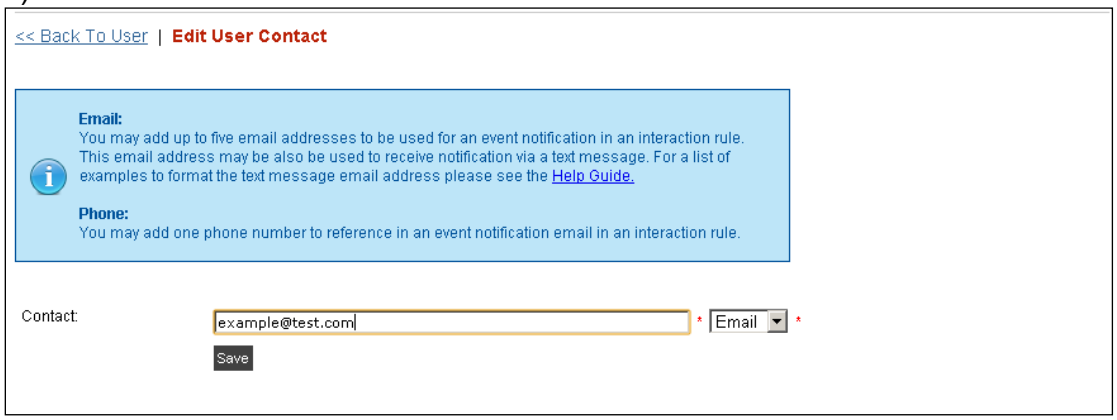
If there is only one primary contact then that user will automatically be assigned to the case.

If there is only one backup contact then that user will automatically be assigned to the case if the primary contact does not respond.

How to Setup an Event Rule for Notifications

1) Enter User Email / Text Messaging Addresses, click on Users then click on the user to edit

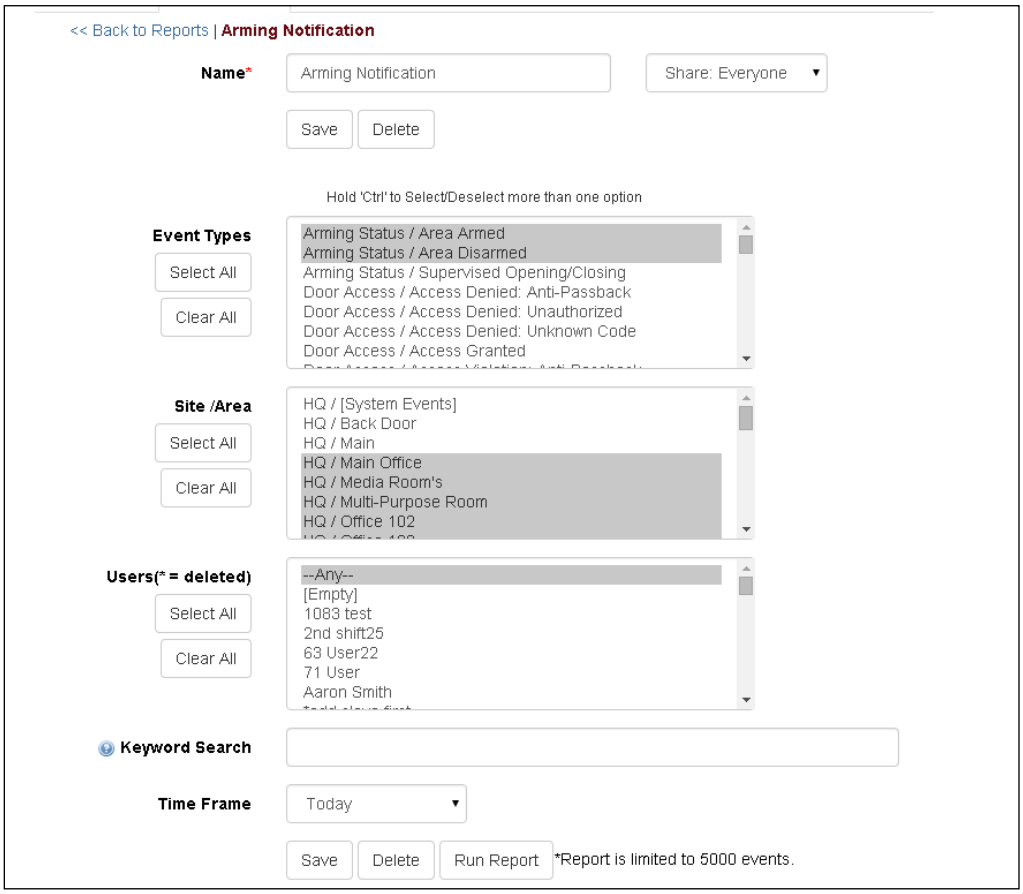
2) Click on “Add” next to Contact Information



3) Enter a email address or text messaging address, click Save

Repeat steps 2 and 3 for each address for this user

4) Create a Filter Report (or specify filters within event rule) – click on Reporting, then Custom Reports, then Create a New Report



5) Select the Event Type(s), Site Area(s), and User(s) to filter, and optional Keyword Filter
6) Enter a Name for the report and click Save

Hint:
This screenshot shows how to setup a filter for arming, disarming, and supervised open/close events, that are limited to the main office and media room areas only.

Use the “Site / [System Events]” area selection for event types such as AC Power, Communication Troubles, etc., that are not related to a specific area. For these types of events choose the “Any” user option as these will not be related to a particular user.

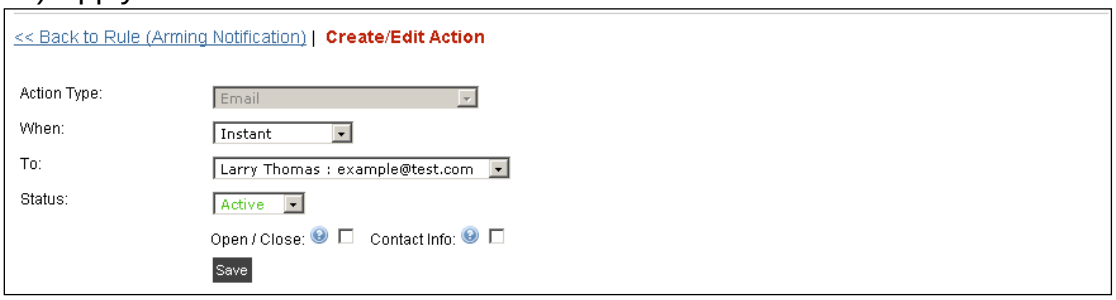
When filtering by user, be certain that the event will be generated by that user. For instance do not choose a user when filtering for alarm events, as the control panel does not know who generated the alarm, so use the “Any” user option.

The keyword option can be used to filter by door name, zone name, etc. For example, to only filter alarms on the front door zone, choose the event type alarm and enter a keyword of Front Door, exactly how it is listed in the zone name.

7) Enter an Event Rule, click on Interaction then Create a New Event Rule

8) Enter an appropriate Name
9) Select the Filter Report you created in step 4.
10) You may choose to limit this action by a schedule. For instance if you only want to receive the notification outside of normal business hours choose the “Not During” timeframe and enter 8:00 to 17:00 Mon-Fri. This will only notify you if the event occurs outside of these times and not during the normal hours.
11) Click Save
12) Add an Action

13) Choose Email for email and text messages, click Continue
14) Apply this action



15) Select “When” to receive the notification, Instant, or in a Daily or Weekly Report. If Daily or Weekly the notification will occur at midnight and include all of the events that occurred in a report form.
16) Click Save

Cases

The Connect ONE Case Management Module was designed in response to customers looking for streamlined methods to track critical event responses, incidents, and repairs at one or multiple locations. The module interfaces directly with the security system application or can be deployed as a standalone service. Ideal for building and property management companies, multifamily and multi-tenant users or national accounts with numerous locations.

Permissions are designated in the User's Profile. A user may be allowed to only create and view their own cases.

A case may be created under the following types:

Event – Reserved for use when an Event Rule triggers a case creation
Incident
Repair
Support
Other

When a case is created it will follow any notifications which may exist in an Interaction->Case Rule.

An unlimited amount of notes can be stored for a case. Notes cannot be changed once stored but additional notes may be appended.

Attachments may be stored for a case; allowed formats are pdf and images. Allowed storage of up to 5GB of attachments.

Cases may be created manually from the Cases section or automatically from an action in an Event Rule.

Cases can be used in conjunction with an Event Rule to automatically create cases upon certain events occurring. This may be used to track event responses including real-time updates from users notified of the case creation.

Assets

The Asset Management Module provides streamlined methods to track assets to locations and/or users including the generation of custom user authorization templates upon issuing and/or returning. A specified return date will notify the assigned user via email if overdue.

Use to Track:

- Physical Keys
- Badges
- Equipment
- Electronics
- Inventory
- Tools
- Other

Assets may be created manually one-by-one and/or imported via a spreadsheet from Utilities.

Once created they may be assigned to a location and/or issued to a user. When issuing or returning from a user a pre-defined authorization template may be selected and sent to the user's email address or shown onscreen for completion by the user.

Typically authorization templates are used as waivers when receiving or returning an asset.

When assigning the asset to a location this is a good way to track where the asset resides and the current inventory of the location, i.e. how many assets are currently assigned.

Utilities

System Information
Click on a system in the list to view.

Status - Shows current status conditions
Last Transmission - This is the last date&time that the system reported.
AC Power
Battery
Communication Status

Commands
NOTE: Not all commands listed here may be available. All update commands will be processed in the background. Normally update commands are not necessary; they should only be used if programming was performed outside of the application from the keypad or a network interruption occurred for several hours.
Update System Status - If you feel the current status displayed should be updated, send this command.
Perform Lockdown - This will deactivate all users that have a profile enabled for lockdown deactivation and lock all access doors.
Restore from Lockdown - This will reactivate all users that have a profile enabled for lockdown deactivation however all access doors will remain in the current state.
Send Alarm Silence Command - If the system is currently in Alarm and you want to silence the sirens but not disarm the area, send this command.
Send Sensor Reset Command - If a 24-Hour zone tripped into alarm, a sensor reset needs to be performed, send this command.
Update All Schedules from Panel - If you feel the current alarm/access, door, or output schedules should be updated, send this command.
Update Holidays from Panel - If you feel the current holidays should be updated, choose this option.
Set Panel Time & Date - If your keypad is displaying the wrong date or time you may send this command to correct it. The time is set by the server so your computer time does not have to be accurate. NOTE: Once per day your panel automatically syncs the time to the server.

System Codes

A list will appear showing the system codes currently programmed into this system.

Commands
Print System Codes - Open a window that will list all the system codes programmed into this system which may be printed.

Update Users from Panel - If you feel the current user list should be updated, send this command.
Forgive All Users (Anti-Passback) - If your system was configured for Anti-Passback and a user did not properly enter an area, choose this option to forgive the user and allow them to resume normal operation of their door access. Most systems do not have this configured.
Update System Profiles from Panel - If you made any system profile changes at the keypad, send this command to update those changes.

Arm/Disarm, Zones & Sensors, Doors & Outputs
These sections allow items to be renamed, you may also set environmental sensors with thresholds for low and high alarm limits.

Settings
Application Settings – configure application-wide settings
Custom Field Parameters – select count of fields, rename labels, and set options
Password Policy Configuration – select a security policy for new passwords
Single Sign-On (SSO) Identity Provider – SEE APPENDIX K

Credentials
Import a batch of access cards to be applied when creating a new system code.
Import a batch of Farpointe Conekt Bluetooth mobile credentials. When applying a Bluetooth credential to a system code, the how-to-use instructions may be sent to the user via email or SMS message.

System Code Import Utility

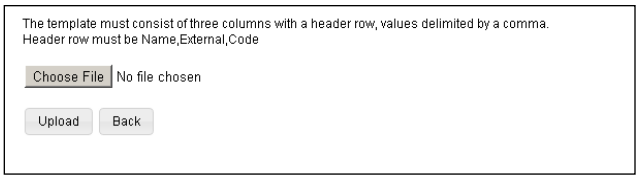
Create a csv file, easiest way is from excel. Start with a download of the sample sheet, there must be a header row and it must be labeled for each respective column. Once each row is filled in with the codes to import, then save the file and choose the type as “CVS (Comma delimited) (*.csv)”.

Example Listing:

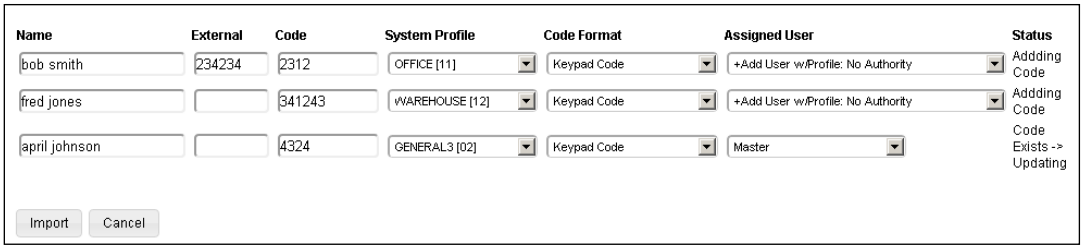
Name	External	Code
Bob Smith	234234	2312
Fred Jones	5678	341243
April Johnson	3456	4324

Go to Utilities and select the system. Click on System Codes, then the “Import System Codes from File (csv)” link on the right under Commands.

From here you will upload the csv file and click Upload.



A new page will load showing all the codes to be added/changed. From here you select which profile you would like for each code and whether to assign it to an existing user or create a new user from the code.



Appendix A: Event Type Descriptions

Arming Status	
Area Armed	An area on a system was armed
Area Disarmed	An area on a system was disarmed
Access	
Access Granted	A user was granted access to an area
Access Denied: Anti-Passback	A user was denied access because they previously did not egress the area
Access Denied: Unauthorized	A user was denied access because either the system was armed, the current time doesn't match their allowed schedule, or the area doesn't match their allowed areas list
Access Denied: Unknown Code	A code or access card was used at a keypad or door that doesn't match any programmed user
Access Violation: Anti-Passback	A user was granted access but violated a virtual anti-passback rule because they previously did not egress the area
Access Violation: Unauthorized	A user was granted access but violated a time or area restricted set on their User Profile, or failed the Safe Passage verification.
Interaction	
Notification	Success/Failure messages generated from Event Rules
Onscreen Alert	Success/Failure messages generated from Event Rules
Warning	Failure messages generated when commands sent from an Event Rule are not able to process.
Time Violation	An area was either Late to Open/Late to Close or other Time Rule Failures occurred These may be system generated or Connect ONE generated based on a Time Rule
Status	
AC Power	Primary Power Failures/Restores
Alarm	Zones that have generated an Alarm
Bypass	Zones that have been Bypassed by a User, either from the keypad or Connect ONE
Door Status	Door/Zone Opening/Closing
Force-Arm	Zones that have been Force Armed during an Arming Command

Output Status	Outputs Turning On/Off
Restore	Zones that have Restored to a Normal Condition
Standby Power	Secondary Power, ex) Low Battery Failures/Restores
Trouble	Zones that have been in a Trouble Condition
Unbypass	Zones that have been Restored from a Bypass Condition
Weather Status	Weather alerts and condition changes such as Clear, Rain, Snow, etc.
Zone Status	Zone state changes when in a non-alarm status, such as Open or Closed
System	
General	General System Messages
Maintenance	Equipment Service Messages
Connection	System programming troubles or restores
Communication	System event communication troubles or restores
Lockdown	System lockdown enabled/disabled
Technician Test	Test events when the system is being serviced
User Command	Commands initiated in Connect ONE
Arm Command	
Door Command	
General Command	
HVAC Command	
Light Command	
Output Command	
Task Command	
Zone Command	
User Modification	Changes to any section in Connect ONE ex) Schedule modified by User
General Modification	
Interaction Modified	
Profile Modified	
Report Modified	
Schedule Modified	
Time/Date Modified	
User Modified	
Case Modified	
Asset Modified	

User Session	
User Event	Events generated by user (via Task Rule or using the EmailAPI)
User Login/Logout	Events generated when a user logs in/out
User Acknowledgement	User comments stored during an Onscreen Alert
Visitor Check-in/out	Recorded when visitor checks in/out

Appendix B: Live/Playback Video - IT Instructions

1) Add or assign a user on the DVR for Connect ONE Live Viewing Access of all Cameras

2) Configure Router for Port Forwarding public port (# of their choosing) to local IP address of DVR on port 80

3) Configure Firewall to pass TCP traffic on port (# of their choosing) to local IP address of DVR on port 80

4) Notify dealer of public IP address, public port, local IP address, username and password

Appendix C: User Integration (EmailAPI / Web Link)

You may enable the user integration feature which will allow this user to generate events and task activations via email (EmailAPI) and/or task integration via web link.

To Activate a Task Rule (web):
URL: A web page link will be shown and sent to the user when enabled.
The PIN must be a 6-digit number and it is entered on the web page. For convenience when activating tasks in succession, it will be stored for 60 minutes.

To Activate a Task Rule (email):
Send an email to UID+task@userapi.connected.cc
Subject of Email = PIN
The first line of the body of the email must be the name of the task rule to activate. This user must have permission to activate the task rule.

To Generate an Event:
Send an email to UID+event@userapi.connected.cc
Subject of Email = PIN
The first 150 characters on the first line of the body of the email will be parsed into an event with an event type of User Session / User Event.

An acknowledgement or error response email will be delivered to this user's email address after processing.

EmailAPI Requirements:
The email must be delivered securely using TLS transport encryption.
The from address of the email must match this user's email address.
The pin must be a 6-digit number and the only item in the Subject.

Event emails are rate limited to 45/hour, Task activations are rate limited to 30/hour. If the rate limit is reached it will auto-clear after a timeout period otherwise the integration may be disabled then re-enabled.

Possible Uses:
External calendar integration to activate tasks – such as locking/unlocking doors
Voice Task Activation via Mobile Phone
Geolocation Notices/Activations via Integration of IFTTT www.ifttt.com
Monitoring of 3rd party systems

Appendix D: GeoView System Mapping

This modules maps real-time status and control of systems to Google Maps.

To configure the map, go to Monitor->GeoView and then from there Options->Edit Map. Clicking anywhere on the map you can add marker points. Marker points can be dragged to a new location as required, just press Save after dragging.

Overlay images, such as interior floorplans, may be uploaded from Utilities, then added to the map just like a marker. Once placed on the map it can be dragged to the proper position, size, and rotation angle.

Appendix E: Safe Passage

The Safe Passage Module provides a framework for a one-time/periodic self-approval process and visitor self check-in. If required and not completed, upon access by the individual, violation events are generated so a manager can ensure the user is safe to be at the site in regard to health and/or hazard concerns. Documentation is stored with the user account showing they have answered the proper questions and approved any company terms such as an NDA.

An administrator may create multiple safe passage templates. They may specify a name, description, re-approval interval, required checkpoint(s), protected area(s), custom messages, and custom terms which need to be answered properly to be approved. When a user is applied to the template, they may be applied to multiple templates, they will receive an email/SMS which contains a link for them to complete the terms of the template. If the user's profile is set to a Visitor then after completing safe passage they will be shown check-in/out options to complete.

A required checkpoint option means their approval is dependent on entering the premises via the designated area and passing an additional condition such as a temperature scan. In this case, they will need to be approved via the terms listed in the template and then they will be in a pending state requiring the checkpoint access. Otherwise if they access a different door then an Access Violation event is generated and managers can be notified.

The protected area(s) selection allows the template to only apply to certain areas if required. For instance, the customer may have a safety template which must be approved prior to entering a potentially dangerous area of the facility. The user may enter any other area without concern but if they have not been approved and they enter any of the protected area(s), an Access Violation event will be generated along with associated notifications.

Upon completion of the form by a user, they will see the status, approved or declined, and receive an email with the status plus a pdf copy of the completed form. The form is stored in the cloud for archival purposes and may be viewed by an administrator if required. If the template contains a re-approval expiration time and that time has expired, they will receive a new email with instructions to complete the process again.

The user's mobile badge is dynamically updated based upon their safe passage approval status, approved (green border), expired (orange border), declined (red border labeled "Safe Passage DECLINED"), and when approved but pending checkpoint access (blue border labeled "Safe Passage CHECKPOINT REQUIRED.)"

Appendix F: InstantCard Badge Printing Integration

Connect ONE is fully integrated with the cloud badge printing service, InstantCard. You can use InstantCard (instantcard.net) which allows you to create custom badge templates and InstantCard handles the printing and shipping of the badge to you. The integration with Connect ONE allows you to associate a user with a badge template to automatically supply the user information and image to the template at InstantCard, and you can complete an order for a badge print. Once the badge is purchased, the same badge template will also become the Mobile Badge within Connect ONE so the user can display it via the Connect ONE App as well as physically on person.

Appendix G: Weather Monitoring

The weather module is an add-on to any customer site.

Monitor National Weather Service Alerts, updated every 30 seconds, alerts are categorized as:

1. Extreme Temperature
2. Environmental
3. Severe Weather
4. Extreme Weather
5. Emergency Alert

These categories provide detection of critical alerts for automatic processing via reporting and interaction event rules for notifications and system interaction including common alerting protocol (CAP) translation for pushing out messages to mass notification systems.

Monitor 6 weather metrics, updated every 30-60 minutes:

1. Temperature
2. Relative Humidity
3. Current Condition
4. Wind Speed
5. Barometric Pressure
6. Dew Point

Each of the metrics can be programmed with a low and high threshold limit which can deliver notifications and interact with other devices onsite such as the alarm/access systems and thermostats. Historical reporting is also possible for each metric which can show readings recorded over a time period.
In addition, if set, the current condition such as Clear, Rain, Snow, etc. can be monitored for changes and logged as an event. The event can follow custom Event Rules based upon keyword. This may include notification but could also include Task Rule activation including the possibility of Lockdown triggering.

Appendix H: UserAPI – Integration with Business Software

REST API

- Creating, modifying, & deleting users/system codes & cards
- Creating, modifying, & deleting cases
- Retrieving alarm areas, zones, doors, and outputs for status updates and command control, such as arming/disarming, unlocking a door, etc.
- Pushing system events to external services for additional logging and/or processing
- Integration with Microsoft Teams (see Appendix I)

Complete API documentation is available upon request.

Appendix I: Microsoft Teams Integration

Utilizing the UserAPI (Appendix H) system event push method, integration with Microsoft Teams can be achieved for a unified method of delivering critical event information to personnel.

To add an incoming webhook in Microsoft Teams:

1) Navigate to the channel where you want to add the webhook and select (•••) More Options from the top navigation bar.
2) Choose Connectors from the drop-down menu and search for Incoming Webhook.
3) Select the Configure button, provide a name, and, optionally, upload an image avatar for your webhook.
4) The dialog window will present a unique URL that will map to the channel. Make sure that you copy and save the URL—you will specify this in step 2.a.i below.
5) Select the Done button. The webhook will be available in the team channel.

To configure in Connect ONE:

1) Go to Reporting->Create a New Report
    a. Select your filters for what type(s) of events, site/area location, user(s) and/or keywords and save the report with a name.
2) Go to Interaction->Event Rules and create a new event rule using the report created in step 1.a.
    a. Add an action, choose Type: HTTP(s) Server Push.
        i. Specify the server endpoint (Teams incoming webhook url) and the JSON payload, for example, {"text":"$type: $text"}. This would make the text of the Teams message something like "Alarm: Panic Zone:501 Front Reception". The $type is Alarm, and the $text is Panic Zone:501 Front Reception. This is just one example, there are many other ways to specify a message.

Appendix J: Emergency Messaging Hub

Integration with Mass Notification Systems

The Emergency Messaging Hub provides a unified feed of emergency messages from multiple systems for an associated site. It works by receiving Common Alerting Protocol (CAP) messages from Mass Notification and other Emergency Response platforms and by translating device native events to the CAP format. All CAP messages are published to the hub for all external services to consume in a single atom feed.

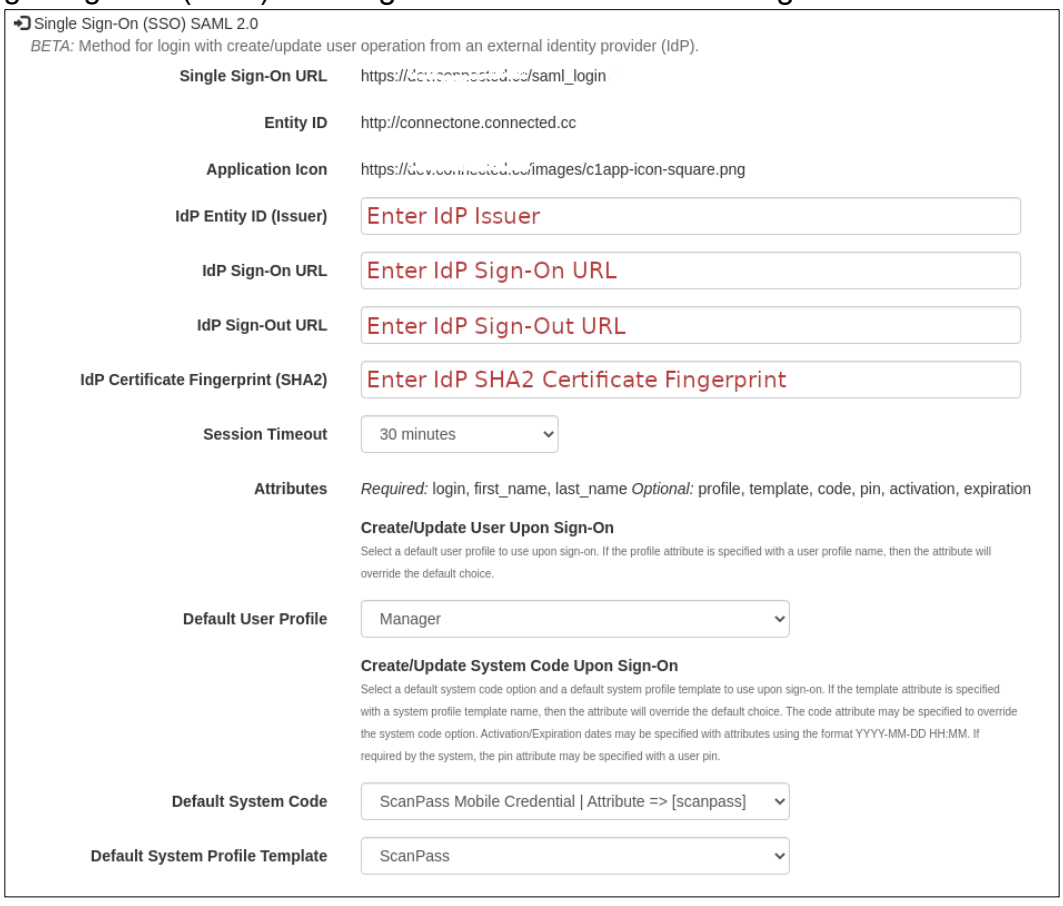
This module is intended for supplementary notification only, not for primary dispatch of police, fire, ambulance, or other emergency authorities.

Appendix K: Single Sign-On (SSO)

Many organizations are using Identity Providers (IdP) to centralize their user directory database across multiple applications. The integration with Identity Providers is supported using SAML 2.0. This allows for users to be created and updated automatically from the external single sign-on process.

This integration was developed for and verified with Okta however since it is based upon SAML 2.0 it should work for other Identity Providers such as Microsoft Azure AD.

Single Sign-On (SSO) is configured from Utilities → Settings.

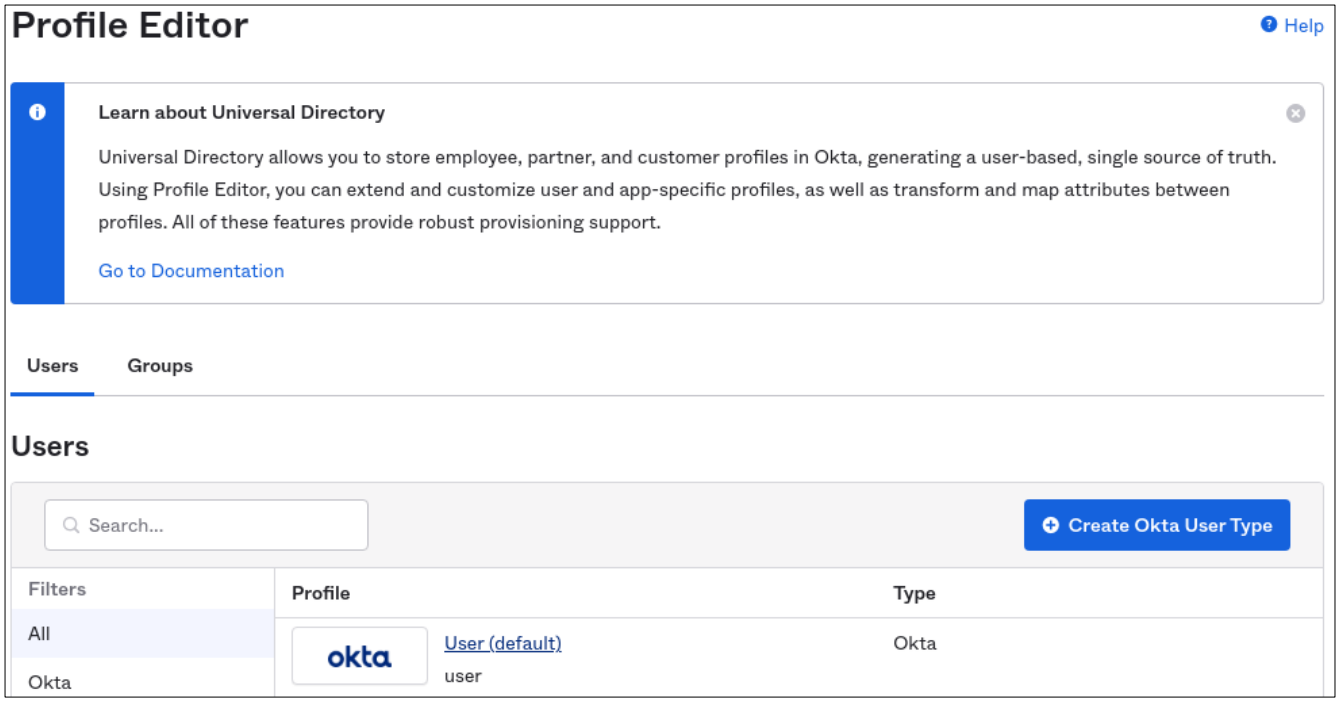


Download the Application Icon to your device, this will be uploaded to your Identity Provider (IdP). The Single Sign-On URL, Entity ID, and Certificate Fingerprint will be supplied in the application setup process with your IdP. To begin, create your user profile attributes.

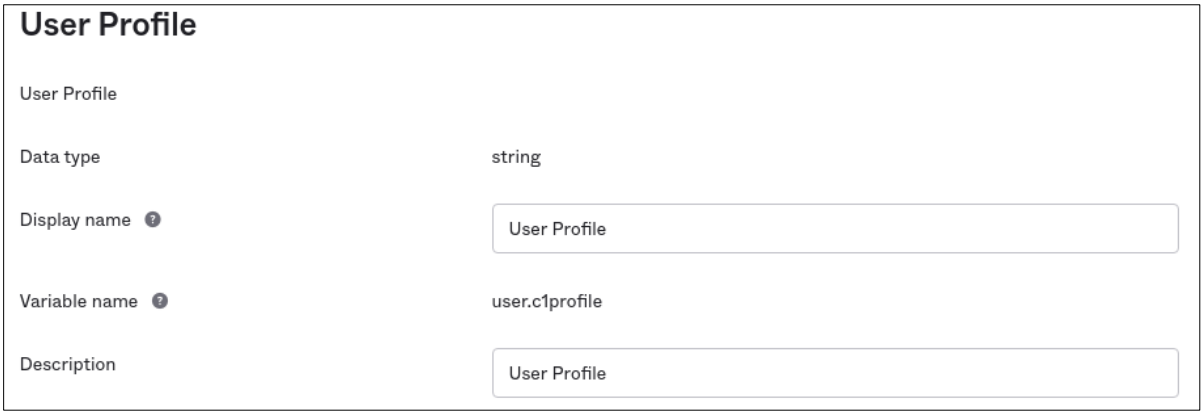
The following attributes are required: login, first_name, last_name. These should already exist in the profile.

Optionally you can add the following attributes: profile, template, code, pin, activation, expiration, and custom# (example custom1, custom2, custom3, etc).

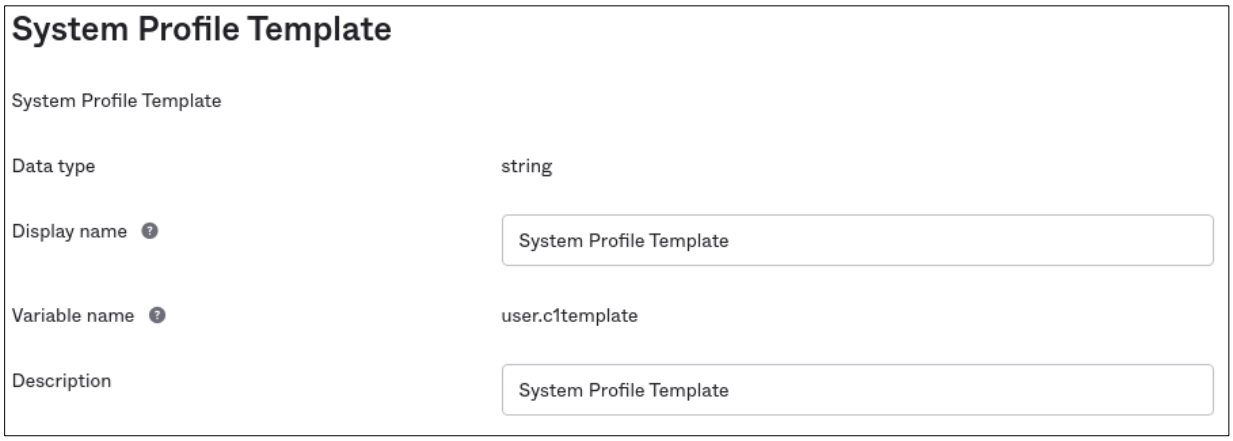
Using Okta, select Directory then Profile Editor, then select the Okta User (default) option.



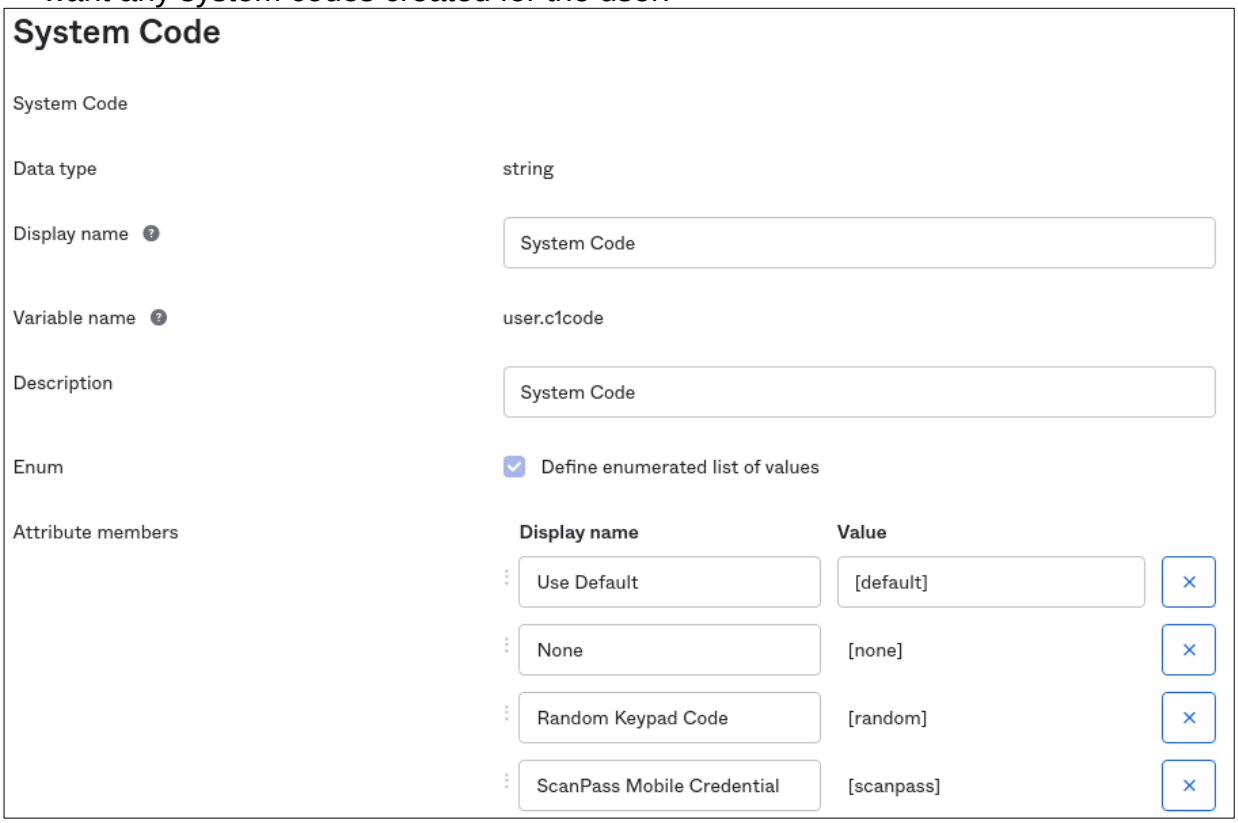
Create a new attribute called, User Profile. If the profile attribute is specified with a user profile name, then the attribute will override the default choice from Settings.



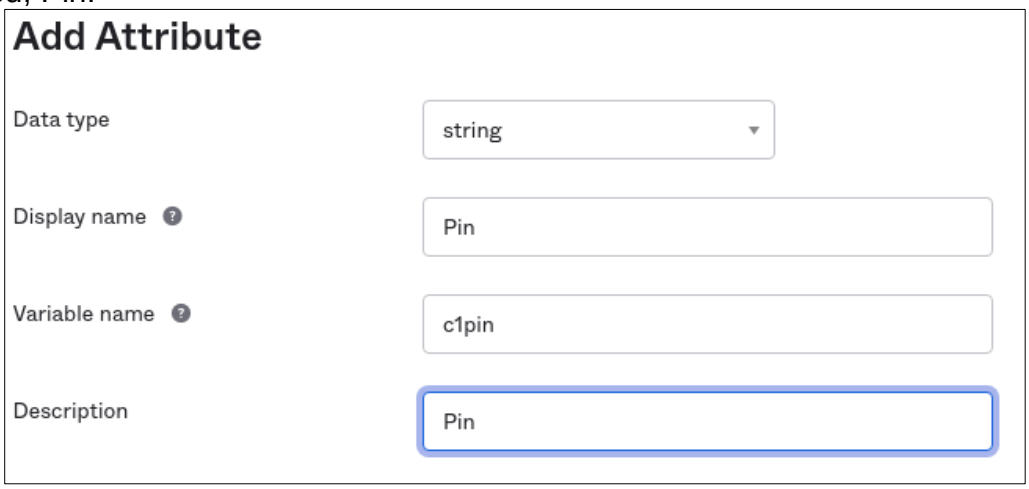
Create a new attribute called, System Profile Template. If the template attribute is specified with a system profile template name, then the attribute will override the default choice from Settings. System Profile Templates are used to create/update the user's system code permission upon sign-on.



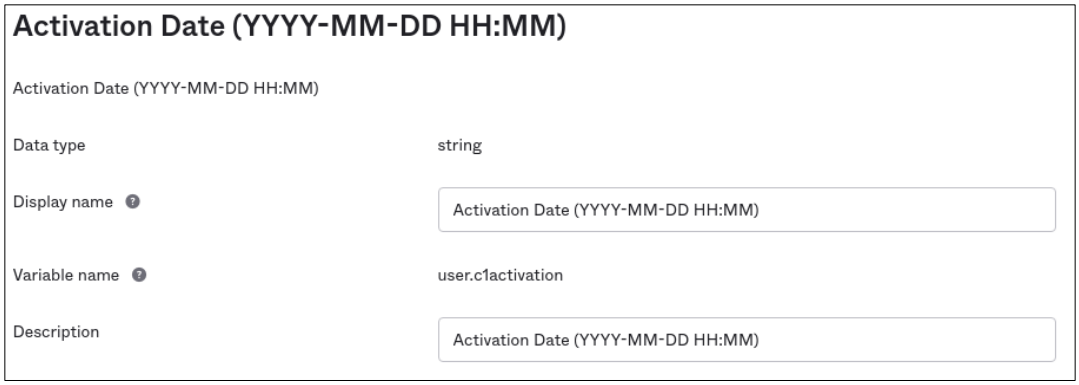
Create a new attribute called, System Code. The code attribute may be specified to override the system code option from Settings. Set to [none] if you do not want any system codes created for the user.



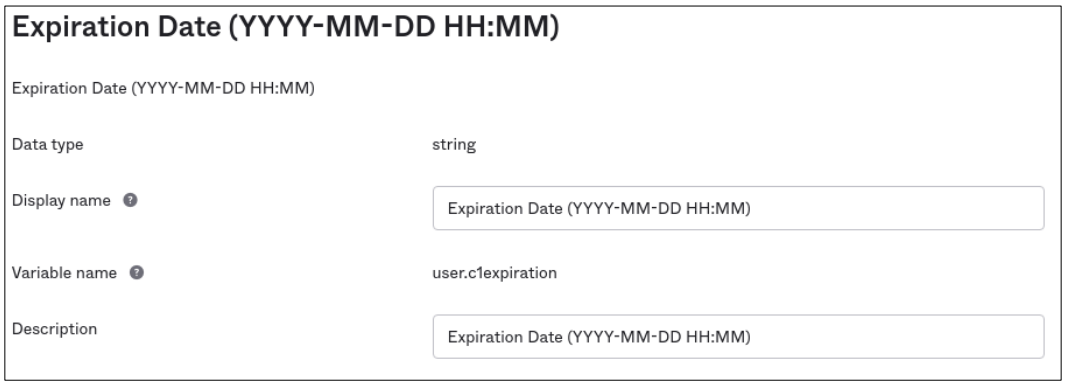
If your system requires the use of a separate pin then create a new attribute called, Pin.



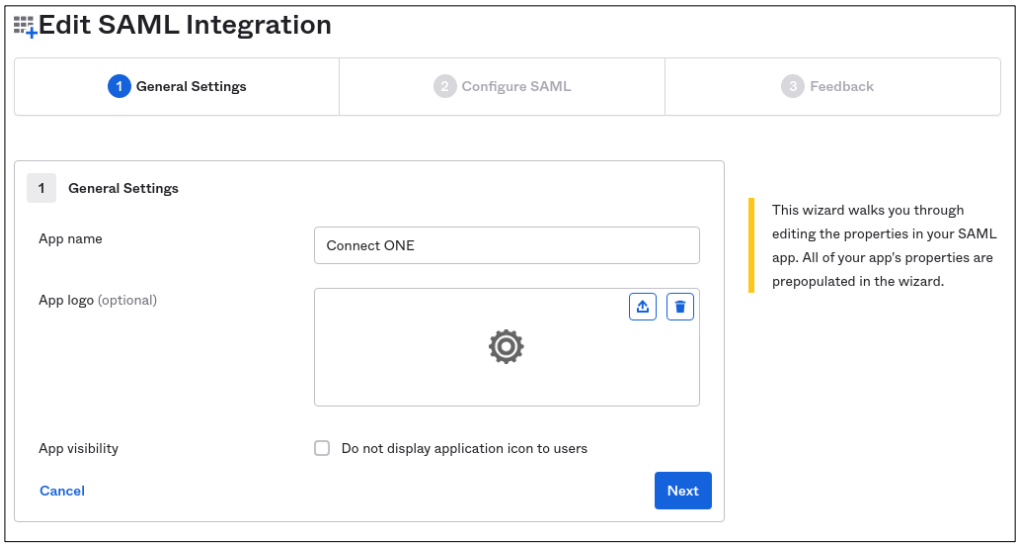
Create a new attribute called, Activation. The activation attribute may be specified which will be applied to both the user account and their assigned system code.



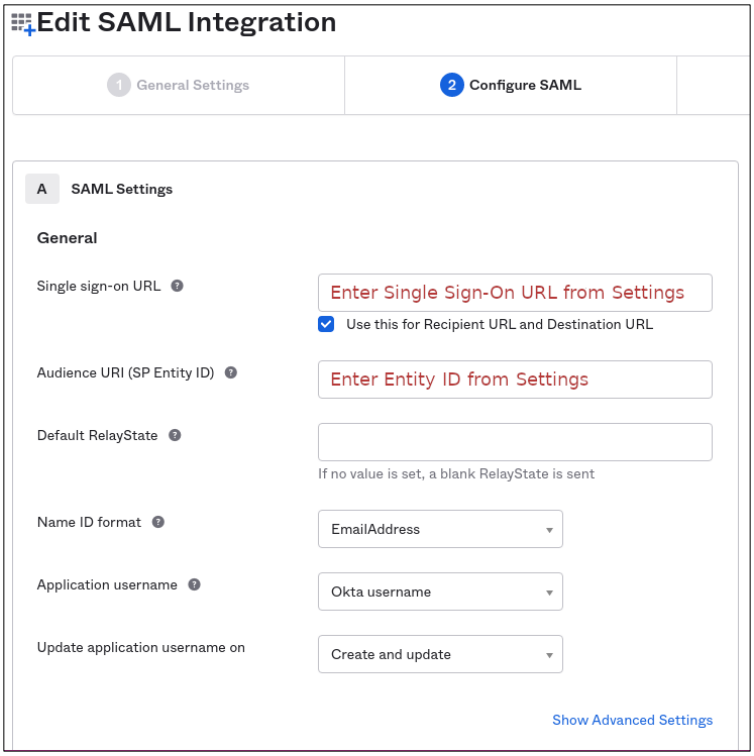
Create a new attribute called, Expiration. The expiration attribute may be specified which will be applied to both the user account and their assigned system code.



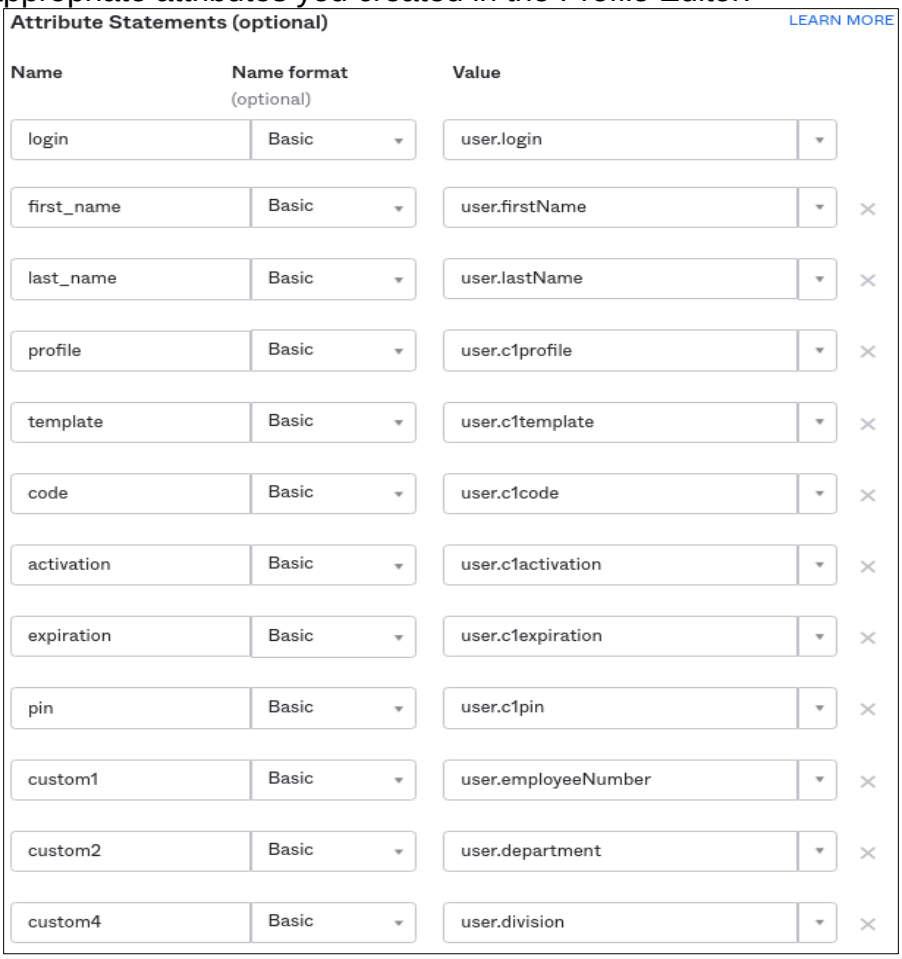
Connect ONE uses SAML 2.0 for SSO integration. From your IdP, create a new app using SAML 2.0. An example with Okta is below. Name the application and upload the application icon.



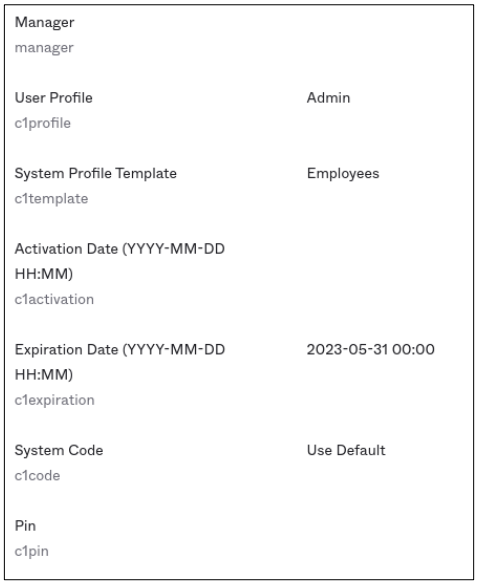
Enter the Single Sign-On URL and Entity ID, copy/paste from Settings.



Set the appropriate attributes you created in the Profile Editor.



An example of specific attributes set to a Okta User below:



From Okta	→ Utilities:Settings
App Sign-On Metadata Details: Copy the “Issuer”	→ “IdP Entity ID (Issuer)”
“Sign on URL”	→ “Idp Sign-On URL”
“Sign-Out URL”	→ “Idp Sign-Out URL”
“SHA2 Certificate Fingerprint”	→ “IdP Certificate Fingerprint SHA2”

Set the session timeout you’d like to use for the user after a period of inactivity.

Set the default User Profile to use for the user upon sign-on, this can be overridden from the Okta User’s profile attribute.

Set the Default System Code & Default System Profile Template, if you want a System Code created for the User upon sign-on. These values may be overridden from the Okta User’s attributes.

Save the Settings Changes.

Lastly, assign the app to a Okta User.