# Dealer Admin Help File

To access the searchable online help file click here.

Exported on 09/26/2025

# Table of Contents

# 2 Get Started

*Part 1: The Basics of Using Dealer Admin*

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/476043661

*Part 2: Manage Your Business Using Dealer Admin*

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/479081391

Dealer Admin is a centralized, cloud-based administrative portal that combines many keypad and Remote Link programming features with powerful tools like system analytics. Dealer Admin enables you to quickly program systems, optimize your services, run reports, update your panels remotely, manage your customers, and much more.

For help with other products, like Virtual Keypad, visit the DMP Help Files page.



## 2.1 Get a Dealer Admin Account

To get a Dealer Admin account, contact SecureCom Customer Service at 877-300-8030 or customerservice@securecomwireless.com.

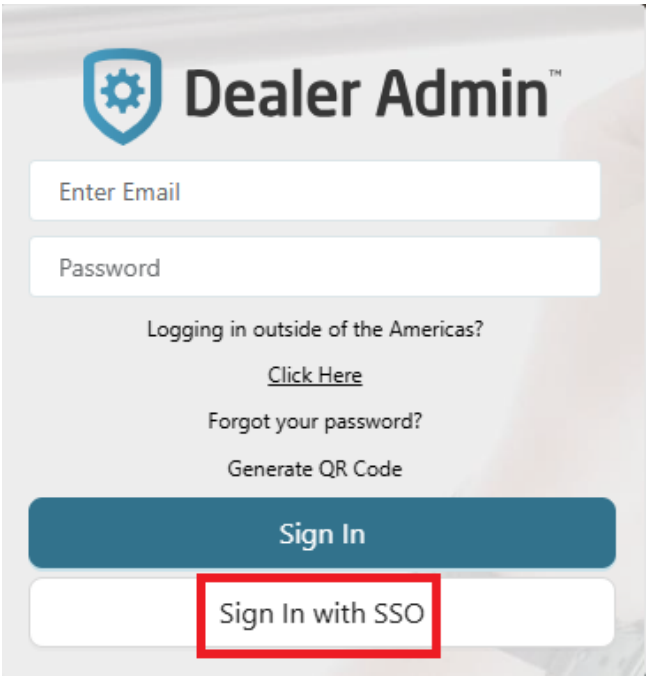
## 2.2 Sign In

1. Go to Dealer Admin.
2. Enter your **Email** and **Password**.
3. Select **Sign In**.

## 2.3 Use Single Sign-On

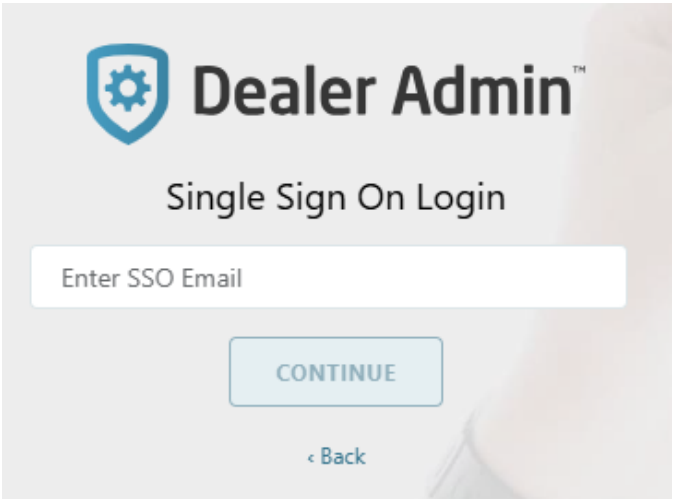
SSO allows you to log in to multiple applications with one set of credentials. To use SSO, complete the following steps:

1. Go to Dealer Admin.
2. Select **Sign In with SSO.**




**1 SSO Login**

3. Enter your **SSO Email**, then select **Continue**.




**2 SSO Email**

4. You are navigated to your company login page. Enter your email and password.

You are automatically returned to Dealer Admin and successfully logged in.

## 2.4 Reset Your Forgotten Password

> **Note**: Resetting your password is not available for SSO passwords. If you need to reset your SSO password, contact your Administrator.

1. On the login page, select **Forgot Your Password**.
2. Enter your **Email** address.
3. Select **Reset Password**. This will send you an email with a link to set up your new password.

4. Find the auto-generated email in your email inbox and select **Update Password**.
5. Enter your new password, then re-enter it to confirm.
6. Select **Update Password**.
7. Use your new password to log in.

## 2.5 Sign Out

Select your avatar, then select **Sign Out**. You are signed out and automatically redirected to the login page.

## 2.6 Edit Your Account Settings

To change account settings like your username, email, or user image, or to set up Two-Factor Authentication, select the Avatar icon and go to **Settings**.

### 2.6.1 Change Your Password

1. Select the Avatar icon and go to **Settings**.
2. Under **Options**, select **Change Password**.
3. Enter your current password.
4. Enter your new password, then re-enter it to confirm.
5. Select **Submit**.

### 2.6.2 Set Up Two-Factor Authentication

> **Note**: Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) is not available for Single Sign-On. If 2FA or MFA is required, it should be enabled through the Identity Provider (IdP).

1. Select the Avatar icon and go to **Settings**.
2. Under **Options**, select **Two-Factor Authentication**.
3. Select how you want security codes sent to you.
    a. If you select **Text**, you will need to enter your phone number.
    b. If you select **Email**, the email you logged in with will automatically be selected.
4. Enter the code sent to your phone number or email.
5. Select **Confirm Code**.

Personnel can opt in to Two-Factor Authentication themselves or Administrators can require it. To require personnel to use Two-Factor Authentication, enable it in a custom role, then assign that role to personnel. For more information, refer to Add, Edit, and Delete Custom Roles.

# 3 Search

Dealer Admin offers two ways to use search. The search field on the **Customers** page provides a quick and powerful way to find specific information. The search field in the sidebar on the left side of the screen can help you find more general information by category. To search Dealer Admin from the menu, complete the following steps:

1. After signing in to Dealer Admin, select **Search** in the sidebar on the left.
2. Choose an option from the **Select a Category** dropdown to narrow down your search results. Searchable categories include **Customers**, **Users**, **Systems**, **Video Device MAC\Serial Numbers**, **Video Doorbell**, and **XV Series MAC address**.
3. Search terms must be at least three characters long. Enter the word or phrase that you want to search for into the search field.
4. Press Enter or select **Search**.

# 4 Dealer Dashboard

Dealer Dashboard enables you to track, analyze, and manage your business from Dealer Admin.



**Prefer a Video?**

In this clip, we'll show you how to use Dealer Dashboard.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/611091393

## 4.1 Requirements

To access this feature, personnel need Admin authority or a Custom Role with **Dealer Dashboard** permissions. For more information, refer to Personnel Roles.

## 4.2 Features

### 4.2.1 Trailing 12 Month Sales Trends

This section displays your DMP year-to-date sales, a comparison of the previous year's sales, and a sales trend graph for the past 12 months. This section also contains color-coded dealer levels, so you can see your current level and the direction your company is trending:

| | |
|---|---|
| **Red** | Trending towards previous dealer level |
| **Green** | Maintaining current dealer level |
| **Blue** | Trending toward next dealer level |

### 4.2.2 Dealer Overview

This section includes some of the following information:

- How far you are from your next dealer level
- Your month-to-date (MTD) sales
- Orders shipped year to date
- RAN (return authorization number) units for year

### 4.2.3 Dealer Information

This section includes the following detailed information:

- How long you've been a dealer
- Your current dealer level
- Your number of tech support calls and topics most called about
- Training and certifications data

### 4.2.4 Top Ten Products Purchased

This section includes metrics for the top 10 products that you've purchased, including the part number and how many products you've ordered.

### 4.2.5 New Products & Services

This section includes a table of the newest products and services with their adoption rate and totals.

### 4.2.6 Virtual Keypad

This section includes a table of adoption rates and totals of systems with enabled features in Virtual Keypad, such as some of the following features:

- Arm Only App
- Standard App
- Cameras
- Z-Wave Products
- Traffic Count
- Login Rate (%)
- Video Doorbell

# 5 Customers

The **Customers** page includes a list of your customers and their systems and, if you chose to display it, an interactive map. From this page, you can add, edit, and delete customers.



## 5.1 Add a Customer

To add a customer, complete the following steps.

1. Go to **Customers**.
2. Select the blue **Add** icon next to the heading.
3. Enter the customer's name and email.
4. Enter the customer's address.
5. Select **Save**.

## 5.2 Edit a Customer

To edit a customer's information, complete the following steps.

1. Go to **Customers**.
2. Select the customer's name.
3. In the top summary section, select **Edit**.
4. Edit the information as needed.
5. Select **Save**.

## 5.3 Delete a Customer

To delete a customer, complete the following steps.

1. Go to **Customers**.
2. Select the customer's name.
3. Select the **Delete** button in the upper right corner of the **Customer Summary** section.
4. A dialog box displays to confirm your decision. To permanently delete the customer, click **Delete**.

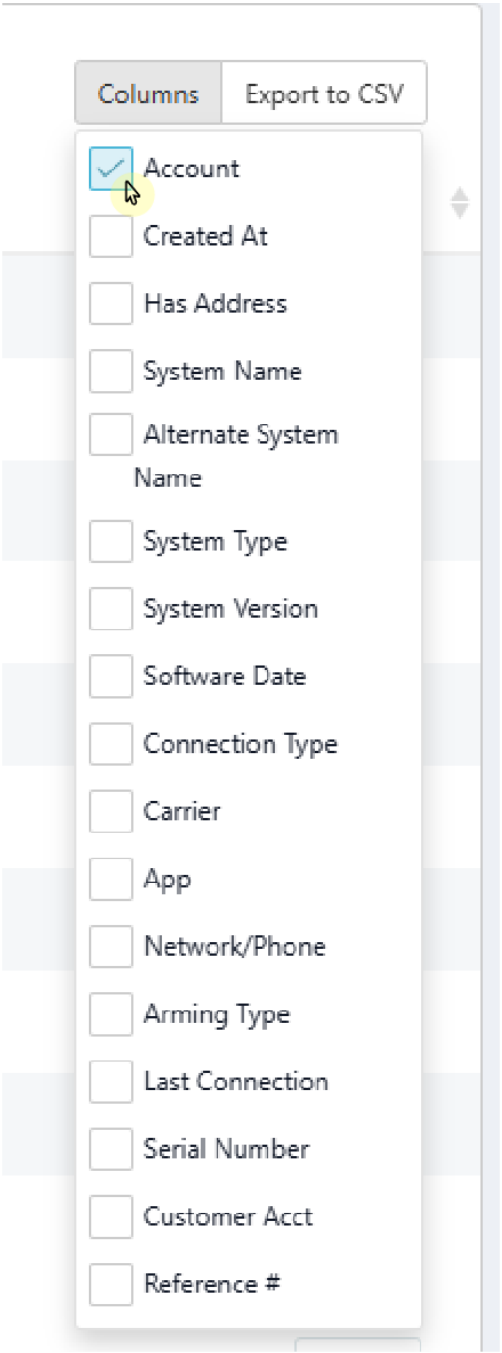
## 5.4 Customer Information

The Customers page includes a table with information about your customers and their systems. By default, the table displays the account, customer, system, system type, system version, and connection columns. You can add or remove columns to display various categories.

You can also use the embedded search bar to find or filter customers. For example, if you want a list of all your customers that use the XR550, you can type XR550 in the search bar to show only the customers who use that system.

### 5.4.1 Add or Remove Categories

1. Select the **Columns** button.
2. To add a category to the table, select ☐ next to the category you want to add.
3. To remove a category from the table, select ☑ next to the category you want to remove.



### 5.4.2 Column Categories

| Category | Description |
|---|---|
| Account | The account number associated with a system. |
| Customer | The name of the customer associated with a system. |
| Created At | The date the system was programmed for the customer. |
| Has Address | The address of the customer is available and can be used to filter your search. |
| System Name | The name given to a system. |
| Alternate System Name | A personalized system name chosen by the customer to view in Virtual Keypad, different from System Name. |
| System Type | The panel model (XTLplus, XTLtouch, XT Series Control Panels, XR Series Control Panels, iComSL, CellCom, or DualCom). |
| System Version | The firmware version of the system. |
| Software Date | The date the software version was updated on the system. |
| Connection Type | How the system connects to SecureCom servers. |
| Carrier | The type of carrier the system uses. |
| App | The app the customer's system is associated with. |
| Network/Phone | The contact phone number associated with a system. |
| Arming Type | The type of arming the system is programmed to use (home/sleep/away, all/ perimeter, or areas). |
| Last Connection | The last date and time a customer accessed the app. |
| Serial Number | The serial number on the panel of the system. |
| Customer Acct | The customer's unique account number. |

| Category | Description |
|---|---|
| Reference # | A billing account number specifically for Dealer use, not used by SecureCom. It appears on the invoice. |

### 5.4.3 Export Customer Information to CSV

Select **Export to CSV** in the top right corner of the table. The CSV file downloads to your device.

## 5.5 Interactive Map

The map shows the location of all your systems. You can filter which systems are displayed on the map by system, connection, carrier, and status by clicking on the arrow labelled **Filters** on the left-hand side of the map. You can also view the weather conditions worldwide.

To display the interactive map, press the **Show Map** button in the top right side of the page. To hide it, select the same button.

### 5.5.1 Map Icon Descriptions

 — Toggle fullscreen mode

 — Show weather condition by type

 — Show cellular map by type

 — Toggle dark or light mode

 — Open street view

 — Zoom In

 — Zoom Out

# 6 Digital Key Credentials

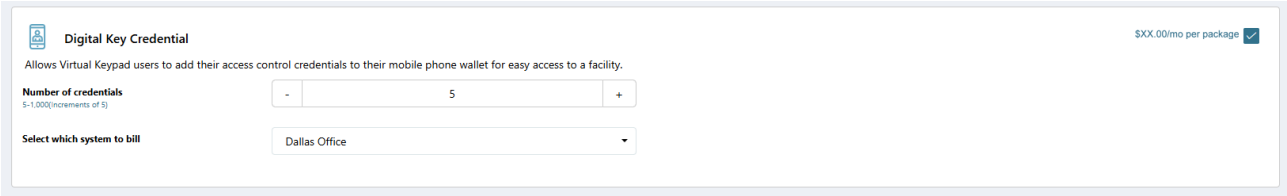
This section covers how an Administrator purchases Digital Key credentials for a customer in Dealer Admin. These steps should be completed after the compatible NFC multi-technology reader is installed.

To purchase and issue Digital Key credentials in Dealer Admin, you need an **Administrator** role.

## 6.1 Enable Digital Key Credentials

To enable a pool of reusable Digital Key Credentials, complete the following steps:

1. Go to **Customers**.
2. Select the customer name.
3. At the top of **Customer Summary**, select **Edit**.
4. Scroll to the bottom of the page. Go to **Digital Key Credentials** and select the checkbox to enable the credentials.

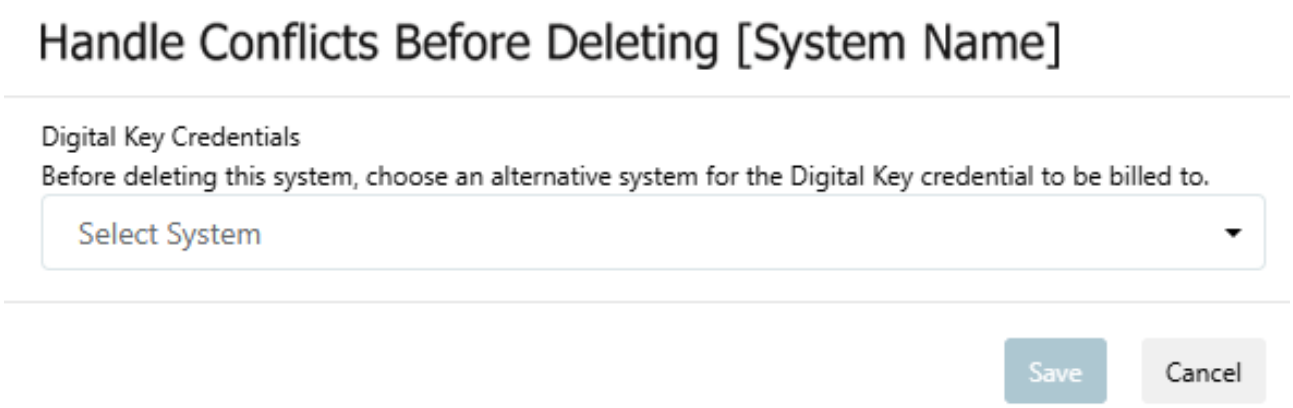



**Note**: Digital Key credentials can only be enabled if **Store User Codes** is turned on. If **Store User Codes** is not enabled, a dialog box displays to enable the feature. Select **Proceed** to automatically enable Store User Codes for all systems.

5. Next to **Number of credentials**, use the plus **+** and minus **-** buttons to adjust the number of reusable credentials you want to enable. You can select credentials in increments of 5, ranging from 5 to 1,000 credentials.
6. In the **Select which system to bill** drop-down menu, select the system you wish to invoice the credentials to for a recurring monthly charge.
7. At the top of the page, select **Save**.
8. Notify your customer that you completed their purchase.

If you wish to delete a system that is set as the current billable system, you will be prompted to choose a new system to invoice the credentials to for a monthly charge. To choose a new billable system, complete the following steps:

1. Go to **Customers**.
2. Select the customer name.
3. In the row of the system that you want to delete, select the More icon.
4. Select **Delete**.
5. If the system is set as the current billable system, a dialog box displays to choose an alternative system for the Digital Key credentials to be billed to.
6. In **Digital Key Credential**, select the new system to invoice the monthly charge in the drop-down menu.
7. Select **Save** to delete the current system and set the new system to bill the credentials to.




## 6.2 Public Card Formats

| CARD FORMAT | WEIGAND CODE LENGTH | SITE CODE POSITION | SITE CODE LENGTH | USER CODE POSITION | USER CODE LENGTH | USER CODE DIGITS |
|---|---|---|---|---|---|---|
| DMP Wavelynx 40-Bit | 40 | 0 | 1 | 0 | 40 | 10 |

# 7 Single Sign-On

Single Sign-On allows customers and users to log in to multiple applications with one set of credentials. Single Sign-On is compatible with the following SAML platforms:

- Generic SAML 2.0 provider
- Microsoft Entra ID
- Microsoft Active Directory Federation Service (AD FS)
- Okta
- Auth0
- Google
- OneLogin
- PingOne
- JumpCloud
- Rippling
- OpenID Connect Provider

For more information on enabling SSO, contact DMP Inside Sales or your Regional Sales Manager.

# 8 Systems

Dealer Admin helps you install and manage your customers' systems. In this section, you'll learn how to add, edit, and delete a system. For information about programming systems, refer to Programming.

For more information, refer to the appropriate installation and programming guides from DMP.com/resources.

**Prefer a Video?**

In this clip, we'll walk you through the System Information, System Status, and System Test pages.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/571843472

## 8.1 Add a System

To add a new system to a customer, complete the following steps.

- Step 1: Program Your App Key
- Step 2: Set Up the System
- Step 3: Configure Virtual Keypad Options
- Step 4: Configure Other Features

**Prefer a Video?**

In this clip, we'll show you how to add a system.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/570037277

### 8.1.1 Step 1: Program Your App Key

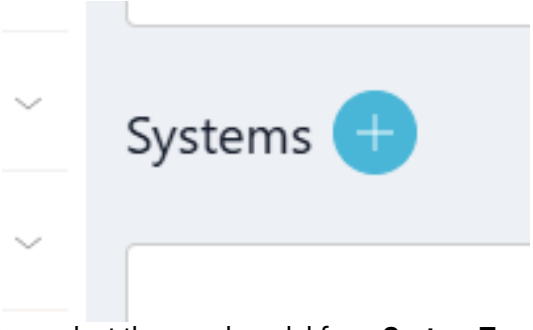
Before adding a system in Dealer Admin, program your App Key into the panel in **REMOTE OPTIONS** unless using the default App Key. If your panel uses the default App Key, it will be automatically programmed by SecureCom. The App Key is a dealer specific code that allows Dealer Admin and Virtual Keypad to connect to a panel. To view your App Key, go to **Settings > Dealer**. For more information about App Keys, review this training video.

### 8.1.2 Step 2: Set Up the System

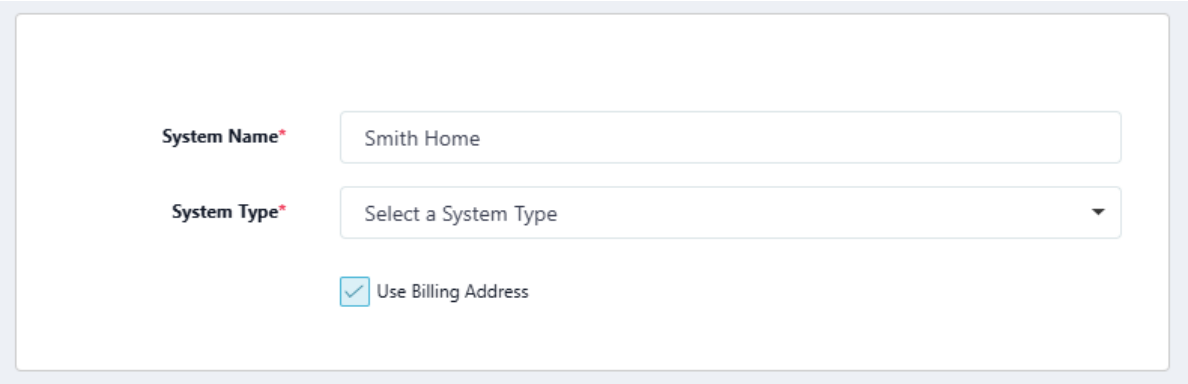
The options available to you during system setup will depend on the device and connection type. Before you can program or remotely update a panel, you must add it and connect to the panel from Dealer Admin.

**Note:** EASYconnect only works on panels that are capable of wireless or wired network communication. For EASYconnect or network connections, ensure **ALLOW NETWORK REMOTE** is set to **YES** in the panel's **REMOTE OPTIONS**. For EASYconnect, network outbound port 4001 must be open.

1. Go to **Customers**.
2. Select a customer to open the **Customer Summary**.
3. In **Systems**, select the Add icon.



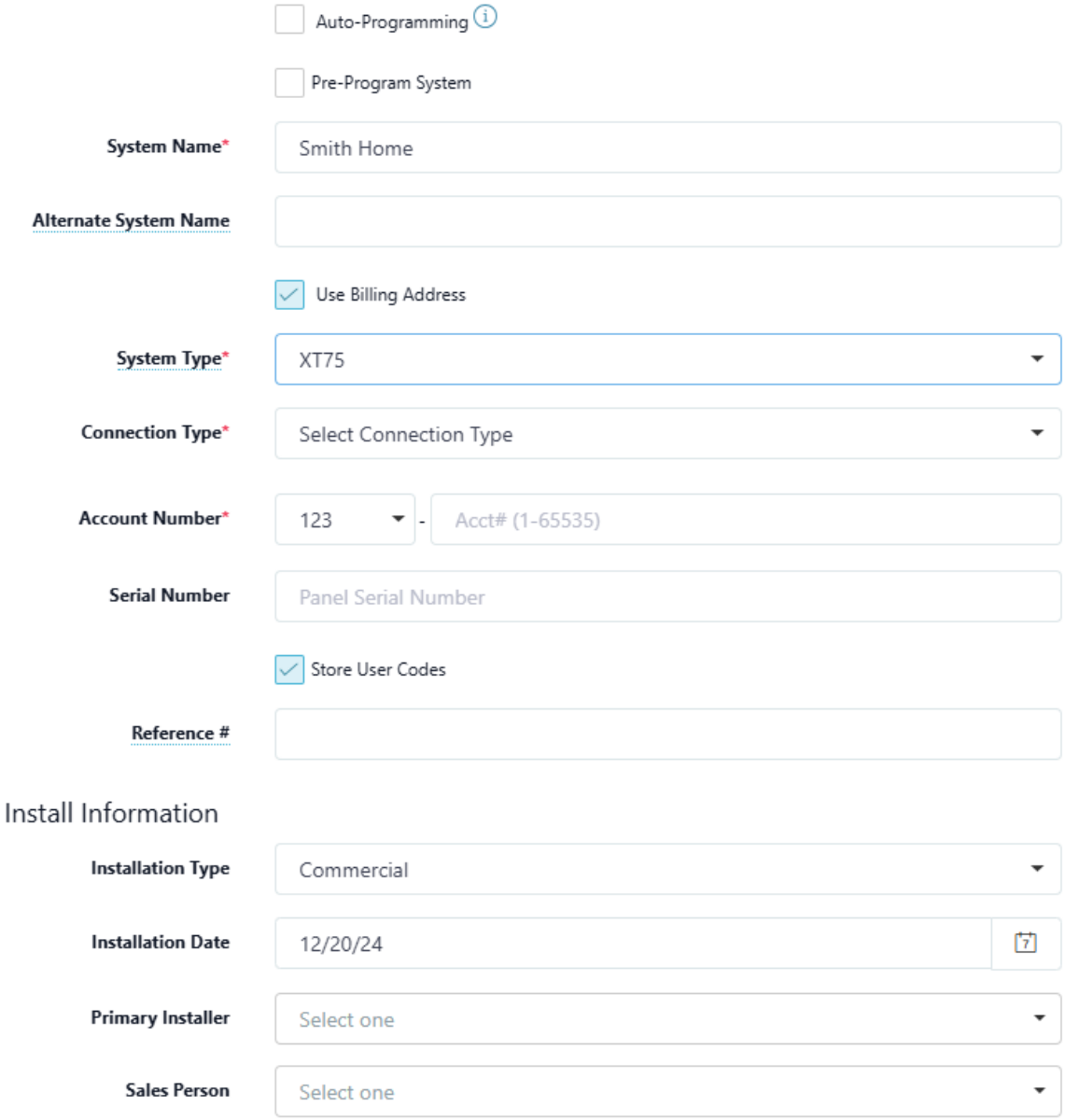

4. Enter the system name, then select the panel model from **System Type**.



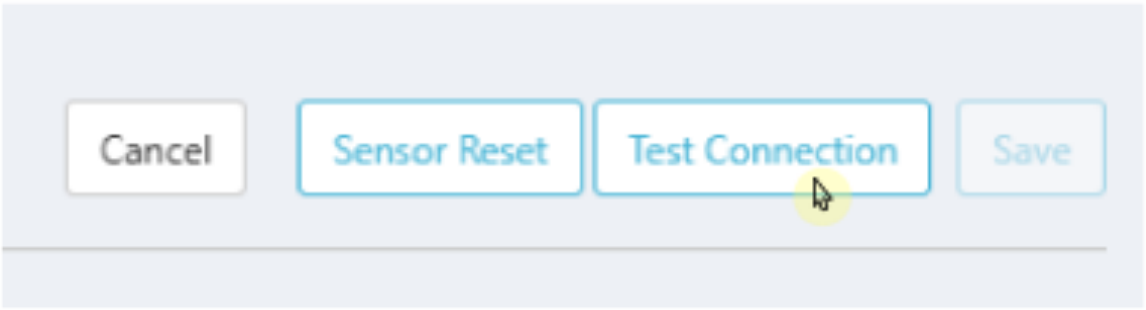

5. Enter an **Alternate System Name** if necessary and if the customer has not already created one.
6. Select a **Connection Type**. Enter the required connection information as follows:
    - For a **Cellular** connection, enter or scan a SIM number, then select **Get Status**. If the module is inactive, select **Activate**. To schedule cell activation, refer to Auto-Program a System.
    - For a panel that only uses **EASYconnect**, enter or scan the panel serial number In **Serial Number**.
    - For a panel that uses **EASYconnect + Cell Backup**, enter or scan a SIM number, then select **Get Status**. If the module is inactive, select **Activate**. Enter the panel serial number In **Serial Number**.
    - For a **Network** connection, enter the panel network's public IP address or DDNS hostname in **Network Address**.

**Note**: To enable DualSIM, choose **Cellular** or **Easyconnect + Cell Backup** as the Connection Type, then select the checkbox next to **Use DualSIM**. Enter the **First Serial Number** and the **Second Serial Number**, then select **Get Status** for each SIM number. If the module is inactive, select **Activate** next to each SIM number.

7. In **Account Number**, enter the system's receiver number in the leftmost field and the system account number in the rightmost field.
8. If you've programmed a remote key in the panel's **REMOTE OPTIONS** menu, enter it in **Remote Key**. To change the remote key, click the **Change Remote Key** button and enter the new remote key number.
9. Configure additional options as needed.




10. To establish connection, select **Test Connection**, then select **Yes** to start the test. If the connection fails, troubleshoot connection type settings in Dealer Admin, panel **COMMUNICATION** and **REMOTE OPTIONS** programming, and physical configurations.




11. Continue to the next section to configure Virtual Keypad options. Otherwise, select **Save**.

### 8.1.3 Step 3: Configure Virtual Keypad Options

Configuring Virtual Keypad options determines how your users interact with their system in the app. Dealer Admin allows you to choose a system package, then enable or disable any of the options as needed.

1. Choose a system package.
2. In **Additional Features**, select any features that you want to activate.
3. If necessary, add tracked outputs, sensors, and doors.
4. For access systems, choose any doors that you want to include in the app.
5. In **Video**, choose any options that you want to include.
6. Continue to the next section to configure other features. Otherwise, select **Save**.

### 8.1.4 Step 4: Configure Other Features

Select any other features from **Additional Options**, **Virtual Keypad Access,** and **Video** that you want to include in the system, then select **Save**.

## 8.2 Edit a System



### 8.2.1 Edit System Information

To edit a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the **System Information** page, select the **Edit** button in the upper right corner.
4. Edit the system information as needed.
5. Select **Save**.

#### System Images

System Images allows you to upload an image of the system in its install location. To add a System Image, complete the following steps:

1. Select the blue Add icon next to **System Images.** A dialog box opens.
2. Select **Browse** to access your computer files and select your image, or drag and drop the image file into the box.
3. A preview of the image appears in the dialog box. Check that it is the correct image, then select **Upload.**
4. A small preview image appears in **System Images**.

#### Download or Delete a System Image

To Download or Delete a System Image, complete the following steps:

1. In **System Images**, select the preview of the image.
2. In the dialog box, select either **Download** or **Delete.**
    a. If you select **Download**, the image file automatically downloads to your computer files. You can then close the dialog.
    b. If you select **Delete,** a confirmation box appears. Select **Yes** to delete the image. The dialog box closes automatically.

### Tech Notes

Tech Notes are notes which include information relating to the customer or system, and can act as a reference material. To add a Tech Note, complete the following steps:

1. Select the blue Add icon next to **System Images.** A dialog box opens.
2. Fill in the necessary information in the dialog box. Select **Save.**
3. The dialog box closes automatically. A preview of the note will appear in Tech Notes.

#### Delete or Edit a Note

To Delete or Edit a System Image, complete the following steps:

1. Select the note you want to edit or delete. It will open as a dialog box.
    a. To edit the note, click in the text box and edit the text as needed. Select **Save.** The dialog box closes automatically.
    b. To delete the note, select **Delete.** A confirmation box appears. Select **Yes** to delete the image. The dialog box closes automatically.

## 8.2.2 Change a System's Account Number

1. Go to **Customers**.
2. Select the system name.
3. In the **System Information** page, select the **Edit** button in the upper right corner.
4. Next to **Account Number**, select **Change Account Number**.
5. Edit the account number, then select **Change Account Number**.
6. A dialog pops up to confirm your decision. Select **Yes**.
7. Select **Save**.

# 8.3 Delete a System

Deleting a system from Dealer Admin removes the system and its programming but doesn't deactivate cellular modules. To deactivate a SIM before deleting a system, edit the system, select **Deactivate Cellular Device**, then save the changes.

**Note**: If mobile wallet credentials are enabled and the system you are deleting is set as the billable system for mobile wallet credentials, you will be asked to choose a a new billable system. For more information, refer to Mobile Credentials.

To delete a system from Dealer Admin, complete the following steps:

1. Go to **Customers**.
2. Select the customer's name.
3. In the row of the system that you want to delete, select the More icon.
4. Select **Delete**.
5. A dialog pops up to confirm your decision. To delete the system, select **Delete**.

## 8.4 Replace a System

If a panel needs to be replaced, you can install a panel of the same model then send programming directly to it or retrieve programming from it. **Send Programming to New Panel** overwrites existing programming in the replacement panel. **Retrieve Programming from New Panel** overwrites existing programming in Dealer Admin.



### 8.4.1 Replace a System

For easier installation, program the original panel's App Key into the replacement panel before completing this replacement process.

1. Go to **Customers.**
2. Select the system name.
3. At the top of **System Information**, select **Edit.**
4. Next to the **Serial Number**, select **Replace Panel.**
5. Enter or scan the **Serial Number** of the replacement panel.
6. Send or receive programming from another panel.
    - To send programming to the new panel, select the version of programming from the original panel that needs to be copied over in the **Data Source** drop-down menu. Then select **Send to System.**
    - To copy programming from another panel to the new panel, select **Retrieve Programming From New Panel.**
    - For more information on which programming options are sent or retrieved, refer to Supported Programming Actions.
7. After initial programming is completed, **Programming** opens. Make additional changes if necessary.

### 8.4.2 Supported Programming Actions

The following programming actions are supported when sending or retrieving programming from the new panel. Some programming options only apply to specific panel models.

| Panel Programming Options | Send Programming to New Panel | Retrieve Programming from New Panel | Applies to Panel Model |
|---|---|---|---|
| Communication | Yes | Yes | All |

| Panel Programming Options | Send Programming to New Panel | Retrieve Programming from New Panel | Applies to Panel Model |
|---|---|---|---|
| Network Options | Yes | Yes | All |
| Messaging Setup | Yes | Yes | All |
| Device Setup | Yes | Yes | All |
| Remote Options | Yes | Yes | All |
| System Reports | Yes | Yes | All |
| System Options | Yes | Yes | All |
| Bell Options | Yes | Yes | All |
| Output Options | Yes | Yes | All |
| Output Information | Yes | Yes | XT and XR Series Control Panels |
| Output Setup | Yes | Yes | XTLplus |
| Output Groups | Yes | Yes | XR Series Control Panels |
| Status List Displays | Yes | Yes | XR Series Control Panels |
| Area Information | Yes | Yes | All |
| Zone Information | Yes | Yes | All |
| Key Fobs | Yes | Yes | All |
| Lockout Code | No | No | All |
| Schedules | Yes | Yes | All |

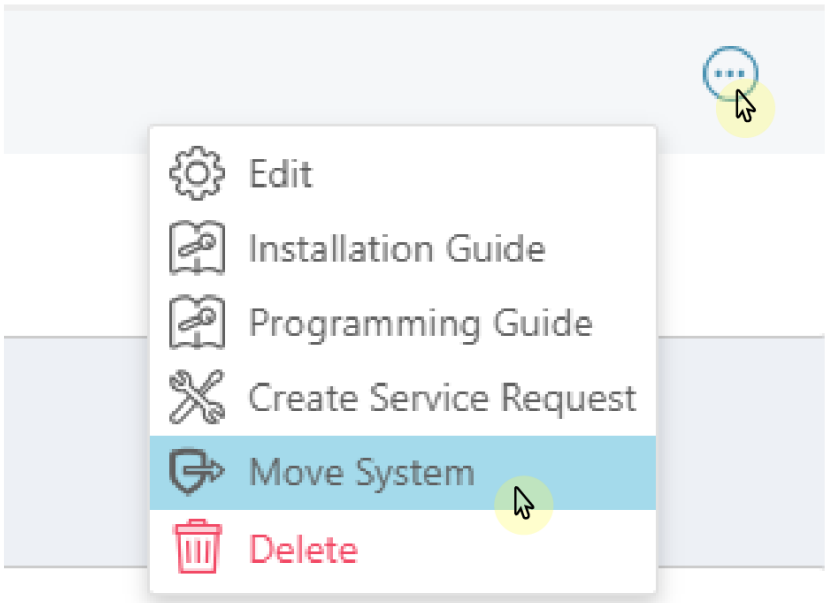
| Panel Programming Options | Send Programming to New Panel | Retrieve Programming from New Panel | Applies to Panel Model |
|---|---|---|---|
| Profiles | Yes | Yes | XR Series Control Panels |
| Groups | Yes | Yes | XT75 and X1 |
| User Codes | Yes | Yes | All |
| Favorites | No | Yes | All |
| Z-Wave Devices | No | Yes | All |
| Push Notification Settings | Yes | No | All |

## 8.5 Move a System

Move an existing system from one customer to another in the same dealer account. To move a system, personnel must be Administrators or have the **Move Systems** custom role permission.

To move a system, complete the following steps:

1. Go to **Customers** and select the customer's name.
2. In the row of the system that you want to move, select the **More** icon.
3. Select **Move System**.




4. Start typing to search for the customer that you want to move the system to, then select the customer from the list.
5. Select **Move System**.
6. A dialog box displays to confirm your decision. To move the system, select **Yes**.

**Warning**: For systems with mobile credentials enabled, you will not be able to move the system until all mobile wallet credentials assigned to users are removed in Virtual Keypad.

## 8.6 Connection Types

When creating or editing a system, the system **Connection Type** determines how the panel connects to our servers. After configuring the required fields for your connection type, select **Test Connection** to perform initial connection to the panel.

**Note:** If you enable **Auto-Programming** when you create a system, you must enter or scan the panel's serial number regardless of connection type.

- Cellular
- EASYconnect
- EASYconnect + Cell Backup
- Network

### 8.6.1 Cellular

Uses cellular to communicate with the panel. Requires a cell module to be installed on the panel.

To activate a cell module, enter or scan the SIM or MEID, select **Get Status**, then select **Activate**. To deactivate a cellular device, select **Deactivate Cellular Device**.

### 8.6.2 EASYconnect

Uses the panel serial number and app key to establish initial communication with the panel. Requires a panel with network communication capability (Wi-Fi or Ethernet).

In both Dealer Admin and the panel, program matching account numbers and serial numbers in System Options. In panel the **REMOTE OPTIONS** menu, program your app key and ensure that **ALLOW NETWORK REMOTE** is set to **YES** and network outbound port 4001 must be open.

### 8.6.3 EASYconnect + Cell Backup

Uses EASYconnect to establish connection to the panel, then uses cellular for a backup connection. Requires a panel with network communication capability (Wi-Fi or Ethernet) and an installed, active cellular module.

In both Dealer Admin and the panel, program matching account numbers and serial numbers in System Options. In panel the **REMOTE OPTIONS** menu, program your app key and ensure that **ALLOW NETWORK REMOTE** is set to **YES** and that network outbound port 4001 is open. To activate a cell module, enter or scan the SIM or MEID, select **Get Status**, then select **Activate**. To deactivate a cellular device, select **Deactivate Cellular Device**.

### 8.6.4 Network

In panel the **REMOTE OPTIONS** menu, ensure that **ALLOW NETWORK REMOTE** is set to **YES**. This connection type uses a standard network protocol to communicate with the panel over Wi-Fi or Ethernet.

In **Network Address**, enter the panel network's public IP address or DDNS hostname.

## 8.7 System Backups

> **Note:** To use backups, **Store User Codes** must be enabled in Dealer Admin. This allows SecureCom to send full programming and user codes back to the panel, eliminating the need to manually reprogram user codes after a system is restored.

When a system is created in Dealer Admin, programming is backed up automatically and once per month afterward. Each panel has a total of three backups in Dealer Admin. One is permanently reserved for initial programming created within 24 hours of the installation. The other two can be overwritten and are used for automatic or manual backups. To access Backups, go to **System Information**.

## 8.8 System Reports

Dealer Admin helps you manage your customers' systems with reporting. In this section, you'll learn how to run a User by System Report, an Events by Date Range Report, a Profiles Report, and how to export reports.

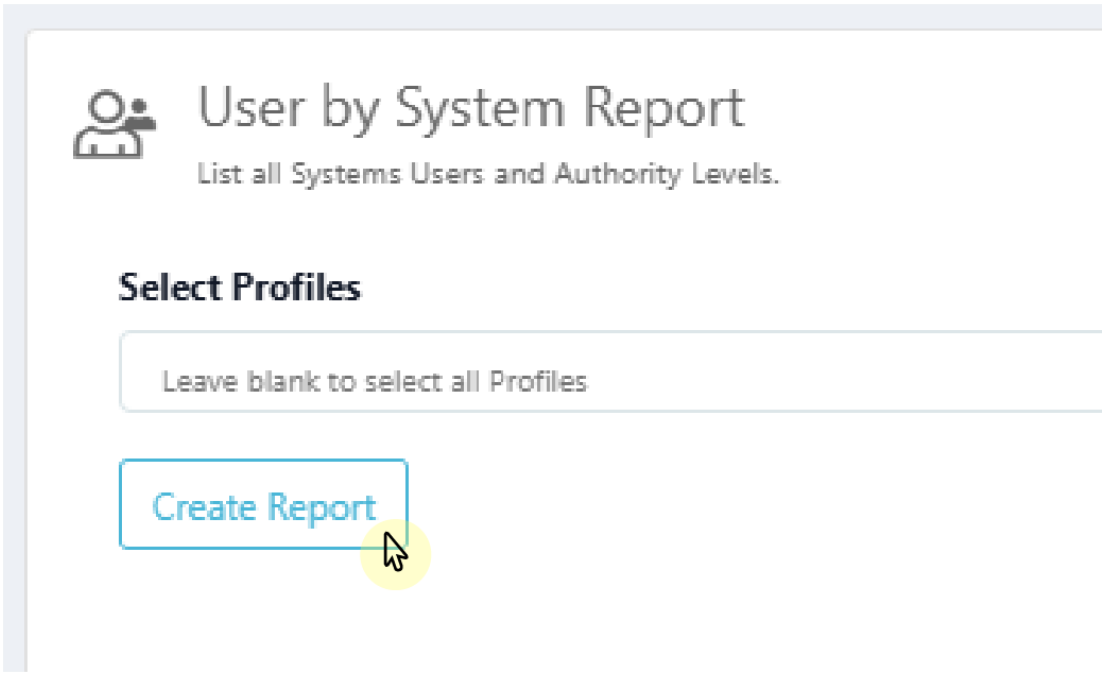
- A **User by System Report** lists the system's user codes and their associated authority levels.
- An **Events by Date Range Report** lists system events by type and a date/time range.
- On XR Series systems, a **Profiles Report** lists all the profiles associated with a system.

### 8.8.1 Run a User by System Report

To run a User by System Report, complete the following steps:

1. Go to **Customers**.
2. Select the system name.

3. In the sidebar on the left, go to **System Reports**.
4. Select **User by System Report**.
5. To run the report on specific profiles, in **User by System Report**, search for and select profiles from the results.
6. To generate and open the report, select **Create Report**.

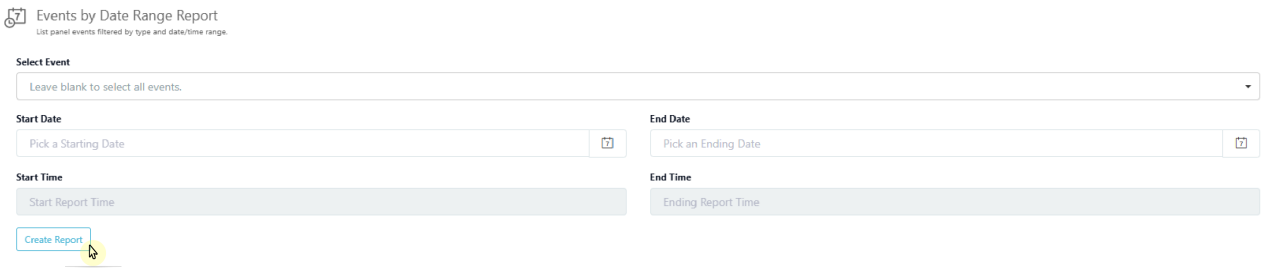



Use **Search** to find a specific user if necessary. Use the **Previous**, **Next**, and number buttons to view other pages. If you want to save your report, refer to Export a Report.

## 8.8.2 Run an Events by Date Range Report

To run an Events by Date Range Report, complete the following steps:

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **System Reports**.
4. Select **Events by Date Range Report**.
5. To run the report for specific panel events, in **Select Event**, enter an event type or leave the box blank to select all events.
6. If needed, enter a **Start Date**, **End Date**, **Start Time**, and **End Time** to restrict the report to a specific timeframe.
7. To generate and open the report, select **Create Report**.



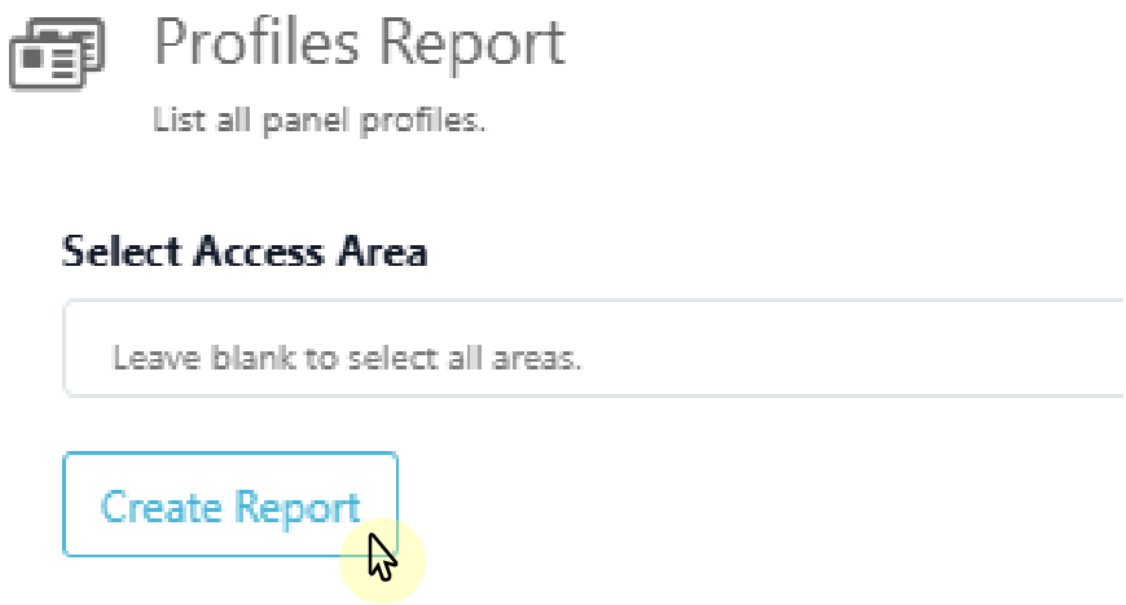
Use **Search** to find a specific user if necessary. Use the **Previous**, **Next**, and number buttons to view other pages. If you want to save your report, refer to Export a Report.

## 8.8.3 Run a Profiles Report

> **Note:** A Profiles Report can only be run for XR Series systems.

To run a Profiles Report, complete the following steps:

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **System Reports**.
4. Select **Profiles Report**.
5. To run the report on specific access areas, in **Select Access Area**, search for and select areas from the results.
6. To generate and open the report, select **Create Report**.




Use **Search** to find a specific profile if necessary. Use the **Previous**, **Next**, and number buttons to view other pages. If you want to save your report, refer to Export a Report.

## 8.8.4 Export a Report

To export a report, complete the following steps.

1. After creating a report, select **Export**.
2. Before downloading the report, you can choose to save it as a **CSV**, **Excel**, or **PDF** file.
3. A dialog box displays to ask where you want to save the file. Choose a location, then select **Save**.

# 8.9 System Status

**Note:** To remotely manage systems in Dealer Admin, personnel must be an **Administrator** or have a custom role with **Arming** permission. For more information, refer to Personnel.



**Prefer a Video?**

In this clip, we'll show you how to use the System Status page.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/571843472

Learn how to arm or disarm a system, check zone status, and handle faulted zones by completing the following steps. To access system status, complete the following steps:

1. Go to **Customers**.
2. Select the system's name.
3. In the sidebar on the left, go to **System Status**.

## 8.9.1 Arm or Disarm a System

Systems operate in one of three ways: All/Perimeter, Home/Sleep/Away, or Area. To arm or disarm a system, select the appropriate option:

### All/Perimeter Systems

**All**

Arm or disarm both the perimeter and the interior of your customer's home.

**Perimeter**

Arm or disarm only the perimeter of your customer's home.

### Home/Sleep/Away or Home/Away Systems

**Home**

Arm or disarm only the perimeter of your customer's home.

**Sleep**

Arm or disarm the perimeter of your customer's home as well as a portion of the interior. Bedrooms and nighttime parts of the home are left unarmed, allowing residents access to parts of your home during the night. Other areas of the house that are not used at night are armed.

**Away**

Arm or disarm the perimeter, interior, and bedrooms of your customer's home.

### Area Systems

**Area**

Arm or disarm individual areas. You can also choose to arm or disarm the entire system by selecting **Arm All** or **Disarm All**.

## 8.9.2 Check Zone Status

All the zones programmed on that system display with **Faulted Zones** listed first, followed by **OK Zones**. An icon is displayed in each zone's row under the **Status** column:

- A green check mark means the zone is normal.
- A yellow caution triangle with an exclamation point in it means the zone is faulted.
- An orange circle with a forward slash through the middle means the zone is bypassed.
- A red circle with an "X" in the middle means the zone is missing.

## 8.9.3 Manage Faulted Zones

> **Note:** Fire, Panic, Emergency, Supervisory, and 24-Hour zones cannot be bypassed.

When arming a system, some zones may not be in a normal condition. For instance, a window has been left open or a door is not fully closed. A list of **Faulted Zones** is displayed in **Zone Status**. Depending on system configuration, you can choose how the system handles the faulted zones from the following options:

- **Okay:** The faulted zones will be armed when they return to normal, such as when the faulted door or window is shut properly.
- **Bypass:** The zones will be ignored even if they return to normal while the system is armed. If the zones return to normal, they will be included the next time the system is armed.
- **Cancel:** Arming is cancelled and the system remains disarmed.

## 8.9.4 Manage Access Control Doors

> **Note:** Viewing doors requires that **Advanced Reports** is enabled in **System Information**. Locking, unlocking, and granting access to doors requires that **Door Control** is enabled in **System Information**.

| | |
|---|---|
| Lock the door |  |
| Unlock the door |  |
| Grant temporary access to the door |   |

## 8.9.5 More Tab

Selecting the **More** icon in the upper right corner displays additional options for your system.

### Alarm Silence

Remotely silence an alarm.

### Sensor Reset

Perform a remote sensor reset.

### Set Time and Date

Synchronize the panel time and date with the local computer's time and date.

### Test Connection

Remotely test the panel connection.

### LX-Bus Diagnostics

Perform routine diagnostics of the panel LX-Bus. Normal zones will not appear in this window.

### Forgive User

Remotely clear a failure to exit violation when using anti-passback.

### Lockdown

Initiate a system lockdown.

### Refresh

Refresh the arming and zone status.

# 8.10 System Tests

Learn how to remotely test a system.



**Prefer a Video?**

In this clip, we'll show you how to perform system tests.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/571843472

## 8.10.1 Available Tests

Dealer Admin enables you to perform the following system tests:

- **Communications Test**—Perform a communication test according to connection type.
- **Standard Walk Test**—Perform a standard walk test of a system's programmed zones.
- **Wireless Test**—Perform a test to determine whether programmed wireless devices are checking in with the panel.
- **Z-Wave Test**—Perform a diagnostics test to determine whether Z-Wave devices are communicating with the panel. Tests up to 10 devices at a time.
- **Z-Wave Optimization**—Optimize a system's Z-Wave mesh network.
- **PIR Test**—Perform a PIR walk test.

## 8.10.2 Test a System

To conduct a system test, complete the following steps:

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **System Test**.
4. If you want to test connection to the panel, select **Test Connection**.
5. Select the test that you want to conduct.
6. Select **Start Test**.

When testing system communication, Dealer Admin displays the same pass or fail messages at each stage as a keypad would. For more information about what these messages mean, refer to Communication Test Reference.

## 8.10.3 Communication Testing and Troubleshooting

When conducting a communication test, refer to the following sections for cellular and network test details. For more information, refer to the DMP Troubleshooting Guide and DMP Tech FAQs.

## Cell

Refer to the following sections when testing and troubleshooting cellular communication.

### Cell Test Messages

In order for the communications test to pass, the panel must pass all stages. When one stage fails, the entire test fails and the panel stops testing.

| Cell | | |
|---|---|---|
| **Stage** | **Pass Message** | **Fail Message** |
| 1 | Modem Operating | No Modem Found |
| 2 | Identified | No SIM Card |
| 3 | Tower Detected | No Tower |
| 4 | Registered | Not Registered |
| 5 | APN Accepted | APN Error |
| 6 | Comm Path Good | No ACK Received |
| | | Not Activated |
| | | Connect Error |
| | | No Signal |

### Troubleshoot Cell Communication

When troubleshooting port configurations, refer to the Important Ports for DMP Whitepaper.

| Issue | Likely Causes | What to Try |
|---|---|---|
| **No Modem Found** | • The panel can't communicate with the modem.<br>• The modem may be damaged or incorrectly installed.<br>• Panel firmware does not support the modem type.<br>• The cell card is 3G (CDMA or HSPA) and is no longer supported by the carrier in your area. | • Check the cell module installation and antenna.<br>• Check panel hardware.<br>• Check panel firmware version. Refer to DMP Tech FAQs for a list of firmware requirements.<br>• Upgrade the panel.<br>• Upgrade to a 4G cell card. |
| **No SIM Card** | • After reading the SIM, the panel received an error from the modem.<br>• The SIM card is not installed or it's installed incorrectly. | • Install a SIM.<br>• Go to **System Information** and check SIM status. |
| **No Tower** | • The modem can't find a tower.<br>• The SIM is not activated, signal strength is poor, or the tower is down/ | • Go to **System Information** and check SIM status.<br>• Go to **System Analytics** or **Tools > Reporting & Analytics** and check cell trouble and tower information. |
| **Not Registered** | • The modem tells the panel that registration is denied.<br>• The modem is not registered, the modem has extremely poor signal and has failed repeatedly to connect, the APN is incorrect. | • Go to **System Analytics** or **Tools > Reporting & Analytics** and check cell trouble and tower information.<br>• Go to **Communication** and check **Cell APN**. |

| Issue | Likely Causes | What to Try |
|---|---|---|
| **APN Error** | • The panel received an error from the modem related to PDP context.<br>• No IP address or port is configured in panel communication programming.<br>• The APN is not configured or is incorrect.<br>• The modem is registered but is now deactivated. | • Go to **Communication** and check APN; For XR Series v192 and higher, ensure an IP address is programmed.<br>• Go to **System Information** and check SIM status.<br>• Go to **System Analytics** or **Tools > Reporting & Analytics** and check cell trouble and tower information. |
| **No ACK Received** | • The modem sent a message but didn't receive an acknowledgement in the allotted time.<br>• The IP or port is incorrect or port forwarding is not configured.<br>• Ports are not configured for UDP outbound.<br>• The receiver is down. | • Go to **System Information** and check communication options.<br>• Go to **Communication** and check APN, TCP/UDP protocol, and receiver IP/ Port settings. |
| **Not Activated** | • The modem is not active.<br>• The modem hasn't been activated or failed to OTA. | • Go to **System Information** and check SIM status. |
| **Connect Error** | • The modem is unable to open a socket to send a message.<br>• The internet gateway is down or the modem hasn't been activated. | • Go to **System Information** and check SIM status.<br>• Go to **System Analytics** or **Tools > Reporting & Analytics** and check cell trouble and tower information.<br>• Check your local communications service. |
| **No Signal** | • Configuration is correct, but communication can't be established due to poor signal. | • Go to **System Analytics** or **Tools > Reporting & Analytics** and check cell trouble and tower information.<br>• Check your local communications service. |

## Network

Refer to the following sections when testing and troubleshooting network communication.

### Network Test Messages

In order for the communication test to pass, the panel must pass all stages. When one stage fails, the entire test fails and the panel stops testing.

| Network | | |
|---|---|---|
| **Stage** | **Pass** | **Fail** |
| 1 | Link OK | Link error |
| 2 | DHCP OK | DHCP error |
| 3 | Gateway found | No gateway |
| 4 | Destination found | No destination |
| 5 | Network communication Good | Not connected |
| | | Remote connect |
| | | Invalid port |
| | | No ACK received |

### Troubleshoot Network Communication

When troubleshooting port configurations, refer to the Important Ports for DMP Whitepaper.

| Issue | Likely Cause | What to Try |
|---|---|---|
| **Link Error** | • Panel is not connected to the network.<br>• Hardware may be damaged, or incorrectly installed. | • Check cabling.<br>• Check panel hardware.<br>• Check the network's hardware such as routers and switches. |

| Issue | Likely Cause | What to Try |
|---|---|---|
| **DHCP Error** | • The DHCP server is not receiving the panel's request for an IP address. | • Go to **Network Options** and check DHCP and other network configuration options.<br>• Go to **Communication** and check IPv6 and related communication options.<br>• Check your local network's configuration. |
| **No Gateway** | • The panel can't reach the gateway address.<br>• The IP address is incorrect, or ports between panel and gateway are configured incorrectly. | • Go to **Network Options** and check the IP, subnet, and gateway addresses.<br>• Check port configurations.<br>• Check the customer's local network's configuration.<br>• Check the ISP's network status and settings. |
| **No Destination** | • The IP address is incorrect<br>• Ports are configured incorrectly. | • Go to **Network Options** and check IP, subnet, and DNS settings.<br>• If using IPv6, go to **Communication** and check settings for that protocol.<br>• If connecting with Wi-Fi, check for sources of interference.<br>• Check router configuration and DNS settings on the local network. |
| **Not Connected** | • The IP address is incorrect.<br>• The ports are configured incorrectly.<br>• Receiver IP address or port is incorrect. | • Go to **Network Options** and check settings.<br>• Go to **Communication** and check receiver IP and port settings.<br>• Check the network for closed ports and port conflicts.<br>• Check local network configuration and network firewall settings. |

| Issue | Likely Cause | What to Try |
|---|---|---|
| **Remote Connect** | • Cannot test because a remote programming connection is open. | • Wait for programming changes to be saved and the remote connection to be closed, then retry. |
| **Invalid Port** | • The port is not a valid value or ports are configured incorrectly. | • Go to **Communications** and check the receiver port.<br>• Check the network for closed ports and port conflicts.<br>• Check local network configuration and network firewall settings. |
| **No ACK Received** | • The panel is connected but received no acknowledgement from the server. | • This may be a temporary interruption in service; try again.<br>• If connecting with Wi-Fi, check for sources of interference.<br>• Check router configuration and local network status. |

## 8.11 System Glossary

### 8.11.1 System

- **Auto-Program** enables you to automatically push programming to a system when it connects to our servers for the first time. If enabled, you must select a panel firmware version. You must also enter the panel serial number regardless of communication type. Auto-programming is designed for initialized panels, so it will overwrite any existing programming in the panel. If you want to send programming manually, you can do so by enabling pre-programming and not enabling auto-programming. For more information, refer to Auto-Program a System.
- **Pre-Program** enables you to program the panel with a specific firmware version.
- **System Name** is required. Give your system a descriptive name that differentiates it from other systems.
- **Alternate System Name** allows you to choose a personalized system name for the customer to view in Virtual Keypad, different from the System Name in Dealer Admin. Users can also create an Alternate System Name in Virtual Keypad. This is visible to all users associated with the system.
- **Use Billing Address** automatically fills in the customer's address based on their address in **Customer Summary**. For more information, refer to Add a Customer.
- **Edit Service Address** enables you to edit the customer's address for this system. Only visible if **Use Billing Address** is not enabled.
- **System Type** is the panel model. This field is required.

- **Firmware Version** enables you to select a specific panel firmware version. Required if **Auto-Program** or **Pre-Program** is enabled.
- **Templates** enables you to send programming to a system from one of your templates. For more information, refer to Templates.
- **Connection Type** determines how the system communicates with our servers. This field is required. For detailed information, refer to Connection Types.
- **Sim Number** (Cellular connection) is the SIM number assigned to the panel's cellular communicator.
- **Status** (Cellular connection) is the activation status of the cellular communicator.
- **Rate Plan** (Cellular connection) enables you to select panel's cellular rate.
- **Account Number** is the account number that you choose to identify a system. You can enter a two-digit receiver prefix from 1-99 and a five-digit account number from 1-65535. Both the receiver prefix and account number are required.
- **Cellular Number** (Cellular connection) is the number of the cellular communicator. Filled out automatically if you activate a new SIM. This field is required for cell.
- **Network Address** (Network connection) is the address of the network that you are connecting the system to. This field is required for network.
- **Serial Number** is the panel serial number. This field is required if you choose an EASYconnect connection type or if you enable **Auto-Programming**.
- **Remote Key** if you've changed the default remote key in the panel, enter it in this field to enable remote connection.
- **Store User Codes** allows Dealer Admin to save and display user codes. Required for system backups. For more information, refer to System Backups.

## 8.11.2 Installer Information

- **Installation Type** is filled out automatically depending on system type chosen. Options are **Commercial** or **Residential**.
- **Install Date** defaults to the date the system is created.
- **Primary Installer** defaults to user currently signed in.
- **Sales Person** enter the name of the person who sold the system.

## 8.11.3 Virtual Keypad

- **Arming** restricts the Virtual Keypad app to arm/disarm only.
- **Standard** includes all items from **Included Features**.
- **Standard + Video Doorbell** (Residential and XT30/XT50 Commercial installations) includes all standard system features plus **Video Doorbell**.
- **Virtual Keypad Access** (Commercial Installations for XR Series and XT75 Control Panels) includes all standard system features plus access control with **Advanced Reports** (non-cellular systems only).
- **None** disables Virtual Keypad.

## 8.11.4 Additional Features

- **Automation** enables Z-Wave devices like lights, locks, thermostats, and appliances.
- **User Code Management** allows app users with adequate permissions to fully manage their users in Virtual Keypad.
- **Schedule Management** allows app users with adequate permission to maintain Arming, Doors, Favorites and Output Schedules based on a system configuration.

- **Geofencing** enables users to create geofences so favorites are activated when they leave or enter a geographical area.
- **Traffic Count** enables tracking and reporting for zone activity counts.
- **Visible Outputs** allows app users with adequate permission to control system outputs.
- **Sensor Activity** enables users to receive notification on activity for up to 50 zones.

### 8.11.5 Virtual Keypad Access

- **Door Control** allows app users with adequate permission to lock, unlock temporarily grant access, and lock down public doors.
- **Advanced Reports** enables real-time status for access control doors and allow users to receive reports on related events.

### 8.11.6 Video

- **SecureCom Video and NVRs** enables SecureCom video devices. Stream live video from up to two eight-channel NVRs. Or view recorded clips from up to 16 SecureCom or Digital Watchdog/DMP video cameras.
- **Video Doorbell** enables the SecureCom Video Doorbells.
- **Central Station Video Verification** provides Video Verification services to the monitoring center.
- **Hikvision NVR** enables Hikvision NVR integration.
- **EagleEye** enables Eagle Eye Cloud-to-Cloud integration.
- **DW Spectrum®** enables Digital Watchdog Spectrum IPVMS and DW Cloud integration.
- **Hanwha WAVE®** enables Hanwha Wisenet WAVE integration.

# 9 Update Firmware

You can update system firmware remotely from Dealer Admin using **Remote Update**. You can also monitor updates from **Tools > Remote Update**. To perform remote updates, complete the following steps:

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **System Remote Update**.
4. If you want to view details before updating, go to **View Release Notes** and select the Open PDF icon.
5. Select **Update System**.

If you go to a different page, the system will continue updating in the background.

**Prefer a Video?**

In this clip, we'll show you how to use the Remote Update feature in Dealer Admin.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/showcase/588505078

## 9.1 Update Multiple Systems

**Prefer a Video?**

In this clip, we'll show you how to update multiple systems.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/588505078

To update multiple systems, complete the following steps.

1. In the menu, go to **Tools > Remote Update**.
2. In the **Bulk Update** tab, select applicable filters from **Model**, **Connection**, and **System Firmware** to filter your systems.
3. Select the checkboxes next to the systems that you want to update.
4. At the top of the page, select **Update Selected Systems**.
5. A dialog box pops up to confirm your decision. To update the selected systems, select **Confirm**.
6. A pop-window confirms that updates have been submitted for the selected systems. To view the status of updates, select **View Status** or go to **Tools > Remote Update > Update Dashboard**.

## 9.2 Update Keypad Firmware

You can update keypad firmware remotely from Dealer Admin using **Remote Update**. To perform remote updates, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **System Remote Update**.

4. Next to the keypad name, select **Update**.

**Note:** Remote Update capabilities are only available for 7-Inch Touchscreen Keypads.

# 10 Reset Sensors

When some kinds of sensors are tripped, they need to be reset before the system can work properly. You might need to reset sensors to restore a system after lockdown, reset a smoke detector, or reset a device after you change its batteries.

To remotely reset a sensor, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. At the top of the page, select **Sensor Reset**.
4. An alert pops up when the sensor reset command is sent to the panel.

# 11 Programming Overview

Dealer Admin helps you remotely program your customers' systems. You'll learn how to fast program a system, fully program a system, mass program panels, and view print programming.

For quick reference when programming devices, zones, or outputs, see the Quick Programming Reference Guide. For complete information, refer to the appropriate installation and programming guides from DMP.com/resources.

## 11.1 Auto-Program a System

Auto-programming allows you to automatically push programming to a new or initialized panel when it connects to Dealer Admin for the first time.

- Requirements
- Auto-Program a System
- Schedule Cell Activation

**Prefer a Video?**

In this clip, we'll show you how to use auto-programming and pre-programming.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/617184064

### 11.1.1 Requirements

Auto-programming requires the following:

- Panel Series: XR150/XR550, XT30/XT50, XT75, XTLplus, XTLtouch, CellCom, or DualCom
- Users with **Preset Roles** require the **Administrator**, **Operator**, or **Technician** role
- Users with **Custom Roles** require that **Permissions > System** is set to **View, add, and edit** and that **System Programming** has **Full/Fast Programming** enabled

### 11.1.2 Auto-Program a System

**Note:** Auto-programming overwrites all existing programming in the panel.

1. Go to **Customers**.
2. Select a customer to open the **Customer Summary**.
3. In **Systems**, select the Add icon.
4. Enter the system name.
5. Select a **System Type**.
6. Select **Auto-Programming**.
7. Select a panel firmware version.
8. Select a **Connection Type** and enter the appropriate connection information. For more information, refer to Connection Types.
9. Enter an **Account Number**.
10. Enter or scan the panel **Serial Number**.
11. Select other system options as needed. For more information about initial system creation options, refer to Add a System.

12. Select **Save**.

After saving the system, you can create programming in Programming, Profiles, User Codes, and Schedules and select **Save to Dealer Admin** so it's pushed to the panel on connection. Existing programming cannot be retrieved from the panel until a connection is established.

You can view the **Auto-Programming Errors** report in **Tools > Reporting & Analytics** to see any issues that occurred when attempting auto-programming. This report also provides details about any auto-programming performed after the system's original installation date.

### 11.1.3 Schedule Cell Activation

When a new system is pre-programmed or auto-programmed, cellular modules are automatically scheduled for activation on the panel's installation date.

1. When adding a new system, select **Auto Programming** or **Pre-Program System**.
2. When **Install Information** pops up, select an **Installation Date**. This determines when the panel communicator's SIM is activated.
3. Choose **Cellular** as the connection type.
4. Enter or scan the communicator's SIM number.
5. Select **Get Status** to finish scheduling activation.
6. Finish entering required information for the new system, then select **Save**.

## 11.2 Fast Programming

Fast programming enables you to quickly modify several basic programming functions of a system.

**Note:** Fast programming is only applicable to XTLplus, XTLtouch, iComSL, CellCom, and DualCom systems. Fast programming is not applicable to XT Series or XR Series systems. Refer to the appropriate system programming guide for more information.



### 11.2.1 Use Fast Programming

**Prefer a Video?**

In this clip, we'll show you how to use fast programming.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/616336201

To use fast programming, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **Fast Programming**.

4. Modify fast programming settings such as the **Receiver IP**, **Weather ZIP Code**, **System**, and additional options as needed.
5. Select **Send to System**.

### 11.2.2 Manage Zones

In **Zone Information**, you can add or remove zones as needed.

#### XTLplus and XTLtouch

1. To add a zone, select the Add Zone icon and enter or scan the device's **Serial Number**.
2. To remove a zone, select the Remove Zone icon.
3. Select **Send to System**.

#### iComSL, CellCom, and DualCom

1. Select **Add Zone**.
2. Enter a **Zone Name**, **Zone Number**, and **Zone Type**.
3. Configure settings in the **Advanced** and **Action** tabs as needed.
4. Select **Send to System**.

## 11.3 Mass Programming

Mass programming enables you to program multiple systems at once with the same settings.

**Prefer a Video?**

In this clip, we'll show you how to use mass programming.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/618093167

To program multiple systems, complete the following steps.

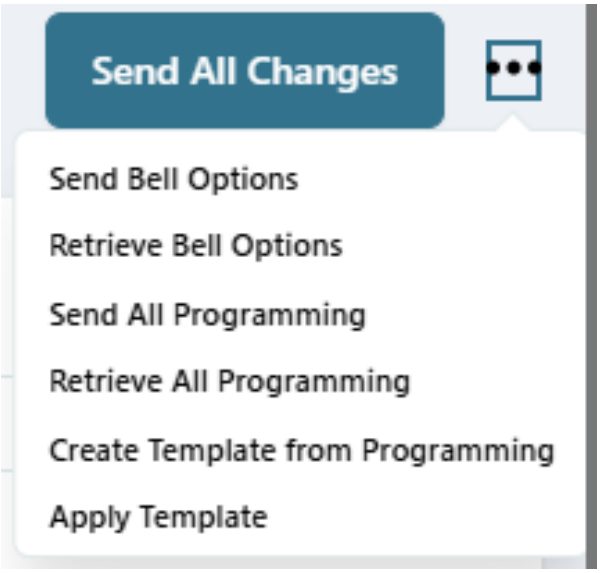
1. In the sidebar on the left, go to **Tools > Mass Programming**.
2. Select the **Add** icon.
3. In **System Type**, select the appropriate system family.
4. In **Reason for Change**, enter a brief description of the changes.
5. Expand a category to see programming options. Select the checkbox next to the items that you want to change and configure the settings as needed.
6. Select **Add Systems** and select the systems that you want to program.
7. When you've finished adding the systems, select **Send**.
8. A dialog pops up to confirm the changes. To send the changes to all of the selected systems, select **OK**.

## 11.4 Retrieve and Send Programming

Programming allows you to configure more settings during system installation than fast programming. To program your system, complete the following steps:

1. Go to **Customers**.

2. Select the system name.
3. In the menu, go to **Programming**.
4. To retrieve programming from a panel or apply a template, select the **More** icon in the upper right corner, then select one of the following options:
    - **Retrieve [Programming Category]:** Only retrieves programming changes for a specific programming category from the panel.
    - **Retrieve All Programming:** Overwrites all Dealer Admin programming with panel programming.
    - **Apply Template:** Applies saved templates of programming settings.
5. Select a category name from the small sidebar on the left to expand the programming options. Configure the settings in each category as needed. For descriptions of each category, see Programming Categories.
6. Send the programming to the system. To send programming, select the **More** icon. Select one of the following options:
    - **Send [Programming Category]:** Only sends programming changes for a specific programming category to the panel.
    - **Send All Programming:** Overwrites all panel programming with Dealer Admin programming. This does not include items that aren't programmed in Programming like User Codes, Profiles, and Schedules.
7. Save the programming for future applications by selecting the More icon, then selecting **Create Template From Programming.**



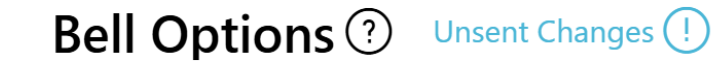

**3 Retrieve and Send Programming Options**

## 11.4.1 Programming Statuses

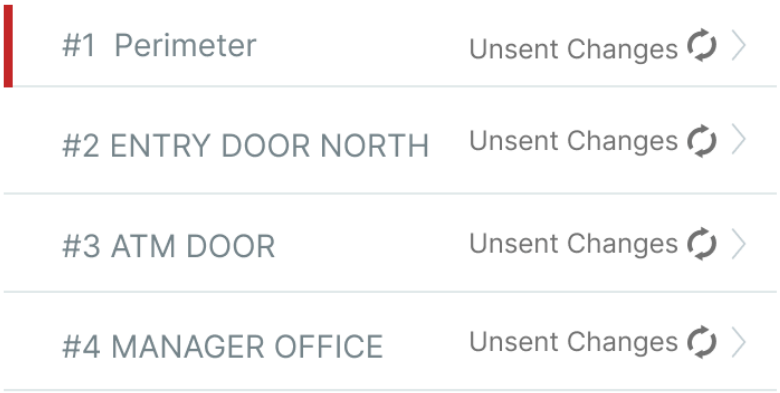
Programming statuses provide real-time updates on programming changes, indicating whether there are unsent changes and if the panel has retrieved any changes. The following statuses appear in Dealer Admin programming:

- **Unsent Changes** — Programming changes have not been sent to the panel.

This status displays at the top of the screen next to the programming option, in the side menu, and next to each individual programming change within the selected programming option.




**4 Main Programming Changes**

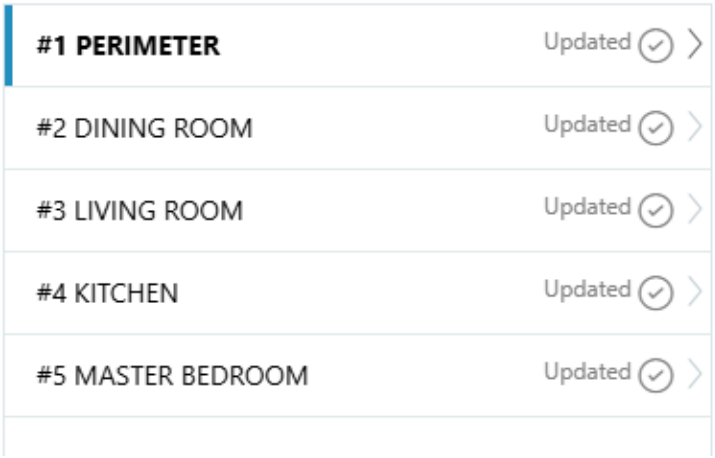



**5 Individual Programming Changes**

- **Updated** — Programming changes have been sent and updated in the panel.

This status displays at the top of the screen next to the programming option and next to each individual programming change within the selected programming option.

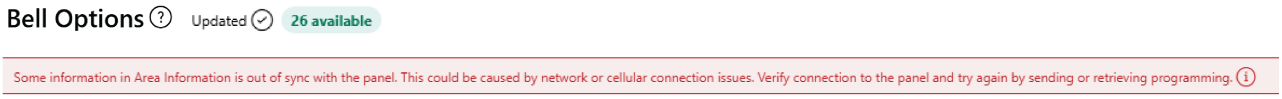

**6 Main Programming Changes**




**7 Individual Programming Changes**

- **Error Sending** — Programming changes were sent to the panel but the panel did not receive and acknowledge the update.

An alert appears, providing details about the specific changes that failed to send to the panel, such as certain areas or zones.




**8 Error Banner**

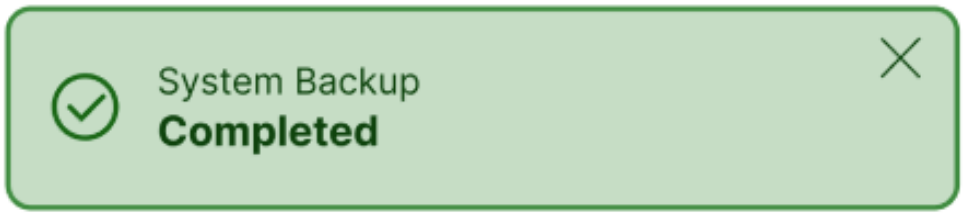
To try to resend changes, select the **More** icon next to **Send All Changes** and choose of the following options:

- Send [Programming Category]
- Retrieve [Programming Category]
- Send All Programming
- Retrieve All Programming

## Programming Status Notifications

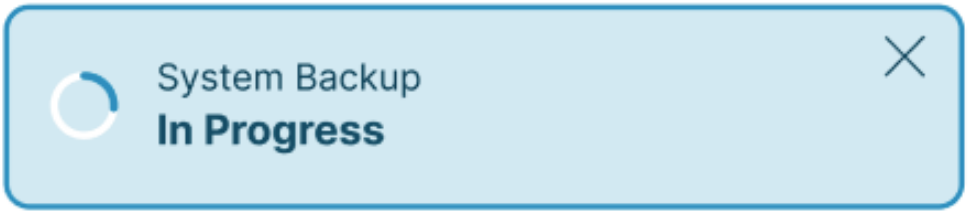
You can continue making programming changes while previous changes are still being processed. Each notification is specific to its corresponding change. The following notifications display at the bottom of the screen in Dealer Admin:

- **Completed** — The programming change is complete and retrieved by the panel. The notification automatically disappears after 10 seconds.



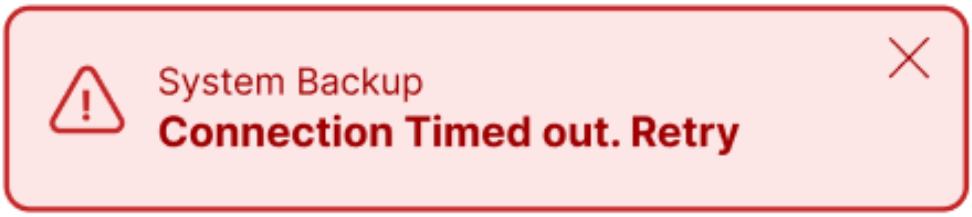

**9 Completed Notification**

- **In Progress** — The programming change is in the process of being updated. The notification remains on the screen until it is manually dismissed or the pending action is updated with a **Completed** or **Error** notification.




**10 In progress Notification**

- **Error** — There was an error in updating the programming change. The specific problem is detailed in the alert. The notification remains on the screen until manually dismissed.



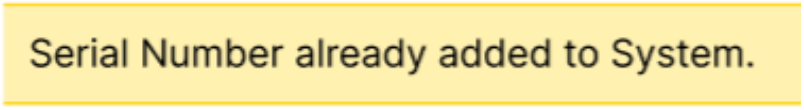

**11 Error Notification**

## 11.4.2 Glossary

### Programming Categories

The following section contains descriptions of each category in the small sidebar menu in **Programming**. For more detailed information, reference the appropriate DMP guides. When programming devices, zones, or outputs, refer to the Quick Programming Reference Guide.

> **Note**: Entering duplicate serial numbers is valid when programming both internal and external contacts. If a duplicate serial number is entered, a notification appears to inform you that the serial number already exists. You can choose to proceed or make corrections as needed.




**12 Duplicate Serial Number Banner**

- **Communication:** Choose how the system communicates and modify communication settings. Additionally, you can modify receiver settings. For XR Series systems, the number of available communication paths is displayed at the bottom of the **Communication** section.
- **Network Options:** Program the system's network connection settings, such as the local IP address, gateway, and ports. Edit the DNS Field here if **DHCP** is enabled.
- **Messaging Setup:** Enable messaging for the system. This feature is not supported for panels with Version 202 or higher firmware.
- **Device Setup:** The number of devices that you can add depends on panel type and the number of feature keys you have enabled. Select **Add Device** and enter or scan the device's information. You can also delete existing devices. For XR Series panels and XT75 Control Panels, you can program access control devices. The number of available devices to program displays at the bottom of the **Device Setup** section.
- **Remote Options:** Modify how the system interacts with the Virtual Keypad App, Remote Link, and Entré.

> **Note:** To change the remote key, select the **Change Remote Key** button in System Information and enter the new remote key number. For more information, refer to Add a System.

- **System Reports:** Determine which reports the system will generate. Additionally, you can enter the **Late to Open** and **Early to Close** times.
- **System Options:** Modify various settings for a system, such as the system arming type, entry and exit delays, bypass settings, time settings, and more.
- **Bell Options:** Modify the system's bell settings and enable automatic bell tests.
- **Output Information:** Add outputs to the system depending on system type. You can also delete existing outputs.
- **Output Options:** Enter the system's outputs, as well as other information for the system's outputs.
- **Output Groups:** Assign outputs to groups. Output groups can be assigned to output options or alarm actions like single outputs, allowing an entire group of outputs to turn on and off as required.
- **Area Information:** Add or delete areas. The type and number of areas you can add are dependent on the arming type of the system. Select an area's name to edit that area's settings.
- **Zone Information:** Add or delete zones. The number of zones that can be added depends on the system's capabilities. Select a zone's name to edit its **Wireless**, **Advanced**, and **Actions** settings.

**Note**: Zones can be filtered using the following options: **Zone Type**, **Area**, and **Wireless** (Enabled or Disabled). Zones can also be filtered numerically or alphabetically.

- **Key Fobs:** Add or delete key fobs.
- **Feature Keys:** View and activate feature keys for XR550 Control Panels.
- **Lockout Code:** Program a lockout code which limits the ability to program the system locally.

## 11.5 Print Programming

To view a system's programming reference sheet, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **Print Programming**.
4. The **Programming Sheet** opens.
5. To print the programming sheet, right-click the page and select **Print**.
6. Choose the appropriate settings, then select **Print**.

## 11.6 Feature Keys

The following feature keys can be activated and programmed in Dealer Admin:

| Feature Key | Description |
|---|---|
| **32 Door Add-On A**<br>(64 total doors) | Add 32 more doors to the panel, increasing the maximum number of doors to 64.<br>Requires XR550 Series with firmware Version 111 or higher. |
| **32 Door Add-On B**<br>(96 total doors) | Add 32 more doors to the panel, increasing the maximum number of doors to 96.<br>Requires XR550 Series with firmware Version 111 or higher and 32 Door Add-On A. |
| **Encryption**<br>(128-bit AES or 256-bit AES) | Enable encryption on XR550 Series panels with Network capability.<br>Requires XR550 Series with Network. |

### 11.6.1 Activate a Feature Key

To activate a feature key, complete the following steps.

1. Go to **Customers**.
2. Select the Customer.
3. Select the System Name.
4. In the sidebar, go to **Programming > Feature Keys**.
5. To retrieve current feature key programming from the system, select the More icon in the upper right corner, then select **Retrieve Feature Keys**.
6. To get your new feature key, call DMP Customer Service at 866-266-2826 and give the representative the panel serial number from **Serial No**.

7. Enter the key in the text box, then select **Send Key**.

## 11.7 Auto Configure ECP and DSC Passthru

After setting up host panel and installing the communicator, complete the following steps to remotely configure the communicator.

- ECP Setup
- DSC Setup

### 11.7.1 ECP Setup

1. Go to **Customers**.
2. Find and select the system name.
3. In the sidebar on the left, go to **Programming > System Options**.
4. In **Keypad Input**, select **ECP**.
5. In **ECP Partition**, enter the number of the partition where you want the communicator to operate.
6. Select **Begin ECP Setup**.
7. If the host panel is a VISTA 128, turn on **VISTA 128**.
8. Enter the host panel's installer code in **VISTA Installer Code**.
9. Select **Begin**.
10. After setup is complete, Dealer Admin automatically retrieves zones from the host panel. If you need to retrieve zones again later, open **System Options** and select **Get Zones**.

### 11.7.2 DSC Setup

1. Go to **Customers**.
2. Find and select the system name.
3. In the sidebar, go to **Programming > System Options**.
4. In **Keypad Input**, select **DSC**.
5. Select **Begin DSC Setup**.
6. Enter the host panel's installer code in **Installer Code**.
7. Select **Begin**.
8. After setup is complete, Dealer Admin automatically retrieves zones from the host panel. If you need to retrieve zones again later, open **System Options** and select **Get Zones**.

# 12 Devices

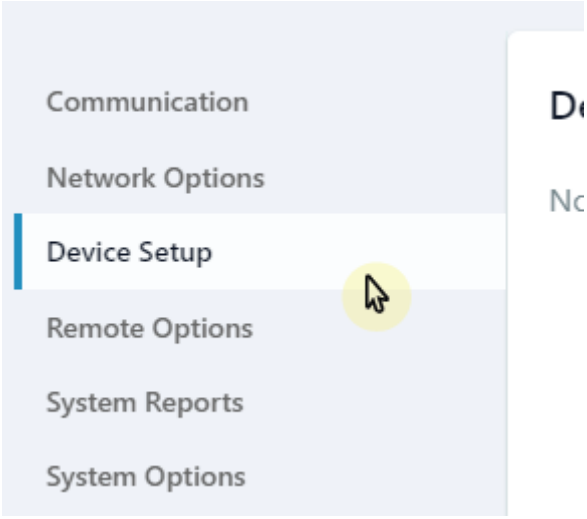
Dealer Admin helps you manage devices on your customers' systems. In this section, you'll learn how to add, edit, and delete devices.

For quick reference when programming devices, zones, or outputs, see the Quick Programming Reference Guide. For complete information, refer to the appropriate installation and programming guides from DMP.com/resources.

## 12.1 Add a Device

To add a device to a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar to the left, go to **Programming**.
4. Select **Device Setup** from the options on the left.




5. Select **Add Device** in the upper right corner.
6. Enter a number and name for the device.
7. Choose a **Device Type** and **Device Communication Type**.

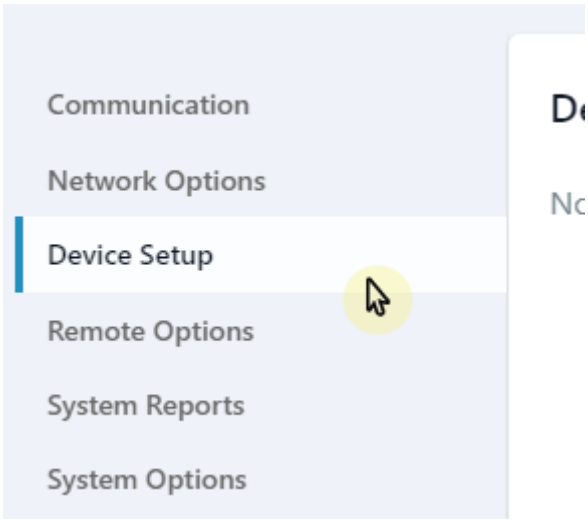
5. For wireless devices, enter or scan additional device information, such as the device **Serial Number** and **Supervision Time**.

9. Select **Send Device Setup**.

## 12.2 Edit a Device

To edit a device, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **Programming**.
4. Select **Device Setup** from the options on the left.

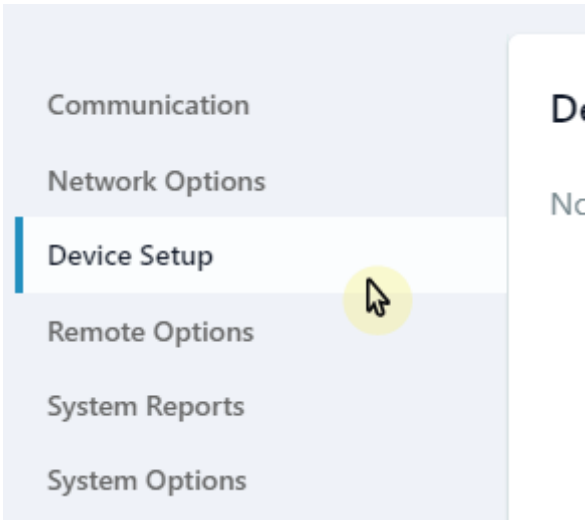



5. Select a device.
6. Edit the device information as needed, such as the **Device Number** and **Device Name**.
7. Select **Send Device Setup**.

## 12.3 Delete a Device

To delete a device from a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **Programming**.
4. Select **Device Setup** from the options on the left.




5. Find the device that you want to delete and select **Delete**.
6. A dialog pops up to confirm your decision. To delete the device, select **OK**.

## 12.4 Access Control Doors

For quick reference when programming devices, zones, or outputs, see the Quick Programming Reference Guide. For complete information, refer to the appropriate installation and programming guides from DMP.com/resources.

To add an access door to be managed in Virtual Keypad, complete the following steps:

- Add the Device
- Add the Door to Virtual Keypad

## 12.4.1 Add the Device

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **Programming**.
4. Expand **Device Setup**.
5. Select **Add Device**.
6. In **Device Name**, give the door a name according to its location or purpose.
7. In **Device Type**, select **Door**.
8. To make the door a private door that can only be accessed by the profiles it's assigned to, turn on **Private Door**.
9. In **Device Communication Type**, select the appropriate connection for the door.
10. Configure other options as needed.
11. To add a card format, expand **Card Formats**, select **Add Card Format**, and configure the options as needed.
12. Select **Send Device Setup**.

## 12.4.2 Add the Door to Virtual Keypad

1. In the sidebar on the left, go to **System Information** and select **Edit**.
2. Go to **Virtual Keypad Access**.
3. In **Door Control**, select **Add**.
4. Select the doors that you want to add, then select **OK**.
5. Select **Save**.

To configure Profile Options, see Edit a Profile and Profiles Reference.

To configure Group Options, see Edit a Group and Groups Reference.

# 13 Outputs

Dealer Admin helps you manage outputs on your customers' systems. In this section, you'll learn how to add, edit, and delete outputs.

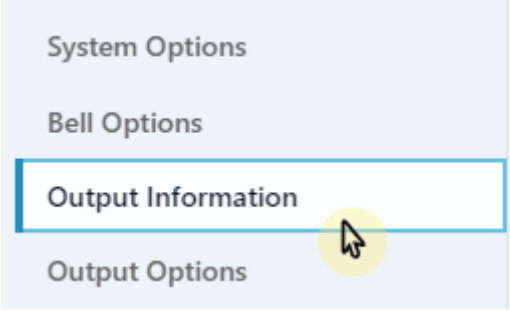
For quick reference when programming devices, zones, or outputs, see the Quick Programming Reference Guide. For complete information, refer to the appropriate installation and programming guides from DMP.com/resources.

## 13.1 Add an Output

> **Note:** Dealer Admin has tooltips that can help you determine what to put in each output field. Hover over text with a blue underline to view the tooltips.

To add an output to a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Programming**.
4. Select **Output Information** from the options on the left.




5. Select **Add Output**.
6. Enter the output number, name, serial number, and supervision time.
7. If needed, select **Trip with Panel Bell**.
8. Select **Send Output Information**.

### 13.1.1 Add an Output to Virtual Keypad

> **Note:** Before starting, you'll need to record the **Output Number** and **Output Name** of each output that you want to add to Virtual Keypad.

1. In the sidebar, go to **System Information** and select **Edit**.
2. Go to **Additional Features > Visible Outputs**.
3. In **Tracked Outputs**, select **Add**.
4. Select the Add icon.
5. In the **Output** field, enter the **Output Number**.
6. In the **Output Name** field, enter the name of the output as you want it displayed in Virtual Keypad.
7. Select **OK**.
8. In **System Information**, select **Save**.

## 13.2 Edit an Output

To edit an output, complete the following steps.

> **Note:** Dealer Admin has tooltips that can help you determine what to put in each output field. Hover over text with a blue underline to view the tooltips.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **Programming**.
4. Expand **Output Information** and select an output.
5. Edit the output information, such as the **Output Number**, **Output Name**, **Serial Number**, and **Supervision Time**.
6. To keep your changes, select **Send Output Information**.

## 13.3 Delete an Output

To delete an output from a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **Programming**.
4. Go to **Output Information**.
5. Find the output that you want to delete. Select More and then **Remove**.
6. A dialog pops up to confirm your decision. To delete the output, select **OK**.

# 14 App Users

Dealer Admin helps you manage Virtual Keypad app users on you customers' systems. In this section, you'll learn how to add, reset, edit, and delete app users.

## 14.1 Add an App User

To add an app user, complete the following steps.

1. Go to **Customers**.
2. Select the customer's name.
3. In **App Users**, select the Add icon.
4. Enter the user's email address.
5. Enter the user's first and last name.
6. Select an authority level:
    - To allow the user to manage multiple systems, set the user's authority level to **Administrator**.
    - To allow the user to manage a single system, set their authority level to **Standard**.
    - To grant the user temporary door access, set their authority level to **Access Only**.
7. If you want to email the user video clips, select the **Email Video Clips** checkbox.
8. Select the systems and permissions that you want your user to have authority to access. If you want to allow Virtual Keypad users to initiate a system panic from the app and website, enable any of the following options:
    - Police Panic
    - Fire Panic
    - Emergency Panic

> **Note**: To initiate a system panic, sign in to Virtual Keypad, open the Menu icon, and select **Panic**. Press and hold the desired panic option for three seconds.

9. Select **Save**.

After you add an app user in Dealer Admin, the user will be sent a welcome email with a link to finish setting up their account by creating a password.

## 14.2 App User Forgets Password

> **Note**: Users can select **Forgot Password** at the login and then fill out the form to update their password or it can be done through Dealer Admin.

If an app user forgets their password or needs their password reset, complete the following steps:

1. Go to **Customers**.
2. Select the customer's name.
3. In **App Users**, find the user whose password needs to be reset.
4. Select the More icon and click **Reset Password**. When editing an App User, you can also select **Reset Password**, then click **Save**.

## 14.3 Edit an App User

To edit an app user, complete the following steps.

1. Go to **Customers**.

2. Select the customer's name.
3. In **App Users**, find the user's row and select the More icon.
4. Select the Edit icon.
5. Edit the user's **Email**, **Authority Level**, and optional settings as needed.
6. Select **Save**.

## 14.4 Delete an App User

To delete an app user, complete the following steps.

1. Go to **Customers**.
2. Select the customer's name.
3. In **App Users**, find the user's row and select the More icon, then select the Delete icon.
4. A dialog box pops up to confirm your decision. To delete the user, select **Delete**.

# 15 User Codes

Dealer Admin helps you manage user codes on you customers' systems. In this section, you'll learn how to add, edit, and delete user codes.

## 15.1 Default User Codes

**WARNING:** To protect customer security, DMP strongly recommends changing the default user code after installation is complete.

### 15.1.1 XR Series, XT30/XT50, and COM Series Version 194 or Lower

The default user code is **99**.

### 15.1.2 XR Series, XT30/XT50, XT75, and COM Series Version 194 and Higher

Panels ship with a unique 4-digit master code on the serial number label in parentheses next to the serial number. The code can be modified or deleted in panel programming. To revert the default code to 99, use a programming keypad and go to the Initialization menu, then select **Clear All Codes**.


## 15.2 Add a User Code

For more information about user authority levels, refer to Authority Level Reference. For more information about profiles, refer to Profiles.

- Add a Standard User Code
- Add an Ambush User Code

### 15.2.1 Add a Standard User Code

**Note:** If you plan to add an ambush (duress) code to a system, reserve User Code 1 for that code. For more information, refer to Add an Ambush User Code in this section.

To add a user code to a system, complete the following steps:

1. Go to **Customers**.

2. Select the system name.
3. In the sidebar on the left, go to **User Codes**.
4. Select the Add icon.
5. Enter the **User Name**.
6. To use the next available user number on the system, select the **Next Available Number** checkbox. Otherwise, enter a **User Number**.
7. Select the **Credential Type**. For a typical user code that can be used at a keypad or in the Virtual Keypad app, select **Code**. For a physical credential that is used for access control, select **Card**.
8. Depending on the credential type you selected, enter either a code or an external card number.
9. To make the user temporary, select the **Temp User** checkbox and specify a **Start** date and **End** date.
10. To create a single-use user code, select the **Single Use** check box. This code can only be used once and is automatically deleted by the system once it's used.
11. To send the code to all Z-Wave locks installed on the system, select **Send to Locks**.
12. Set the user's authority level:
    - For XT Series Control Panels, edit the user's authority level by selecting **Master**, **Arm Only**, or **Temporary**.
    - For XR Series Control Panels, select profiles for the user.
13. Select the **Apply to Multiple Systems** checkbox to choose multiple systems for this user code to access. Use the search bar to select customers.
14. Select **Send**.

## 15.2.2 Add an Ambush User Code

An ambush code sends a silent duress signal when the user disarms a system with User Code 1. To add an ambush code to a system, complete the following steps:

> ⚠ **Caution:** After creating the code, enable Ambush Reports on each system where you want User Code 1 to function as a duress code. If Ambush Reports are not enabled on a system, User Code 1 functions as a standard code. For more information, refer to the appropriate panel programming guide.

1. Go to **Customers**.
2. Select the system name.
3. In the menu, go to **User Codes**.
4. Select the Add icon.
5. In **User Name**, enter a descriptive name for the ambush code.
6. Deselect the **Next Available Number** checkbox.
7. In **User Number**, enter **1**.
8. For **Credential Type**, select **Code**.
9. In **User Code**, enter a unique code.
10. To create a single-use user code, select the **Single Use** checkbox. This code can only be used once and is automatically deleted by the system once it's used.
11. Select profiles, groups, or authority levels as needed. For a complete list of all the permissions a user can perform, refer to Authority Level Reference and Profiles.
12. Select the **Apply to Multiple Systems** checkbox and choose applicable systems for the ambush code.
13. Select **Send**.
14. In the sidebar on the left, go to **Programming**.
15. Go to **System Reports**.
16. Turn on **Ambush Reports**.
17. Select **Send All Changes**.

## 15.3 Edit a User Code

To edit a user code, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the menu, go to **User Codes**.
4. In the row of the user code that you want to edit, select the Settings icon.
5. Edit the **User Name**, if necessary.
6. Set the user's authority level:
    - For XT Series Control Panels, edit the user's authority level by selecting **Master**, **Arm Only**, or **Temporary**.
    - For XR Series Control Panels, select profiles for the user.
7. Select the **Apply to Multiple Systems** checkbox and choose applicable systems for user code.
8. Select **Send**.

## 15.4 Deactivate a User Code

There may be instances when you want to deactivate a user code rather than delete it. For example, when a card is lost, you can quickly deactivate the user code that has the card assigned to it, which automatically revokes all of the profile and access permissions assigned to that user.

To deactivate a user code, complete the following steps:

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **User Codes**.
4. In the row of the user code that you want to deactivate, select the Settings icon.
5. Click the slider to set the user code from **Active** to **Inactive**.


6. Select **Send**.

## 15.5 Delete a User Code

To delete a user code from a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the menu, go to **User Codes**.
4. In the row of the user code that you want to delete, select the Delete icon.

5. A dialog pops up to confirm your decision. To delete the user code, select **Confirm**.

## 15.6 Authority Level Reference

When creating a user code, you either select an authority level or assign profiles to the user depending on the system type. For more information about profiles, refer to Profiles.

The following sections include definitions of authority level types, the permissions that each level has, and definitions of each permission.



### 15.6.1 Authority Level Types

- **Master**: The highest authority level. The user is granted all system permissions.
- **Standard**: The user is granted all system permissions except administrative permissions.
- **Limited**: The user is granted all system permissions except administrative permissions and they cannot bypass zones.
- **Scheduled**: The user is granted basic system permissions that don't include administrative or maintenance permissions.
- **Arm Only**: The user can only arm the system.
- **Temporary**: The user code expires at the date and time that you specify. Any authority level except Master can be defined as a temporary code.

### 15.6.2 Permissions by Authority Level

| Permission | Master | Standard | Limited | Scheduled | Arm Only |
|---|---|---|---|---|---|
| Arm | X | X | X | X | X |
| Disarm | X | X | X | X | |
| Door Access | X | X | X | X | |
| Alarm Silence | X | X | X | X | |
| User Check-in | X | X | X | X | |
| Zone Activity Check | X | X | X | X | |
| Sensor Reset | X | X | X | X | |
| Display Events | X | X | X | X | |

| Permission | Master | Standard | Limited | Scheduled | Arm Only |
|---|---|---|---|---|---|
| Zone Monitor | X | X | X | X | |
| Output On/Off | X | X | X | | |
| System Test | X | X | X | | |
| Favorites Setup | X | X | X | | |
| Bypass Zones | X | X | | | |
| Z-Wave Setup | X | | | | |
| Wi-Fi Setup | X | | | | |
| User Codes | X | | | | |
| Schedules | X | | | | |
| Extend | X | | | | |
| Set Time | X | | | | |
| Service Request | X | | | | |

## 15.6.3 Permission Definitions

- **Arm**: Arm the system.
- **Disarm**: Disarm the system.
- **Door Access**: Grant temporary door access.
- **Alarm Silence**: Silence a system alarm.
- **User Check-in**: The system checks in to determine if the user is on the premises.
- **Zone Activity Check**: Monitor a zone for non-activity. This could be used for a person living alone to detect when they have not moved about to trip a disarmed zone within a programmed period of time. This feature is optional. The Zone Activity Check is disabled when a schedule is entered to allow for sleeping hours and is automatically enabled when an area is disarmed.
- **Sensor Reset**: Reset all system sensors. A sensor reset is required for all smoke detectors, flood sensors, and temperature sensors that have triggered an alarm, as well as system restoral after a lockdown is ended. A sensor reset is also required to clear a low battery (LOBAT) message after changing a wireless device's batteries.
- **Display Events**: View system events.
- **Zone Monitor**: Enable the chime function.

- **Outputs On/Off**: Turn outputs on or off.
- **System Test**: Initiate a system test from the User Menu.
- **Favorites Setup**: Configure Z-Wave favorites for the system.
- **Bypass Zones**: Bypass zones when arming the system.
- **Z-Wave Setup**: Add, edit, and delete Z-Wave devices like appliances, locks, lights, and thermostats.
- **Wi-Fi Setup**: View the system's Wi-Fi settings, connect to available Wi-Fi networks, and use WPS association.
- **User Codes**: Add, change, or delete user codes.
- **Schedules**: Add, edit, or delete schedules.
- **Extend**: Extend a schedule for 2, 4, 6, or 8 hours.
- **Set Time**: Change the system date and time from the User Menu.
- **Service Request**: Request a service call from your alarm provider.

## 15.7 Bulk Import User Codes

Import User Codes with a Remote Link export file or a CSV template from Dealer Admin. To perform a Bulk User Code Import, complete the following steps.



### 15.7.1 Use a Remote Link Export File

Remote Link Export only works with XR Series Control Panels. To bulk import user codes from any compatible panel model, use the Dealer Admin CSV Template.

1. In Remote Link, open the appropriate panel, then go to **Program > User Codes**.
2. Select **Batch**, then open the **Export** tab.
3. Select the users that you want to export.
4. Select the More button next to **File Name**.
5. Name the file, select **Save**, then select **Export**.
6. In Dealer Admin, go to **Customers** and select the system name.
7. In the menu, go to **User Codes**.
8. Select **CSV Import**.
9. In **Import From**, select **Remote Link User Code Export**.
10. Select the **Upload Remote Link File** button and select Remote Link file that you just exported.

### 15.7.2 Use the Dealer Admin CSV Template

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **User Codes**.
4. Select **CSV Import**, then select **Download CSV Template**.
5. Enter user information in the relevant columns. For more information, refer to CSV Template Field Reference in this section.
6. Save and close the template.
7. On the system **User Codes** page in Dealer Admin, select **CSV Import**.
8. In **Import From**, select **CSV File**.
9. Select the **Upload File** button and select the saved template.

### 15.7.3 CSV Template Field Reference

**Note:** If you enter an **External Number**, the user is imported with a card credential type. Otherwise, the user is imported with a code credential type.

**XT30/XT50, XTL Series, COM Series**

- **Name**—Enter the user's name as you want it displayed.
- **Code**—Enter the user code. If this is a card credential user, this is the card's Internal Number.
- **PIN (optional)**—If the user has Card Plus PIN enabled, enter their PIN.
- **Level**—Enter a level for the user: Master or Standard.
- **External (optional)**—If this is a card credential user, enter their card's External Number. Otherwise, leave this field blank.
- **Areas**—Enter the area numbers that you want the user to access separated by a comma. These numbers cannot exceed the total number of areas in the system.

**XT75 Control Panels**

- **Name**—Enter the user's name as you want it displayed.
- **Code**—Enter the user code. If this is a card credential user, this is the card's Internal Number.
- **PIN (optional)**—If the user has Card Plus PIN enabled, enter their PIN.
- **Groups**—In each column, enter a group **Number** that you want to assign to the user. Otherwise, leave these fields blank.
- **External (optional)**—If this is a card credential user, enter their card's External Number. Otherwise, leave this field blank.
- **Areas**—Enter the area numbers that you want the user to access separated by a comma. These numbers cannot exceed the total number of areas in the system.

**XR Series**

- **Name**—Enter the user's name as you want it displayed.
- **Code**—Enter the user code. If this is a card credential user, this is the card's Internal Number.
- **PIN (optional)**—If the user has Card Plus PIN enabled, enter their PIN.
- **Profiles**—In each column, enter a profile **Number** that you want to assign to the user. Otherwise, leave these fields blank.
- **External (optional)**—If this is a card credential user, enter their card's External Number. Otherwise, leave this field blank.
- **Areas**—Enter the area numbers that you want the user to access separated by a comma. These numbers cannot exceed the total number of areas in the system.

## 15.8 Card Plus PIN

Card Plus PIN requires a user to present their card to a reader and enter their user code at a keypad to access a restricted area.



### 15.8.1 Step 1: Enable Card Plus PIN

These instructions assume that you've already created a profile. To learn more about creating and configuring profiles, refer to Profiles.

1. Go to **Customers**.
2. Select the system name.

3. For XR systems, in the menu, go to **Profiles**.
4. In the row of the profile that you want to edit, select the Settings icon.
5. In **Options**, turn on **Card Plus PIN**.
6. Select **Send Changes to System**.

### 15.8.2 Step 2: Add a PIN to a User

These instructions assume that you've already enabled Card Plus PIN in a profile and created a user code. To learn more about creating and configuring user codes, refer to User Codes.

1. If you need to open the system, go to **Customers** and select the system name.
2. In the menu, go to **User Codes**.
3. In the row of the user that you want to edit, select the Settings icon.
4. For XR systems, in **Select Profiles for this User**, select the profile that has Card Plus PIN enabled.
5. In **Pin**, enter a PIN for the user.
6. Select **Send**.

# 16 Key Fobs

In this section, you'll learn how to add, edit, and delete key fobs from a system.

For quick reference when programming devices, zones, or outputs, see the Quick Programming Reference Guide. For complete information, refer to the appropriate installation and programming guides from DMP.com/resources.

## 16.1 Add a Key Fob

For detailed information about programming key fobs and panic buttons, refer to the appropriate installation and panel programming guides. To add a key fob to a system, complete the following steps.

- Optional: Enable Wireless Encryption and Panic Supervision
- Add a Key Fob

### 16.1.1 Optional: Enable Wireless Encryption and Panic Supervision

Enable **Wireless Encryption** for encrypted key fob models. **Both** allows both encrypted and unencrypted key fob models to operate on the system. **All** requires that all key fobs programmed must be encrypted models.

Enable **Panic Supervision** if you want fobs to have a 30-day supervision that reports transmitter lost or low battery conditions without requiring a **Supervision Time** for the key fob.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Programming**.
4. Expand **System Options**.
5. To enable wireless encryption, go to **1100 Wireless Encryption**, select **Both** or **All**.
6. To enable panic supervision, turn on **Panic Supervision**.
7. When you're done, select **Send System Options**.

### 16.1.2 Add a Key Fob

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Programming**.
4. Expand **Key Fobs**.
5. Select **Add Key Fob**.
6. In **Key Fob Number**, enter a number depending on your system type. Refer to the table following this section.
7. In **Number of Buttons**, select **1**, **2**, or **4**. Default is **4**.
8. In **User Number**, select an existing user.
9. In **Serial Number**, enter the 8-digit key fob serial number. Valid range is 05000000-05999999.
10. If the key fob should be supervised, select a **Supervision Time**. For applications where the key fob may be taken off site, supervision time should be **None**. Default is **None**.
11. Program each button as needed, including the **Action**, **Select Time**, **Output** (panic), **Output Action** (panic), and **Areas**.
12. Select **Send Key Fobs**.

| Panel Model | Key Fob Zone Numbers |
|---|---|
| XR Series Control Panels | 400-449 |
| XT75 Control Panel | 400-449 |
| XT30/XT50 Control Panels | 31-34 (slow)<br>41-44 (fast) |
| XTLplus and XTLtouch | 51-54 (slow)<br>61-64 (fast) |

## 16.2 Edit a Key Fob

To edit a key fob, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Programming**.
4. Expand **Key Fobs** and select a key fob.
5. Edit key fob programming as needed.
6. Select **Send Key Fobs**.

## 16.3 Delete a Key Fob

To delete a key fob from the system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Programming**.
4. Expand **Key Fobs**.
5. Find the key fob that you want to delete and select **Delete**.
6. A dialog pops up to confirm your decision. To delete the key fob, select **OK**.

# 17 Z-Wave

**Note:** You can view lists of Z-Wave Favorites and individual Z-Wave devices associated with your customer's systems. However, Z-Wave devices can only be added and deleted from the Tech APP.

Dealer Admin helps you manage Z-Wave devices on your customers' systems. In this section, you'll learn how to enable or disable Z-Wave device types and how to view system automation.

## 17.1 Enable Z-Wave Devices

To enable a Z-Wave device type for a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. At the top of **System Information**, select **Edit**.
4. In **Additional Features**, select **Automation (Lights, Locks, Thermostats, & Appliances)**.
5. In **Allow Editing**, select **Enabled** or **Disabled**.
6. Select **Save**.

## 17.2 Disable a Z-Wave Device Type

To disable a Z-Wave device type for a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. At the top of **System Information**, select **Edit**.
4. In **Additional Features**, clear **Automation (Lights, Locks, Thermostats, & Appliances)**.
5. Select **Save**.

## 17.3 View Automation

To view all of the favorites and Z-Wave devices on a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Automation**.
4. To update Z-Wave device information, select **Retrieve from System** at the top of the page.

# 18 Schedules

**Note:** Some of the options available to you, as well as the look of the **Schedules** interface, may change depending on the system type. Additionally, schedules can only be applied to systems of the same series.

Dealer Admin helps you configure and manage schedules on your customers' systems. In this section, you'll learn how to add, edit, and delete a schedule. You'll also learn how to configure area settings.

## 18.1 Add a System Schedule

To add a schedule to a system, complete the following steps.



### 18.1.1 Prerequisites

- **Schedule Management** must be enabled in **System Information**
- For areas to be included in Arming (permanent) schedules, **Automatic Arming** and **Automatic Disarming** must be turned on for areas in **Programming > Area Information**
- To create output schedules, an output must be programmed first in **Programming > Output Information**
- To create favorite schedules, a favorite must be programmed in Virtual Keypad.
- To create door lock/unlock schedules, doors must be enabled in **System Information**, programmed in **Programming > Device Setup**, and added to **System Information > Door Control**. For complete instructions, refer to Access Control Doors.
- If you want to use Sunrise and Sunset times, ensure a **Weather Zip Code** is programmed in **Programming > System Options**

### 18.1.2 XR Series and XT75 Control Panels

1. Go to **Customers**.
2. Select the system name.
3. In the menu, go to **Schedules**.
4. Select the Add icon.
5. Enter a schedule name and number.
6. In **Times**, enter the begin and end times for the schedule in the appropriate day slots in either 24-hour or 12-hour format. For 12-hour format, enter the time with either **AM** or **PM**.
7. To add multiple opening and closing times for the schedule, select **+** under the desired day. You can create up to 8 opening and closing times per day.
8. To set specific times for holiday schedules, enter them in the holiday slots (**Hol A**, **Hol B**, or **Hol C**).

**Note:** Holiday schedules can only be created from VirtualKeypad.com or the panel User Menu. To create a holiday schedule, finish configuration in Dealer Admin, then Log In as a Customer.

1. Choose **Areas**, **Outputs**, **Favorites**, and **Doors** for the schedule, if applicable.

2. In **Copy to Systems**, select the schedule types to send to the system.
3. Select systems to be affected by the schedule.
4. Select **Send Changes to System**.

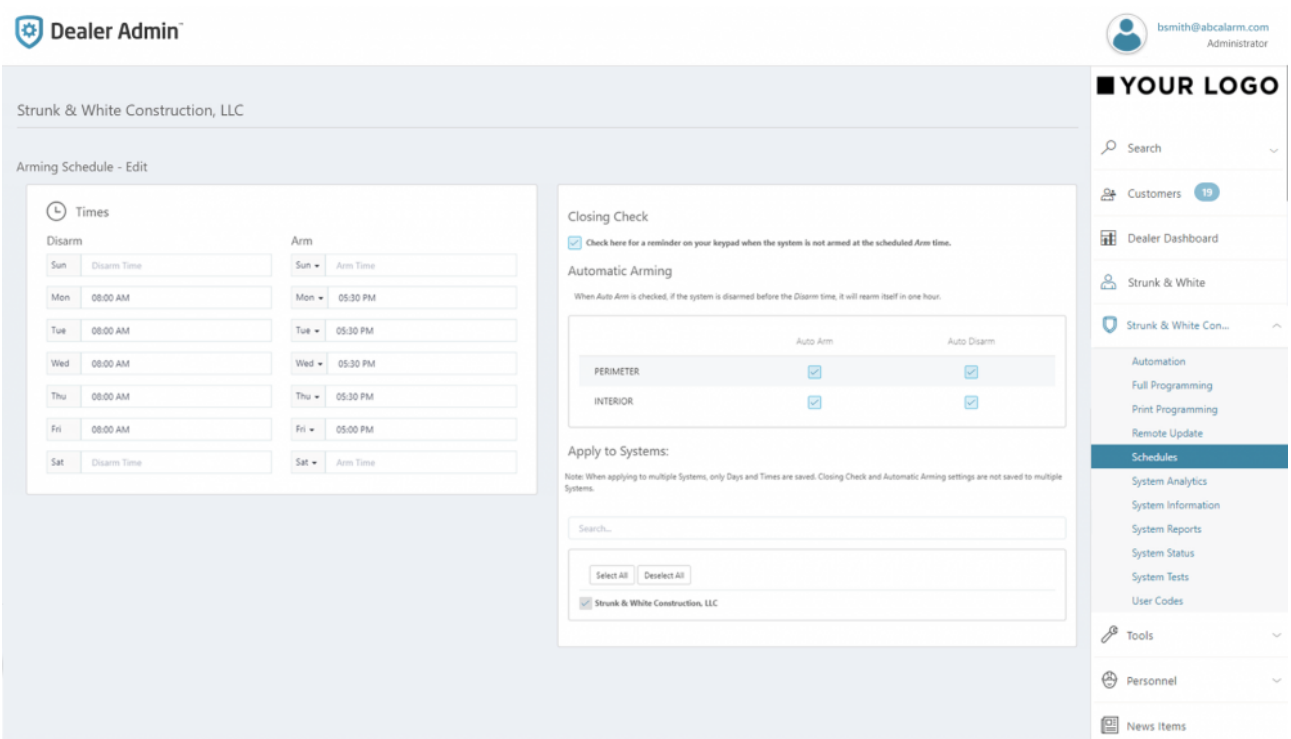
## 18.1.3 XT30/XT50 Control Panels

### Create an Arming (Permanent) Schedule

You can create one arming schedule per XT30/XT50 system. To create a permanent schedule for an XT30/XT50 panel, complete the following steps:

1. Go to **Customers**.
2. Select the system name.
3. In the menu, go to **Schedules**.
4. In the row of the **Arming Schedule**, select the Edit icon.
5. Enter days and times for the system to automatically disarm and arm.
6. If you want the keypad to annunciate a reminder when the system is not armed at the schedules time, turn on **Closing Check**.
7. Select the areas that you want to include in **Automatic Arming**.
8. In **Copy to Systems**, select the schedule types to send to the system.
9. Select systems to be affected by the schedule.
10. Select **Send Changes to System**.

**Example:** Program the system to disarm automatically at 8:00 AM and arm at 5:30 PM Monday – Thursday.

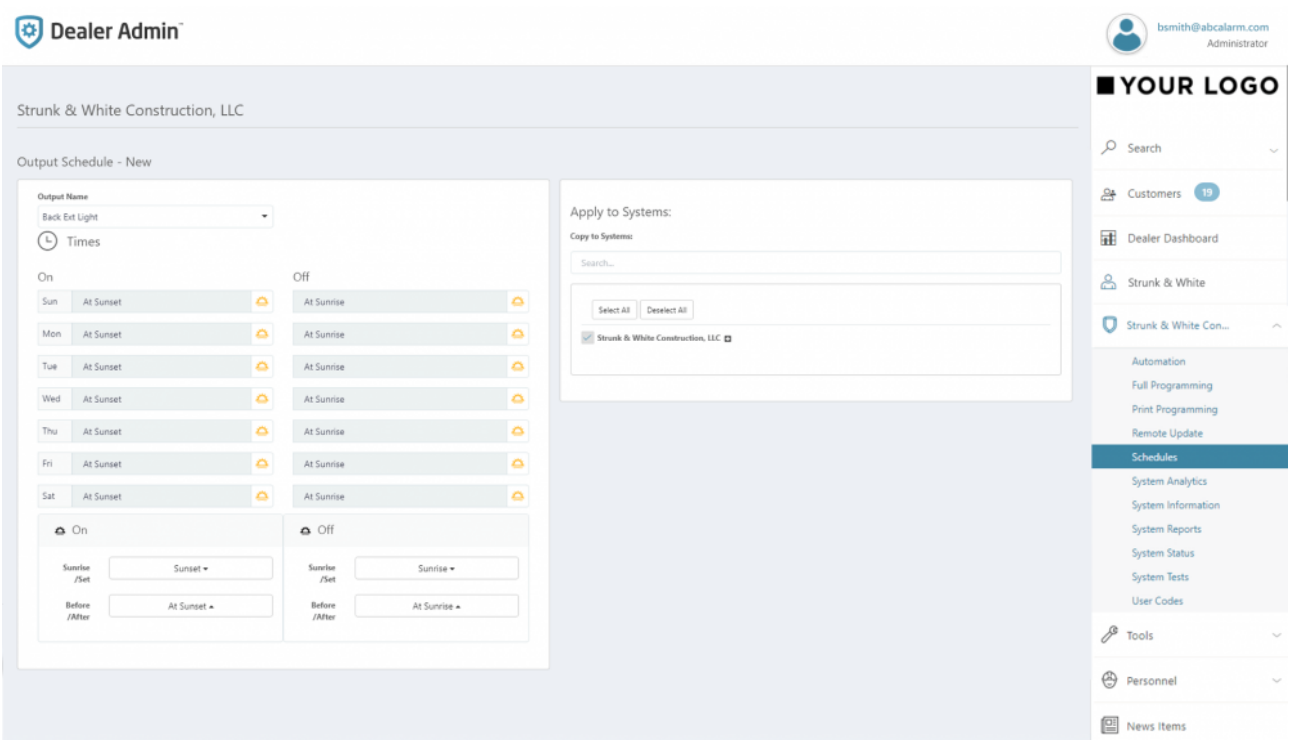


### Create an Output or Favorite Schedule

You can create up to 4 output schedules and 20 favorite schedules per XT Series system. To create an output or favorite schedule for an XT30/XT50 Panel, complete the following steps:

1. Go to **Customers**.
2. Select the system name.
3. In the menu, go to **Schedules**.
4. Select **Add Schedule**, then select the type of schedule that you want to create.
5. Select the output that you want to turn on, turn off, or activate with the schedule.
6. Enter days and times for the output to turn on or off.
7. In **Copy to Systems**, select the schedule types to send to the system.
8. Select systems to be affected by the schedule.
9. Select **Send Changes to System**.

**Example:** Program a schedule so a light turns on automatically at sunset and off at sunrise.




## 18.2 Edit a Schedule

To edit a system schedule, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar on the left, go to **Schedules**.
4. In the row of the schedule that you want to edit, select the Settings icon.
5. Edit the schedule's information, such as the **Schedule Name**, **Times**, and additional options as needed.
6. Select systems to be affected by the schedule.
7. Select **Send Changes to System**.

## 18.3 Delete a Schedule

**Note:** You can delete schedules from an XTLplus, XTLtouch, or XR Series system in Dealer Admin.

To delete system schedules, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the menu, go to **Schedules**.
4. In the row of the schedule that you want to delete, select the Delete icon.
5. A dialog box pops up to confirm your decision. To delete the schedule, select **Confirm**.

## 18.4 Configure Area Settings

You can enable auto arming and disarming as well as closing checks for schedules on a system from Dealer Admin. These settings apply to every schedule on the system. To configure area settings, complete the following steps:

1. Go to **Customers**.
2. Select the system name.
3. In sidebar on the left, go to **Schedules**.
4. Select **Area Settings**.
5. If you want a reminder when the system is not armed on time, select **Closing Check**.
6. In, Automatic Arming, select **Auto Arm** or **Auto Disarm** to enable auto arming or disarming for specific areas.
7. Select **Send Changes To System**.

# 19 Profiles

**Note:** Profiles are only applicable to XR150/XR550 Series systems.

Dealer Admin helps you manage user profiles on XR150/XR550 Series systems. The profiles assigned to a user determine their permissions and access areas within a system. In this section, you'll learn how to view, add, edit, and delete profiles.

## 19.1 View Profiles

To view a list of system profiles, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the menu, go to **Profiles**.

The system's profiles page opens with a list of all the profiles that are set up on the system. From this page, you have the option to **Edit**, **Delete**, or **Add** a profile. You can also search for existing profiles.

If you make changes to a system's profiles and they don't automatically show on the **System Profiles** page, try refreshing the profiles by selecting **Refresh**.

## 19.2 Add a Profile

To add a profile to a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Profiles**.
4. Select the Add icon.
5. Enter profile information as needed, such as **Profile Name**, **Rearm Delay**, **Output Group**, **Access Areas**, and additional options. For more information, refer to Profiles Reference.
6. Select **Send Changes to System**.

## 19.3 Edit a Profile

To edit a profile, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Profiles**.
4. In the row of the profile that you want to edit, select the Settings icon.
5. Edit the profile information as needed, such as the **Profile Name**, **Rearm Delay**, **Output Group**, **Access Areas**, and additional options. For more information, refer to Profiles Reference.
6. Select **Send Changes to System**.

### 19.3.1 Configure Profile Options

1. In the sidebar, go to **Profiles**.
2. In the row of the profile that you want to edit, select the Settings icon. Otherwise, create a new profile.
3. In **Access Areas**, select the areas that you want profile users to have the ability to access.
4. If necessary, go to **Private Doors** and select the doors that you want profile users to access.

5. In **Options**, select the access control options that you want profile users to have. For more information, refer to Profiles Reference.
6. Select **Send Changes to System**.

## 19.4 Delete a Profile

To delete a profile, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Profiles**.
4. In the row of the profile that you want to delete, select the Delete icon.
5. A dialog pops up to confirm your decision. To delete the profile, select **Confirm**.

## 19.5 Profiles Reference

Refer to the following reference information when configuring profiles.

- Profile
- Options

### 19.5.1 Profile

- **Number**: The id number automatically assigned to the profile.
- **Rearm Delay**: Delay automatic rearming by the number of minutes entered when the user disarms an area outside of a schedule. To disable this feature, enter **0**. Range is 0 – 720 minutes.
- **Output Group**: Assign outputs to groups, allowing an entire group of outputs to turn on or off as required. Enter the number of the output group that you want to assign to the profile. To disable this feature, enter **0**.
- **Inactive User Audit Days**: Enter a number of days that a user code can remain unused before it is automatically deactivated. To disable this feature, enter **0**. Range is 0 – 425 days.
- **Access Areas**: Allow profile members to access selected areas. This setting supersedes **Door Access** settings in **Options**.
- **Arm/Disarm Areas**: Allow profile members to arm or disarm selected areas. This setting supersedes **Arm** and **Disarm** settings in **Options**.
- **Access Schedules**: Allow profile members to access and edit a schedule. This setting supersedes **Schedules** settings in **Options**.
- **Private Doors**: Allow profile members to access selected private doors. Only doors that have **Private Door** turned on in **Device Setup** are displayed in **Profiles**. When enabled, these permissions allow profile members to access up to 4 private doors.

### 19.5.2 Options

When enabled in a profile, these permissions allow profile members to perform the following actions:

- **Arm**: Arm the system according to the options configured in **Arm/Disarm Areas**.
- **Disarm**: Disarm the system according to the options configured in **Arm/Disarm Areas**.
- **Alarm Silence**: Silence a system alarm.
- **Sensor Reset**: Reset all system sensors. A sensor reset is required for all smoke detectors, flood sensors, and temperature sensors that have triggered an alarm, as well as system restoral after a lockdown is ended. A sensor reset is also required to clear a low battery (LOBAT) message after changing a wireless device's batteries.
- **Lockdown**: Initiate a lockdown.

- **Door Lock/Unlock**: Lock and unlock doors.
- **Door Access**: Grant temporary door access.
- **Armed Areas**: View armed areas at a keypad.
- **Outputs On/Off**: Turn outputs on or off from the User Menu.
- **Anti-Passback**: Use anti-passback. Profile members are required to properly exit (egress) an area previously accessed. Users cannot re-access the area until they properly exit it. **Egress Areas** are configured in **Device Setup**.
- **Easy Arm/Disarm**: Arm or disarm all areas that are assigned to a code automatically.
- **Use Secondary Language**: Display a secondary language.
- **Card Plus PIN**: Use Card Plus Pin. Profile members are required to use two access methods to operate the system from a keypad. The first method must be a credential such as a proximity patch, card, or key fob. The second method must be a PIN number entered at the keypad.
- **Wi-Fi Setup**: View the system's Wi-Fi settings, connect to available Wi-Fi networks, and use WPS association.
- **Lockdown Override**: End a lockdown and restore the system. **Sensor Reset** is also required to override a lockdown.
- **Profiles**: Add, change, or delete profiles.
- **User Codes**: Add, change, or delete user codes.
- **Schedules**: Add, edit, or delete schedules.
- **Extend**: Extend a schedule for 2, 4, 6, or 8 hours.
- **Time**: Change the system date and time from the User Menu.
- **Display Events**: View system events.
- **Service Request**: Request a service call from your alarm provider.
- **Fire Drill**: Initiate a fire drill.
- **Zone Status**: View the status of zones.
- **Bypass Zones**: Bypass zones when arming the system.
- **Zone Monitor**: Enable the chime function.
- **System Status**: View the system's status.
- **System Test**: Initiate a system test from the User Menu.
- **Technician User**: Use the profile for test purposes. A technician user cannot disarm a system that has been armed by a standard user. If the system is armed by a Test User, that person can disarm it.
- **Dual Authority**: Requires two user codes to be entered within 30 seconds of each other at a system keypad to arm or disarm a specific area. Dual Authority must be enabled in Area Information to use this feature.

# 20 Groups

Dealer Admin helps you manage user groups on XT75 systems. The groups assigned to a user determine their permissions and access areas within a system. In this section, you'll learn how to view, add, edit, and delete groups.

## 20.1 View Groups

To view a list of system groups, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Groups**.

The system's groups page opens with a list of all the groups that are set up on the system. From this page, you have the option to **Edit**, **Delete**, or **Add** a group. You can also search for existing groups.

If you make changes to a system's groups and they don't automatically show on the **System Groups** page, try refreshing the groups by selecting **Refresh**.

## 20.2 Add a Group

To add a profile to a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Groups**.
4. Select the Add icon.
5. Enter group information as needed. For more information, refer to Groups Reference.
6. Select **Send Changes to System**.

## 20.3 Edit a Group

To edit a group, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Groups**.
4. In the row of the group that you want to edit, select the Settings icon.
5. Edit the group information as needed. For more information, refer to Groups Reference.
6. Select **Send Changes to System**.

### 20.3.1 Configure Group Options

1. In the sidebar, go to **Groups**.
2. In the row of the group that you want to edit, select the Settings icon. Otherwise, create a new group.
3. In **Access Areas**, select the areas that you want group users to have the ability to access.
4. If necessary, go to **Private Doors** and select the doors that you want group users to access.
5. In **Options**, select the access control options that you want group users to have. For more information, refer to Groups Reference.
6. Select **Send Changes to System**.

## 20.4 Delete a Group

To delete a group, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **Groups**.
4. In the row of the group that you want to delete, select the Delete icon.
5. A dialog pops up to confirm your decision. To delete the group, select **Confirm**.

## 20.5 Groups Reference

Refer to the following reference information when configuring groups.



### 20.5.1 Group

- **Number**: The id number automatically assigned to the group.
- **Name**: The name given to the group.
- **Doors**: Allow group members to access selected doors. When enabled, these permissions allow group members to access up to 8 doors.
- **Areas**: Allow group members to access selected areas. This setting supersedes **Door Access** settings in **Options**.
- **Access Schedules**: Allow group members to access and edit a schedule. This setting supersedes **Schedules** settings in **Options**.

### 20.5.2 Options

When enabled in a group, these permissions allow group members to perform the following actions for XT75 systems:

- **Arm Authority**: Arm the system according to the options configured in **Arm/Disarm Areas**.
- **Disarm Authority**: Disarm the system according to the options configured in **Arm/Disarm Areas**.
- **Swipe Twice to Arm**: Allow group members to swipe twice at any door in this group to arm the alarm panel.
- **Lockdown**: Initiate a lockdown.
- **User Programming**: Allow group members to edit groups, assign users, and assign groups to users.
- **Audit Days**: Enter a number of days that a user code can remain unused before it is automatically deactivated. Range is 0-425 days.

# 21 X1 Series

The X1 Series is a line of cloud-based access controllers programmed entirely in Dealer Admin and managed in Virtual Keypad. This guide explains how to program X1 Series devices after hardware installation is complete. For more information about installing and configuring communication for an X1 Series Door Controller, refer to the following literature:

- X1 Door Controller Installation and Programming Guide
- X1-8 Door Controller Installation and Programming Guide
- X1 Elevator Controller Installation and Programming Guide
- X1 Output Expansion Module Installation and Programming Guide

Before you get started, here are some basics about the X1 Series:

- A **system** can have one or more door controllers
- A **door controller** or **elevator controller** processes access logic when given instructions from card readers or Virtual Keypad
- A **door** is a physically secured point of access managed with door controllers, hardware accessories, card readers, and Virtual Keypad
- A **floor** is a point of access managed by card readers through Virtual Keypad
- The **X1** is a cloud-based door controller with a total of 1 door (integrated)
- The **X1-8** is a cloud-based door controller with a total of 8 doors (1 integrated and 7 modular)
- The **X1-ELEV** is a cloud-based elevator controller with a total of 90 floors (10 integrated and 80 added through the X1-ELEV-EXP and X1-ELEV-PCB)
- The **X1-OUT-EXP** is an accessory to the X1 or X1-8 allowing for a total of 90 additional outputs (10 outputs per module, 9 additional modules per X1 or X1-8)

## 21.1 Add an X1 Door Controller

A customer must exist before you can add a system to their account. To learn about creating customers, refer to Add a Customer.

1. Go to **Customers**.
2. Select the customer's name.
3. In **Systems**, select the Add icon.
4. Enter a name for the system.
5. In **System Type**, select **X1**.
6. Configure billing address and time options as needed.
7. Enter the door controller's serial number.
8. Select **Save**.

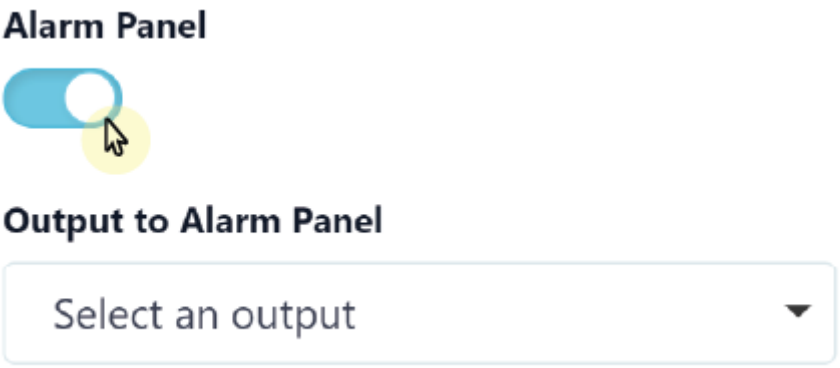
### 21.1.1 Configure an X1 Door Controller

**Note:** OSDP readers must be either new or factory reset so they can bind properly with the system. A unique OSDP secure key is automatically programmed.

If door options don't open automatically, select the X1 that you want to configure.

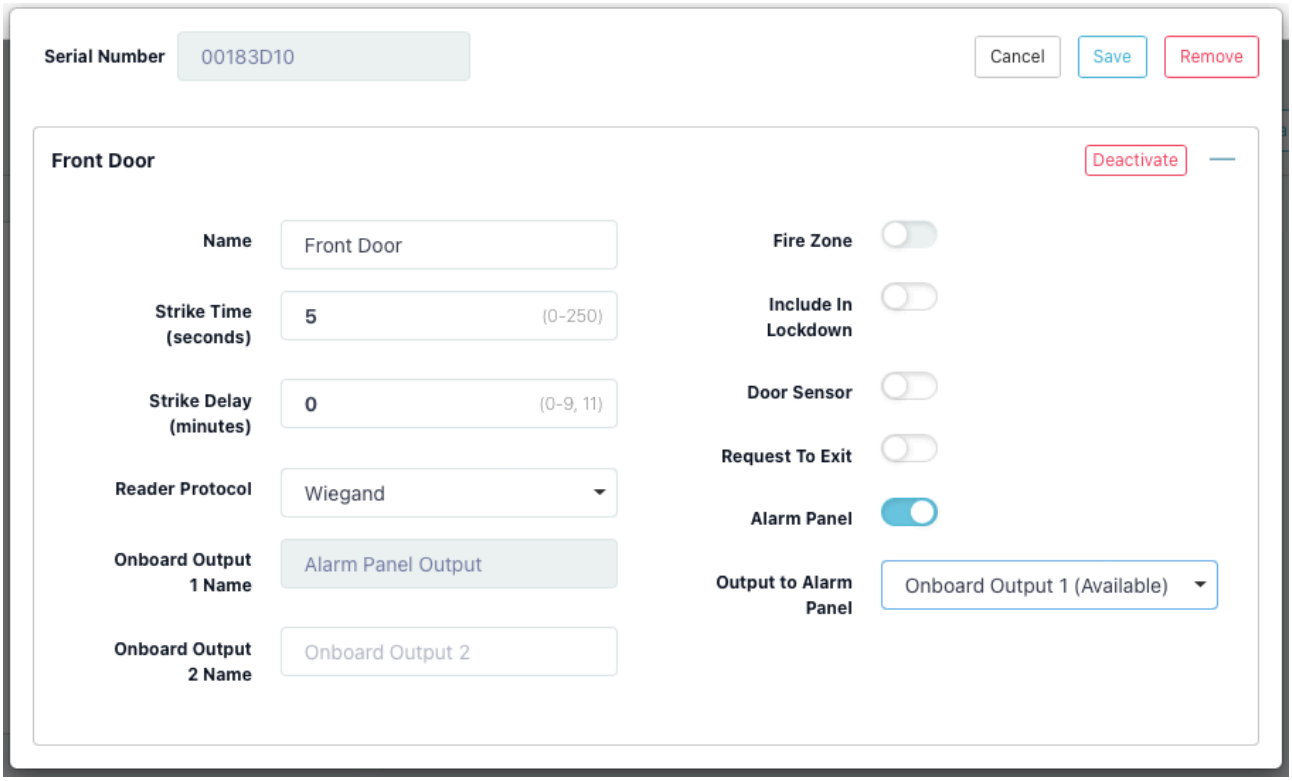
1. Enter a descriptive name for the door.
2. In **Strike Time**, enter the number of seconds that you want the door to unlock when access is granted.
3. In **Strike Delay**, enter the number of minutes that you want to delay the door unlock when access is granted.

4. In **Reader Protocol**, choose a protocol for this door's readers: **Wiegand** or **OSDP**. For OSDP readers, configure buzzer and LED options.
5. In **Authorization**, choose which authorization type can be used to access any of the doors.
6. Turn on other options as needed. For details about each option, refer to Available Door Options.
7. When setting up the controller to be associated with an alarm panel, toggle on **Alarm Panel**. This displays a drop-down menu to select an available output.




**Note:** The **Alarm Panel** option can only be used with a network connected X1 Door Controller.

8. The selected output will be wired to an available zone on the connected alarm panel. The zone must be programmed as an **Arming** or **Keyswitch** zone type. Wire an available output from the connected alarm panel to the Custom input of the X1 controller. The output of the connected alarm panel should be programmed as an armed output.




**13 Output to Alarm Panel**

9. Select **Save**.

### Available Door Options

- **Buzzer** (OSDP) allows the reader to beep when a card is read.
- **LED** (OSDP) allows the reader LED to turn on and operate the same as a Wiegand reader LED, lighting green when the module relay activates. If disabled, the reader LED is turned off and does not operate in any condition.
- **Card** (Authorization) enables the use of cards for any of the doors.
- **Fire Zone** indicates this custom output triggers with a fire alarm.
- **Fire Exit** allows the door to unlock during a fire so people can exit the area.
- **Include in Lockdown** allow this door to be included when a lockdown is initiated.
- **Door Sensor** allows a motion detector mounted near the door to trigger a request to exit.
- In **Prop Time**, enter the number of seconds that you want to allow the door to remain open without triggering an alert.
- **Door Forced Message** sends a status message any time a door is forced open.
- **Request to Exit** (REX) requires people to request exit. REX is usually triggered by motion near the door or a button press.
- **Unlock on REX** appears when the Request To Exit toggle is switched on. Default is switched on. To allow the door to unlock when a Request to Exit input is received, enable the toggle. This is typically for magnetic locks. To allow the door to remain locked when a Request to Exit input is received, disable the toggle. This is typically for door strikes.

## 21.2 Add an X1 Elevator Controller

To add an X1 Series Elevator Controller, complete the following steps.

1. Go to **System Information**.
2. Under **Elevators**, select the Add icon.
3. Enter the serial number of the elevator controller.
4. Enter a descriptive name for the elevator controller.
5. In **Floor Activation Time**, enter the number of seconds that the elevator module relays remain active after access granted. This is provided by the elevator service company and varies by manufacturer.
6. In **Reader Protocol**, choose a protocol for this door's readers: **Wiegand** or **OSDP**. For OSDP readers, configure buzzer and LED options.
7. If using the onboard outputs, enter descriptive names in **Onboard Output 1 Name* and Onboard Output 2 Name***. If not using the onboard outputs, leave the name fields blank.
8. Turn on other options as needed. For details about each option, refer to Available Elevator Options.
9. When the first elevator module populates, enter the name and address of the module. The address is the number that the address rotary dial is set to.
10. Name up to 10 floor relays. If additional elevator control modules are being used, skip to step 1 of Add Additional Floors.
11. Select **Save**.

### 21.2.1 Available Elevator Options

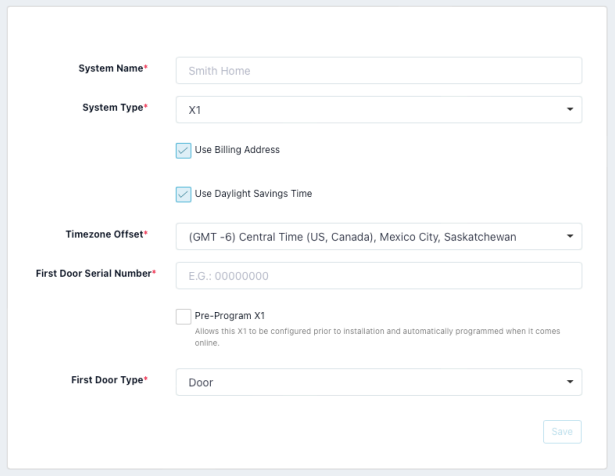
- **Buzzer** (OSDP) allows the reader to beep when a card is read.
- **LED** (OSDP) allows the reader LED to turn on and operate the same as a Wiegand reader LED, lighting green when the module relay activates. If disabled, the reader LED is turned off and does not operate in any condition.
- **Include in Lockdown** allow this elevator to be included when a lockdown is initiated.
- **Request to Exit** (REX) not typically used for elevator access.

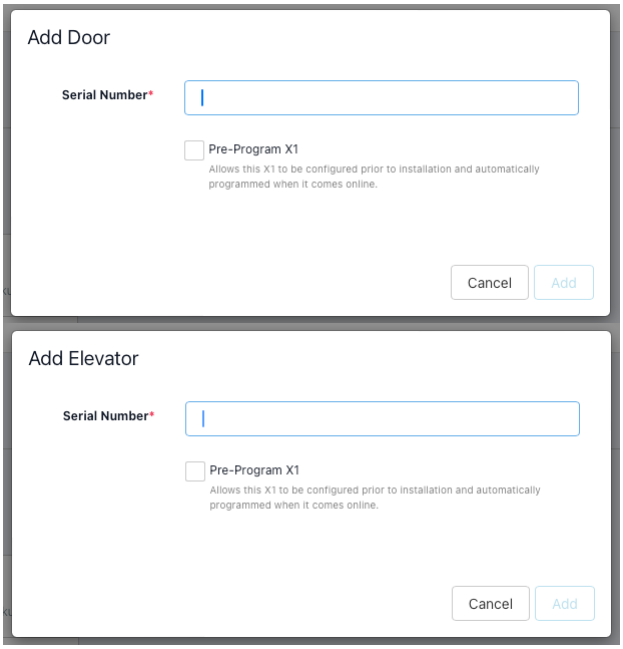
### 21.2.2 Add Additional Floors

1. If additional elevator modules are being used, follow the steps below. Otherwise skip this section.
2. Under **Floors**, select the Add icon.
3. Enter the name and address of the Elevator Module. Unnamed relays will not be programmed.
4. Name up to 10 floor relays.
5. Select **Save**.

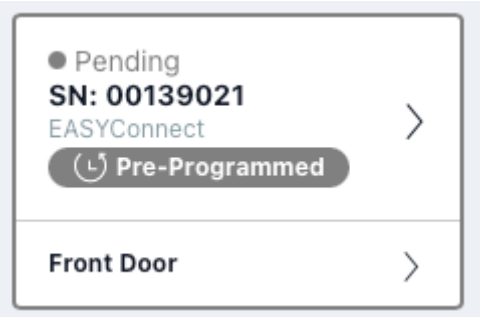
## 21.3 X1 Pre-Programming

1. Add an X1 door or elevator to a new or existing site.
2. In the programming pop-up, click the **Pre-Program X1** checkbox.




3. Add a **Serial Number**, **First Door Type** and **Connection Type** before saving. This will ensure the pre-programming gets sent down to the X1 properly once it comes online.
4. After saving, the pre-programming will appear on the **Site Information** and **Diagnostics** page with a gray highlight around the box and the status as **Pending**.




5. Once the X1 comes online, the programming will automatically be sent down to the X1.

## 21.4 Update an X1 Controller

### 21.4.1 Automatically Update

X1 Controllers automatically update 8 hours after being powered up or 8 hours after the latest firmware is available.

### 21.4.2 Manually Update

If a newly added or an already existing controller needs to be updated sooner than the 8-hour automatic update, an “Update Available” notification appears in System Information. Select **Yes** to update.

## 21.5 Add an X1 Output Expansion Module

Make sure to keep track of the address number that Dealer Admin provides. This is the number that the address rotary is set to.

1. Go to **System Information**.
2. Under **Outputs**, select the Add icon.
3. Select the X1 that the module is connected to.
4. For **Output Name**, use a descriptive name for the output expansion module’s location,
5. For each **Relay**, name each output that you intend to use. Unnamed outputs will not be programmed.
6. Select **Save**.

## 21.6 Add Card Formats

To add card formats to an X1, complete the following steps.

1. In **Card Formats**, select the Add icon.
2. Give the card format a name.
3. Select a card format and configure format settings. For details about each option, refer to Card Format Options.
4. Select **Save**.

### 21.6.1 Card Format Options

- **DMP** (card format) use cards with DMP’s format with a 26 – 45 bit data string.
- **Custom** (card format) use cards with a custom bit length and configuration.
- **Any** (card format) unlock the door with any valid card read.
- **Wiegand Length** is the total number of bits to be received in Wiegand code including parity bits.
- **Site Code Position** is the site code start position in the data string.
- **Site Code Length** is the site code length.
- **User Code Position** defines the user code start bit position.
- **User Code Length** defines the credential user code length.
- **User Code Digits** defines the user code length.
- **Require Site Code** restricts the door so it only unlocks when the card’s site code matches one programmed in **Site Code**.

## 21.7 Enable Video Services

Choose the cameras, NVRs, and third-party video services you want to add to the system.

1. In **Video Services**, select the Add icon.
2. Select the types of cameras or NVRs that you want to enable on the system.
3. Select any third-party applications that you want to enable on the system. This allows users to sign in to their services from Virtual Keypad.
4. Select **Save**.
5. Back on the **System Information** page, select the number of cameras or choose the number of doorbells that you want to add to the system.

## 21.8 Add a Virtual Keypad App User

Adding an app user to an X1 system automatically adds them as a user in Virtual Keypad.

1. Go to **Customers**.
2. Select the customer's name.
3. In the **App Users** section, select the Add icon.
4. For a user that doesn't have a Virtual Keypad account, select **New**. For a user that already has an account, select **Existing**.
5. For a new user, enter their email address. For an existing user, start typing to search for their email and select it from the list.
6. Set the user's authority level to either **Administrator** to manage multiple systems or **Standard** to manage a single system.
7. For a new user, enter their first and last name. If you don't want to generate a random password for the user, clear **Create Random Password** then manually enter one.
8. If you want to email the user video clips, select **Email Video Clips**.
9. Select systems and permissions for the user.
10. Select **Save**.

**Note:** If you receive a message that says the email is already in use, the user already has a Virtual Keypad account. Select **Existing** below the user's email address.

### 21.8.1 Log In as a Customer

To log in to Virtual Keypad and view the system like a customer would, select **Log In as Customer**. This adds you to the system as a temporary app user with admin privileges without the capability to view video. Your temporary app user expires and is automatically removed from the system after 1 hour.

For more information, refer to Virtual Keypad Help.

# 22 Video

In this section, you'll learn how to add, edit, or delete cameras and NVRs/Converters. You'll also learn how to use the XV Gateway with AlarmVision®, enable video doorbells on a system, and use third-party integrations.

## 22.1 Enable Video Devices

To enable video devices on a system, complete the following steps.

- Enable Cameras and NVRs
- Enable Video Doorbells

### 22.1.1 Enable Cameras and NVRs

**Note:** Video Verification must be enabled in **Settings** before enabling it for specific cameras or NVRs. For more information, refer to Set Up Video Verification.

1. Go to **Customers**.
2. Select the system name.
3. At the top of **System Information**, select **Edit**.
4. In **Video**, select the types of cameras or NVRs that you want to enable on the system.
5. If you want to enable Video Verification for your cameras or NVRs, select **Video Verification**.
6. Select **Save**.

### 22.1.2 Enable Video Doorbells

**Note:** Video doorbells must be enabled in Dealer Admin before they can be added to a system from Virtual Keypad. For more information about adding video doorbells to a system, refer to Virtual Keypad App Help.

1. Go to **Customers**.
2. Select the system name.
3. At the top of **System Information**, select **Edit**.
4. In **Video**, select doorbell. Choose the number of doorbells to include.
5. Select **Save**.

### 22.1.3 Add a Camera

**Note:** Video must be enabled on a system to add, edit, or delete cameras. For more information, refer to Enable Video Devices.

To add a camera to a system, complete the following steps. To add a camera to an NVR, follow the steps in Add a Camera to an NVR.

1. Go to **Customers**.
2. Select the system name.
3. In **Video**, select the Add Camera icon and enter the 12-digit MAC Address located on the back of the camera. Select **Next**.
4. Enter a name for the camera.
5. Select the camera's time zone. If necessary, select **Observe Daylight Savings Time**.

6. If the video needs to be flipped because the camera is mounted upside down, toggle **Flip Image**.
7. To allow this camera to be viewed on a keypad, toggle **Visible on Keypad**.
    - **Note:** Cameras are only visible on 7-Inch Touchscreen Keypads.
8. To allow this camera to record motion triggered video clips, select **Clips**.
    - If you only want this camera to offer a live camera view through the Virtual Keypad app, choose **Never Record Motion**.
    - If you want this camera to record video clips any time it detects motion, choose **Always Record on Motion**.
    - If you want the camera to record motion triggered clips only when the system is armed, choose **Record Motion When Armed**.
9. To record video clips continuously during the first minute after the system triggers an alarm, select **Record on Alarm**.
10. Select **Save**.

### Enable Email Clips

1. Go to **Customers**.
2. Select the customer's name.
3. In **App Users**, find the user's row and select the More icon, then select the Edit icon.
4. In **Video**, select **Email Video Clips**.
5. Select **Save**.

### Prevent End Users from Editing Camera Settings

The **Allow End User Settings** option enables you to individually restrict which cameras' settings can be edited by users in Virtual Keypad. These camera settings include **Name**, **Record on motion**, **Record on alarm**, **Flip image**, and **Motion detection regions**.

By default, end users are allowed to edit settings for each camera. To remove these options, turn off **Allow End User Settings**.

## 22.1.4 Edit a Video Device

**Note:** Video must be enabled on a system to add, edit, or delete cameras and NVRs/Converters. For more information, refer to Enable Video Devices.

To edit a video device, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In **Video**, select the name of the video device that you want to edit.
4. Click **Edit**.
5. Edit the device information as needed.
6. Click **Camera Details** to view additional information for the camera, including:
    - Name
    - MAC Address
    - Serial Number
    - Time Settings
    - Last Check-In
    - Wi-Fi Signal Strength
    - Firmware Version
    - Username & Password
    - SD Card Status (V-6000 only)

7. Click **Save**.

### 22.1.5 Delete a Video Device

> **Note:** Video must be enabled on a system to add, edit, or delete cameras and NVRs/Converters. For more information, refer to Enable Video Devices.

To delete a video device, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In **Video**, select the name of the video device that you want to delete.
4. Select **Delete**.
5. A dialog pops up to confirm your decision. To delete the video device, select **OK**.

## 22.2 NVRs and Analog Converters

In this section, you'll learn how to add NVRs and analog converters. You'll also learn how to add a camera to an NVR.

### 22.2.1 Add an NVR/Converter

> **Note:** Video must be enabled on a system before you can add an NVR or analog converter. For more information, refer to Enable Video Devices.

To add an NVR or analog converter to a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In **Video**, select the Add NVR/Converter icon.
4. Enter or scan the **Serial Number** found on the NVR label.
5. Select **Next**. When the NVR has successfully connected, the **NVR Serial Number** is assigned.
6. Select the **Time Zone**. If necessary, enable **Observe Daylight Savings Time**.
7. To create a local user account, enable **Local User**, then create an **NVR Username** and **Password**.
8. Select **Save**.

### 22.2.2 Add a Camera to an NVR

To connect over PoE/Network, connect one end of the network cable to one of the eight provided ports on the back of the NVR. Up to eight cameras can be connected using PoE. The NVR will automatically add any 4000 Series SecureCom camera that is connected to one of the eight PoE ports. When using PoE, no power cable is needed.

- Camera Configuration
  - V-4061DB Admin Verification
  - V-4060DB Admin Verification
  - 5000 Series Default Passwords
  - Default User Names and Passwords
- 4000 Series: Connect a Camera Directly to the NVR
- 5000 Series: Connect a Camera Directly to the NVR
  - Set Up a Static IP
  - Add the Camera to the NVR

- Connect a Camera over Network to the NVR
- Add an ONVIF Camera in Dealer Admin

For more information about connecting specific cameras to the SecureCom NVR, refer to the appropriate Video Installation Guide.

**Note:** Cameras that are connected to an NVR must be assigned a static IP address or have a DHCP reservation configured. When managing 5000 Series cameras with both the V-4408D NVR and Dealer Admin, cameras must be connected to the NVR through a switch.

## Camera Configuration

Refer to the following information for the configuration details of specific camera models.

### V-4061DB Admin Verification

For the V-4061DB Doorbell, the password is the verification code that is on the doorbell's label found under the cover below the serial number.

### V-4060DB Admin Verification

For the V-4060DB Doorbell, the password is a combination of the word "admin" followed by the verification code that is on the doorbell's label found under the cover below the serial number. As an example, if the verification code is **ILGWQM** then the password would be **adminILGWQM**.

### 5000 Series Default Passwords

For V-5012B or V-5052D cameras with lower than D3.2.1_20200818_DMP firmware and V-5014B or V-5054D cameras with lower than D4.2.1_20200818_DMP firmware, the default password is **scw12345user**.

For V-5012B and V-5052D cameras with firmware Version D3.2.1_20200818_DMP and higher or V-5014B and V-5054D cameras with firmware Version D4.2.1_20200818_DMP and higher, the default password is **scw** plus the last six *alphanumeric* characters in the camera's MAC address. As an example, if the MAC address **1A:2B:3C:4D:5E:6F**, the default password is **scw4D5E6F**.

### Default User Names and Passwords

| Model | Management Port | Protocol | Username | Password |
|---|---|---|---|---|
| V-4022C | 8000 | Hikvision | **admin** | blank |
| V-4052D | 8000 | Hikvision | **admin** | blank |
| V-4061DB | 8000 | Hikvision | **admin** | verification code *(See above)* |
| V-4060DB | 8000 | ONVIF | **admin** | blank |
| V-4072MD | 8000 | Hikvision | **admin** | **scw12345user** or **scw** + [last 6 of MAC uppercase] |

| Model | Management Port | Protocol | Username | Password |
|---|---|---|---|---|
| V-5012B* | 80 | ONVIF | **scwuser** | **scw12345user** or **scw** + [last 6 of MAC uppercase] |
| V-5014B* | 80 | ONVIF | **scwuser** | **scw12345user** or **scw** + [last 6 of MAC uppercase] |
| V-5052D* | 80 | ONVIF | **scwuser** | **scw12345user** or **scw** + [last 6 of MAC uppercase] |
| V-5054D* | 80 | ONVIF | **scwuser** | **scw12345user** or **scw** + [last 6 of MAC uppercase] |

*Default password depends on firmware version. Refer to 5000 Series Default Passwords for more information.

## 4000 Series: Connect a Camera Directly to the NVR

On the NVR monitor, make sure **Plug and Play** is selected as the adding method for the port that you want the camera to use. No further configuration is required.

## 5000 Series: Connect a Camera Directly to the NVR

When connecting a 5000 Series camera directly to the NVR, you'll need to start by configuring the camera with a static IP address before connecting the camera directly to the NVR.

### Set Up a Static IP

**Note:** Leave the camera disconnected from the NVR until you've finished configuring the static IP.

1. On the NVR monitor, right-click in the window and select **Menu**. Enter the username and password that you used during activation.
2. Select **Camera** to open the **Camera Management** window. Find the NVR camera port that you want to connect the camera to and record its IP address.
    - This IP address may be in a different address range than other IP addresses used on the network.
3. Connect the camera to the local network.
4. Using the camera's MAC address, determine the IP that the camera is currently using.
5. Open a web browser and enter the camera's IP address.
6. Enter the camera's default username and password.
7. Go to **Network > Network Settings**.
8. In **Network Type**, select **Static**.
9. In **IP setup**, enter the IP address the NVR assigned to the port that you want to use.
10. Change the gateway address to the first address on the NVR's subnet: **192.168.254.1**.
11. Select **Apply**. Disconnect the camera from the network, then connect it to the NVR port that you want to use.

#### Add the Camera to the NVR

1. On the NVR monitor, right-click in the window and select **Menu**.
2. Select **Camera** to open the **Camera Management** window.
3. Select **Edit** to open the **Edit IP Camera** window.
4. Set the **Adding Method** to **Manual**.
5. Use the information from Table 1 to set the **Management Port** and **Protocol**, then enter the username and password.
6. Select **OK**. The NVR attempts to connect to the camera.

### Connect a Camera over Network to the NVR

1. On the NVR monitor, choose **Manual** as the method to add a 4000 Series camera, a V-4060DB doorbell, or a 5000 Series camera.
2. Open a web browser and enter the camera's IP address.
3. Enter the camera's default username and password.
4. Use the information from Table 1 to set the **Management Port** and **Protocol**.
5. Select the **Channel Port** and **Transfer Protocol**, then enter the username and password.
6. Select **OK**. The NVR attempts to connect to the camera.

### Add an ONVIF Camera in Dealer Admin

1. Find the customer and select the relevant account number.
2. In **Video**, find the NVR and select **Edit**.
3. To add the camera, select the Add icon.
4. Enter the camera's name and IP port.
5. Select the type from **Camera Type**.
6. Select **Save**.

## 22.3 Assign a Camera to a Zone

> **Note:** Video devices must be enabled on a system to assign a camera to a zone. For more information, refer to Enable Video Devices.

Dealer Admin allows you to assign cameras to zones. This feature allows clips to be recorded when the area a zone is located in goes into alarm.

To assign a camera to a zone, complete the following steps.

1. Go to **Customers**.
2. Select the system name.
3. In **Video**, select **Assign Cameras to Zones**.
4. In each zone's row, select **Choose a Camera** and select the cameras that you want to assign to that zone.
5. Select **Save**.

## 22.4 Configure Monitoring Center Video Verification

> **Note:** Video Verification does not postpone or interfere with communication with the monitoring center. Additionally, Video Verification feeds are only viewable by authorized personnel and automatically expire after a designated time period.

Dealer Admin supports Video Verification, which allows monitoring center operators to view live or recorded video from system cameras only in the event of an emergency. This feature helps monitoring center operators make faster, better-informed decisions when determining whether to deploy emergency personnel to a customer's home or business.



**Prefer a Video?**

In this clip, we'll show you how to set up Video Verification.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/579601417

## 22.4.1 Set Up Video Verification

To set up Video Verification, configure global settings on the **Dealer** page, then configure system settings in **System Information**.

### Step 1: Configure Dealer Settings

To configure global Video Verification settings, complete the following steps.

1. In the sidebar, go to **Settings > Dealer** and open the **Monitoring Center Video Verification** tab.
2. Select **Allow Monitoring Center Video Verification**.
3. Enter a number for the **Time Window**.
   - The **Time Window** is the amount of time the monitoring center operator has to view the Video Verification page. After the Time Window has ended, they will no longer be able to view the Verification page. The default is **30** minutes.
4. In **Video URL Auth Type**, select either **Require personnel login** or **Use Secure ID**.
   - **Use Secure ID** allows the operator to access video with a URL and does not require them to log in.
   - **Require personnel login** requires the monitoring center operator to log in using a Dealer Admin Personnel login.
5. If necessary, enter a name for the authorization type.
6. Select **Save**.

### Step 2: Configure System Settings

To configure Video Verification for a system, complete the following steps.

1. Go to **Customers**.
2. Select the system name.

3. At the top of **System Information**, select **Edit**.
4. In **Video**, select the types of cameras or NVRs that you want to enable on the system.
5. Select **Monitoring Center Video Verification**. A **Verification URL** will appear.
6. Copy the **Verification URL** and relay it to the monitoring center. They will use this URL to access the Video Verification page associated with your system.
7. Select **Save**.

## 22.4.2 Exclude a Camera from Video Verification

To exclude a camera from monitoring center Video Verification, complete the following steps:

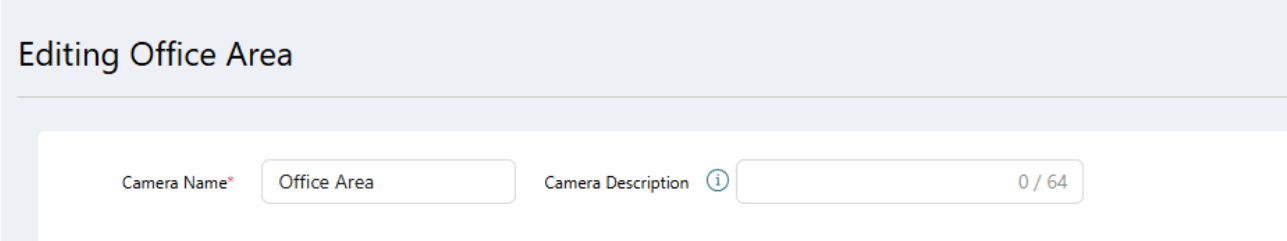
1. Go to **Customers**.
2. Select the system name.
3. In **Video**, select the camera that you want to edit.
4. Select **Edit**.
5. Turn off **Allow Monitoring Center Video Verification**.
6. Select **Save**.

## 22.4.3 Change a Camera Name and Add a Description

When an operator views the cameras in Video Verification, they can see the camera name and hover over it to see the description of the camera for more context.

To change the camera name and add a description, follow these steps:

1. Go to **Customers.**
2. Select the **System Name**.
3. In **XV Gateway with AlarmVision®**, select the camera you want to edit.
4. In **Camera Settings**, locate **Camera Name**. Select the box and enter the new name.
5. Locate **Camera Description**. Select the box and enter a short description of the camera.




4. Select **Save**.

## 22.4.4 2-Way Audio (XV Gateway Only)

By installing and configuring an ONVIF compliant IP-based audio device alongside one of the XV Gateway cameras, an operator can communicate to the area the audio devices are located using live audio broadcast or pre-recorded audio messages. A pre-recorded audio message can also be set to play automatically if an object is detected in a specified region. Additionally, inbound audio can be received from the site if the configured camera or speaker supports a microphone.

The pre-recorded audio messages are as follows:

**Trespassing Warning —** "You are trespassing, please leave the area. This area is under video surveillance, and you have been recorded."

**Loitering Warning —** "You are loitering in an unauthorized area. Please leave immediately or the police will be contacted."

**Generic Instruction —** "Warning, you are under video surveillance. Please leave the area immediately."

**Emergency Warning —** "Attention: please evacuate the area immediately."

**Speaker Test —** "This is a test of an audio device. If you can hear this message, you are being audio and video recorded. This is a test of an audio device."

> **Note:** This audio message is not available in Video Verification, and will only play when **Test Audio** is selected in **Camera Settings** on Dealer Admin.

## Allow Camera Audio

To allow a Monitoring Center operator to use camera audio during Video Verification, follow these steps:

1. Log into Dealer Admin (dealer.securecomwireless.com).
2. Navigate to **System Information**.
3. Select the XV Gateway associated with the system to access **Settings**.
4. In **Options**, locate **Allow Camera Audio**. Toggle it **ON**.
5. Select **Save**.

## Add 2-Way Audio Devices

For 2-Way Audio to function, at least one ONVIF compliant IP-based audio device and one XV Camera should be added to the XV Gateway. To add the necessary devices for 2-Way Audio, complete the following:

1. Log into Dealer Admin (dealer.securecomwireless.com).
2. Navigate to **System Information**.
3. Select **+ Devices to XV Gateway**.
4. Add any cameras or audio devices needed for 2-Way Audio. To learn more about how to add and edit devices on an XV Gateway, visit Add and Edit Devices.

## Assign an Audio Device to a Camera

To assign an audio device to a camera, follow these steps:

1. Log into Dealer Admin (dealer.securecomwireless.com).
2. Navigate to **System Information**.
3. Select the XV camera to access **Camera Settings**.
4. In **Options**, locate **Available for Monitoring Center Video Verification** and confirm it is toggled **ON**.
5. Select the box directly underneath. A drop-down will open, listing all available audio devices.
6. Select the devices you want to associate to the camera.
7. Select **Test Audio** to confirm the appropriate devices have been selected. An audio message will play through all speakers associated to the camera, stating: "This is a test of an audio device. If you can hear this message, you are being audio and video recorded. This is a test of an audio device."
8. Select **Save**.

## Set Automatic Audio Clip

To set an audio clip to play automatically upon detection in a specific region, follow these steps:

1. Log into Dealer Admin (dealer.securecomwireless.com).
2. Navigate to **System Information**.
3. Select the XV camera to access **Camera Settings**.
4. In **Regions & Analytics**, select **+ Region**.
5. Configure the region settings as needed.

6. If you have turned on **Allow Camera Audio**, an option called **Play Audio Clip on Detection** appears beneath the detection options. Toggle it **ON**.
7. Select the drop-down box next to **Select Clip** to set the audio clip that plays upon detection.
8. Select the drop-down box next to **Select Frequency** to set the number of times the clip plays. You can set the clip to play up to five times.
9. Select **Save**.

## 22.5 XV Gateway with AlarmVision® (XV-24, XV-60, XV-96)

The XV Gateway (XV-24, XV-60, XV-96) with AlarmVision® seamlessly integrates cameras, analytics, and the XR Series or XT75 Control Panel to create smart motion detectors that trigger panel responses in real time based on real events for real results.

Virtual Keypad users can view live and recorded HD video clips, define video actions, and receive push notifications of real events in real time for real results.

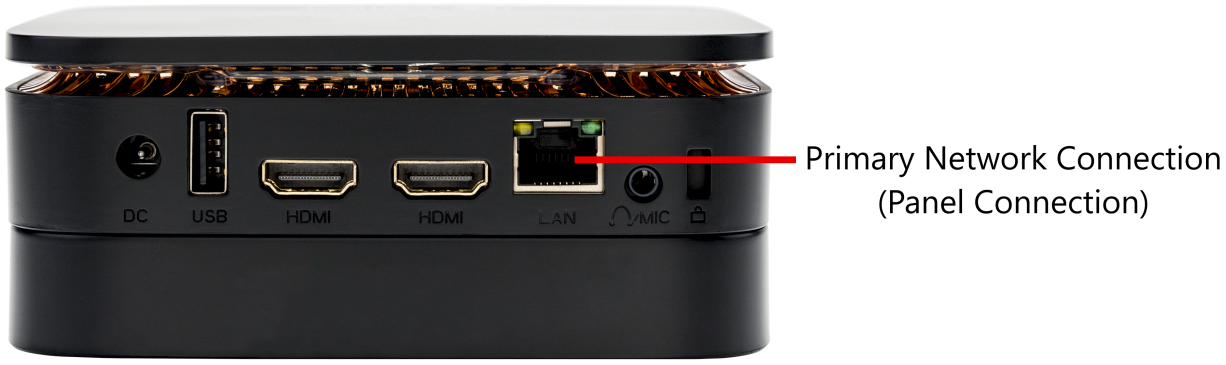
**Note**: You need an active Dealer Admin account at dealer.securecomwireless.com to activate the XV Gateway.

### 22.5.1 Install the XV Gateway

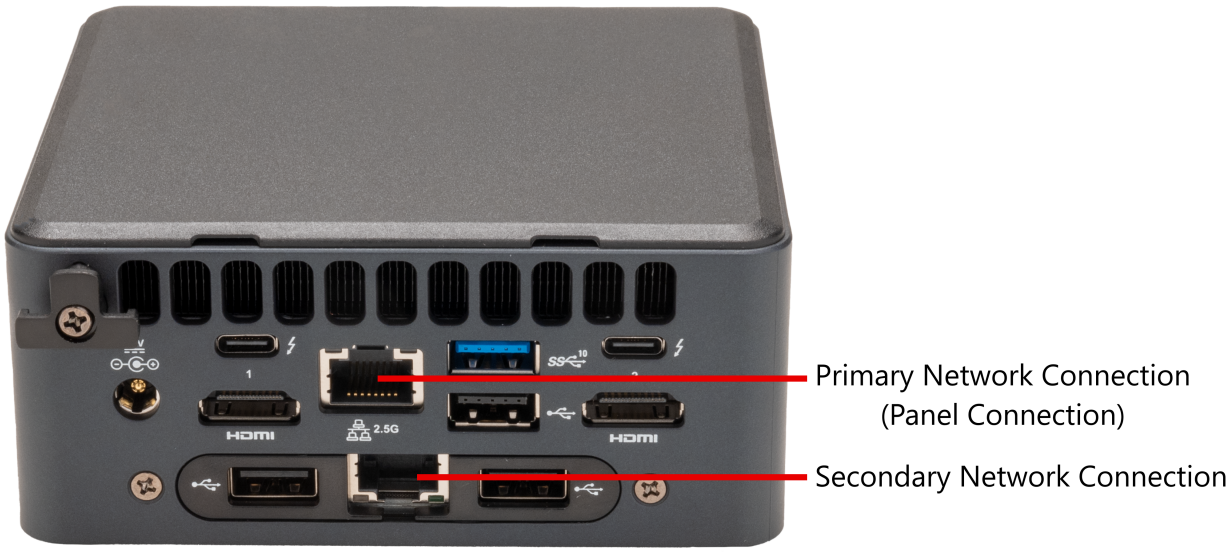
#### Install the XV Gateway

The primary network connection on the XV Gateway and the panel should be connected to the same network switch. You can also use any network switch that is connected to the same subnet that the panel is connected to.

**Note:** The HDMI port does not support an external display of camera streams on the XV-24, XV-60, or XV-96.




**14 XV-24 with Single NIC**




**15 XV-60/XV-96 with Dual NIC**

**Using a Network Switch**

1. Connect a network cable from the panel to a network switch.
2. Connect a network cable from the XV Gateway's primary network connector, located on the back of the device, to the same network switch that the panel is connected to. This ensures that both the panel and the XV Gateway communicate over the same network.

**Using the Same Subnet**

1. Connect a network cable from the panel to a network switch.
2. If the XV Gateway cannot be connected to the same network switch that the panel is connected to, you can use any network switch that is connected to the same subnet the panel is connected to.

**Using Dual NIC**

If you are using a secondary NIC at initial installation, connect the secondary network connection on the XV-60 or XV-96 prior to adding the XV Gateway on Dealer Admin. Ensure the primary network connection is also connected to the XV Gateway.

Refer to *Configure Secondary NIC for Private Camera Network* for more information.

**Note:** The panel can only be connected to the primary network connection through the network switch or subnet.

## Additional Information

**XV Gateway Models**

XV-24: 24 MP Video Analytics-Enabled Motion Detector

XV-60: 60 MP Video Analytics-Enabled Motion Detector

XV-96: 96 MP Video Analytics-Enabled Motion Detector

**Certifications**

NDAA Compliant

**Specifications**

Supports ONVIF and RTSP cameras

One TB internal storage (XV-24)

Four TB internal storages (XV-60 and XV-96)

Up to 24, 60, or 96 MP Processing

Includes Power Supply

## 22.5.2 Activate the XV Gateway

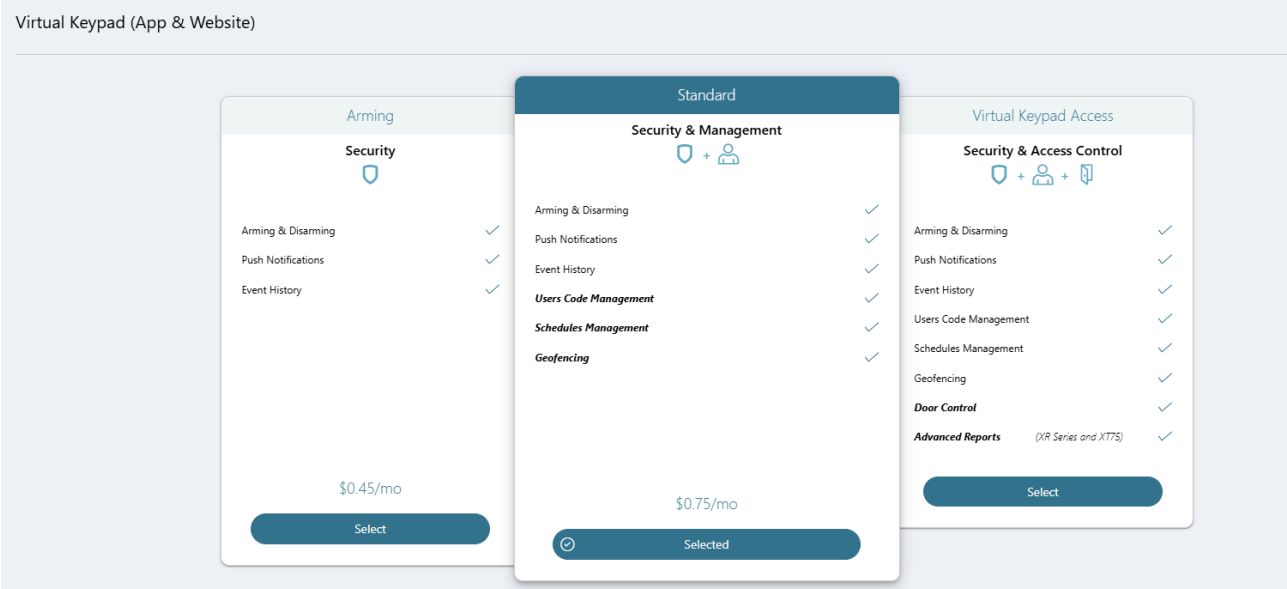
**Note:** To connect an XV Gateway to an XR Series, the panel requires firmware Version 221 or higher.

### Add an XV Gateway

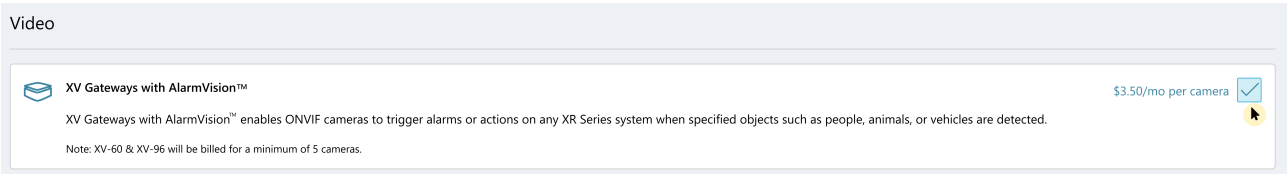
**Note**: If the XV Gateway you want to activate was on a different system before, ensure the XV Gateway has been deleted from the previous system on Dealer Admin before adding it to the new system. Refer to *Delete an XV Gateway* for more information.

1. Log in to Dealer Admin (dealer.securewireless.com).
2. Go to **Customers** and select the **System Name** you want to connect the XV Gateway to.
3. At the top of the screen, select **Edit**.


4. At **Virtual Keypad (App & Website)**, ensure **Standard** or **Virtual Keypad Access** is selected to view additional features.

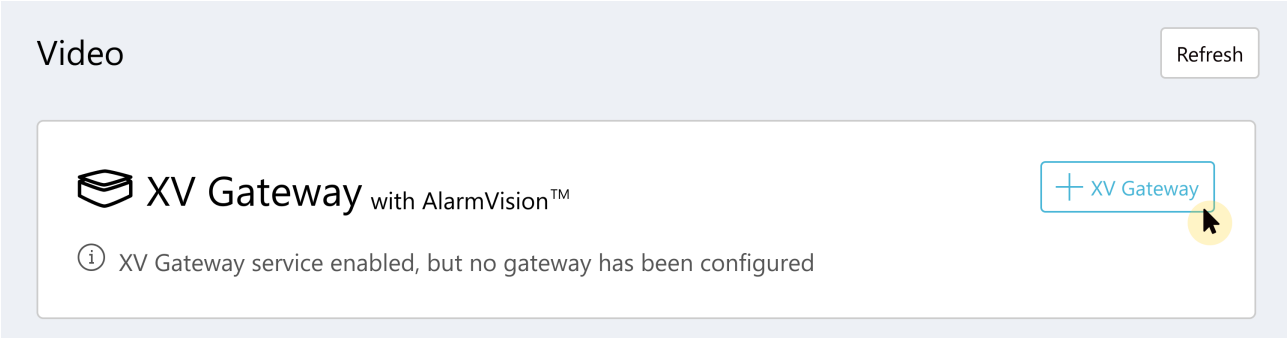



5. Scroll down to **Video**. At **XV Series with AlarmVision®**, select the checkbox to enable the XV Gateway.

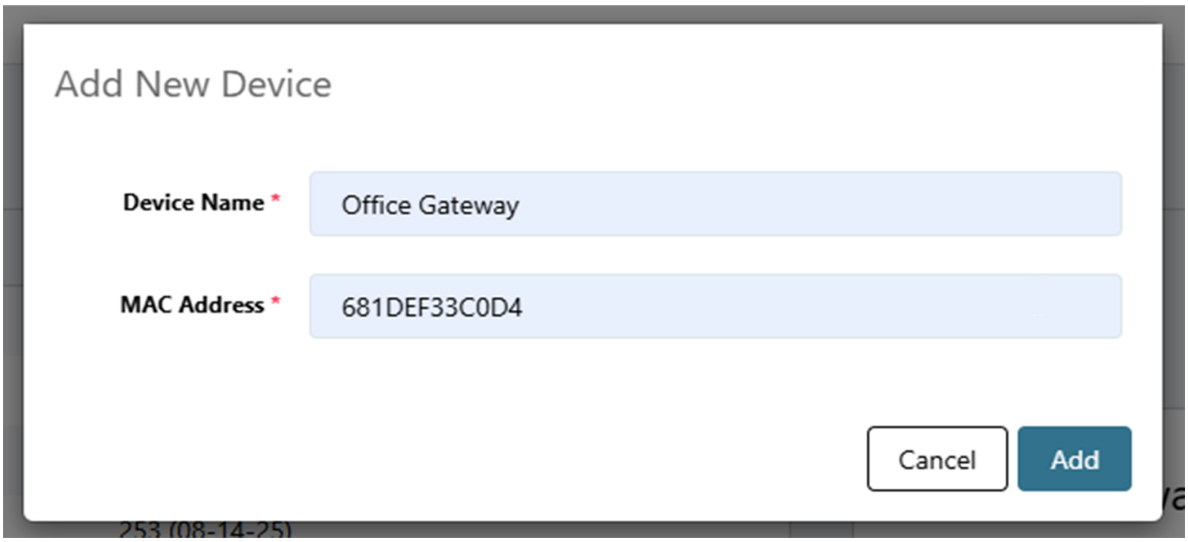



6. In **Monitoring Center Video Verification**, select the checkbox if you want to enable monitoring center video verification services.

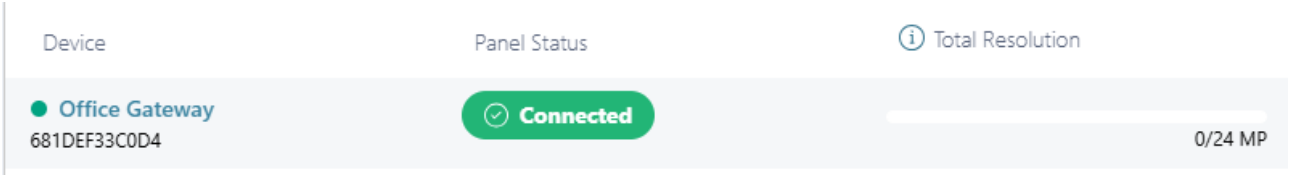

7. At the top or bottom of the screen, select **Save**.
8. At **Video**, select **+ XV Gateway** to add an XV Gateway.




9. Add the XV Gateway **Device Name** and **MAC Address**, then select **Add**. Dealer Admin automatically checks to see which model the XV Gateway is.




10. Once the XV Gateway is connected, the **Device**, **Panel Status**, and **Total Resolution** information displays.




11. To add a device to the XV Gateway, refer to Add Devices to the XV Gateway. To configure the secondary NIC for an XV-60 or XV-96, refer to the steps below.

### Configure the Secondary NIC (XV-60 or XV-96 Only)

You can configure the secondary NIC to use DHCP or a static IP address XV-60 or XV-96 Gateways.

### Should I Use DHCP?

If you can plug in a camera or device into your private network and immediately access other devices on the network, then you likely have a DHCP server. If you configure the secondary NIC to use DHCP, the DHCP Server automatically assigns a dynamic IP address to the XV Gateway so it can change over time.

### Should I Use a Static IP Address?

If your private camera network consists of only cameras and you set up each camera with its own static IP address, then you likely do not have a DHCP server. You can configure the secondary NIC to use a static IP address, which is manually assigned to the XV Gateway and does not change automatically.

To configure the secondary NIC, complete the steps below:

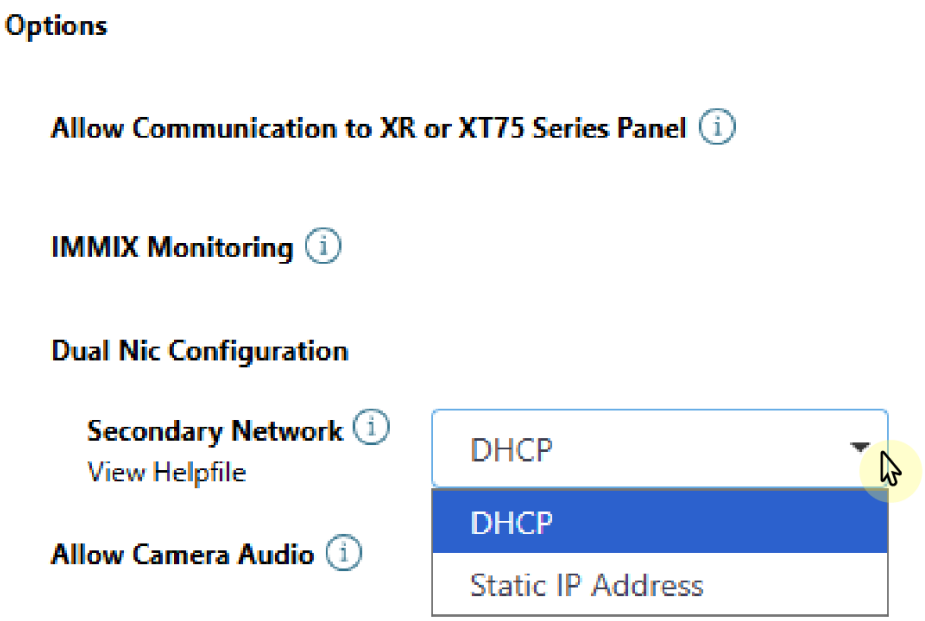
1. Before configuring a secondary network interface in Dealer Admin, connect a network cable to the second network switch.

> **Note:** The panel can only be connected to the primary network connection through the network switch or subnet.

2. Log in to Dealer Admin (dealer.securewireless.com).
3. Go to **Customers** and select the **System Name** that is associated with the XV-60 or XV-96.
4. At Video, select the name of the XV Gateway to configure the XV Gateway's settings.

5. At **Options**, go to **Dual Nic Configuration.** Use the **Secondary Network** drop-down menu to select **DHCP** or **Static IP Address** as the network connection type.

> **Note:** If you selected **Static IP Address** and your private network has a DHCP Server, ensure the **Static IP Address** is reserved.




3. If you selected **DHCP**, select **Save** to apply any changes to the XV Gateway. If you selected **Static IP Address**, enter the **IP Address** and **Subnet Mask** information, then select **Save** to apply any changes to the XV Gateway.

> **Note:** If you selected **Static IP Address**, ensure that the **Static IP Address** and **Subnet Mask** are the same network segment used for the cameras on your private camera network.

## 22.5.3 Add Devices to the XV Gateway

You can connect devices, such as cameras, speakers, or microphones to the XV Gateway to enable analytics, AlarmVision®, and 2-Way Audio.

For optimal performance, DMP recommends that the total resolution of added devices not exceed each XV Gateway model limit (XV-24: 24 MP, XV-60: 60 MP, XV-96: 96 MP). All cameras should have a frame rate of 15 FPS or less and a codec: H.264. Performance may vary based on number of cameras, framerate, codec, and motion detection.

When you add a device to the XV Gateway, it displays as a camera. If the device is a speaker or microphone, you can then add it as an audio device. For more information, refer to the following pages:

- Add Cameras
- Add Audio Devices

## Add Cameras

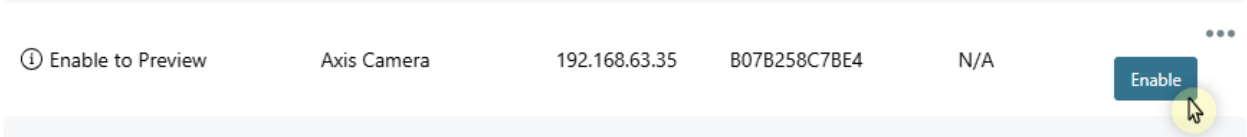
### Add a Camera Using Auto-Discover

Cameras can be automatically discovered if they exist on the same subnet as the XV Gateway.

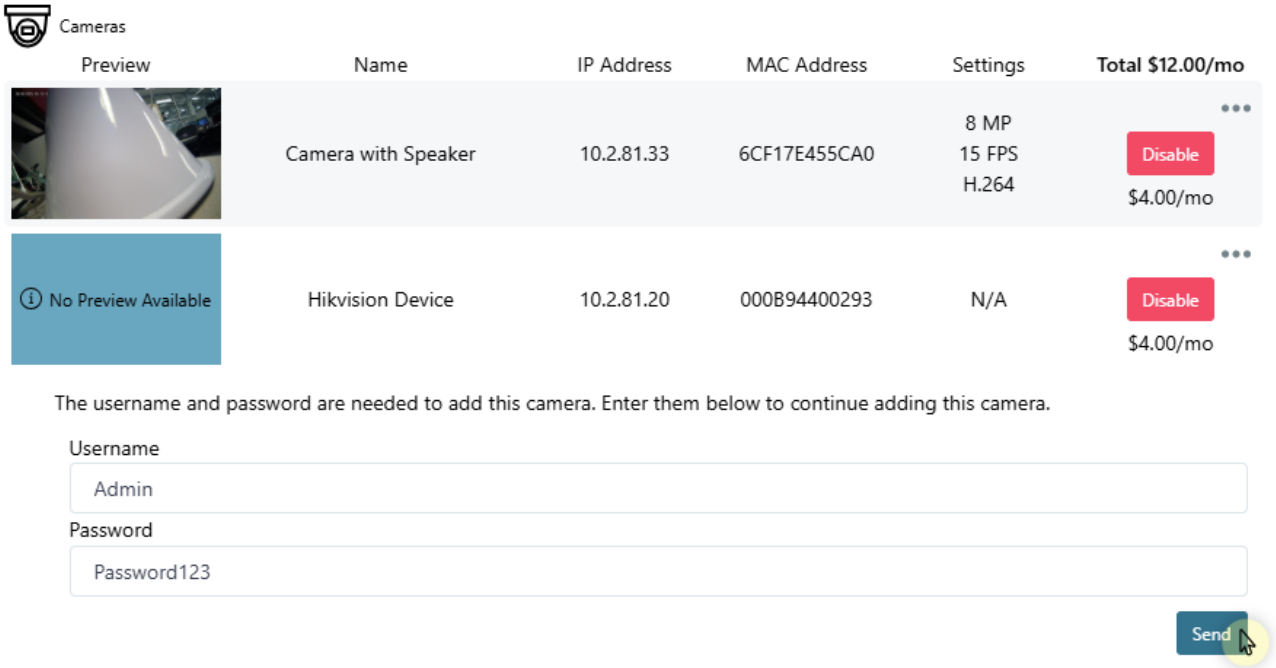
1. Go to **Customers**, then select the **System Name** that the XV Gateway is connected to.
2. Go to **Video**, then select **+ Device to XV Gateway** to add a camera to the XV Gateway.


3. Ensure **Auto Discover Devices** is ON. Cameras that already exist on the same subnet as the XV Gateway automatically display in the **Cameras** list.

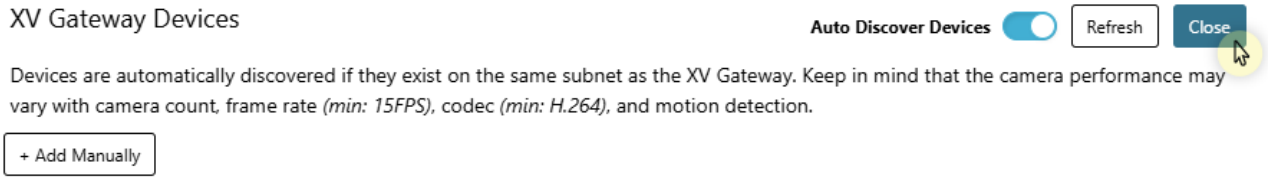

4. In **Cameras**, locate the camera you want to add to the XV Gateway. Select **Enable** to add the camera to the XV Gateway.




5. Enter the default **Username** and **Password** for your camera or the username and password you set previously. Select **Send**. The camera view displays a preview of the field of view.




6. Once the camera has been added, select **Close**

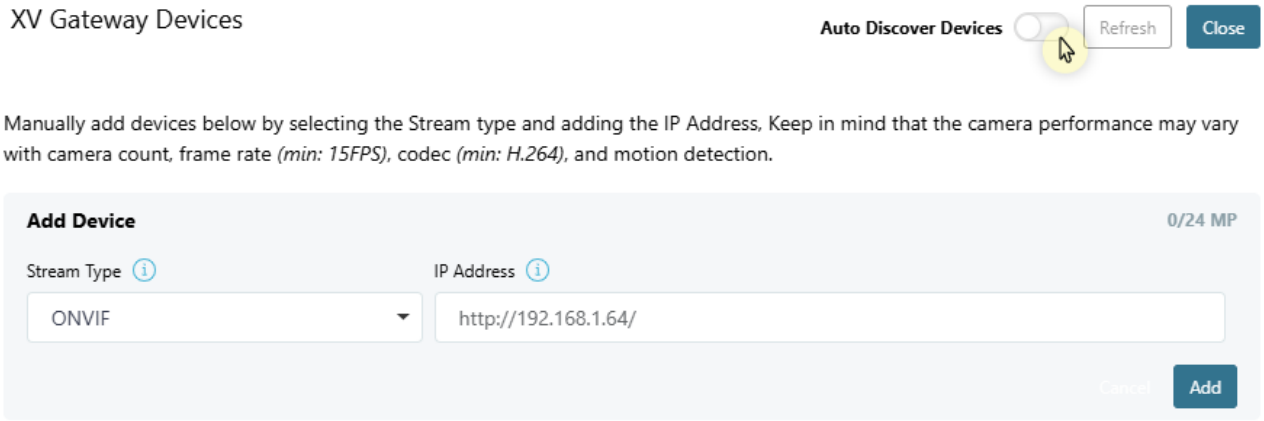


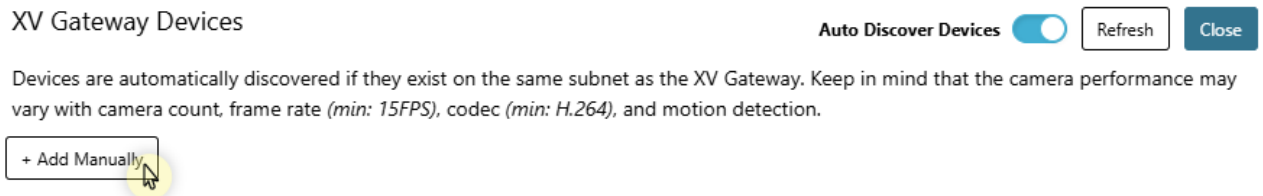

### Manually Add a Camera

Cameras should be manually added when they are outside of the XV Gateway subnet.

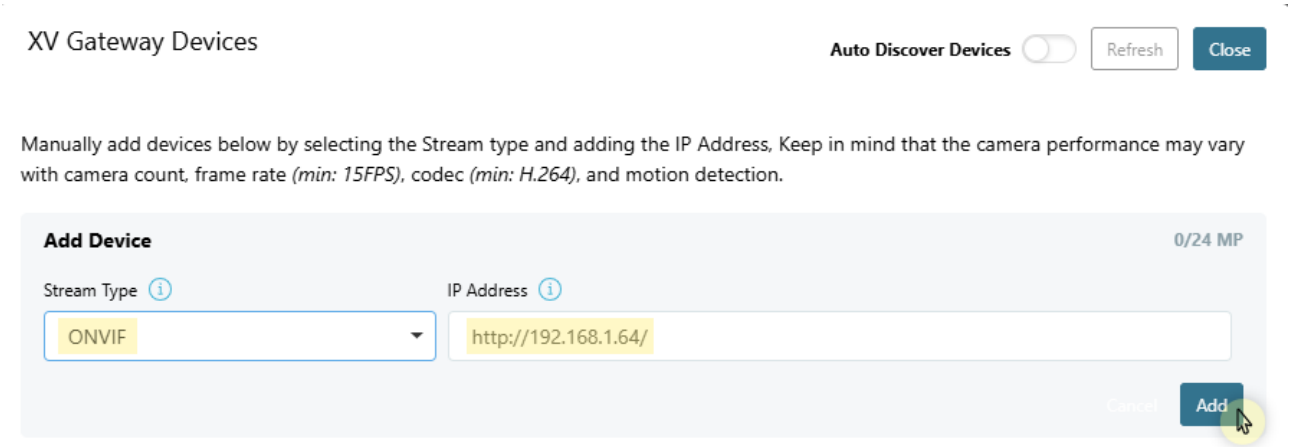
1. Go to **Customers**, then select the **System Name** that the XV Gateway is connected to.
2. Go to **Video**, then select **+ Device to XV Gateway** to manually add a camera to the XV Gateway.


3. Toggle **Auto Discover Devices** OFF or select **Add Manually**.

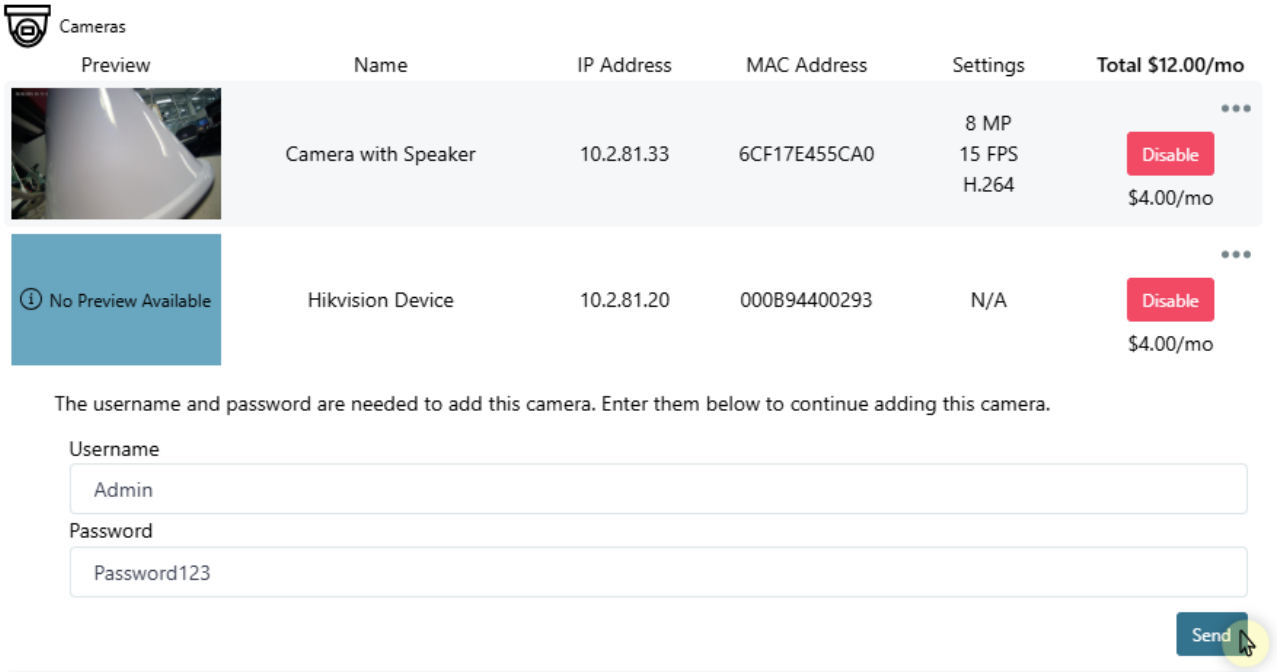



4. At **Stream Type**, select **ONVIF** or **RTSP Stream** from the drop-down menu and enter the camera's **IP Address**. Select **Add**.




5. Enter the default **Username** and **Password** for your camera or the username and password you set previously. Select **Send**. The camera view displays a preview of the field of view.




5. Once you have added the camera to the XV Gateway, select **Close**.

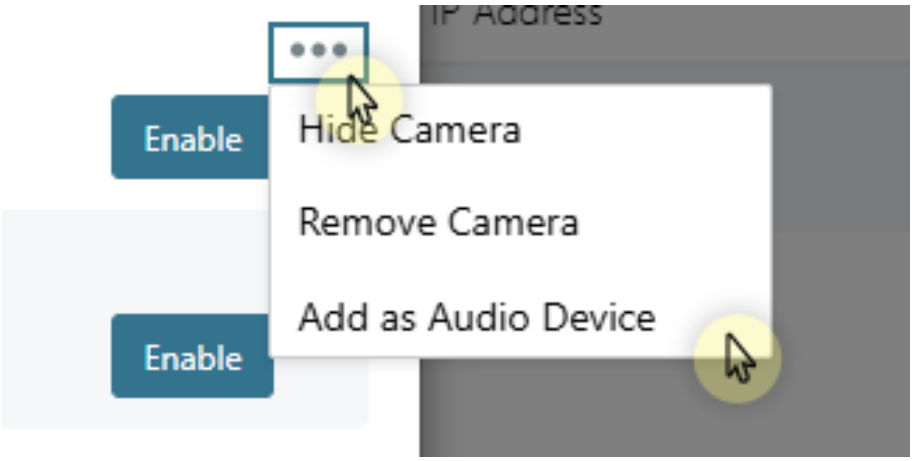

## Add Audio Devices

### Add an Existing Camera as an Audio Device

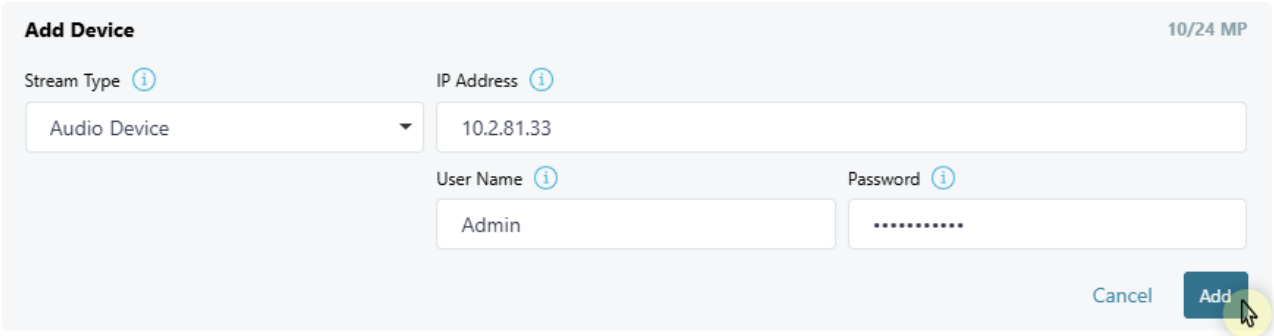
If a camera is already associated with the XV Gateway but also needs to be added as an audio device, follow the steps below:

1. Go to **Customers**, then select the **System Name** that the XV Gateway and camera are connected to.
2. Go to **Video**, then select **+ Device to XV Gateway** to add an existing camera as an audio device to the XV Gateway.

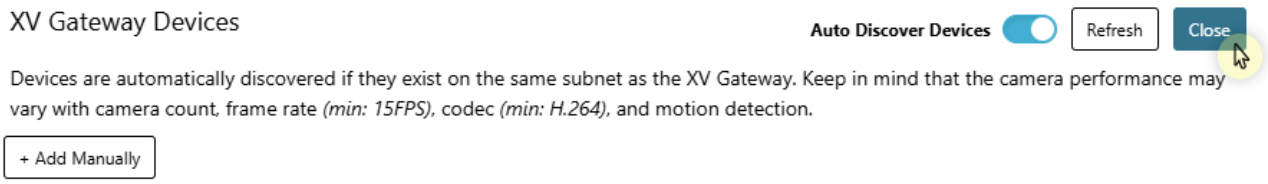

3. Locate the camera you want to add as an audio device to the XV Gateway, then select the **More** icon. Select **Add as Audio Device** to add the camera as an audio device to the XV Gateway.




4. In the **Stream Type** drop-down menu, select **Audio Device**. The IP Address automatically displays. Enter the default **Username and Password** for your camera or the username and password you set previously. Select **Add**.




5. Once the camera has been added as an audio device, select **Close**.




### Add a New Audio Device Using Auto-Discover

If you are adding an external speaker to the XV Gateway using auto-discover, it initially displays as a camera. From the **Cameras** list, you can then add it as an audio device.

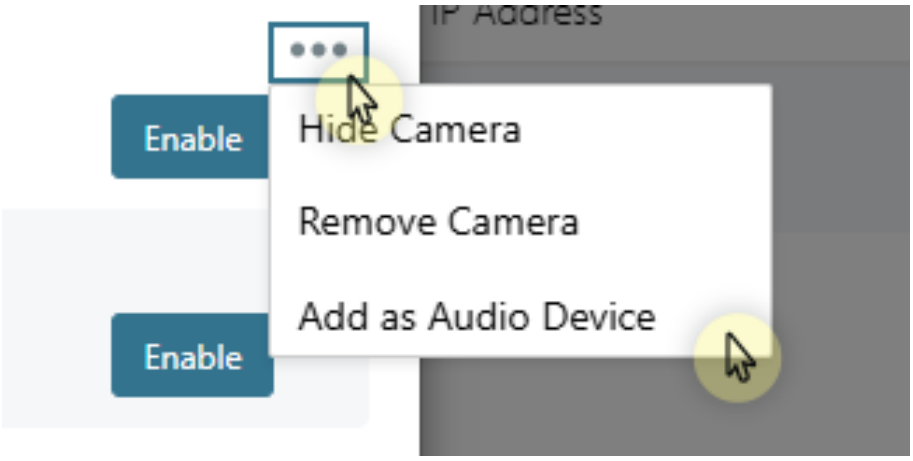
> **Note**: Before adding an audio device, ensure **Allow Camera Audio** is enabled in the **XV Gateway Settings**. For more information, refer to Add 2-Way Audio Devices.

To add an audio device using auto-discover, complete the steps below:

1. Go to **Customers**, then select the **System Name** that the XV Gateway is connected to.
2. Go to **Video**, then select **+ Device to XV Gateway** to add a device to the XV Gateway. Devices that already exist on the same subnet as the XV Gateway automatically display in the **Camera** list.

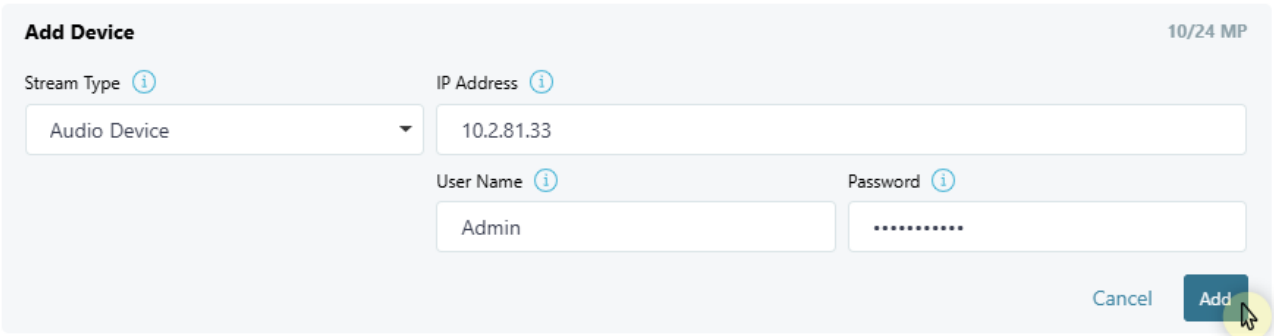

3. Ensure **Auto Discover Devices** is ON. Devices that already exist on the same subnet as the XV Gateway automatically display in the **Cameras** list.


4. In **Cameras**, locate the audio device you want to add to the XV Gateway. Select the **More** icon. Select **Add as Audio Device** to add the device as an audio device.

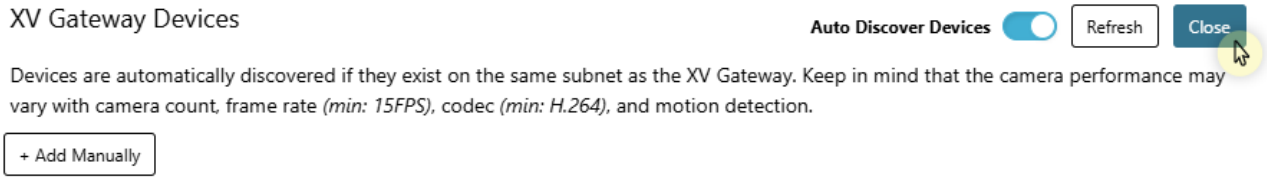



**Note**: If **Add as Audio Device** does not appear, ensure **Allow Camera Audio** is enabled in the **XV Gateway Settings**. For more information, refer to Add 2-Way Audio Devices.

5. In the **Stream Type** drop-down menu, select **Audio Device**. The IP Address automatically displays. Enter the default **Username** and **Password** for your camera or the username and password you set previously. Select **Add**.




6. Once the device displays as an audio device, select **Close**.



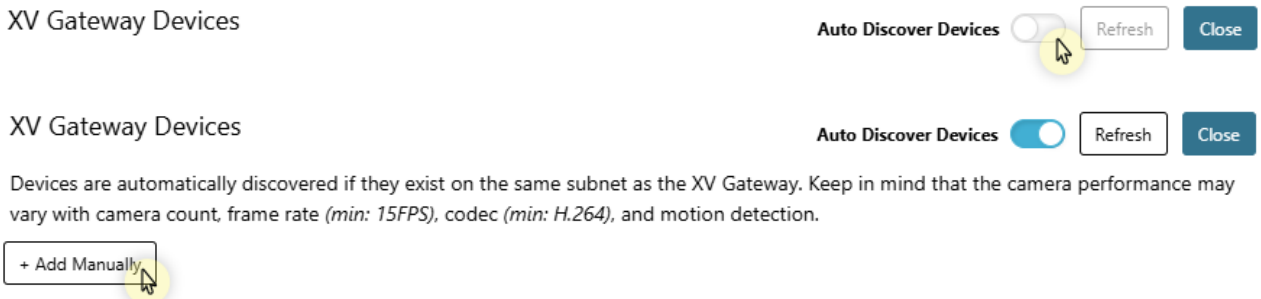

### Manually Add an Audio Device

Audio devices that are not connected to the same subnet as the XV Gateway should be manually added.

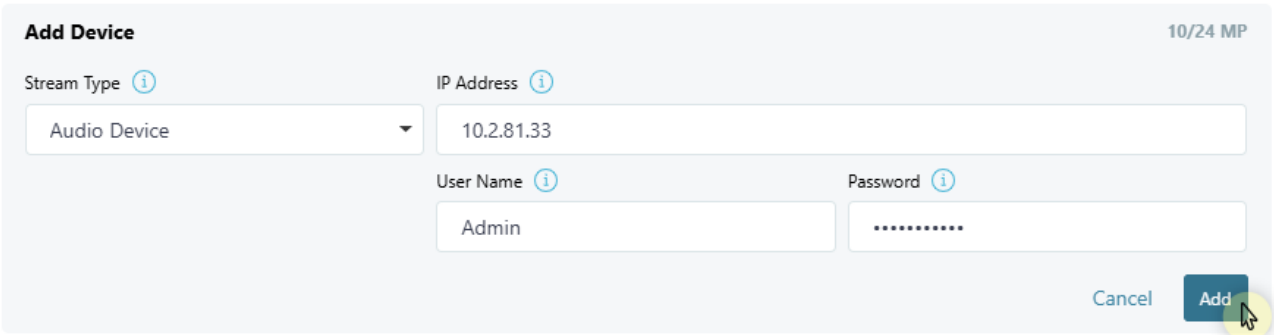
To manually add an audio device, complete the steps below:

1. Go to **Customers**, then select the **System Name** that the XV Gateway is connected to.
2. Go to **Video**, then select **+ Device to XV Gateway** to add a device to the XV Gateway.

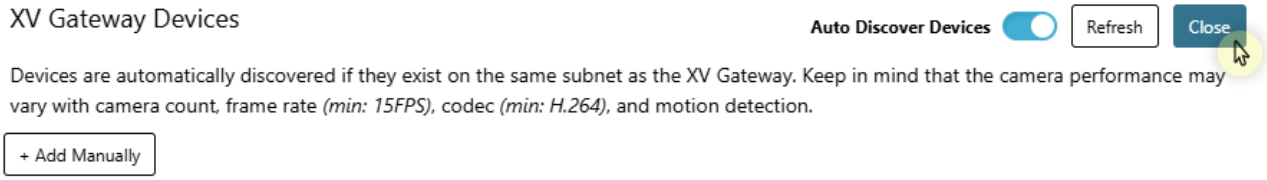

3. To manually add a device, toggle **Auto Discover Devices** OFF or select **Add Manually**.




4. At **Stream Type**, select **Audio Device** from the drop-down menu and enter the **IP Address**. Enter the default **Username** and **Password** for your camera or the username and password you set previously. Select **Add**.



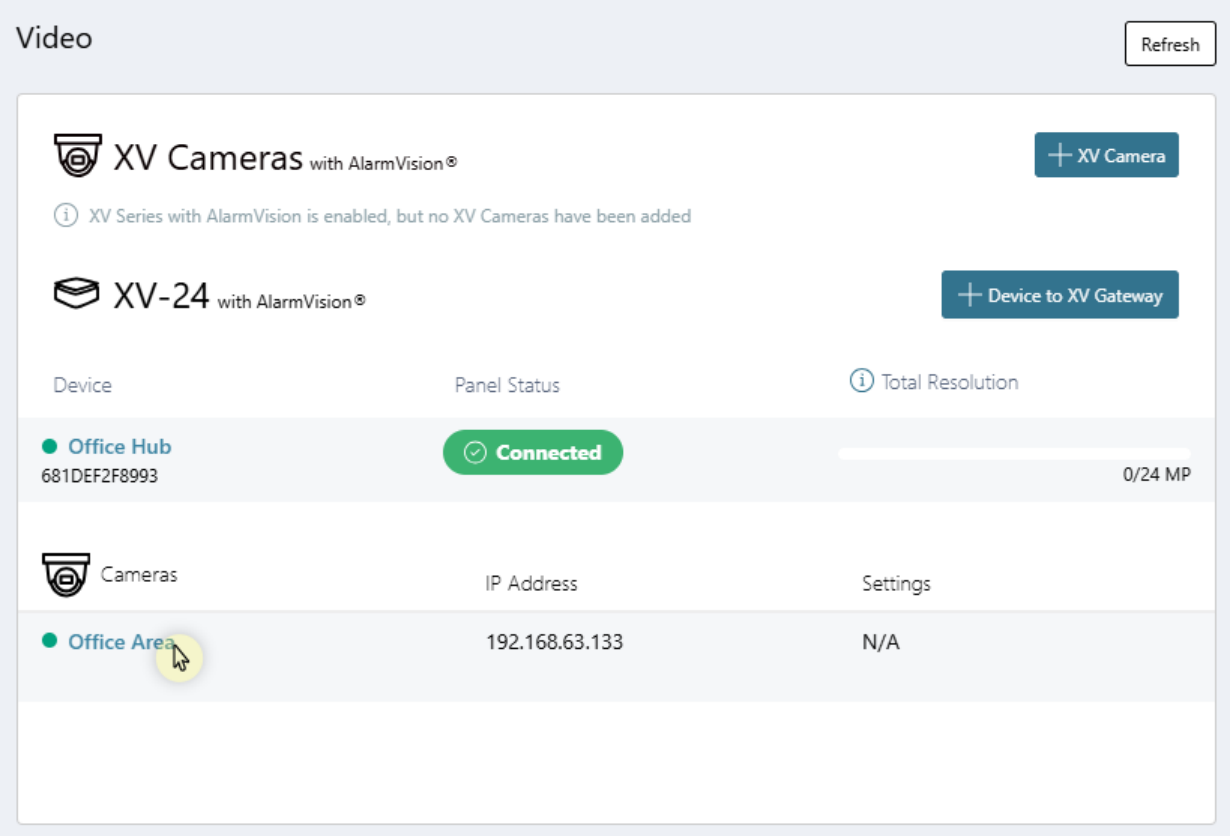

5. Once the device displays as an audio device, select **Close**.



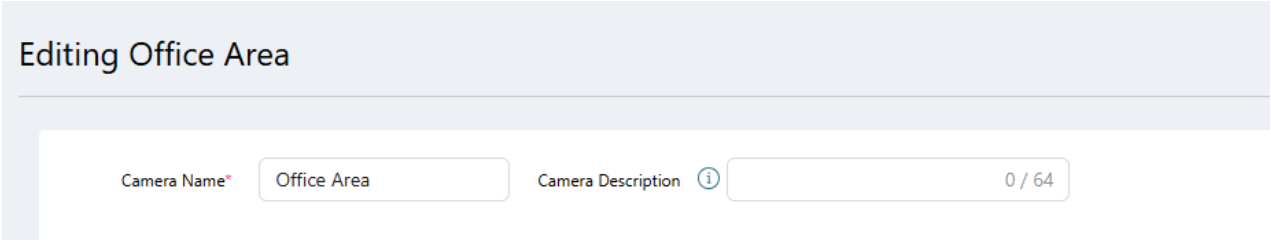
## 22.5.4 Configure Devices on the XV Gateway

### Configure Camera Options

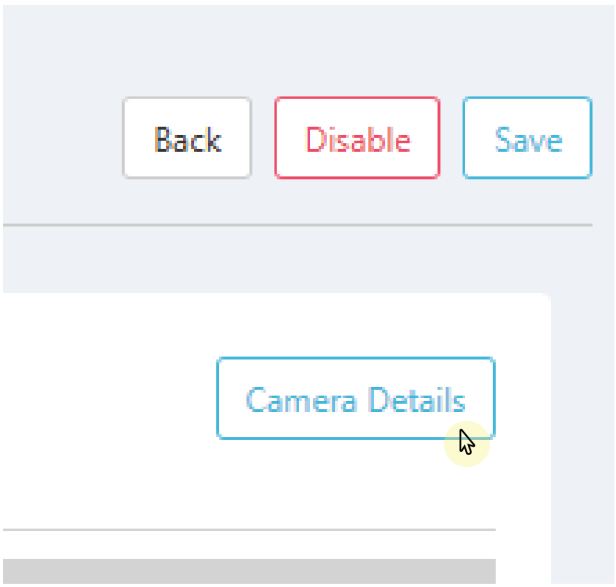
1. Log in to Dealer Admin (dealer.securecomwireless.com)
2. Go to **Customers**, then select the **System Name** that the XV Gateway and camera are connected to.
3. At **Video**, select the camera.

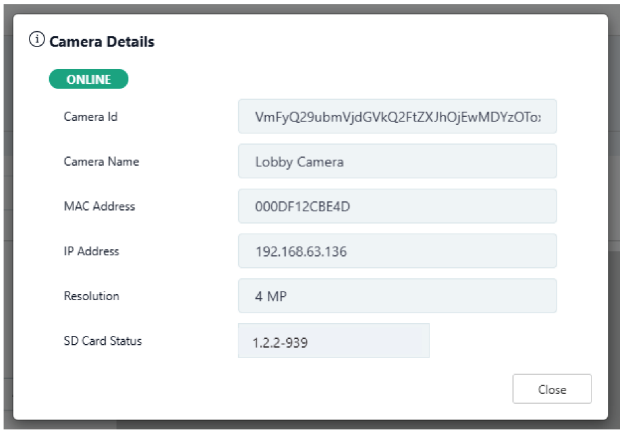



2. Enter a **Camera Name** and **Camera Description** for the camera.



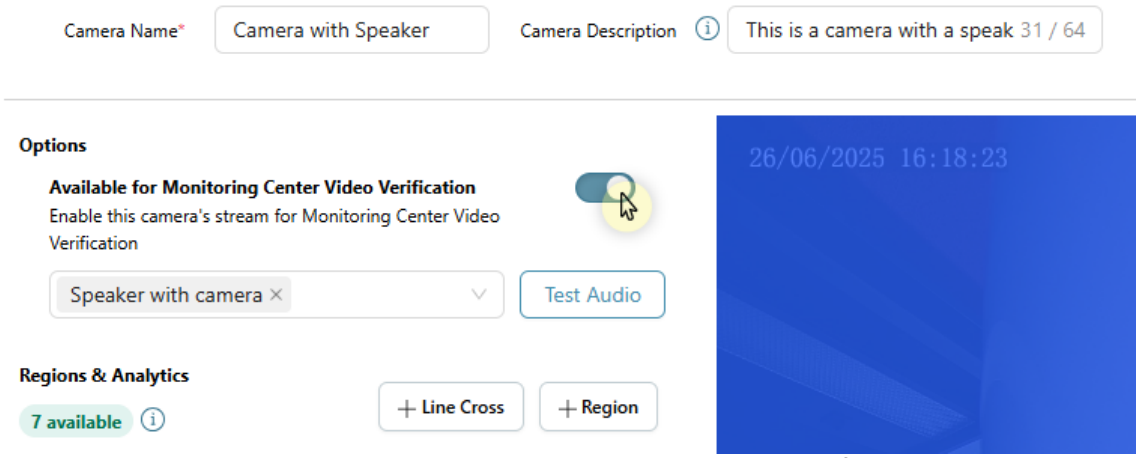

3. At the top right corner of the screen, select **Camera Details** to view the following camera information:
   - **Camera Status**
   - **Camera Id**
   - **Camera Name**
   - **MAC Address**
   - **IP Address**
   - **Resolution**
   - **SD Card Status**



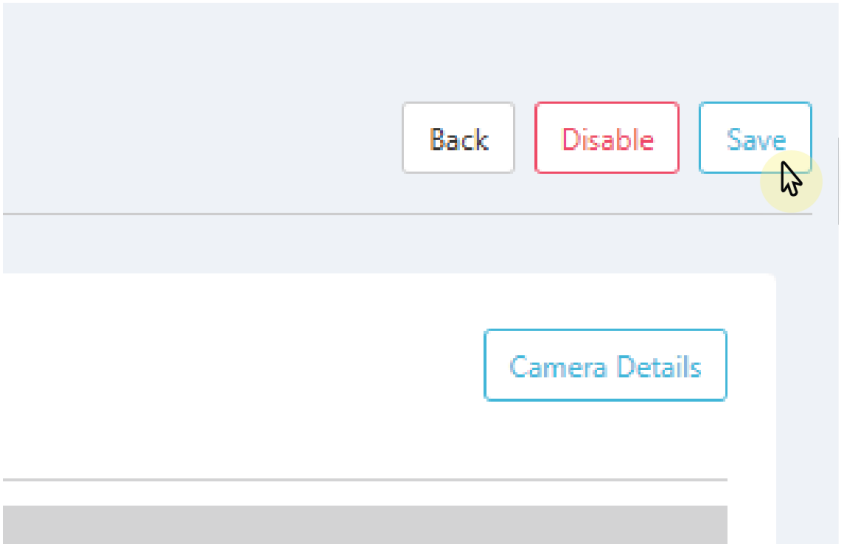




4. Select **Close**.
5. At **Options**, next to **Available for Monitoring Center Video Verification**, ensure the toggle is ON if you want to enable the camera feed for Monitoring Center Video Verification.

> **Note**: If **Monitoring Center Video Verification** does not display, ensure this feature is enabled for your system.
> To enable **Monitoring Center Video Verification** for your system, refer to Enable Monitoring Center Video Verification.



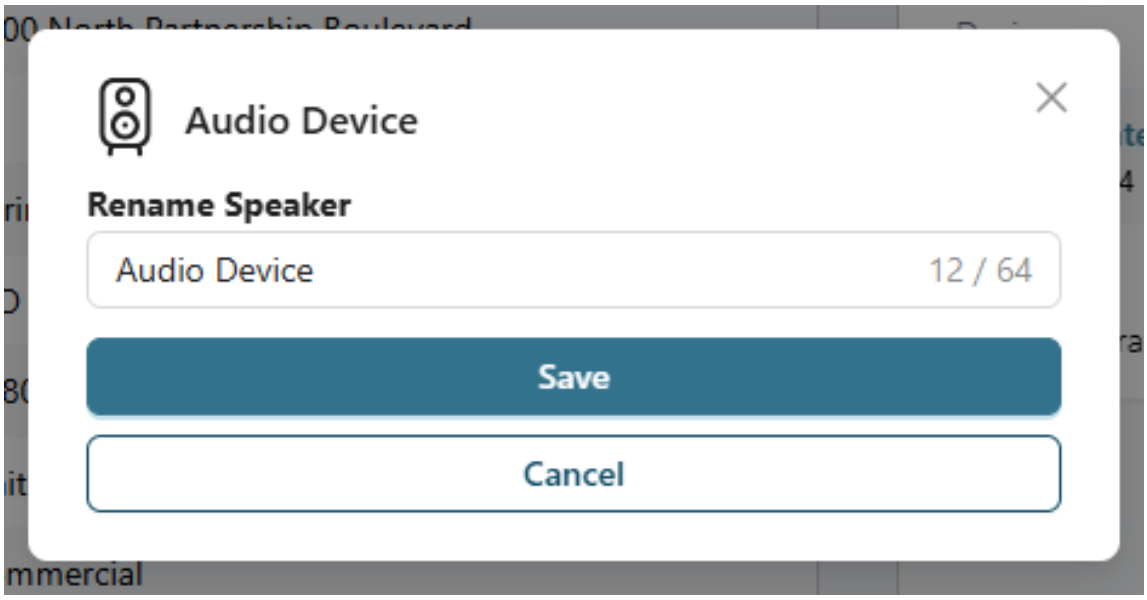

5. Select **Save** in the top right corner to apply any edits to the camera or refer to Add Regions & Analytics to create detection regions or lines for the camera.




## Rename Audio Device

To rename the audio device, complete the following steps:

1. Log in to Dealer Admin (dealer.securecomwireless.com)
2. Go to **Customers**, then select the **System Name** that the XV Gateway is associated with.
3. At **Video**, select the audio device you want to rename.
4. A window displays to rename the audio device. Enter the new name, then select **Save**.




## Add Regions, Analytics, and AlarmVision® Zones

If your camera has **Regions & Analytics settings**, you can add up to **four regions** and **four lines**. Regions and lines allow your camera to detect motion. If your camera does not have at least one region or line set up, it does not detect motion. You can also add **analytics** to your camera.

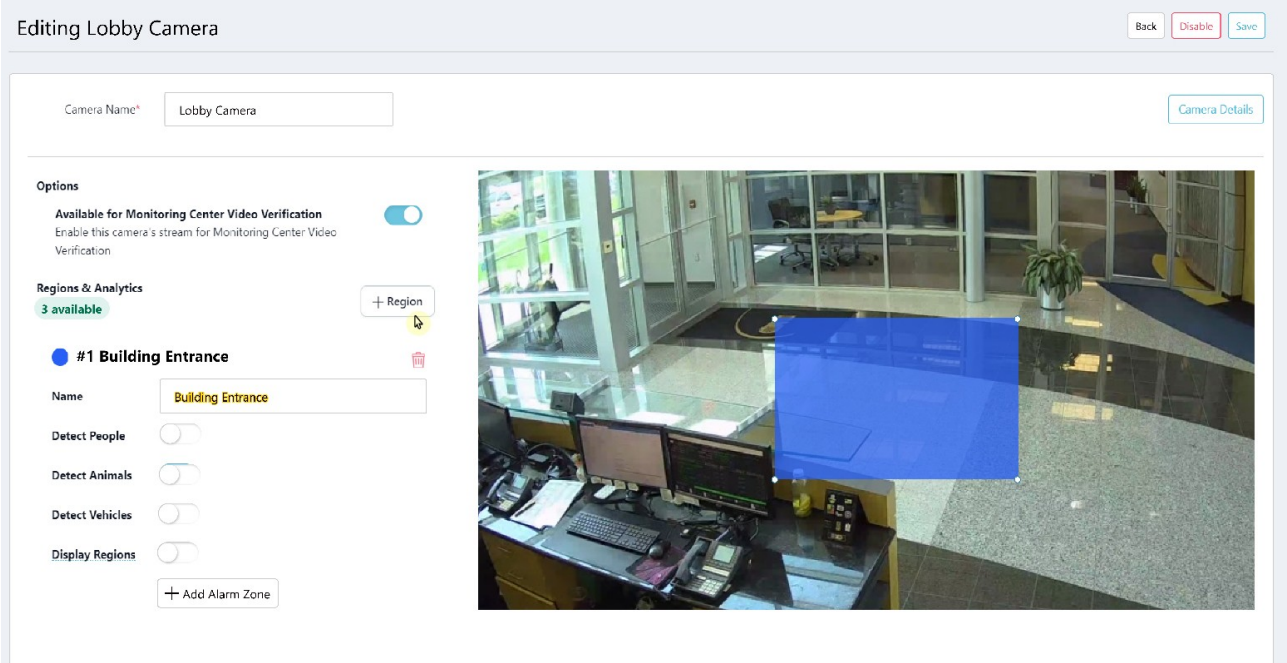
**Regions** are sections of an area where cameras detect motion. Motion that occurs outside a region is not detected. For example, a region covering the doorway to a room only detects motion in the doorway. You can also define a region that requires motion to cross it to be detected.

**Lines** are sections of a room where motion has to cross for the camera to detect motion. For example, a line at the doorway detects motion if someone crosses the line at the doorway.

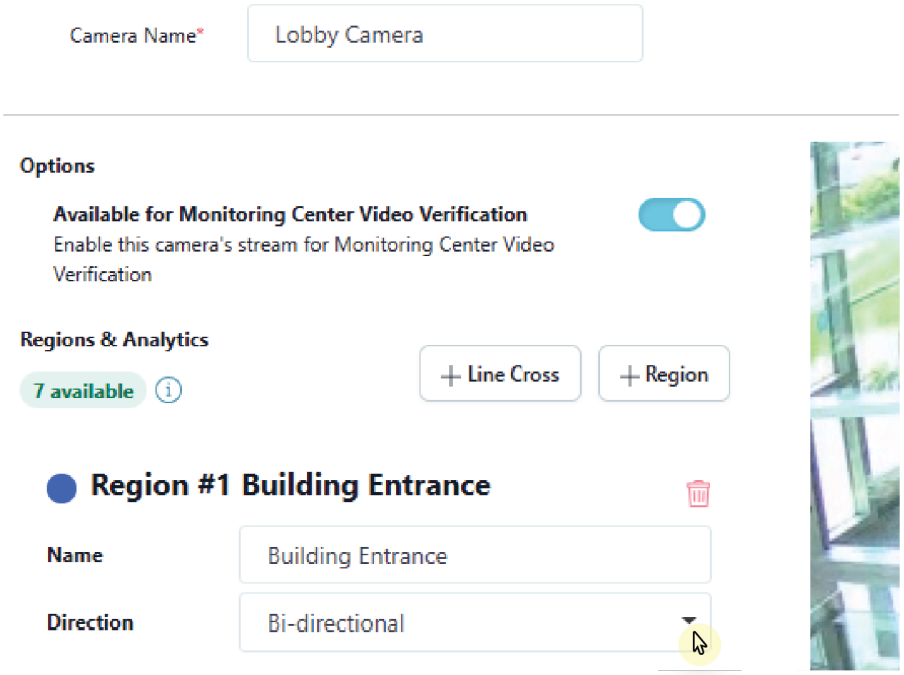
**Analytics** allow your camera to **detect people**, **detect animals**, and **detect vehicles**. When analytics are enabled, your camera records a 30-second clip on motion. The clip is stored in Events with information about what was detected, when, and where.

### Create a Region

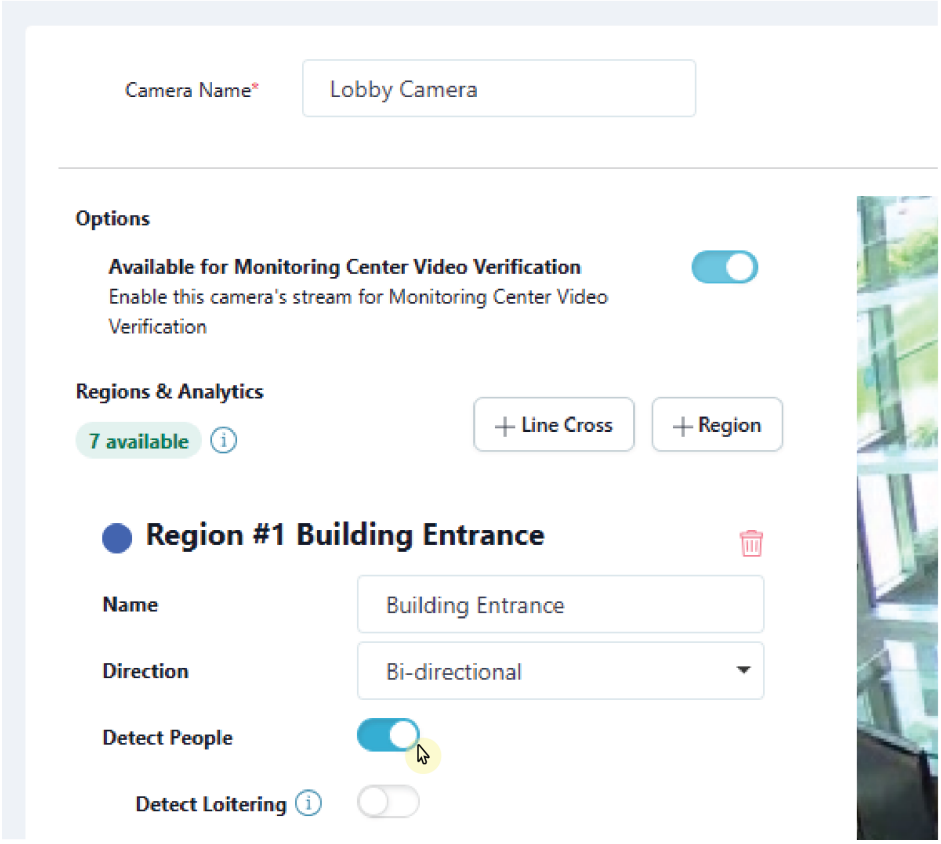
1. Log in to Dealer Admin (dealer.securecomwireless.com).
2. Go to **Customers**, then select the **System Name** that the XV Gateway and camera are connected to.
3. In **Video**, go to **Cameras** and select the camera name you want to create a region for.
4. In the **Edit Camera** page, go to **Regions & Analytics** and select **+ Region**. A box appears in the middle of the camera view screen.
5. Select the box, then drag it across the camera view to place it in the desired detection region. Select and drag the white circles on the corners of the box to manipulate the region.
6. Give the region a **Name**.



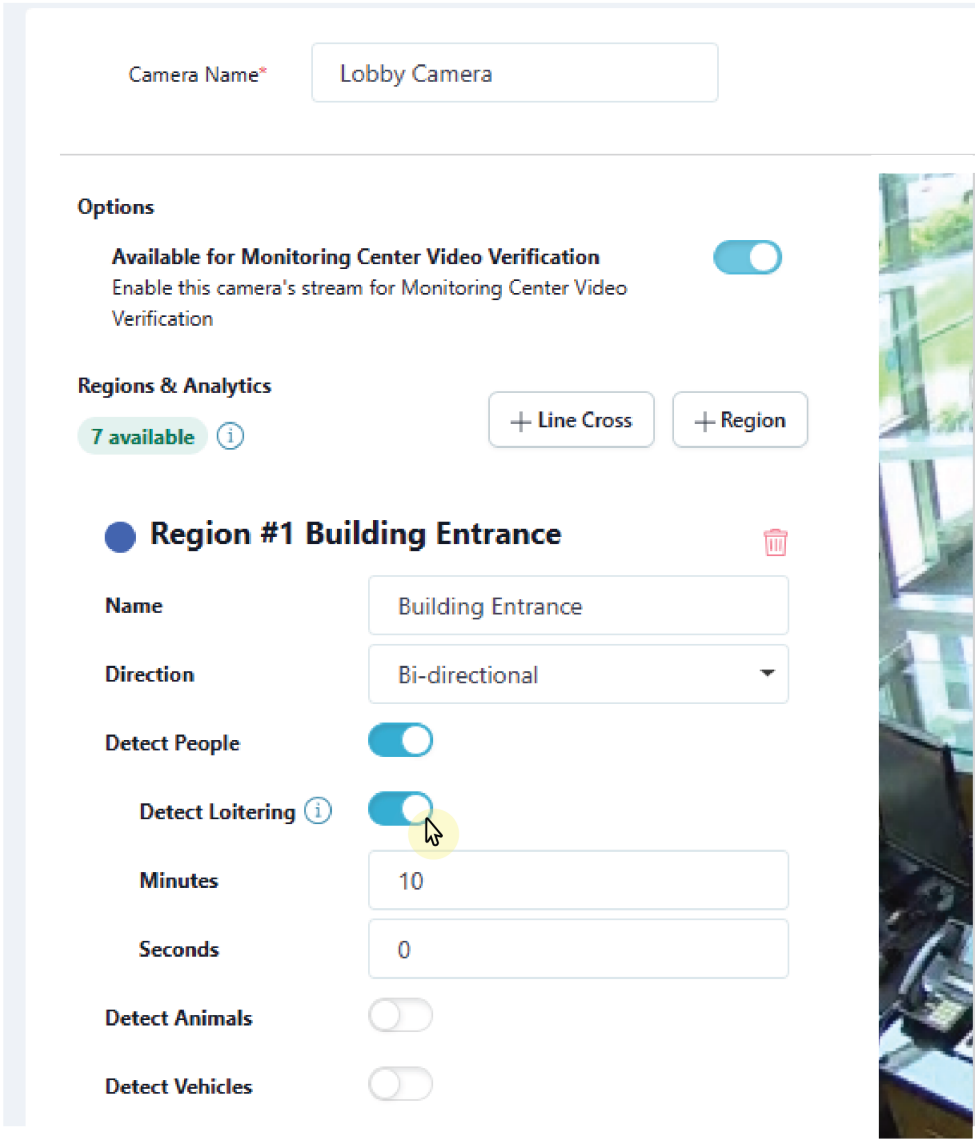

7. In the **Direction** drop-down menu, select one of the following directions if you want to monitor if a person, animal, or vehicle moves in a direction that is a part of a programmed region:
   - **Enter**—Motion has to cross into the detected region, following the arrows pointing inward.
   - **Exit**—Motion has to cross out of the detected region, following the arrows pointing outward.
   - **Bi-Directional**—Motion can cross the box in any direction.



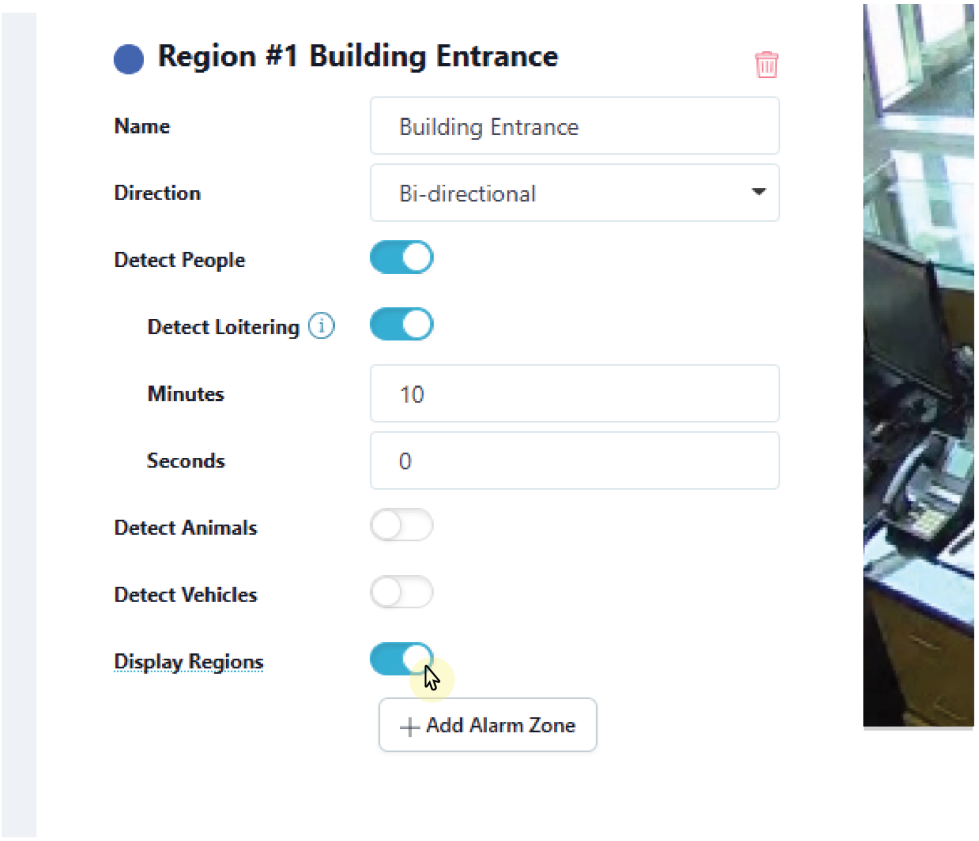

8. Select whether you want the region to detect **People**, **Animals**, **Vehicles**, or any combination of the three.



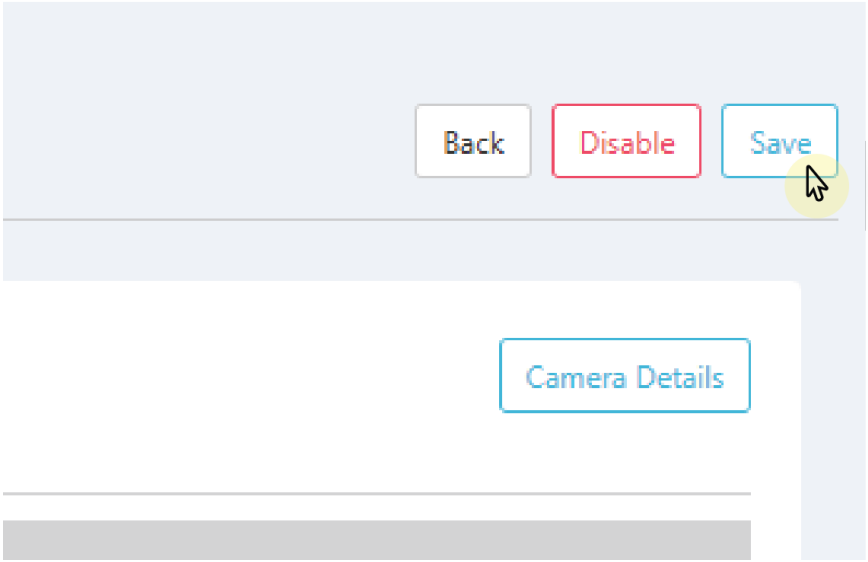
9. If you selected **People** or **Vehicles**, select whether you want the region to detect **Loitering**. Enter a number of minutes, seconds, or both to dictate the amount of time required before the loitering alert is triggered.




10. Select **Display Regions** if you want the configured detection regions to show up on event previews in Virtual Keypad.




11. To add additional regions, repeat steps 1-10 or select **Save** to apply changes and exit the **Edit Camera** page. This saves the detection regions and any camera adjustments made previously. To create a camera alarm zone for added regions, refer to Create a Camera Alarm Zone for more information.

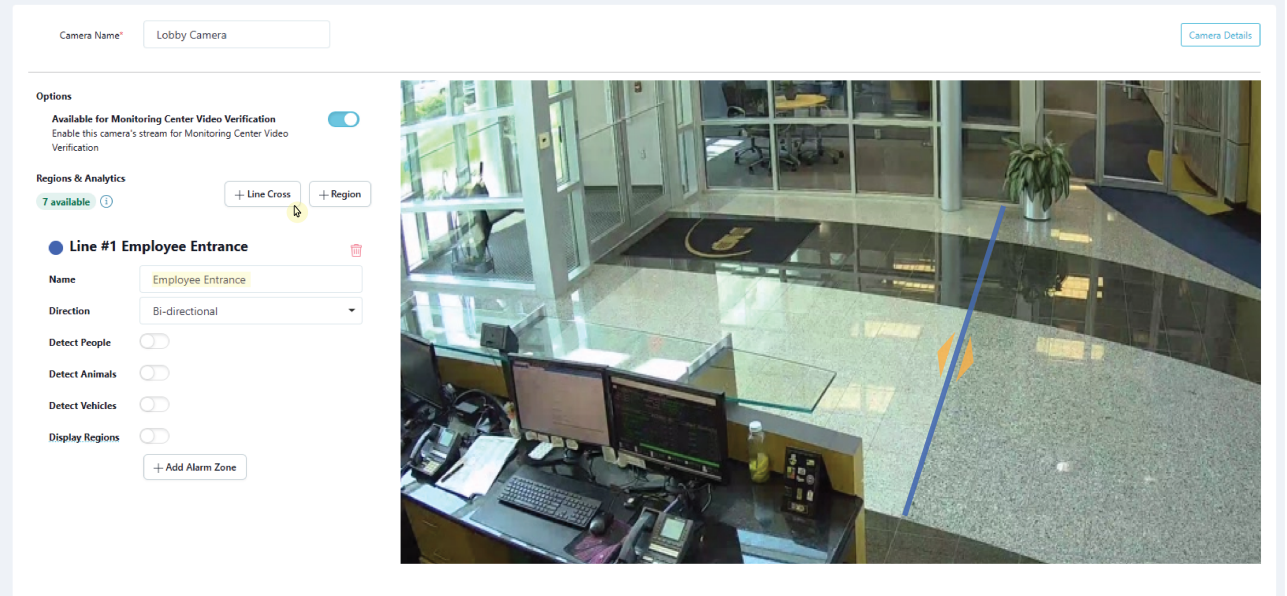



13. To configure end user settings, refer to Virtual Keypad Setup for more information.

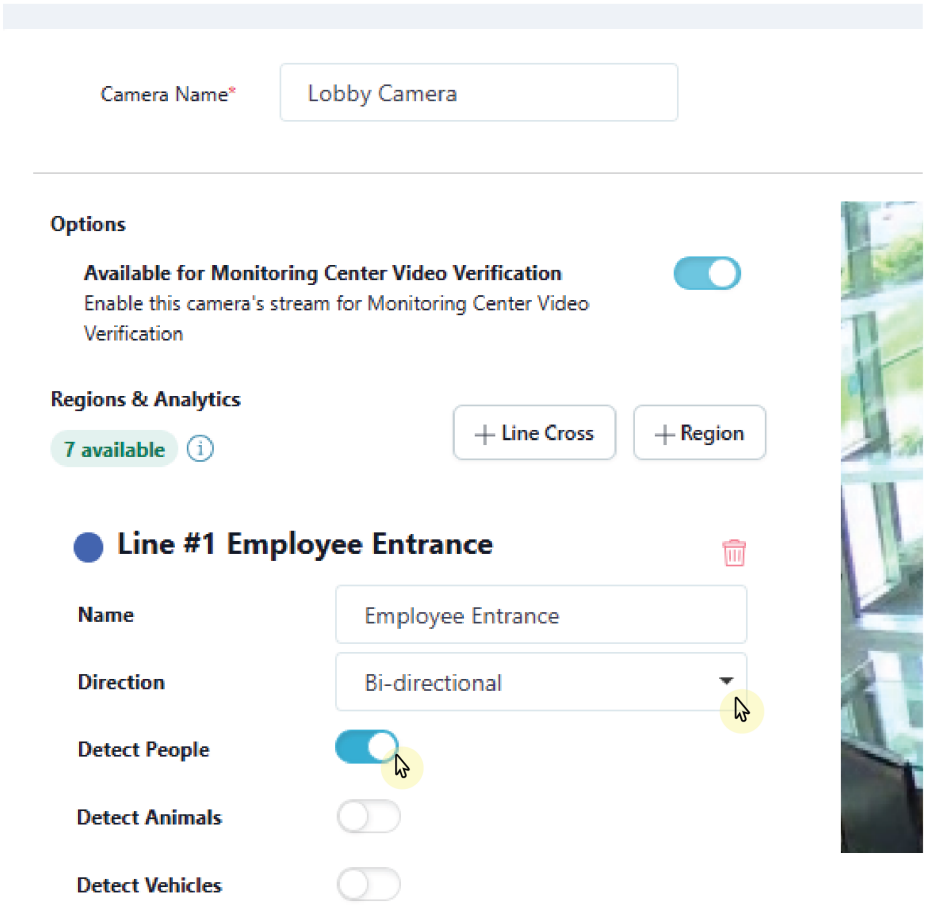
**Create a Line**

1. Log in to Dealer Admin (dealer.securecomwireless.com).
2. Go to **Customers**, then select the **System Name** that the XV Gateway and camera are connected to.
3. In **Video**, go to **Cameras** and select the camera name you want to create a line for.

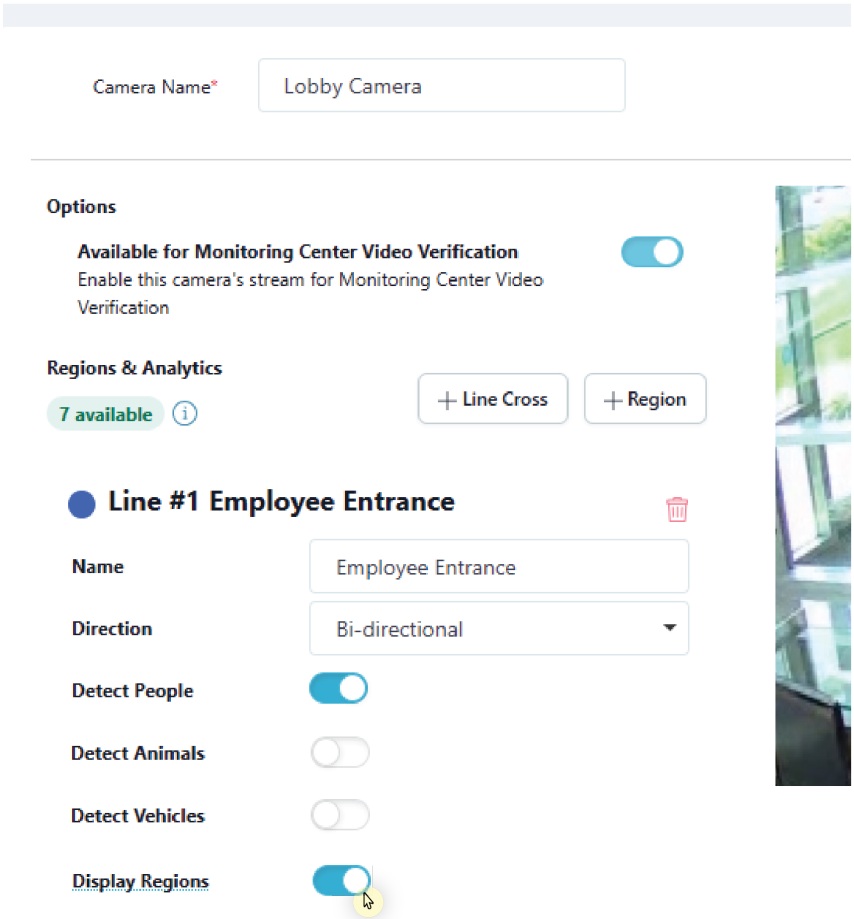
4. In the **Edit Camera** page, go to **Regions & Analytics** and select **+ Line Cross**. A line appears in the middle of the camera view screen.
5. Select and drag the line on the camera's field of view to define the desired detection line.
6. Give the line a **Name**.



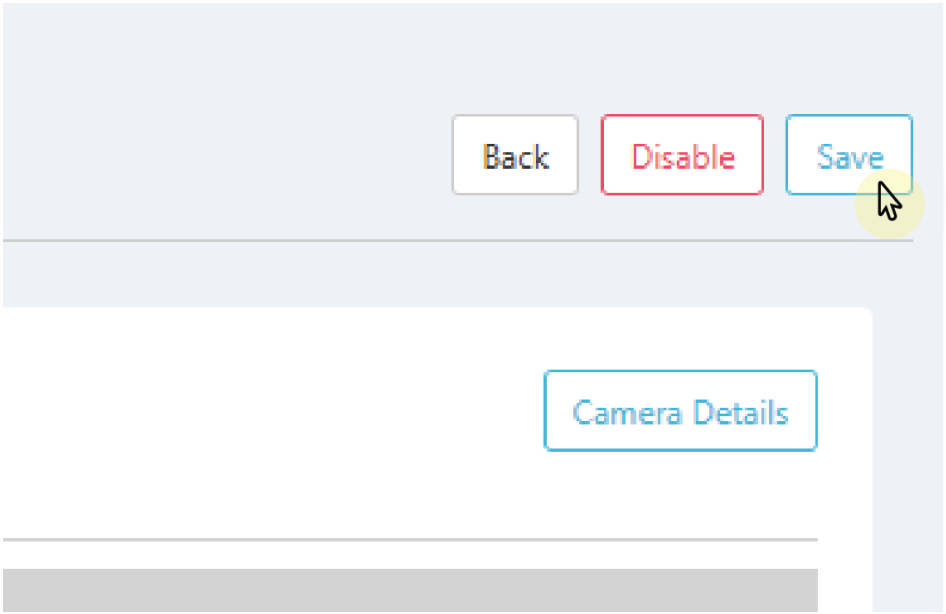

7. In the drop-down menu, select one of the following directions to monitor if a person, animal, or vehicle moves in a direction that is a part of a programmed region:
    - **Enter**—Motion has to cross the line in the direction of the arrow.
    - **Exit**—Motion has to cross the line in the direction of the arrow.
    - **Bi-directional**—Motion can cross the line in either direction.




8. Select **Display Regions** if you want the configured detection lines to show up on event previews in Virtual Keypad.



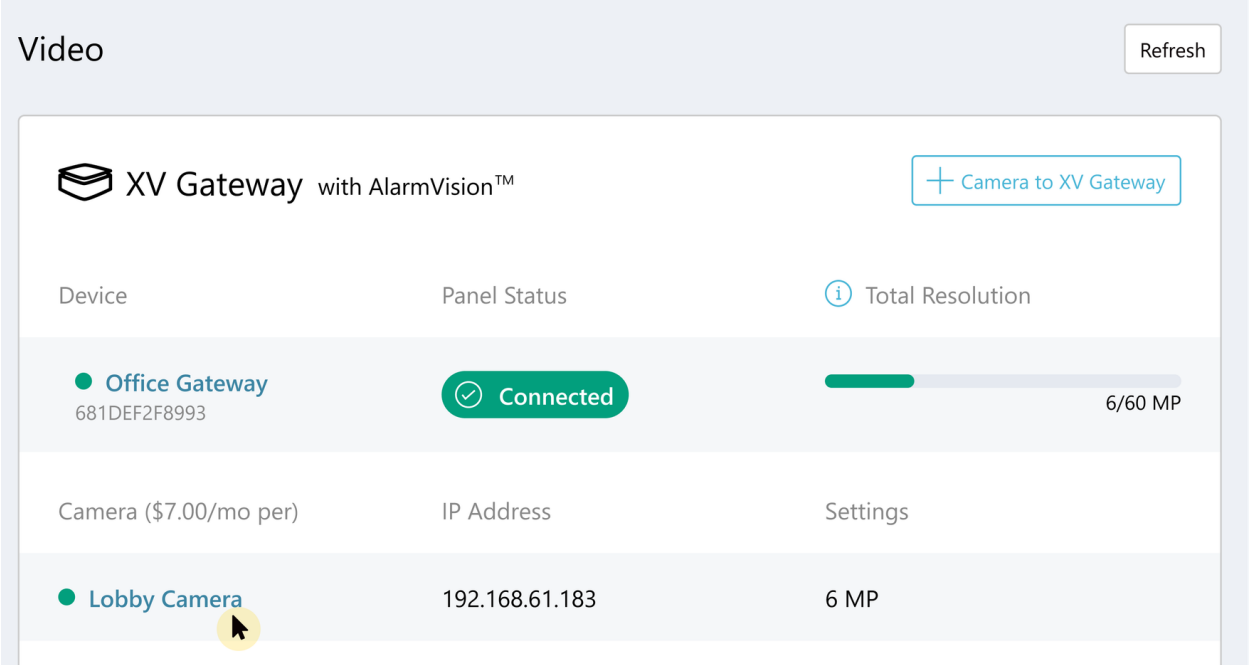

9. To add additional line crosses, repeat steps 1-8. Select **Save** to apply changes and exit the **Edit Camera** page. This saves the line crosses and any camera adjustments made previously. To create a camera alarm zone for added regions, refer to Create a Camera Alarm Zone for more information.



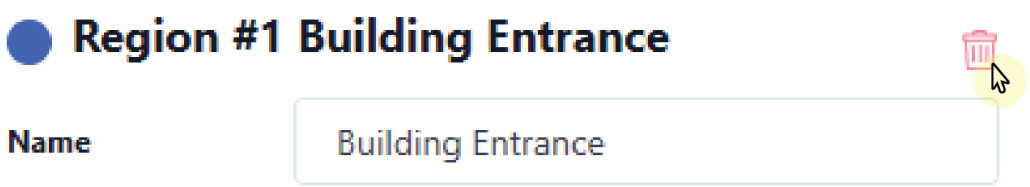

10. To configure end user settings, refer to Virtual Keypad Setup for more information.

**Delete a Detection Region or Line**

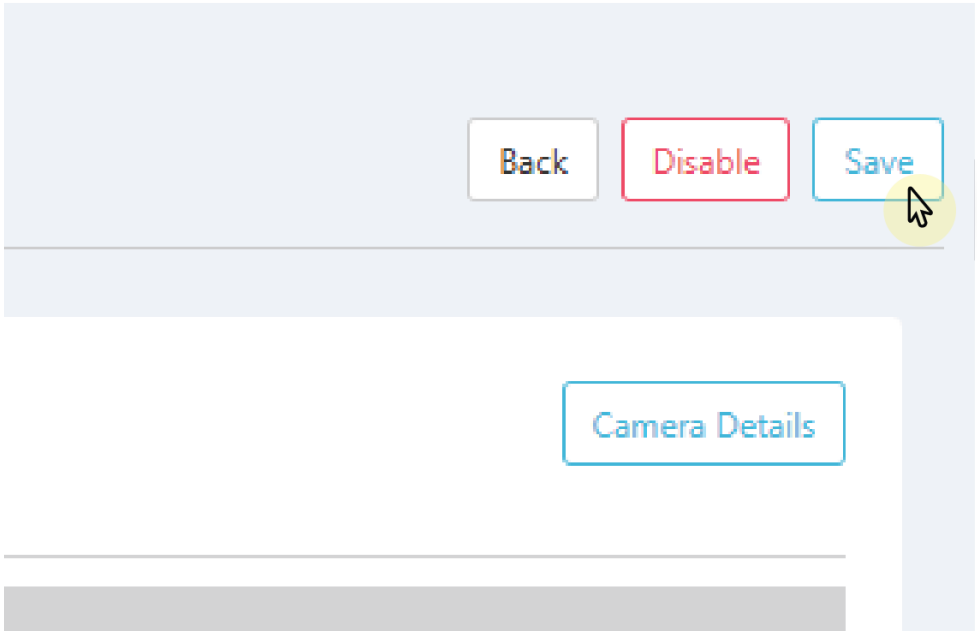
1. Log in to Dealer Admin (dealer.securecomwireless.com).
2. Go to **Customers**, then select the **System Name** that the XV Gateway and camera are connected to.
3. In **Video**, go to **Cameras** and select the camera that is tied to the detection region or line.




4. Select the **Trash Can** icon next to the name of the detection region or line.




5. Select **Save**. This deletes the detection region or line and any zone tied to it.

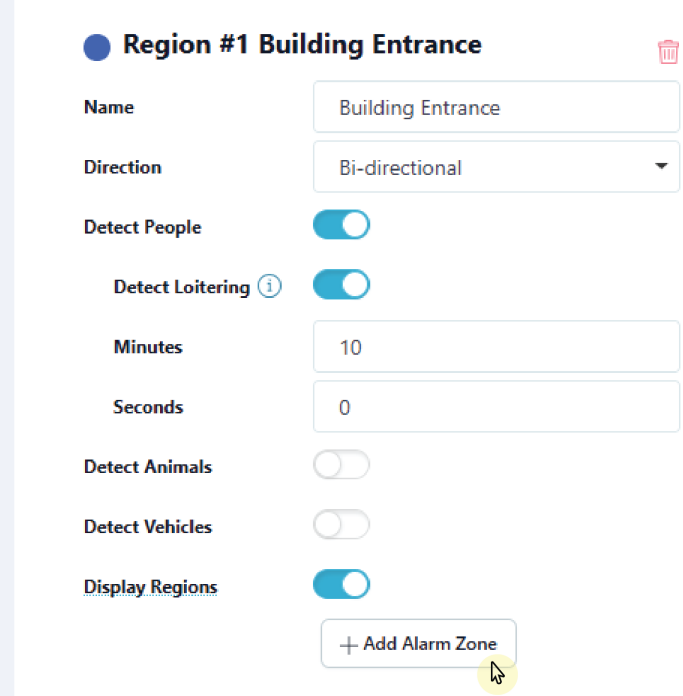



**Create an AlarmVision Zone for Regions and Lines**

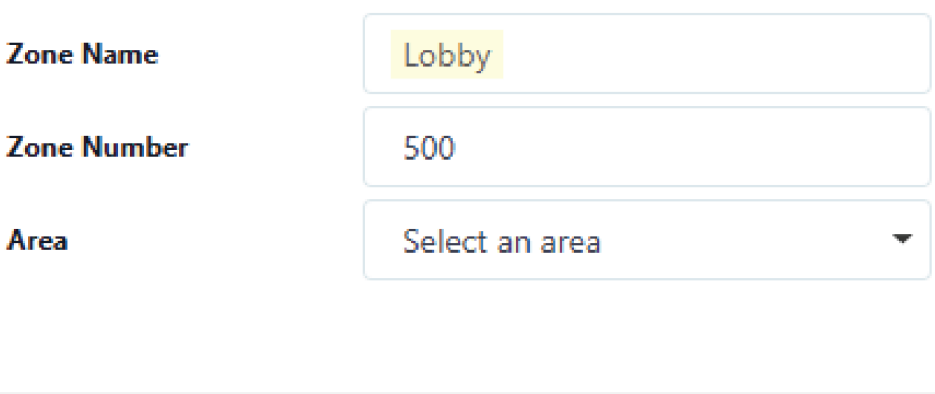
**Note**: If you want to delete an AlarmVision zone tied to a region or line, do not delete the zone in **Zone Information**. If you attempt to delete a zone this way, a message appears that states the panel's detection region will not properly communicate with the panel.
To delete an AlarmVision zone, delete the region or line tied to it. For more information, refer to Delete a Detection Region or Line.

1. Log in to Dealer Admin (dealer.securecomwireless.com).
2. Go to **Customers**, then select the **System Name** that is associated with the XV Gateway.
3. In **Video**, go to **Cameras** and select the camera name you want to create an alarm zone for.
4. In the **Edit Camera** page, go to **Regions & Analytics** and locate the detection line or region you want to create an AlarmVision zone for. If you have not created a Region or Line, refer to Add Regions & Analytics for more information.
5. Select **+ Add Alarm Zone**.

**Note:** All zones are programmed as a **Night Zone** by default. To edit zone programming, refer to Edit Zones.

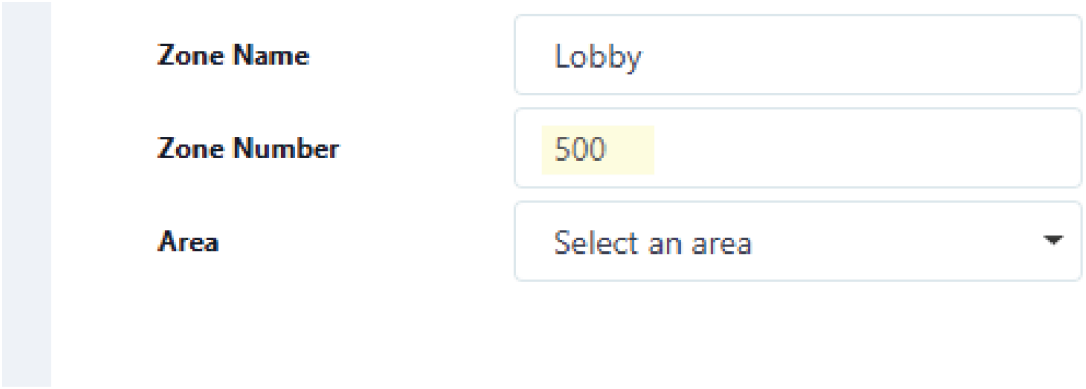



6. Give the zone a **Name**.

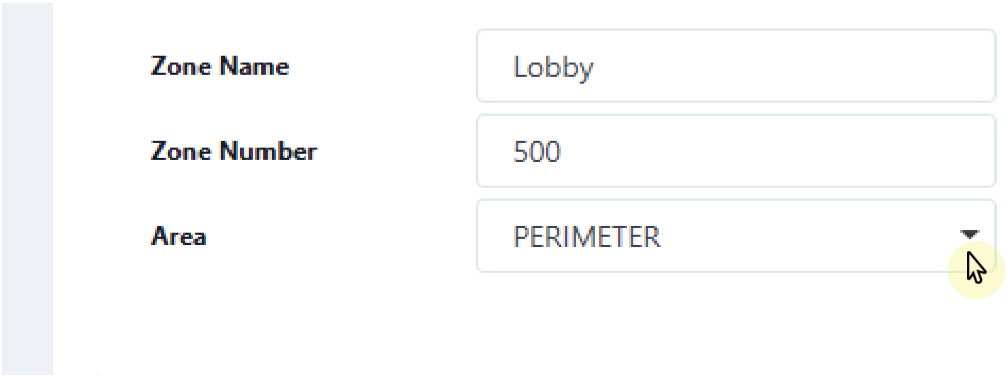



7. The zone number automatically populates with the next available zone number in panel. If desired, you can assign a different zone number. Usable zones are 500-999 for XR Series Control Panels and 500-599 for XT75 Control Panels.

**Note:** Zones cannot be assigned to an AX-Bus.

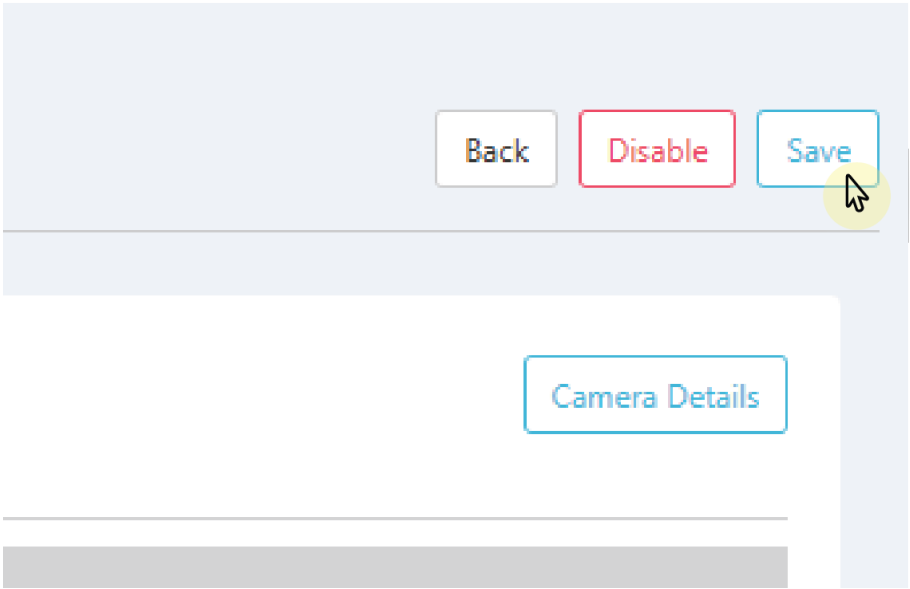



8. Assign the zone to an **Area** by selecting the drop-down menu.




**Note:** If any camera detection region or line is tied to a panel zone, then all detections for that camera only record when the zone is armed and has been tripped.

9. To add additional AlarmVision zones, repeat steps 1-8. Select **Save** to apply changes and exit the **Edit Camera** page. This saves the detection regions, lines, and any zones tied to them, as well as any camera adjustments made previously.



## 22.5.5 Use 2-Way Audio

> **Note**: Ensure **Monitoring Center Verification** is enabled before using 2-Way Audio. Refer to Enable Monitoring Center Verification for more information.

Installing and configuring an ONVIF compliant IP-based audio device with an XV Camera connected to an XV Gateway allows an operator to communicate live audio broadcast or pre-recorded audio messages to the area the audio devices are located in.

A pre-recorded audio message can be set to automatically play if a person, vehicle, or animal is detected in a specified region. Inbound audio can be received from the site if the configured camera or speaker supports a microphone.

The following pre-recorded audio messages can be communicated to the area the audio devices are located in:

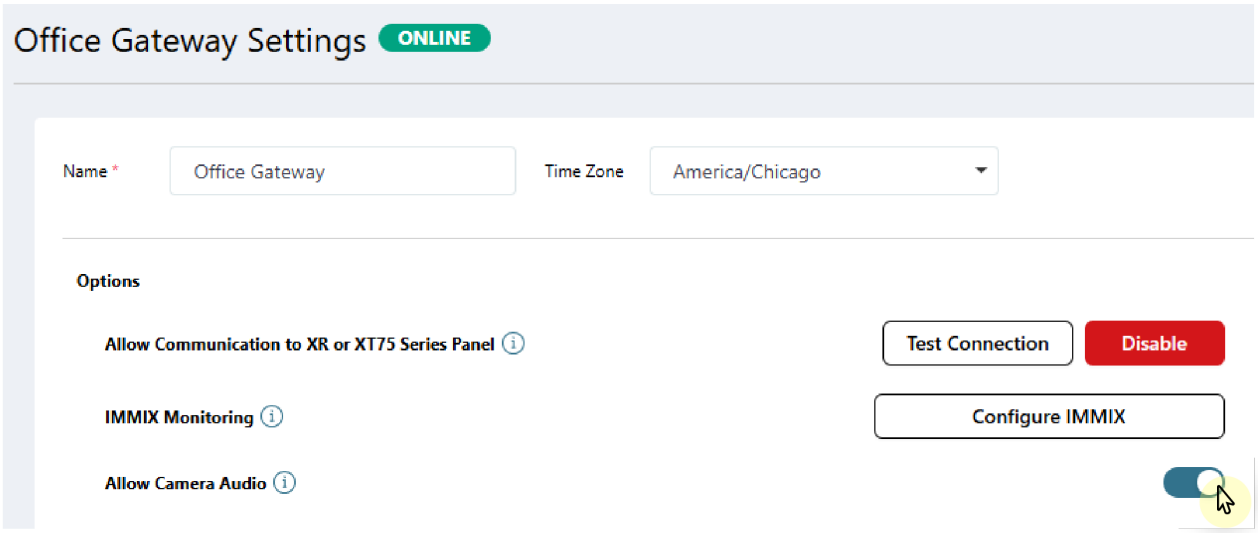
- **Trespassing Warning —** "You are trespassing, please leave the area. This area is under video surveillance, and you have been recorded."
- **Loitering Warning —** "You are loitering in an unauthorized area. Please leave immediately or the police will be contacted."
- **Generic Instruction —** "Warning, you are under video surveillance. Please leave the area immediately."
- **Emergency Warning —** "Attention: please evacuate the area immediately."
- **Speaker Test —** "This is a test of an audio device. If you can hear this message, you are being audio and video recorded. This is a test of an audio device."

> **Note:** The **Speaker Test** audio message is unavailable for video verification and only plays when **Test Audio** is selected in the camera settings. Refer to Test Speaker Audio for more information.

### Add 2-Way Audio Devices

To use 2-Way Audio, at least one ONVIF compliant IP-based audio device and one XV Camera should be added to the XV Gateway. To add the necessary devices for 2-Way Audio, complete the following steps:

1. Log into Dealer Admin (dealer.securecomwireless.com).
2. Go to **Customers**, and select the **System Name** the XV Gateway is associated with.
3. Go to **Video**, then select **+ Devices to XV Gateway**.
4. Add any cameras or audio devices needed for 2-Way Audio. To learn how to add and edit devices on an XV Gateway, refer to Add Devices to the XV Gateway.
5. Once all necessary devices are added, go to **Video**, then select the name of the XV Gateway associated with the 2-Way audio devices.
6. In **XV Gateway Settings**, go to **Options** and toggle **Allow Camera Audio** ON.




7. A the top of the screen, select **Save**. Refer to the steps below to learn how to test a speaker's audio.

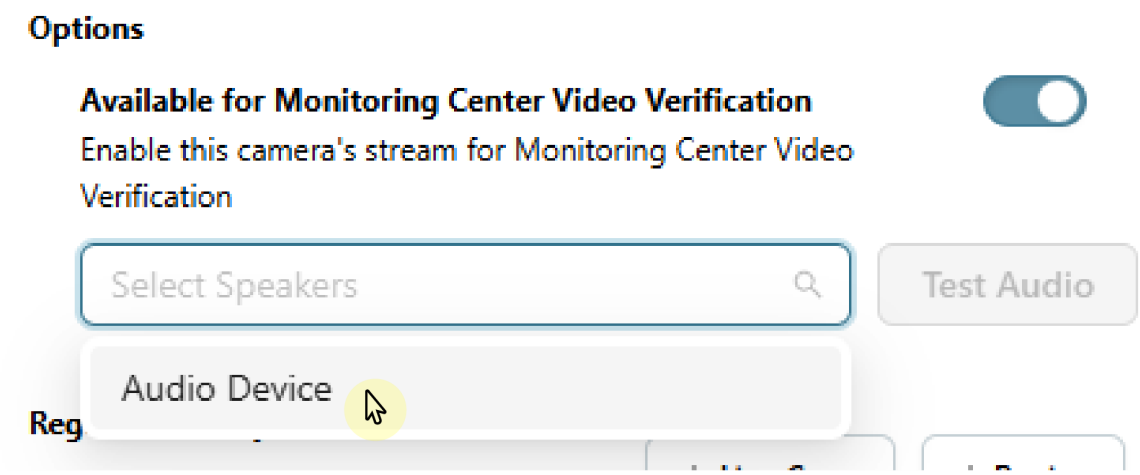
## Test Speaker Audio

Once you've added the necessary devices for 2-Way audio, follow these steps to test the speaker audio associated with the camera:

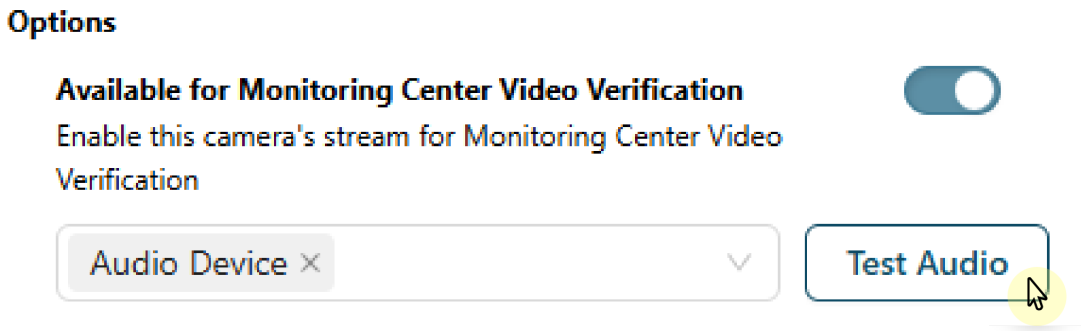
1. Log into Dealer Admin (dealer.securecomwireless.com).
2. Go to **Customers**, and select the **System Name** the XV Gateway is associated with.
3. Go to **Video**, then select the name of the camera associated with the system to access the camera settings.
4. In **Options**, locate **Available for Monitoring Center Video Verification** and confirm it is toggled **ON**.

**Note**: If **Available for Monitoring Center Video Verification** does not display, ensure the feature is enabled. Refer to Enable Monitoring Center Video Verification for more information.

5. In the **Select Speakers** drop-down menu below, select the audio device you want to associate with the camera.



6. Select **Test Audio** to confirm the appropriate devices have been selected. An audio message plays the following message through all speakers associated to the camera: “This is a test of an audio device. If you can hear this message, you are being audio and video recorded. This is a test of an audio device.”




7. Select **Save** or refer to the steps below to learn how to set an automatic audio clip.

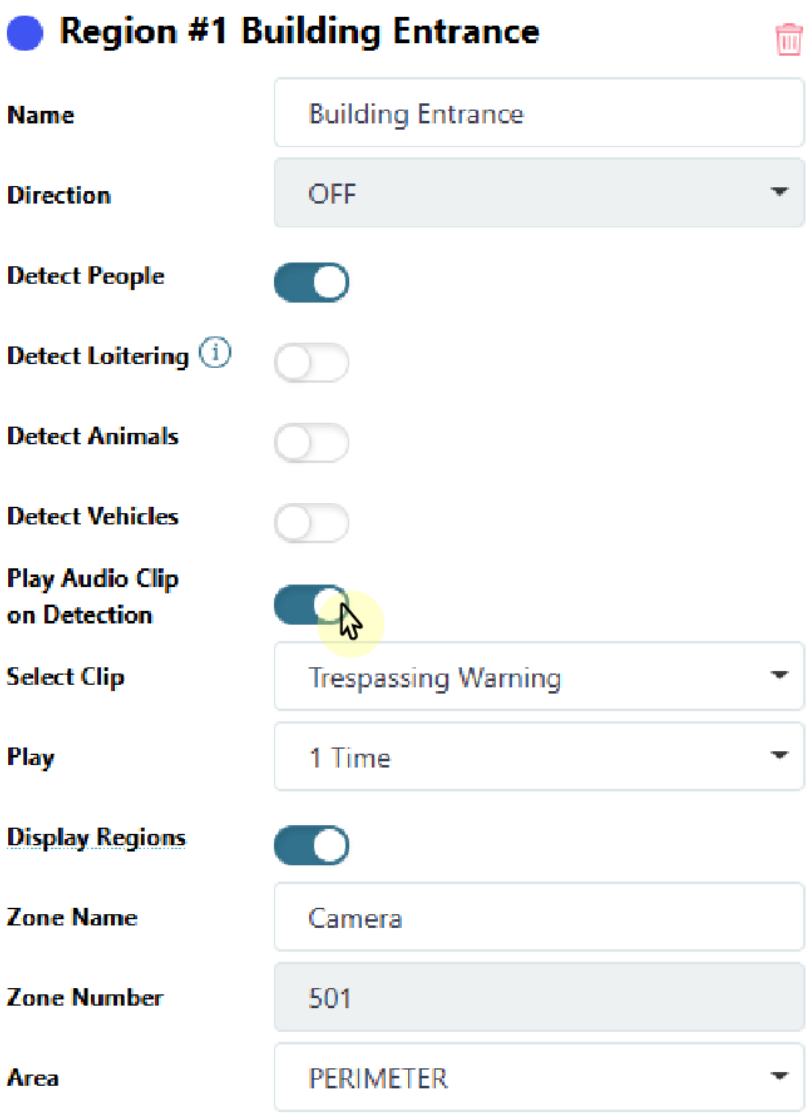
## Set Automatic Audio Clip

**Note**: If **Play Audio Clip on Detection** does not display, ensure **Allow Camera Audio** is enabled. Refer to Add 2-Way Audio devices for more information.

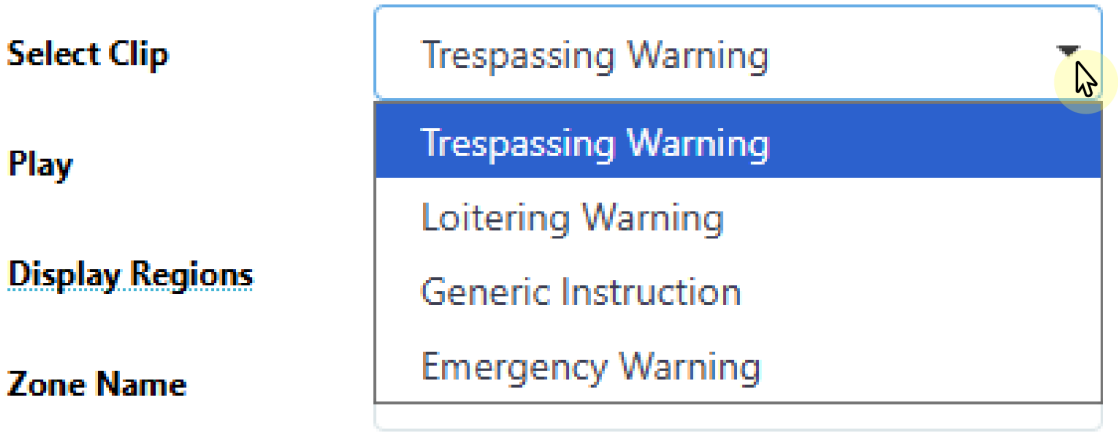
To set an audio clip to play automatically upon detection in a specific region, follow these steps:

1. Log into Dealer Admin (dealer.securecomwireless.com).
2. Go to **Customers**, and select the **System Name** the XV Gateway is associated with.
3. Go to **Video**, then select the name of the camera associated with the system to access the camera settings.
4. In **Regions & Analytics**, find the region or line that you want the audio clip to play for when an armed zone is tripped. For more information about how to create a region, line, or camera alarm zone, refer to Add Regions and Analytics Settings and Create a Camera Alarm Zone.
5. Toggle **Play Audio Clip on Detection** ON.

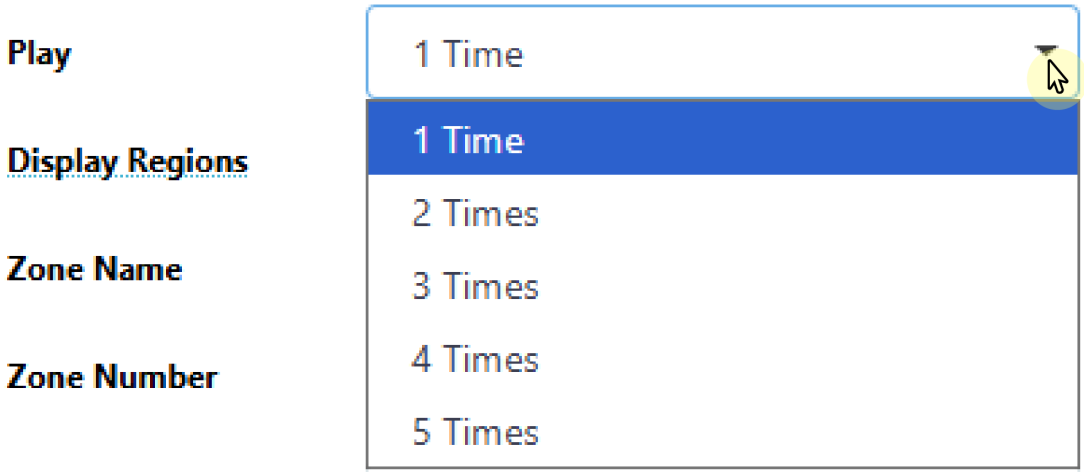
**Note**: The audio clip feature is unavailable for line crossing and for regions with a set direction. If you have a direction tied to a region or line, **Play Audio Clip on Detection** does not display.




6. Select the drop-down box next to **Select Clip** to set the audio clip that plays upon detection.



7. Select the drop-down box next to **Play** to set the number of times the clip plays. You can set the clip to play up to five times.




8. Select **Save** to apply the changes. Once a detection has been triggered, the alarm sounds and the audio clip plays. If there are multiple detections, the clip plays for each detection.

## 22.5.6 Use IMMIX Monitoring

Prior to enabling the IMMIX integration, ensure the inbound and outbound connections listed below are properly configured.

### Inbound (Forwarded from the IMMIX IP Address to the XV Gateway)

**HTTPS:** TCP/443

- Used by IMMIX to gather camera and alert information from the XV Gateway

**RTSP:** TCP/554 and UDP/554

- Video streaming from XV Gateway to IMMIX

**Source:** Hostname provided by your IMMIX provider

### Outbound

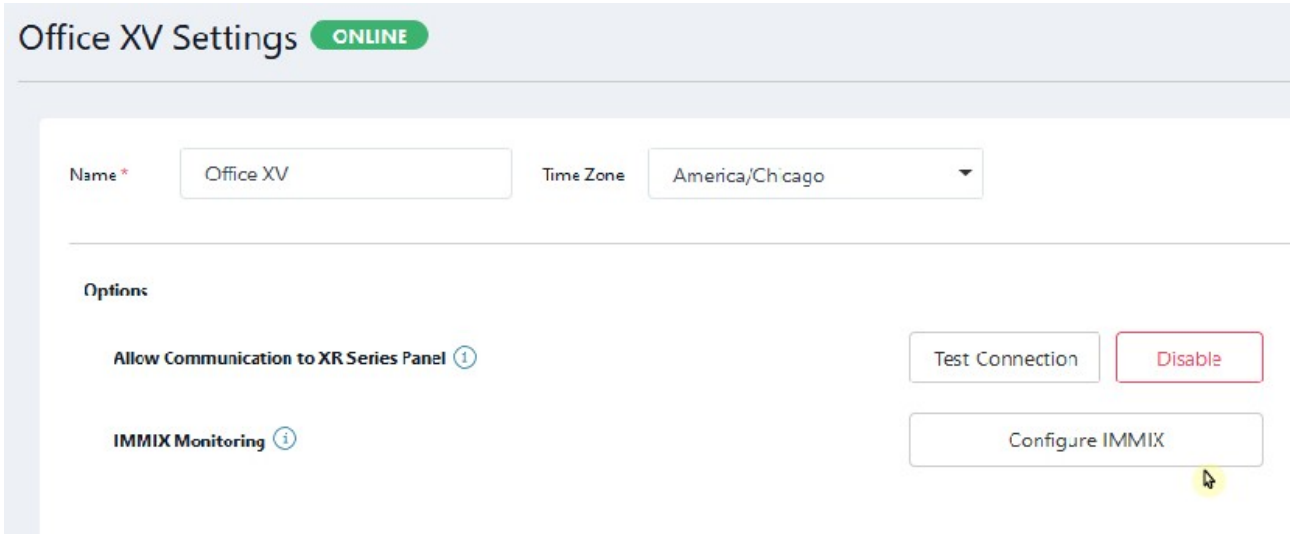
- **SMTP:** TCP/25
  - Alerts from XV Gateway to IMMIX
  - If your ISP blocks port 25, try port 1025.
  - If port 1025 is also blocked, contact your ISP
- **Destination:** Same address used in the SMTP Server field in **Dealer Admin Final Setup**

### Enable IMMIX Monitoring with the XV Gateway

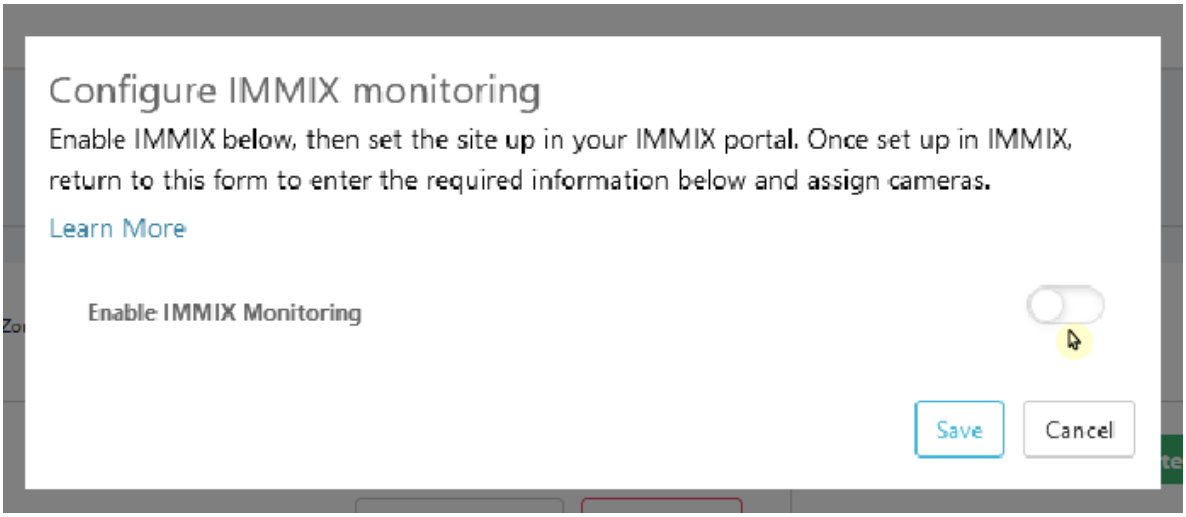
> **Note:** Ensure all devices are added to the XV Gateway before adding it to your IMMIX account. Refer to Add Devices to the XV Gateway for more information.

1. Log in to Dealer Admin (dealer.securecomwireless.com).
2. Go to **Customers**, then select the **System Name** that the XV Gateway is connected to.
3. At **Video**, select the name of the XV Gateway.
4. In **XV Gateway Settings**, select **Configure IMMIX**.

**Note**: If **Configure IMMIX Monitoring** does not display, ensure the **Monitoring Center Video Verification** feature is enabled. Refer to Enable Monitoring Center Video Verification for more information.



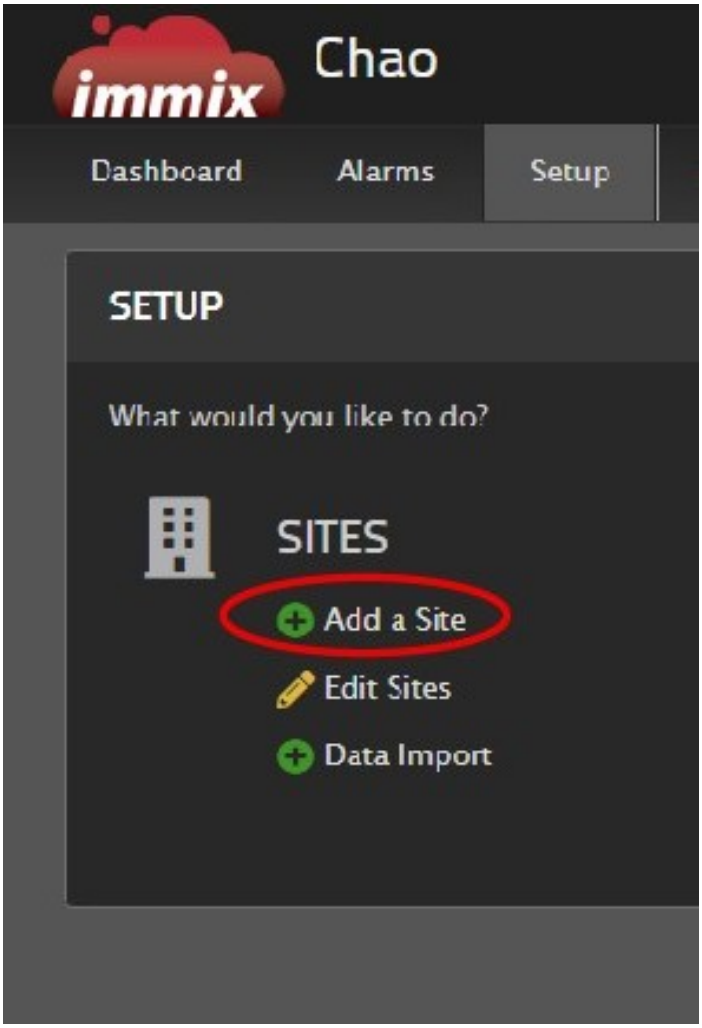

4. Toggle **Enable IMMIX Monitoring** ON.



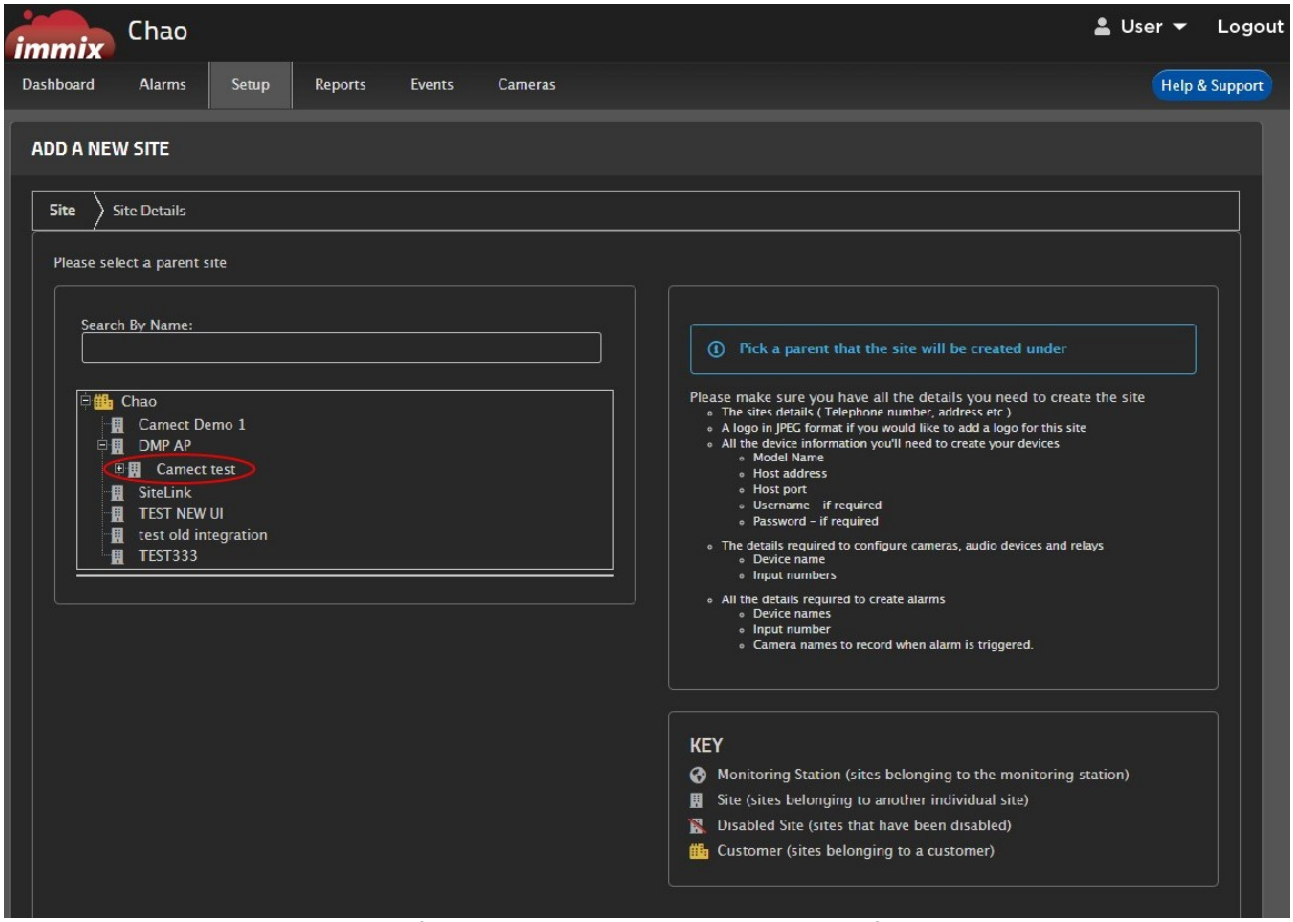

5. Keep the IMMIX pop-up open on Dealer Admin and refer to the the steps below to setup the XV Gateway with IMMIX.

**Setup the XV Gateway with IMMIX**

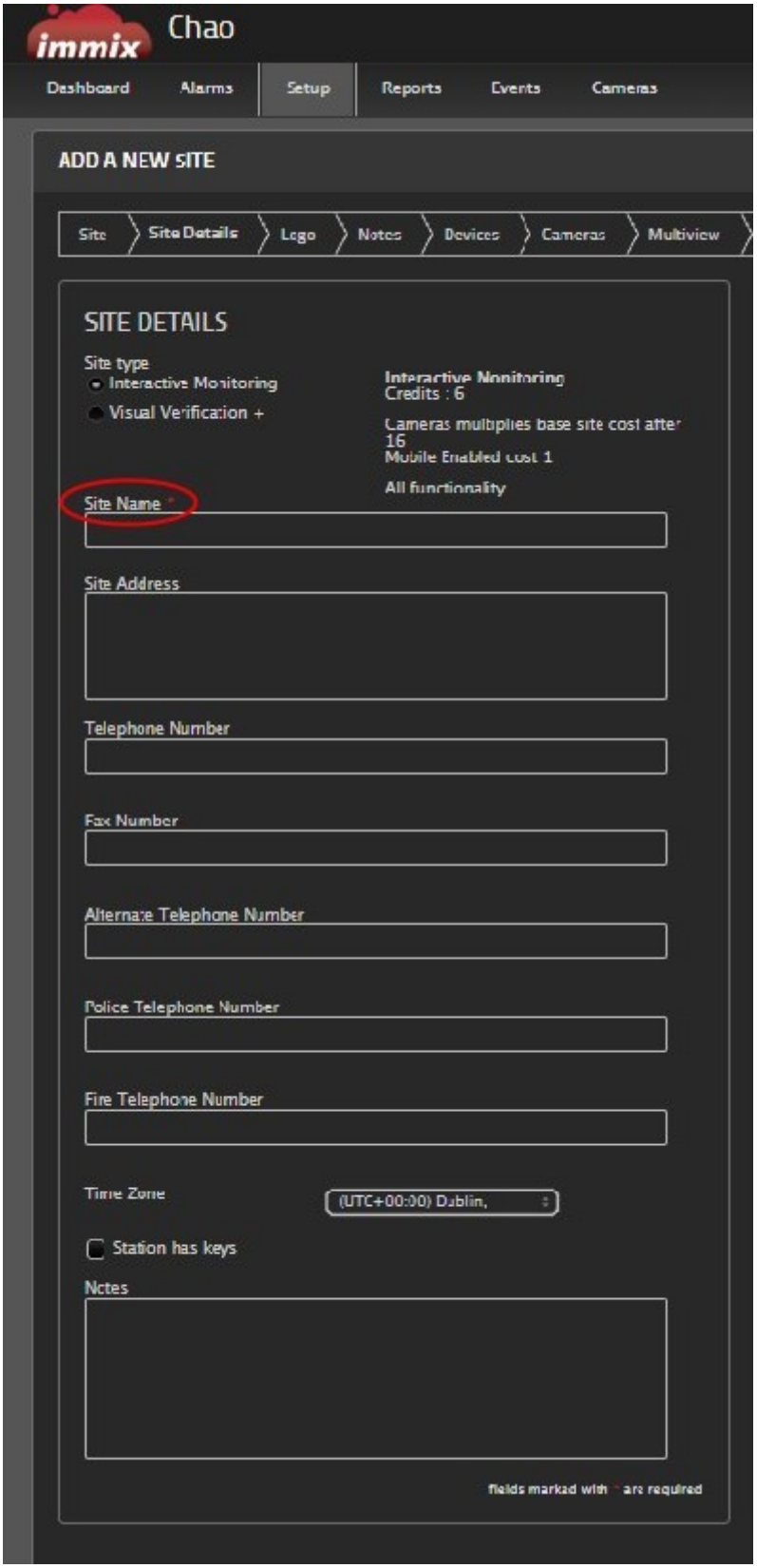
1. Log in to IMMIX (camect.immixcs.net/)
2. At the top of the screen, select **Setup,** then select **Add a Site**.



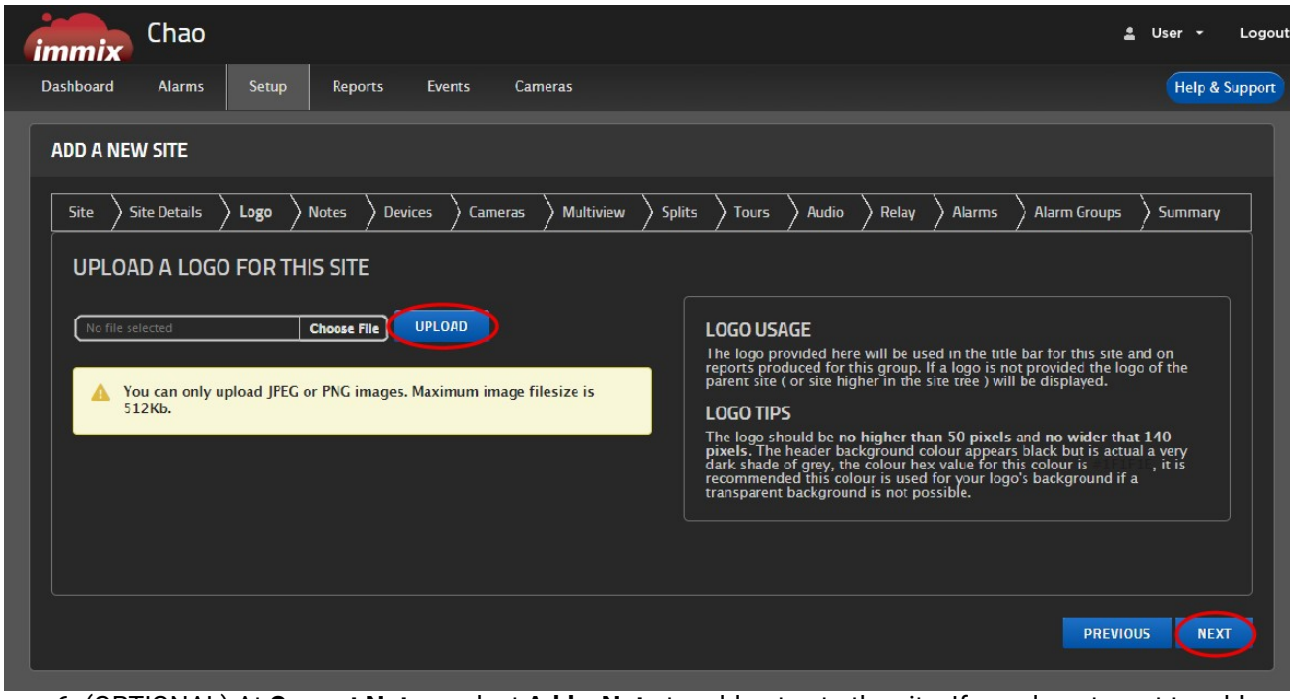

3. In **Site Details**, select a parent site that the site is created under.



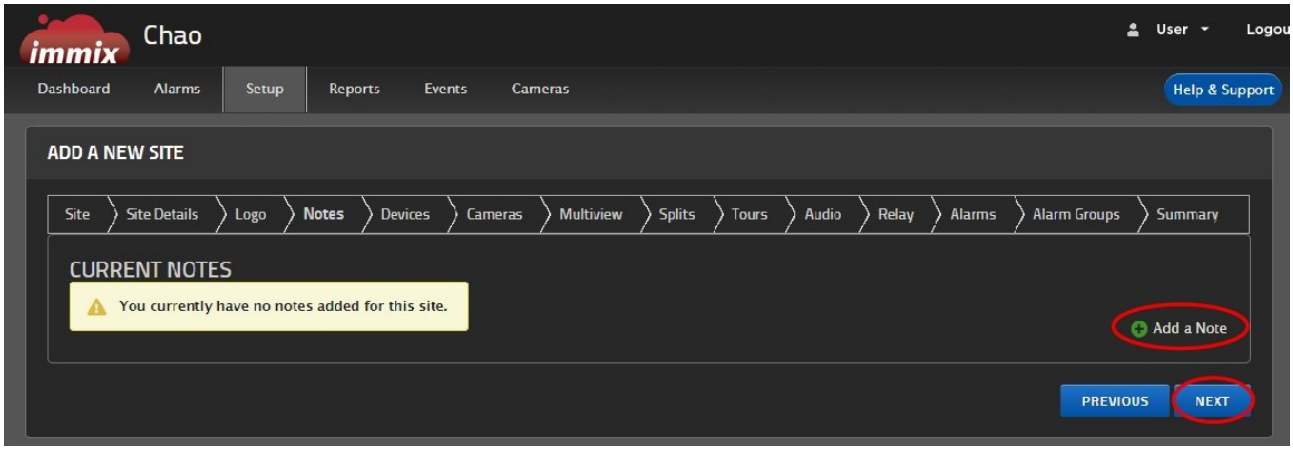

4. At **Site Details**, add a **Name** for the site along with any additional information. Then, select **Next**.


immix
Chao
Dashboard
Alarms
Setup
Reports
Events
Cameras
ADD A NEW SITE
Site
Site Details
Logo
Notes
Devices
Cameras
Multiview
SITE DETAILS
Site type
Interactive Monitoring
Visual Verification +
Interactive Monitoring
Credits : 6
Cameras multiplies base site cost after 16
Mobile Enabled cost 1
All functionality
Site Name *
Site Address
Telephone Number
Fax Number
Alternate Telephone Number
Police Telephone Number
Fire Telephone Number
Time Zone
(UTC+00:00) Dublin,
Station has keys
Notes
fields marked with * are required

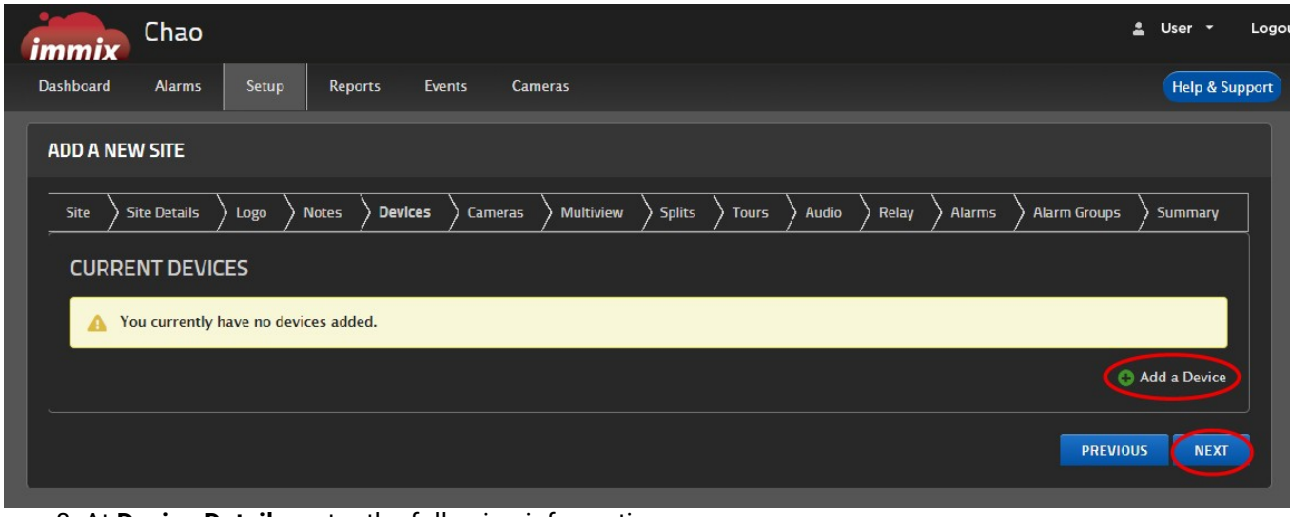

5. (OPTIONAL) At **Upload a Logo For This Site**, select **Upload** to add a logo. If you do not want to upload a logo, select **Next**.



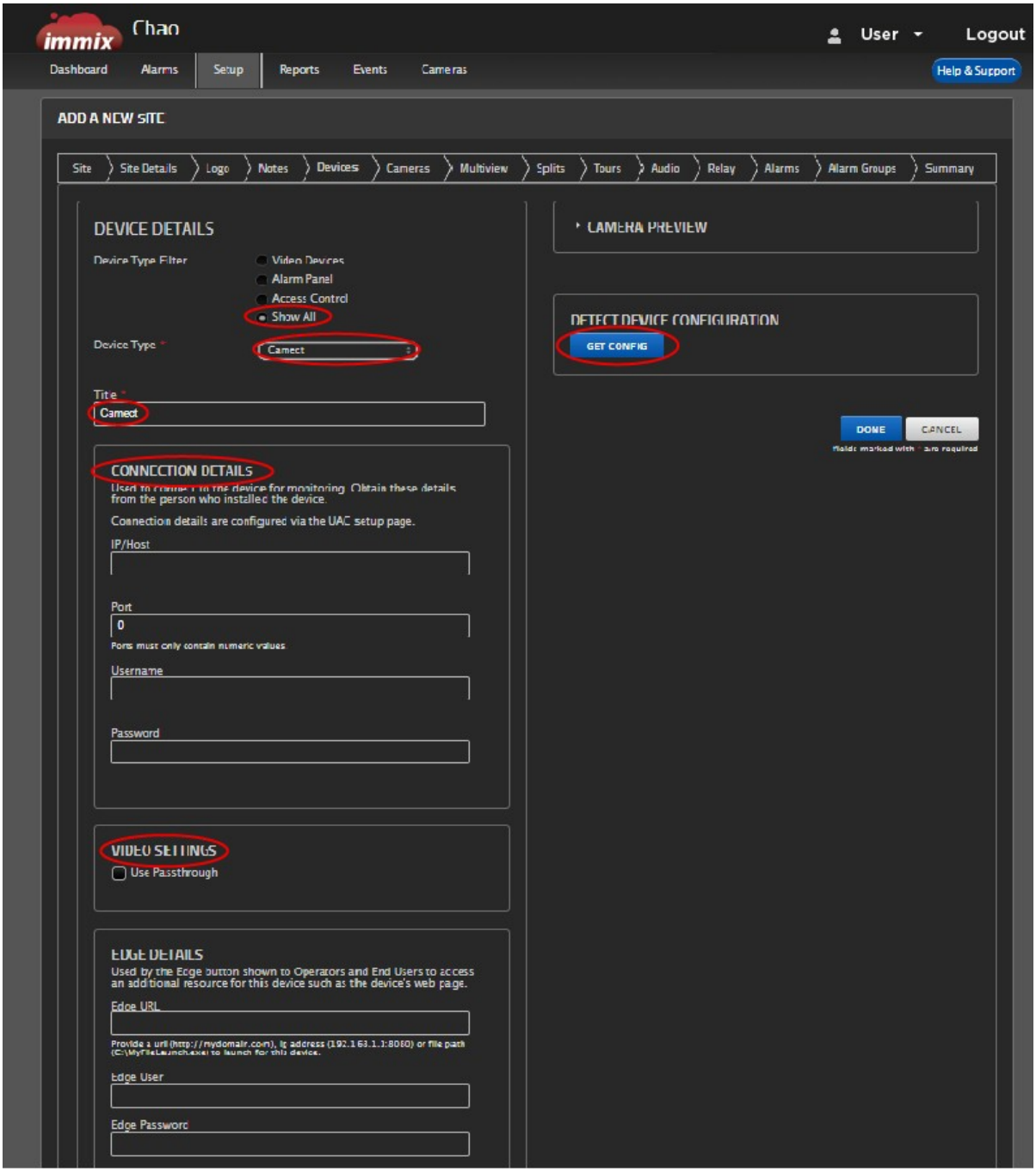

6. (OPTIONAL) At **Current Notes**, select **Add a Note** to add notes to the site. If you do not want to add notes, select **Next**.




7. At **Current Devices**, select **Add a Device**.




8. At **Device Details**, enter the following information.
    - At **Device Type Filter**, select **Show All**.
    - At **Device Type**, use the drop-down menu to select **Camect**.
    - Give the device a **Title**.
    - At **IP/Host**, enter the **WAN** your gateway is connected to.
    - At **Port**, enter **443**.
    - At **Username**, enter **immix**.
    - At **Password**, enter the **MAC Address**.
    - At **Video Settings**, select the **Use Passthrough** checkbox.
    - On the right side of the screen, select **Get Config**. This finds gateway and all of the devices connected to it. Once it has been connected, select **Done**.

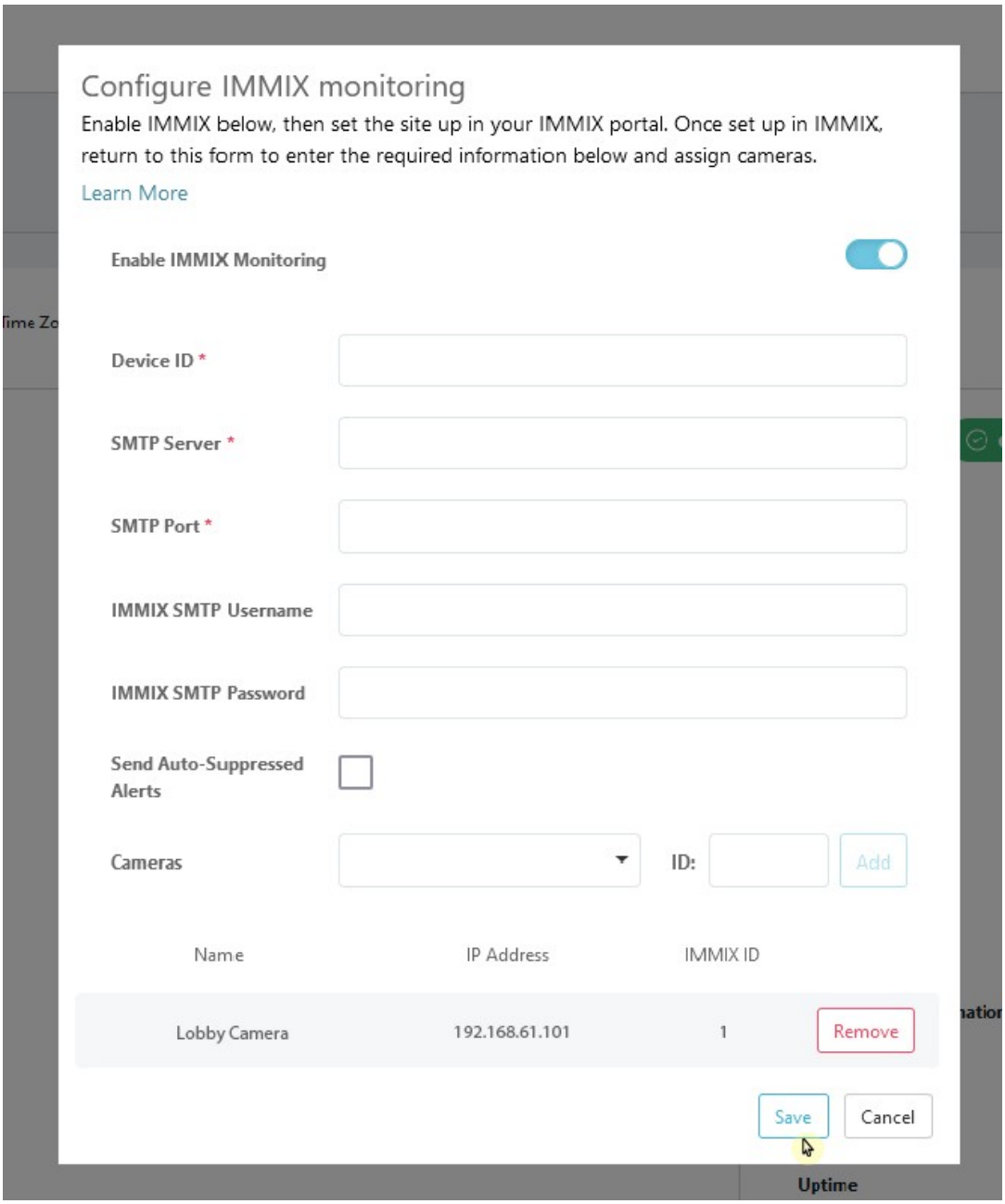



9. Navigate to the **Summary** tab. This includes additional information needed to configure the integration in Dealer Admin.
10. Keep the **Summary** tab open and navigate back to Dealer Admin.

### Configure IMMIX Monitoring on Dealer Admin

1. Use the **Summary** tab in IMMIX to enter the following information in the **Configure IMMIX Monitoring** pop-up in Dealer Admin:
    - **Device ID** (Identifier in IMMIX)
    - **SMTP Server** (SMTP Server Address based on your IMMIX provider)
    - **SMTP Port** (set to **25**)

2. (OPTIONAL) At **IMMIX SMTP Username** and **IMMIX SMTP Password**, enter a username and password for the IMMIX integration.
3. (OPTIONAL) Check the **Send Auto-Suppressed Alerts** checkbox.
4. At **Cameras**, select the drop-down menu to select your camera. Then, add the **ID** that matches what appears in IMMIX for that camera.
5. Select **Save**.




6. Test the connection between the XV Gateway and the Monitoring Center by triggering alarms and ensuring live video and events are being sent.

## 22.5.7 Use Virtual Keypad with an XV Gateway

You can use Virtual Keypad features to monitor cameras connected to the XV Gateway, including customizing the video feed page, viewing video events, creating triggered video actions, and more. Before a user can monitor camera feeds, ensure they are added as a Virtual Keypad App users on Dealer Admin.

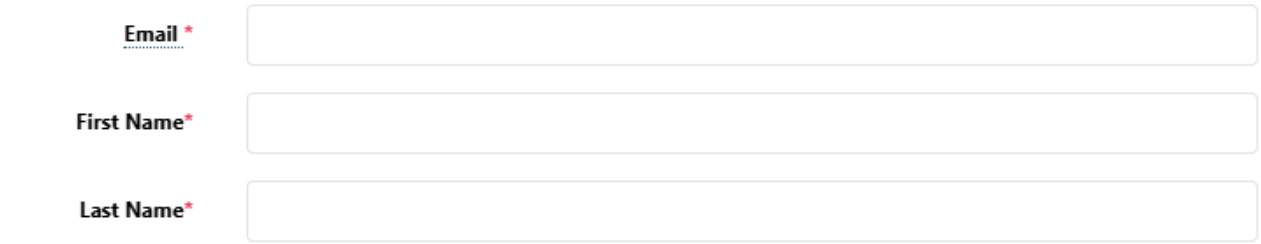
Refer to the following pages for more information about setting up Virtual Keypad with an XV Gateway:

- Add Virtual Keypad App Users
- Enable Video Access to Technicians and Dealers
- Enable Push Notifications
- Customize Video Page
- View Video Events

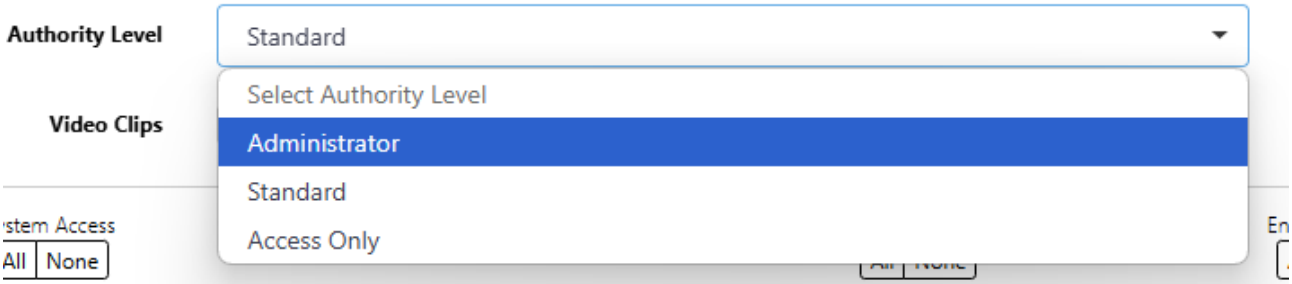
### Add Virtual Keypad App Users

1. Log in to Dealer Admin (dealer.securecomwireless.com)
2. Go to **Customers** and select the customer's name associate with the XV Gateway.
3. Go to **App Users**, then select the **Add** icon.


4. Enter the user's **Email**, **First Name**, and **Last Name**.




5. Select one of the following authority levels:
   a. **Administrator**—The user can manage multiple systems.
   b. **Standard**—The user can manage a single system.
   c. **Access Only**—The user has temporary door access.




6. If you want to email the user video clips, select the checkbox next to **Email Video Clips**.
7. Select the systems you want the user to have authority to access.

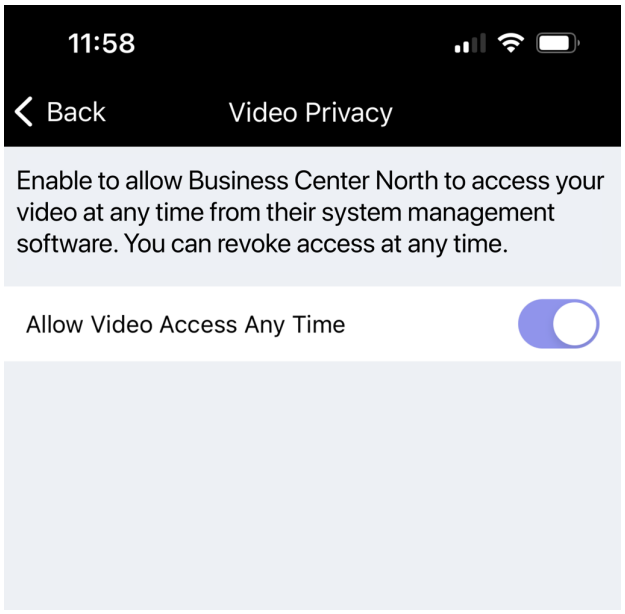
8. Choose if you want users to be able to **View User Codes** or **Enable Reports**. If you want to allow Virtual Keypad users to initiate a system panic from the app and website, enable any of the following options:
    - **Police Panic**
    - **Fire Panic**
    - **Emergency Panic**
9. Select **Save**. After you add an app user in Dealer Admin, the user is sent a welcome email with a link to finish setting up their account by creating a password.

## Enable Video Access to Technicians and Dealers

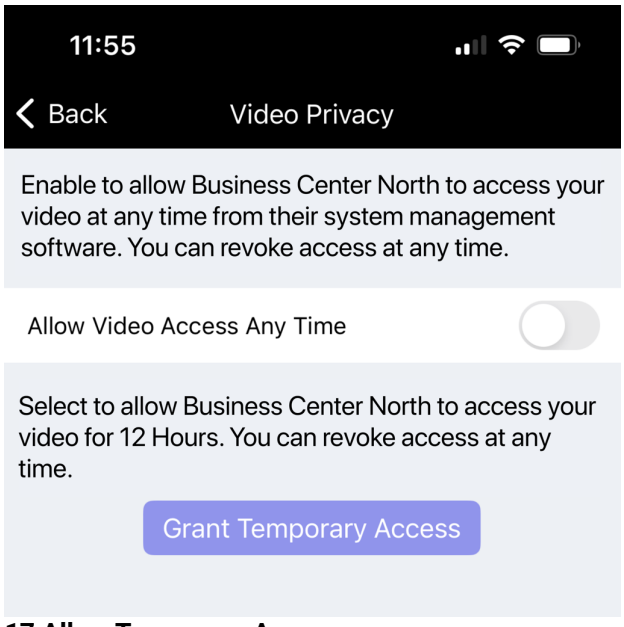
**Note:** All cameras brought online are immediately granted access to the video feed for 12 hours.

In Virtual Keypad, users can choose to allow video access to technicians and dealers. When video access is enabled, all Administrator level app users receive a notification email. To enable video access, follow the steps below:

1. Go to Virtual Keypad app or browser, then enter your user code.
2. Go to **Settings** > **Video** > **Privacy**.
3. Toggle **Allow Video Access Any Time** ON to grant technicians and dealers unlimited access to the video feed. If **Allow Video Access Any Time** is toggled OFF, you can enable **Grant Temporary Access** to allow technicians and dealers access to video for 12 hours. Access can be revoked instantly by selecting **Revoke Access** or disabling **All Video Access Any Time**.




**16 Allow Unlimited Access**




**17 Allow Temporary Access**

## Enable Push Notifications

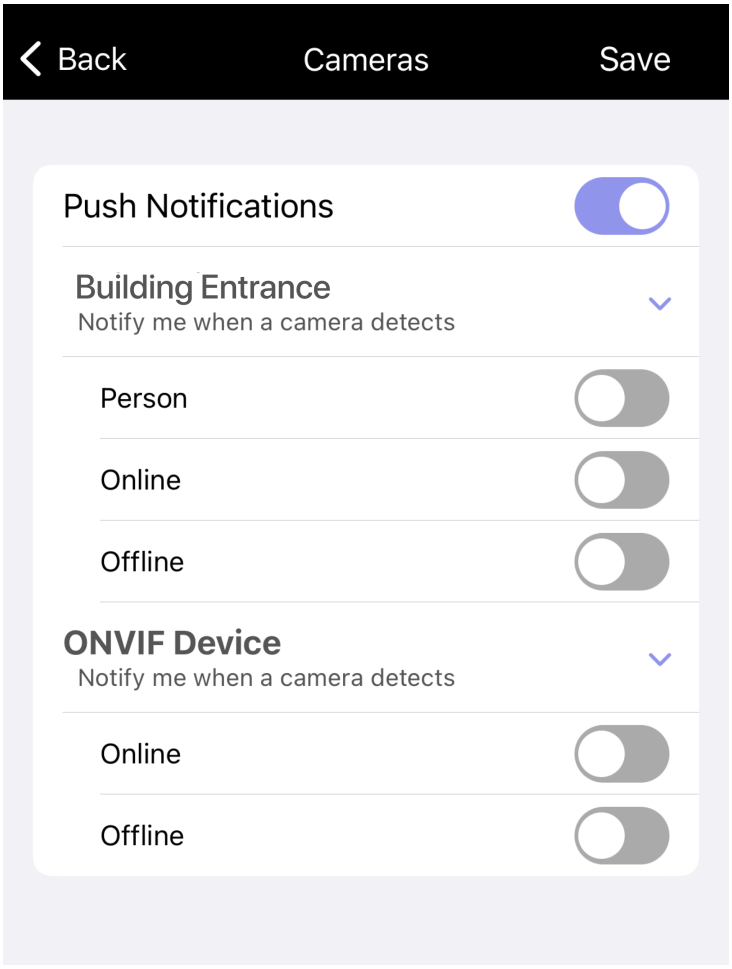
**Note**: If you want to receive push notifications for detection regions or lines, ensure detection regions or lines are configured in Dealer Admin before enabling push notifications in Virtual Keypad.

Refer to Add Regions and Analytics Settings for instructions on how to configure detection regions and lines for cameras on Dealer Admin.

Subscribe to push notifications on your device for online, offline, and defined Dealer Admin detection regions and lines.

1. Open the Virtual Keypad app and enter your user code.
2. Select the **More** icon, then select **Settings**.
3. Go to **Push Notifications**, then select **Cameras**.
4. Push Notifications are enabled by default. Toggle **Push Notifications** OFF to disable push notifications.
5. If **Push Notifications** are enabled, select the toggle for any of the following camera detections you want to be notified for:
    - **Person**
    - **Animal**
    - **Vehicle**
    - **Online**
    - **Offline**

**Note:** If you do not see the **Person**, **Animal**, or **Vehicle** toggles, detection regions or lines are not defined in Dealer Admin.
To learn how to create detection regions and lines for cameras, refer to Add Regions and Analytics Settings.

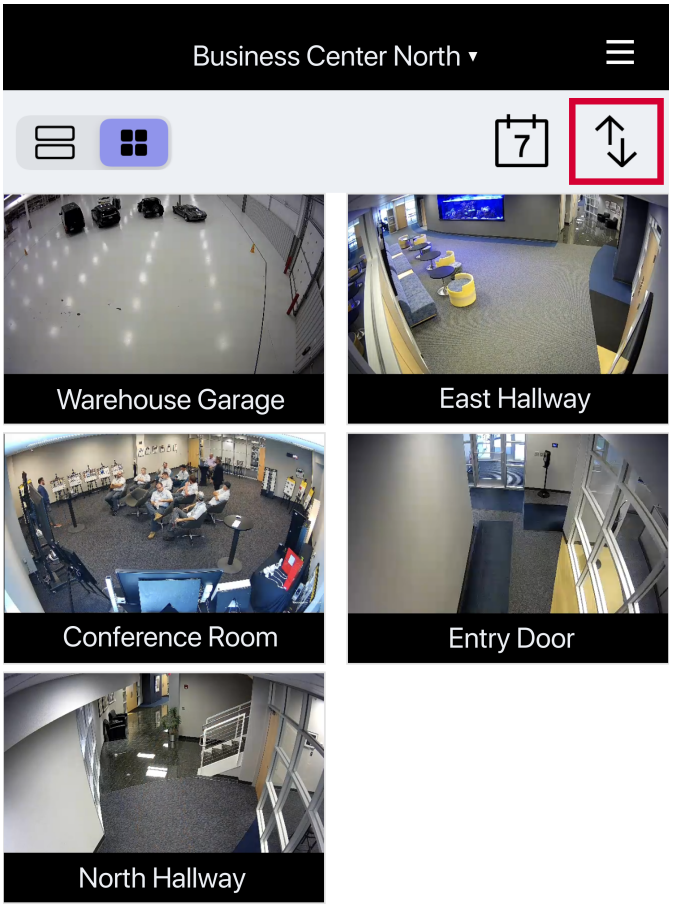



6. Select **Save**. Users receive a push notification any time the camera is set to detect, as defined in Dealer Admin.

## Customize Video Page

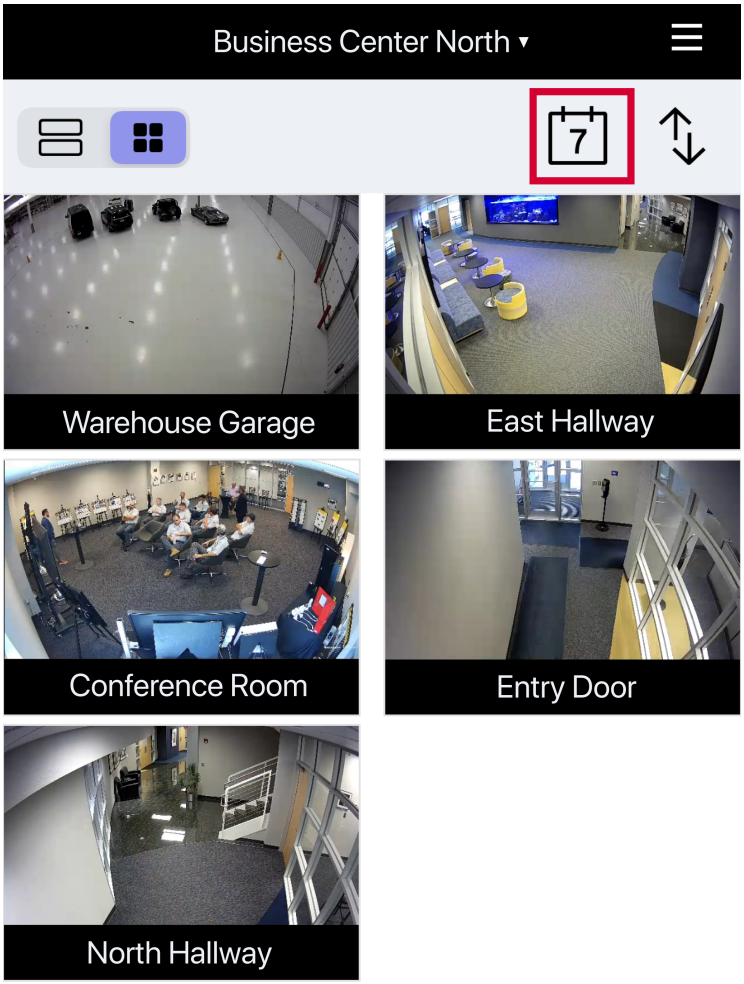
### Reorder Camera Feeds

1. Go to Virtual Keypad app or browser, then enter your user code.
2. Go to **Video**, then select the **Reorder** icon to reorder the camera feeds to display in any order.



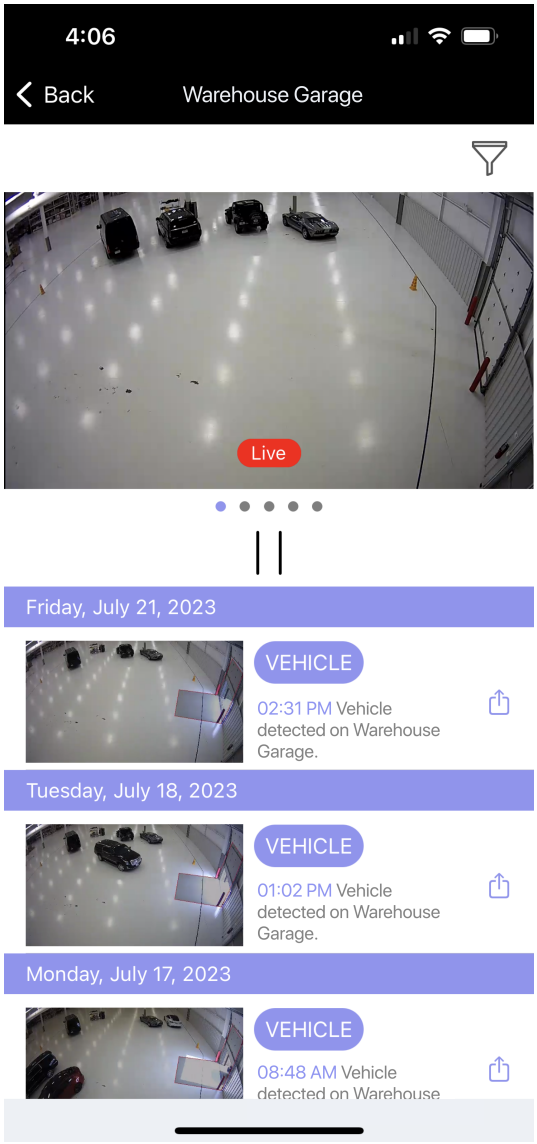

**View Camera Feeds at Specific Times**

1. Go to Virtual Keypad app or browser, then enter your user code.
2. Go to **Video**, then select the **Calendar** icon to filter to a specific time and view the camera playback feed for all cameras at that time.




**Use Single Camera View**

1. Go to Virtual Keypad app or browser, then enter your user code.
2. Go to **Video**, then select a camera from the **Video Page** to see live video and video clips from a single camera. In this section, you can view live feeds, view event lists of a selected camera, download clips, and filter to a specific time or event type.

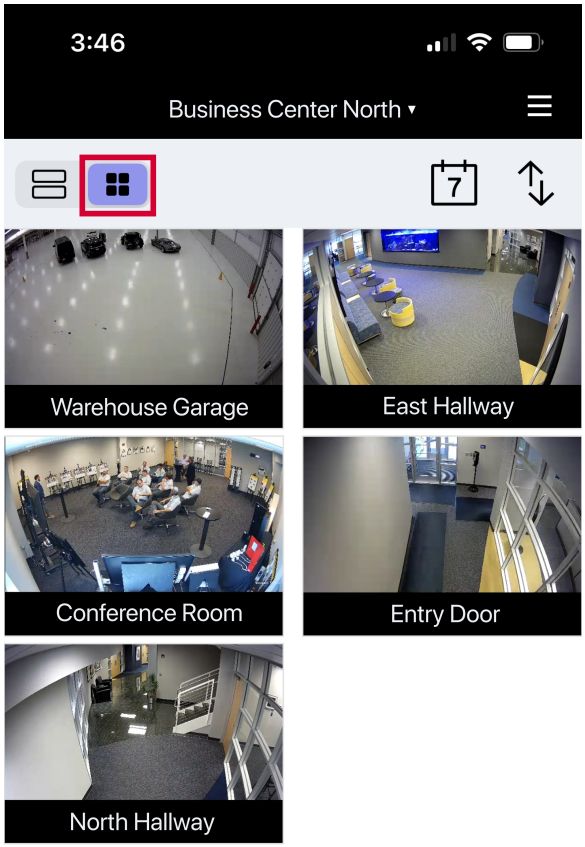



**Use List View**

1. Go to Virtual Keypad app or browser, then enter your user code.
2. Go to **Video** to see live video clips from multiple cameras in a list format. Scroll down to see more cameras.

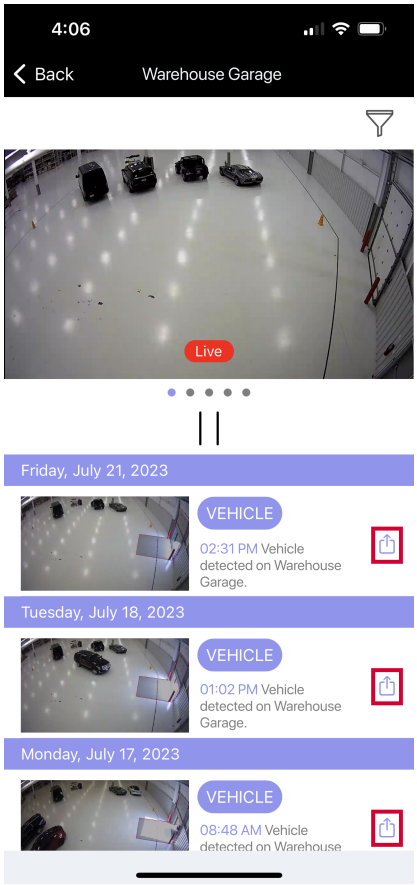

**Use Grid View**

1. Go to Virtual Keypad app or browser, then enter your user code.
2. Go to **Video**, then select the **Grid** icon to see live video clips from multiple cameras in a grid format. Scroll down to see more cameras.




**Download Video**

1. Go to Virtual Keypad app or browser, then enter your user code.
2. Go to **Video**, then select the camera you want to download the video from. Select the **Download** icon.



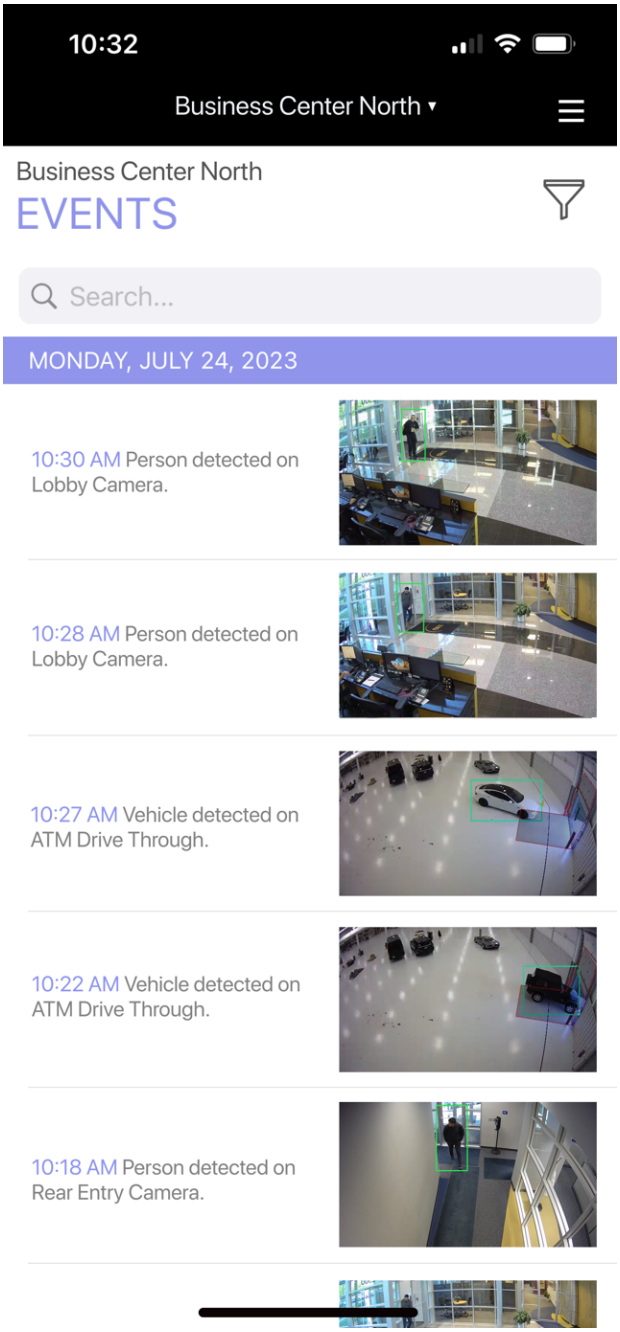

## View Video Events

**Note**: Ensure detection regions or lines are configured in Dealer Admin before viewing events in Virtual Keypad.
Refer to Add Regions & Analytics Settings for instructions on how to configure detection regions and lines for cameras.

### Standard Detection Video Events

Every time a person, vehicle, or animal enters the detection region or line when the panel is armed, the camera records the clip and populates in **Events** on Virtual Keypad.

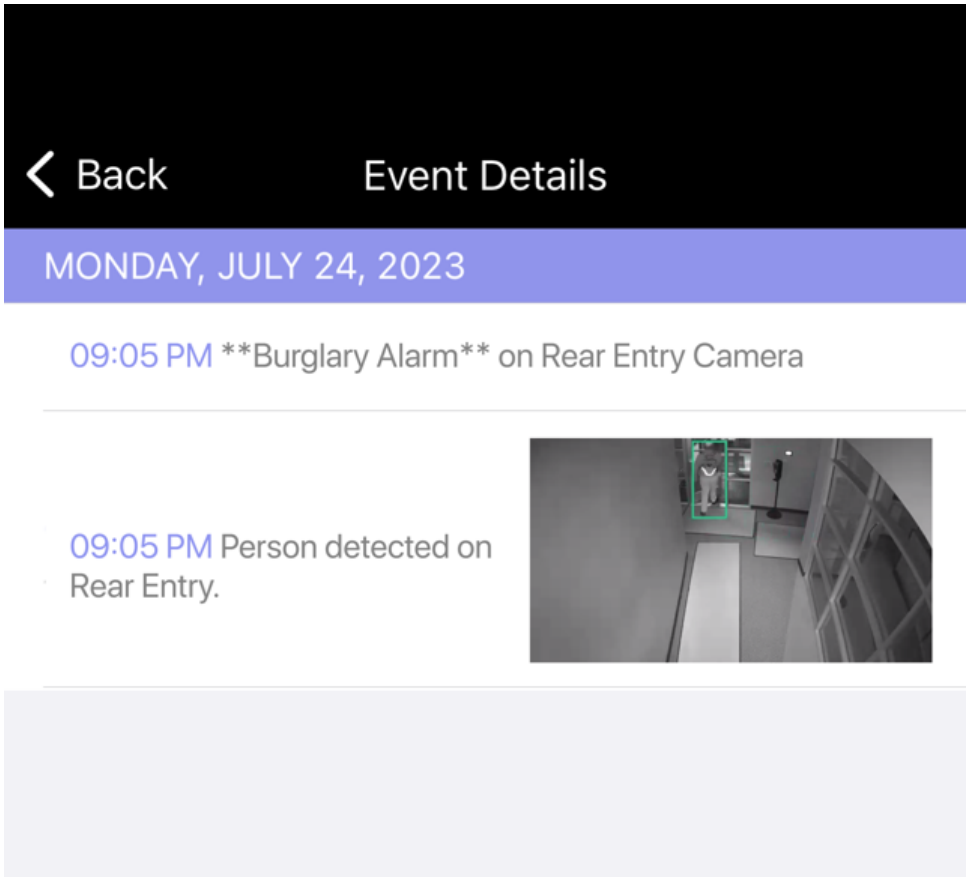
1. Go to Virtual Keypad app or browser, then enter your user code.
2. Select **Video**, then select the camera you want to see events for.
3. Events display on the right side of the screen. To view customize your video page, refer to Customize Video Page. To view recorded events on a timeline, refer to View Recorded Clips on a Timeline.




### Alarm Zone Detection Video Events

When a system is armed and goes into alarm, a clip is recorded and populates in **Events**. If the system is unarmed and a person, vehicle, or animal enters the detection region or line, no event is recorded.

> **Note:** If any detection region or line on the camera is set as an alarm zone, all detections for that camera only record events when the zone is armed and has been tripped.




**View Recorded Clips on a Timeline**

Video timeline lets you quickly scroll through recorded videos. You can adjust the timeline length to display recordings over different time periods from one hour to one month.

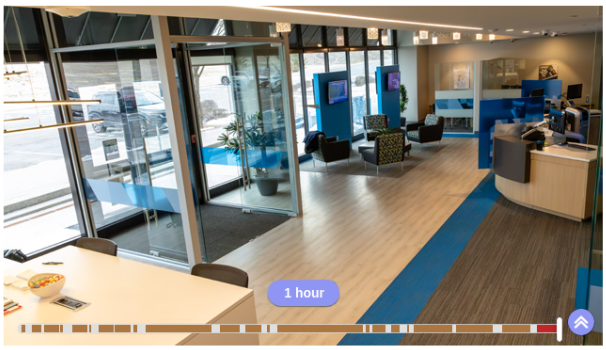
Standard and alarm zone detection events are bookmarked on the timeline, allowing you to skip to those specific sections.

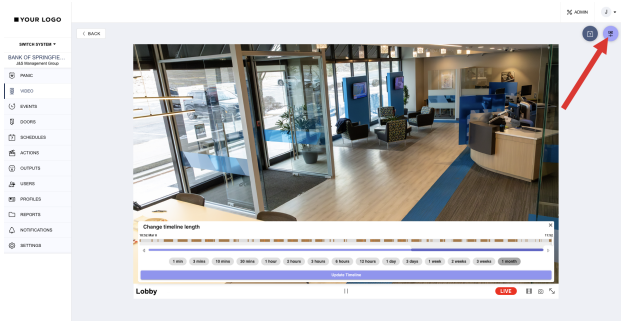
The timeline uses the following colors to indicate the different video statuses:

- **Red** – No footage available
- **Grey** – Default timeline for footage
- **Orange** – Verified analytic detection regions or lines (animal, vehicle, or person)
- **Tan** – Verified motion detection

To view the video timeline, complete the following steps:

1. Go to Virtual Keypad app or browser, then enter your user code.
2. Go to **Video**.
3. Select the **camera** you want to view the clips from.
4. At the top of the page, select the Timeline icon.
5. Scrub through the timeline to view recorded videos.



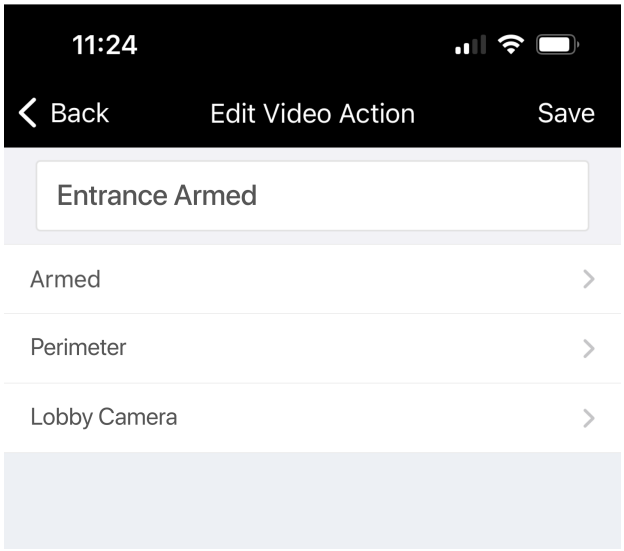

### Create Triggered Video Actions

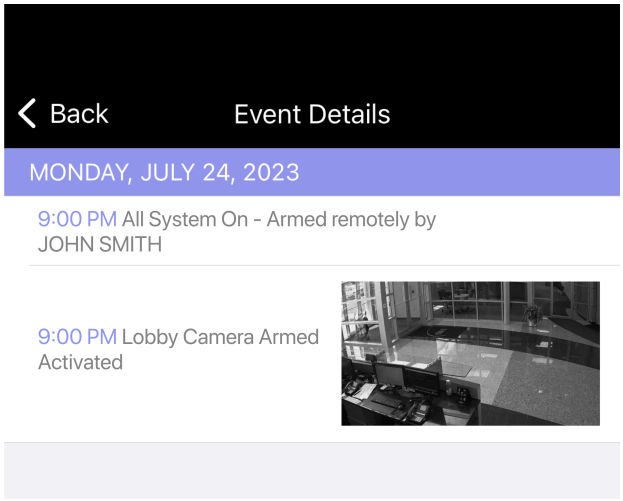
Virtual Keypad allows you to create Video Actions that appear in Events once the defined action is triggered. To create a triggered video actions, complete the steps below:

#### Virtual Keypad App

1. Go to the Virtual Keypad app and enter your user code.
2. Select the **More** icon and choose **Actions**.
3. Select **Video**.
4. Select the **Edit** icon in the top left corner, then select **Add**.
5. Give the action a **Name**.
6. Select **Event Type** and choose one of the following event types:
    - **Alarm**
    - **Door Propped**
    - **Bypass**
    - **Armed**
    - **Disarmed**
7. If you chose **Alarm**, **Armed**, or **Disarmed**, select an **Area** or **Zone** depending on your system type. If you chose **Door Propped** or **Bypass**, select a **Zone**. If you chose **Access Granted** or **Access Denied**, select a **Door**.
8. Select **Camera** and choose a camera.
9. Select **Save**.

**Note:** The triggered video action appears in **Events** when it is finished recording.

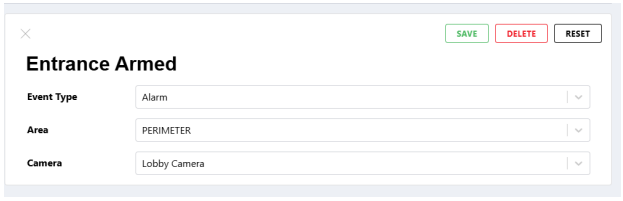


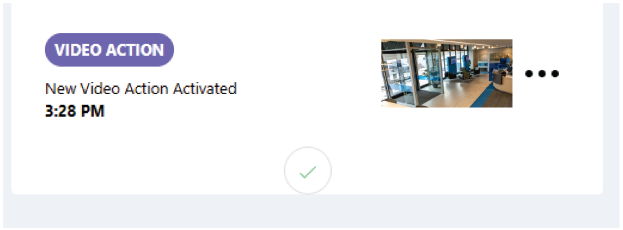




**Virtual Keypad Browser**

1. Go to Virtualkeypad.com and enter your user code.
2. Go to **Actions**, then select **Video Actions**.
3. Select the **Plus** icon to add a video action.
4. Give the action a name.
5. Select an **Event Type** in the drop-down menu. Choose one of the following options:
    - **Alarm**
    - **Armed**
    - **Disarmed**
    - **Door Propped**
    - **Zone Bypassed**
    - **Access Granted**
    - **Access Denied**
6. If you chose **Alarm**, **Armed**, or **Disarmed**, select an **Area** or **Zone** depending on your system type. If you chose **Door Propped** or **Zone Bypassed**, select a **Zone**. If you chose **Access Granted** or **Access Denied**, select a **Door**.
7. Select **Camera** and choose a camera.
8. Select **Save**.

**Note:** The triggered video action appears in **Events** when it is finished recording.



## 22.5.8 Use Cases and Application Videos

### Add and Configure Devices to an XV Gateway

AlarmVision® allows you to instantly use your customers' existing cameras by turning them into smart motion detectors when the system is armed.

Monitor events in real time without having to make changes to existing camera installations.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/829454384?share=copy

### Provide Video to Panel Events

The following videos show how to program cameras on your XV gateway to record video when other panel events occur, such as access granted or denied, door propped, arming and disarming, and alarms.

This section assumes that all cameras have been installed and successfully added to the XV gateway.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/830299591?share=copy

## 22.5.9 Further Information

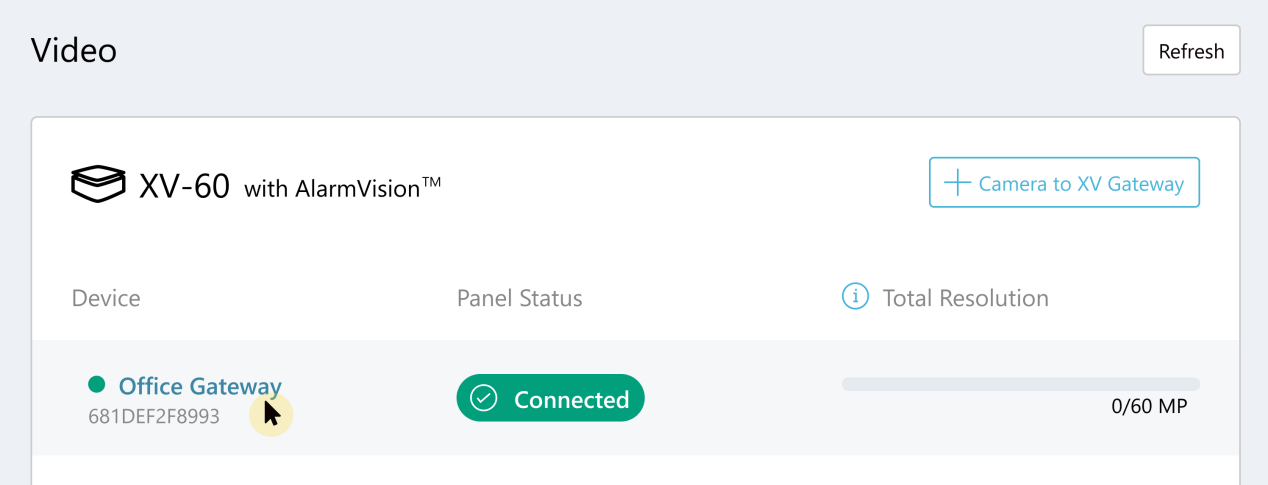
### Enable Monitoring Center Video Verification

1. Log in to Dealer Admin (dealer.securewireless.com).
2. Go to **Customers** and select the **System Name** that is connected to the XV Gateway.
3. In **System Information**, select **Edit** at the top of the screen.
4. Scroll down to **Video**. Toggle **Monitoring Center Video Verification** ON to enable video verification.
5. Select **Save** at the top of bottom of the screen.

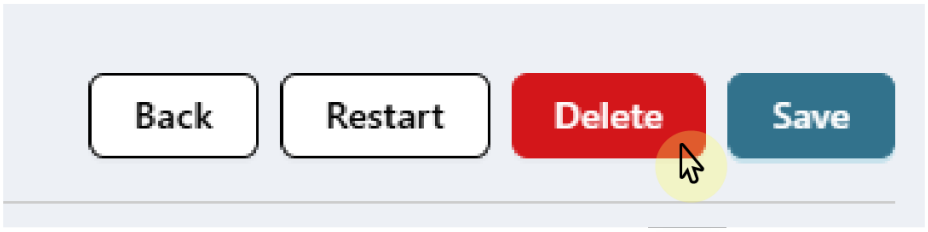
### Delete an XV Gateway

**Note**: Deleting the XV Gateway deletes all devices connected to it and removes all detection regions, lines, zones, and video actions tied to those devices.

1. Log in to Dealer Admin (dealer.securewireless.com).
2. Go to **Customers** and select the **System Name** that is connected to the XV Gateway.
3. In **Video**, select the name of the XV Gateway you want to delete.




4. At the top of the screen, select **Delete**.




5. A window displays to confirm your decision. Select **Yes** to delete the XV Gateway. Select **No** to cancel.


6. To re-add the XV Gateway to Dealer Admin, refer to Activate the XV Gateway for more information.

## Hide a Device

This option disables a device and moves it to the **Hidden Devices** list.

1. Log in to Dealer Admin (dealer.securewireless.com).
2. Go to **Customers**, then select the **System Name** that the XV Gateway is connected to.
3. Go to **Video**, then select **+ Device to XV Gateway**.
4. Locate the device you want to hide. Select the **More** icon, then select **Hide** Device. The device appears in **Hidden Devices** at the bottom of the window.

## Unhide a Device

Enabling a hidden device removes it from the **Hidden Devices** list and re-adds it to the XV Gateway.

1. Log in to Dealer Admin (dealer.securewireless.com).
2. Go to **Customers**, then select the **System Name** that the XV Gateway is connected to.

3. Go to **Video**, then select **+ Device to XV Gateway**.
4. Select **Hidden Devices** at the bottom of the window.
5. Locate the device you want to unhide. Select the **More** icon, then select **Unhide** Device. The device appears in the preview list.

## Remove a Device

> **Note:** Removing a device deletes all detection regions, lines, zones, and video actions tied to the device.

If you made changes to your device network, this option disables and removes the original auto-discovered device from Dealer Admin. Any devices on the same subnet as the XV Gateway are automatically discovered and added to the device list.

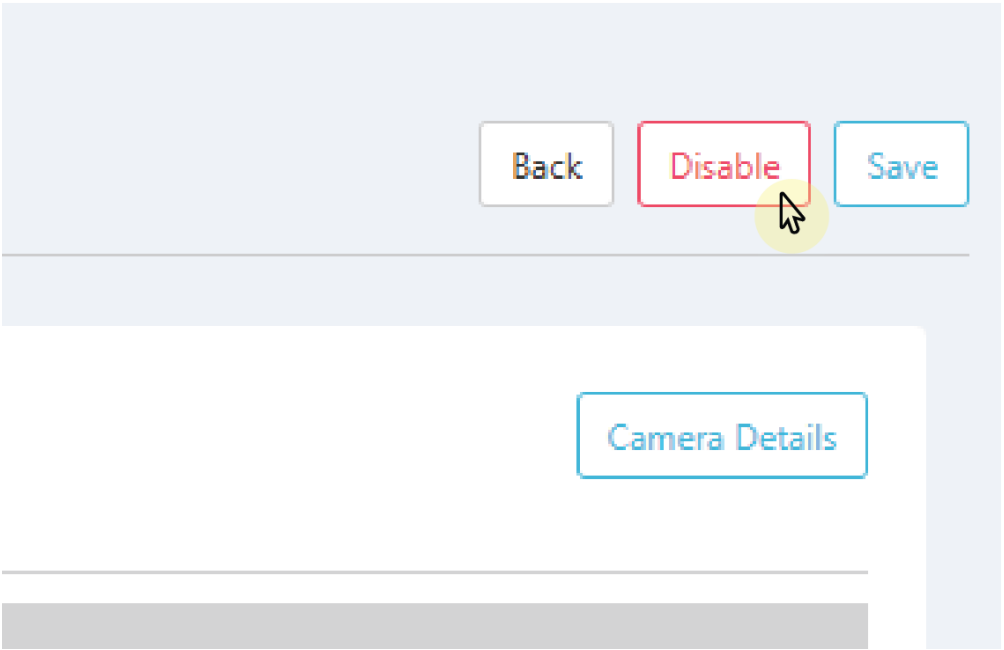
1. Log in to Dealer Admin (dealer.securewireless.com).
2. Go to **Customers**, then select the **System Name** that the XV Gateway is connected to.
3. Go to **Video**, then select **+ Device to XV Gateway**.
4. Locate the device you want to delete. Select the **More** icon, then select **Delete** Device.

## Disable a Device

To disable a camera, navigate to **System Information** for the selected system.

1. Log in to Dealer Admin (dealer.securewireless.com).
2. Go to **Customers**, then select the **System Name** that the XV Gateway is connected to.
3. Go to **Video**, then select the device you want to disable.
4. Select **Disable** in the top right corner to remove the device from the XV Gateway.

> **Note:** Disabling a device deletes all detection regions, lines, zones, and video actions tied to the device.




3. Select **Save**. The device is removed from the **XV Gateway with AlarmVision®** section.

## Update the Device Password

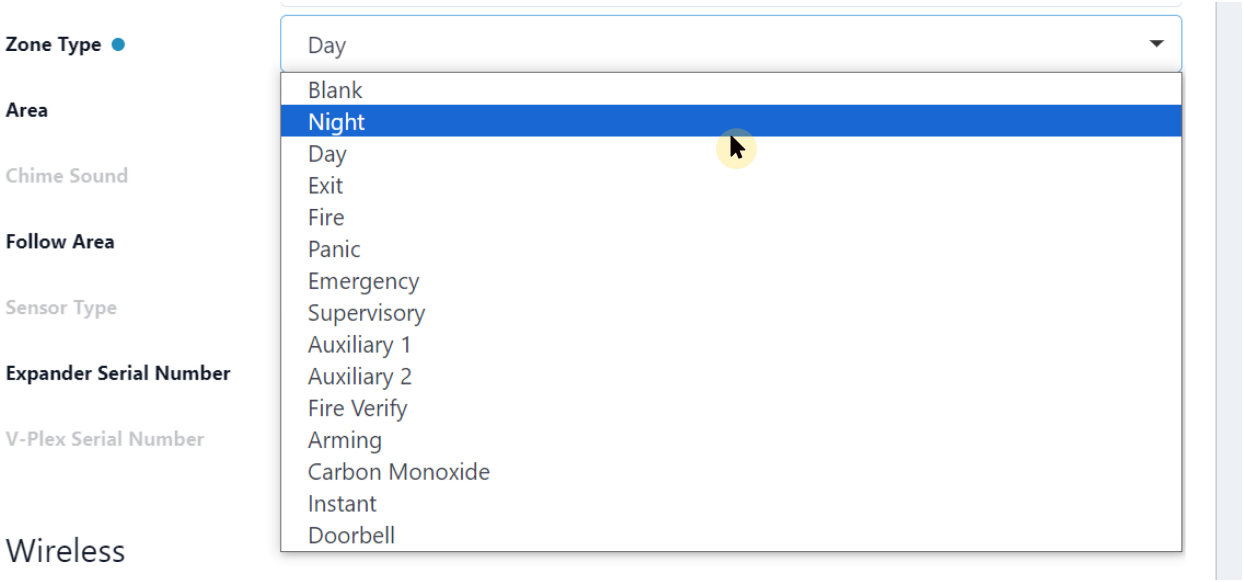
If a user has changed the device password, the XV Gateway requires the updated password to access audio, video, or both. This option sends the device password to the XV Gateway and restores audio, video, or both.

> **Note:** This does not change the device's password; it only re-sends the device's password to the XV Gateway to restore audio or video when the device's password has been changed.

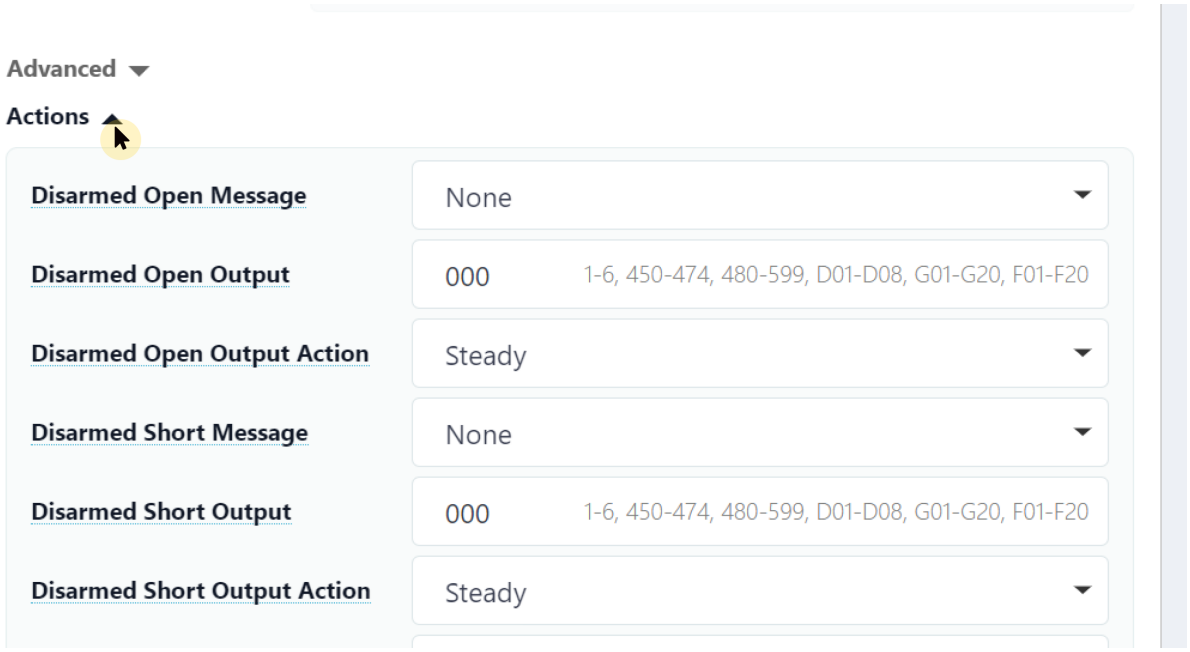
1. Log in to Dealer Admin (dealer.securewireless.com).
2. Go to **Customers**, then select the **System Name** that the XV Gateway is connected to.
3. Go to **Video**, then select **+ Device to XV Gateway**.
4. Locate the device that requires an updated password. Select the **More** icon, then select **Update Password.** Device functionality is restored.

## Edit a Zone

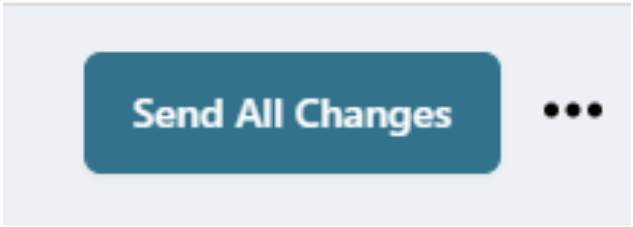
1. Log in to Dealer Admin (dealer.securewireless.com).
2. Go to **Customers** and select the **System Name**.
3. Go to **Programming** for the selected system.
4. Go to **Zone Information** and locate the zone that needs to be edited.
5. At **Zone Type**, select the drop-down to view the zone types that can be assigned.




5. At **Zone Actions**, select the drop-down to view the outputs that can be assigned.




4. When done editing, select **Send All Changes** at the top of the screen to save the changes and send them to the panel.



# 23 Tools

Dealer Admin provides helpful tools for specific Dealer Admin features. In this section, you'll learn how to use tools, including how to create a template, enable mobile credentials, and more.

## 23.1 Templates

Dealer Admin enables you to program panels with templates and automatically push programming to a panel. In this section, you'll learn how to add, edit, and delete templates. You'll also learn how to configure Virtual Keypad templates and program a system with a template.

### 23.1.1 Create a Template

You can use templates to automatically configure features when installing panels with Dealer Admin. To create a template, complete the following steps.

> **Note:** XR Series panels using EASYconnect with firmware Version 191 and lower must have an App Key programmed before using templates.

1. In the sidebar on the left, go to **Tools > Templates**.
2. Select the Add icon.
3. Name the template and choose a **System Type**.
4. To only apply the template to a specific customer's systems, select a **Customer**.
5. Add all programming options according to your customer's needs. For more information about programming, refer to Programming or the applicable panel programming guide.
6. Select **Save**.

### 23.1.2 Edit a Template

To edit a template, complete the following steps.

1. In the sidebar, go to **Tools > Templates**.
2. Select the Settings icon in the row of the template that you want to edit.
3. Edit any information in the template.
4. Select **Save**.

### 23.1.3 Delete a Template

To delete a template, go to **Tools > Templates**. Select **Delete** in the row of the template that you would like to delete.

### 23.1.4 Create Virtual Keypad Templates

To create Virtual Keypad templates, complete the following steps.

1. In the menu, go to **Tools > Templates** and open the **Virtual Keypad** tab.
2. In **App Type**, choose either **Arming** or **Standard**.
3. In **Included Features**, **Add-on Features**, and **App User Defaults**, select the options that you want to include in the default programming for Virtual Keypad.
4. Select **Save**.

### 23.1.5 Program a System with a Template

Templates allows a dealer to manually push programming to a panel during installation.

1. Go to **Customers**.
2. Select a customer to open the **Customer Summary**.
3. In **Systems**, select the Add icon.
4. Enter the system name.
5. Select a **System Type**.
6. Check the box next to **Pre-Program System.**
7. In **Templates**, choose a template.
8. Enter an **Account Number**.
9. Enter the panel **Serial Number**.
10. Select other system options as needed. For more information about initial system creation options, refer to Add a System.
11. Select **Save**.

The programming status is displayed at the top of the system information page and confirms when the process is complete. The process can take up to 10 minutes, depending on the amount of programming to be sent to the panel. To confirm that programming is complete in the field, enter panel programming from a keypad (**6653**), then go to **COMMUNICATION > ACCOUNT NO** and ensure that the correct account number is programmed in the panel.

## 23.2 Reporting and Analytics

To manage your services with Reporting & Analytics, complete the following steps.

- Generate a Quick Report
- Generate a Custom Report
- Export a Report

**Prefer a Video?**

In this clip, we'll show you how to use Reporting & Analytics.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/616188746

### 23.2.1 Generate a Quick Report

1. In the menu, go to **Tools > Reporting & Analytics**.
2. In **Quick Reports**, select a report from the list.
3. To export the report, select **Export**.
4. To return to **Reporting & Analytics**, select **Back**.

### 23.2.2 Generate a Custom Report

1. In the menu, go to **Tools > Reporting & Analytics**.
2. In **Custom Reports**, choose a **Report** type, **System Type**, **Date Range**, and **Connection Type**. Choose additional options as needed.
3. Select **Run Report**. The custom report opens in a new window. You can export the report from this page.

4. If you want to save the report, select **Save Report**. Enter information in the **Save Report** form and select **Save**.

### 23.2.3 Export a Report

1. After creating a report, select **Export**.
2. Before downloading the report, you can choose to save it as a **CSV**, **Excel**, or **PDF** file.
3. A dialog pops up to ask where you want to save the file. Choose a location, then select **Save**.

## 23.3 Service Requests

Create a service request in Dealer Admin that sends a Tech APP notification to the assigned technician. In Dealer Admin, users can also view, edit, close, and delete service requests from the **Service Request Dashboard**.

**Note:** Access to the **Service Request Dashboard** and the ability to manage service requests is restricted to users with Admin authority or the appropriate custom role permissions. Technicians can only view or close service requests in the Tech APP. For more information about these permissions, refer to Personnel Roles.

- Create a Service Request
- Edit a Service Request
- Close a Service Request
- Reopen a Service Request
- Delete a Service Request

**Prefer a Video?**

In this clip, we'll show you how to create and manage service requests.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/575103749

### 23.3.1 Create a Service Request

To create a service request in Dealer Admin, complete the following steps:

1. Go to **Customers**.
2. Select the customer name.
3. In **Systems**, find the row of the system that needs to be serviced, then select the More icon.
4. Select **Create Service Request**.
5. A dialog box displays. In the **Select Technician** drop-down menu, choose the technician that you want to assign to the service request.
6. In **Service Date**, choose a date for service to be completed.
7. If necessary, add details for the request in **Notes**.
8. Select **Save**.

When the technician opens Tech APP, they'll see the new service request that you assigned to them. To view your service requests, go to **Tools > Service Request**.

### 23.3.2 Edit a Service Request

To edit a service request in Dealer Admin, complete the following steps:

1. In the menu, go to **Tools > Service Request**.
2. In the row of the service request that you want to edit, select the More icon.
3. Select **Edit**.
4. Edit the request as needed.
5. Select **Save**.

### 23.3.3 Close a Service Request

To close a service request in Dealer Admin, complete the following steps:

> **Note:** After a service request is closed, it cannot be edited until you Reopen a Service Request.

1. In the menu, go to **Tools > Service Request**.
2. In the row of the service request that you want to close, select the More icon.
3. Select **Edit**.
4. Select **Close Request**.

### 23.3.4 Reopen a Service Request

To reopen a service request in Dealer Admin, complete the following steps:

1. In the menu, go to **Tools > Service Request Dashboard**.
2. Select the checkbox next to **Show Closed Service Requests**.
3. In the row of the service request that you want to reopen, select the More icon.
4. Select **Reopen Request**.

### 23.3.5 Delete a Service Request

To delete a service request in Dealer Admin, complete the following steps.

1. In the menu, go to **Tools > Service Request**.
2. In the row of the service request that you want to delete, select the More icon.
3. Select **Delete**.
4. To delete the service request, select **Confirm**.

## 23.4 Mobile Bluetooth Credentials

This section covers how an Administrator purchases Mobile Bluetooth Credentials for a customer in Dealer Admin. These steps should be completed after the SR3 Bluetooth Reader is installed and associated with a customer's system in Tech APP.

To purchase and issue Mobile Bluetooth Credentials in Dealer Admin, you need an **Administrator** role or a custom role with **Mobile Bluetooth Credential** permissions. For more information, refer to Personnel Roles.

**Prefer a Video?**

In this clip, we'll show you how to purchase Mobile Bluetooth Credentials.

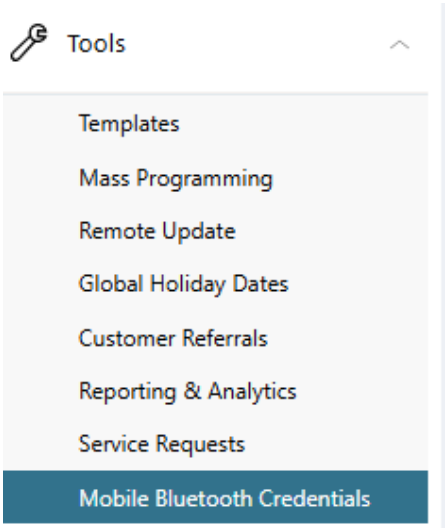
Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/613890240

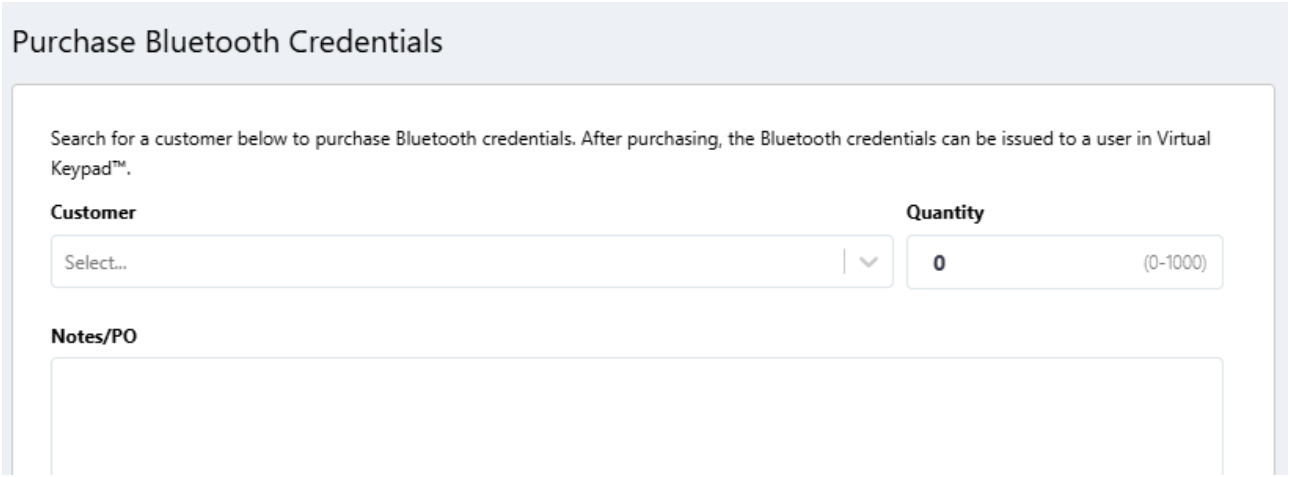
## 23.4.1 Enable Mobile Bluetooth Credentials

To purchase Mobile Bluetooth Credentials, complete the following steps:

1. In the menu, go to **Tools > Mobile Bluetooth Credentials**.




2. Go to the **Purchase Bluetooth Credentials** section.
3. In **Customer**, select a customer you want to enable the credentials for.
4. In **Quantity**, select the number of credentials you want to assign. You can select up to 1,000 credentials.
5. If needed, use the **Notes/PO** field to help you track items like why the credentials were issued and who requested them.




6. To purchase the credentials for your customer, select **Purchase Bluetooth Credentials**.


7. Notify your customer that you completed their purchase.

### 23.4.2 Public Card Formats

| CARD FORMAT | WEIGAND CODE LENGTH | SITE CODE POSITION | SITE CODE LENGTH | USER CODE POSITION | USER CODE LENGTH | USER CODE DIGITS |
|---|---|---|---|---|---|---|
| DMP Bluetooth 56-Bit | 56 | 1 | 16 | 17 | 34 | 10 |

## 23.5 Global Holiday Dates

Global Holiday Dates enables you to create a holiday date and add the date to multiple panels at once in Dealer Admin. Any time a holiday date is changed, the change will automatically be sent down to the associated panels. To create a Global Holiday Date, refer to the steps below.

### 23.5.1 Create a Global Holiday Date

1. In the menu, click **Tools**. Then, select **Global Holiday Dates**.
2. In the **Create Global Holidays** tab, click the Add icon next to **Create Global Holiday Dates**.
3. In the dialog box, fill in the following information:
    - **Name:** Enter a descriptive name for the holiday. This is a required field.
    - **Date:** Enter the date of the holiday. This is a required field.
    - **Class:** Select a class from the drop-down menu. The class enables you to group holidays together for easier schedule management.
    - **Description:** Add any additional information for the holiday.
4. Click **Save**.

### 23.5.2 Send a Holiday Date to a System

#### Send a Holiday Date to Multiple Systems

1. In the **Send Global Holidays** tab, click the Add icon next to **Send Global Holiday Dates**.
2. In **Holiday Dates**, click the checkbox next to the holiday date you want to send to your customer.
3. Next to **Systems**, click **Add Systems**.
4. Click the checkbox next to the customer to send the holiday date to all panels under the customer. Click the checkbox next to the system to send the holiday date to that specific system.
5. Click **Save**.
6. At the top of the page, select **Send**.
7. You will be redirected to the **Send Global Holiday Dates** page. This displays a table with the global holiday dates that have been created.
8. To view an audit of the global holiday date, find the holiday date on the table and click **View**. This displays an audit of who created the date, the systems the date was sent to, and other information.

### Send a Holiday Date to a Single System

1. Go to **Customers**.
2. Select a system from the customer.
3. In the sidebar on the left, click **Schedules**. A list of the holiday dates assigned to the system displays beneath **Holiday Dates**.
4. To add a holiday date to the system, click the Add icon next to **Holiday Dates**.
5. In the dialog box, select a **Holiday** and a **Class** from the drop-down menus.
6. Click **Save**.

## 23.5.3 Edit a Global Holiday Date

1. Navigate to the **Global Holiday Dates** page.
2. Click the Edit icon next to the date you want to change.
3. Select a different date from the calendar.
4. Click **Save**. This is automatically sent to any panel associated with the holiday date and updates the calendar date.

## 23.5.4 Remove a Global Holiday Date

1. Navigate to the **Global Holiday Dates** page.
2. Click the Delete icon next to the date you want to remove. This is automatically sent to any panel associated with the holiday date and removes the date from the panel.

# 24 Personnel

Dealer Admin helps you manage personnel access to specific Dealer Admin features. In this section, you'll learn how to add, edit, and delete personnel.

**Prefer a Video?**

In this clip, we'll show you how to add personnel.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/600484359

## 24.1 Add Personnel

To add personnel, complete the following steps.

1. In the menu, go to **Personnel > Personnel**.
2. In **Personnel List**, select the Add icon.
3. Enter the user's information, including their **First Name**, **Last Name**, and **Email**.
4. If you want to upload an image for the user, select **Add User Image** next to **User Image**. Select **Choose file**, find the image and select it, then click **Open**. For best results, photos should be a 300 × 300 pixel PNG file.
5. Select the user's role. For more information about the permissions associated with each role, refer to Preset Roles or Custom Roles.
6. At the top of the page, select **Save**.

## 24.2 Edit Personnel

To edit personnel, complete the following steps:

1. In the menu, go to **Personnel > Personnel**.
2. In **Personnel List**, select the email address of the user that you want to edit.
3. Edit the user's information as needed. For information about user permissions, refer to Preset Roles or Custom Roles.
4. At the top of the page, select **Save**.

## 24.3 Delete Personnel

To delete personnel, complete the following steps:

1. In the menu, go to **Personnel > Personnel.**
2. In **Personnel List**, find the row of the user that you want to delete, then select the Delete icon.
3. A dialog box displays to confirm your decision. To delete the personnel account, select **OK**.

## 24.4 Personnel Roles

Dealer Admin helps you manage personnel access to specific Dealer Admin features. In this section, you'll learn about personnel roles and permissions.

**Prefer a Video?**

In this clip, we'll show you how to assign preset roles and custom roles.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/600484359

## 24.4.1 Preset Role Permissions

The following tables provide an overview of the abilities associated with each preset role.



### Customers

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **View** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Add** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Edit** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Delete** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

### Systems

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **View** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Add** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Edit** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Delete** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

## Users

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **View** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| **Add** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Edit** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Delete** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

## App Users

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **View** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| **Add** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Edit** | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| **Delete** | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |

## Panels

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **Update** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Program** | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ |

## Reports

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **Create** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |

## Video Devices

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **Test** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Add** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Edit** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Delete** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

## Video Verification

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **Verify** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |

## Dealer Dashboard

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **View** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

## Dealer Settings

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **View** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Edit** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Delete** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

### Log In as Customer

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **View** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Edit** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Delete** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

### Invoices

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **View** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| **Download** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |

### Reset Passwords (All)

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **Reset** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

### Reset Passwords (Self and app users)

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **Reset** | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |

## Service Requests

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **View** | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| **Close** | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| **Add** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Edit** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Delete** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

## Mobile Credentials

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **View, Issue, Purchase** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

## System Status

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **View and Manage** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

## Central Station (Receivers and Integrations)

| | Administrator | Operator | Sales Person | Sales Manager | Video Verifier | Technician | Accountant |
|---|---|---|---|---|---|---|---|
| **View and Manage** | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

## 24.4.2 Custom Roles

In addition to preset roles, Dealer Admin now gives you the ability to create custom roles. This enables you to choose the Dealer Admin features that personnel have permission to manage. For more information about available permissions, refer to Custom Role Permissions.

- Add a Custom Role
- Edit a Custom Role
- Delete a Custom Role

### Add a Custom Role

To add a custom role, complete the following steps:

1. In the menu, go to **Personnel > Custom Roles**.
2. Select the Add icon next to **Custom Roles List**.
3. Enter a **Name** for the role and a brief **Description**.
4. Configure the following options:

**Applications**

1. Select whether you want the role to apply to **Dealer Admin**, the **Tech APP**, or both.
2. Select the checkbox next to **Two Factor Authentication** to require personnel to enter a security code when logging in.

**Day/Time**

1. Select the checkbox next to **All Day** for selected applications to apply to the user for the entire day. Otherwise, enter a **Start Time**, **End Time**, select the **Time Zone** in the drop-down menu, and select the days of the week when you want the applications to apply to the user.
2. Select the checkbox next to **Observe Daylight Saving Time** if you want the applications to apply during during daylight saving time.

**Limit Access**

1. Select the checkbox next to **Only show systems that have performed a system test** to require personnel to perform a system test at the keypad to access the system on Dealer Admin.
    - After selecting the checkbox, a new checkbox displays. Select **Show All Customers** to allow personnel who are adding a new system to choose an existing customer to associate the system with.
2. Select the checkbox next to **Only allow access to Dealer Admin from whitelist IP addresses** to require personnel to only connect to Dealer Admin from the allowed public IP addresses you set. For more information about how to add whitelist IP addresses, refer to IP Whitelisting.
3. In the drop-down menu next to **Tags**, choose a tag to allow personnel to only see the systems or customers that contain the selected tag(s).

**Permissions**

1. Select the permissions from preset roles that you want the user to have. For more information, refer to Preset Role Permissions.
2. For Administrative, Firmware Updates, Reports, and System Programming, select which pages and functions you want the user to have access to. For more information, refer to Custom Role Permissions.

**Assign to Personnel**

At the top of the page, select **Show Personnel** to choose the users that you want to assign the new custom role to. If you have not created any personnel, select **Add Personnel**.

Once you've finished configuring creating the custom role, select **Save** at the top of the page.

### Edit a Custom Role

To edit a custom role, complete the following steps.

1. In the sidebar on the left, go to **Personnel > Custom Roles**.
2. Select the name of the role, then make changes as needed.
3. At the top of the page, select **Save**.

### Delete a Custom Role

To delete a custom role, complete the following steps.

1. In the sidebar on the left, go to **Personnel > Custom Roles**.
2. In the row of the role that you want to delete, select the Delete icon.
3. A dialog box displays to confirm your decision. To delete the role, select **OK**.

## 24.4.3 Custom Role Permissions

The following table outlines role permissions associated with Dealer Admin features. For more information, refer to Add, Edit, and Delete Custom Roles.

- Permissions
- Administrative
- Firmware Updates
- Reports
- System Programming

| Category | Feature | Options |
|---|---|---|
| **Limit Access** | *Only show systems that have performed a system test* | Allow or Deny |
| | *Only allow access to Dealer Admin from whitelist IP addresses* | Allow or Deny |
| | | |

| | | |
|---|---|---|
| **Permissions** | *Customers* | Hidden<br>View Only<br>View & Edit<br>View, Edit & Delete |
| | *Systems* | View Only<br>View & Edit<br>View, Edit & Delete |
| | *App Users* | Hidden<br>View Only<br>View, Edit & Delete |
| | *Personnel* | Hidden<br>View Only<br>View, Edit & Delete |
| | *Users* (User Codes) | Hidden<br>View Only<br>View, Edit & Delete |
| | *Schedules* | Hidden<br>View Only<br>View, Edit & Delete |
| | *Profiles/Groups* | Hidden<br>View Only<br>View, Edit & Delete |
| | *Cellular* | View Only<br>View & Activate<br>View, Activate & Deactivate |
| | *Mobile Bluetooth Credentials* | Hidden<br>View/Issue/Purchase |
| | | |

| | | |
|---|---|---|
| **Administrative** | *Customer List* | Allow or Deny |
| | *Dealer Settings* | Allow or Deny |
| | *Monitoring Center* | Allow or Deny |
| | *Log In as Customer* | Allow or Deny |
| | *Sensor Reset* | Allow or Deny |
| | *Service Requests* | Allow or Deny |
| | *Move Systems* | Allow or Deny |
| | *Tags* | Allow or Deny |
| | | |
| **Firmware Updates** | *System Remote Update* | Allow or Deny |
| | *Bulk Remote Update* | Allow or Deny |
| | *Update Dashboard* | Allow or Deny |
| | | |
| **Reports** | *Dealer Analytics* | Allow or Deny |
| | *Reports & Analytics* | Allow or Deny |
| | *Marketing Central* | Allow or Deny |
| | *Billing & Pricing* | Allow or Deny |
| | *System Analytics* | Allow or Deny |
| | | |

| | | |
|---|---|---|
| **System Programming** | *Programming* | Allow or Deny |
| | *Print Programming* | Allow or Deny |
| | *Templates* | Allow or Deny |
| | *Mass Programming* | Allow or Deny |
| | *Automation* | Allow or Deny |
| | *View User Codes* | Allow or Deny |
| | *Tech Tools* | Allow or Deny |
| | *System Status* | Allow or Deny |

# 25 Resources

The resources page gives you access to additional resources to market your business, learn about DMP products, and access Dealer Admin Help. For more information, refer to the following sections.

> For more information about our products and services or to contact us, visit DMP.com.

- Marketing Central
- DMP University
- News Items
- Downloads

## 25.1 Marketing Central

Order custom materials to help you market your brand. The following materials are available to order or download from Marketing Central:

- Brochures
- Door Hangers
- Invoice Stuffers
- Email Marketing
- Logos
- Demo Boards
- Slide Decks
- Social Media
- Stock Photography
- Products Photography
- Videos

To get started in Marketing Central, visit Marketing Central Help. For more information or to sign up for Marketing Central, visit DMP Marketing Support.

## 25.2 DMP University

Access interactive training courses and quizzes designed to help you learn about DMP products, their features, and product installation. For example, learn how to install and program XR150/XR550 Series panels.

For more information, visit DMP University.

## 25.3 News Items

Stay informed about important updates like new features and products.

## 25.4 Downloads

View and download software updates for Remote Link.

# 26 Settings

Dealer Admin helps you manage your company's interactions with customers. In this section, you'll learn how to view and edit your account information and upload logos.

## 26.1 Monitoring Center

In this section, you'll learn how to manage receivers and configure monitoring centers.

### 26.1.1 Configure Monitoring Center

**Requirement:** To manage monitoring center or receivers, you must have either an **Administrator** role or a custom role that allows you to view, add, edit, and delete **Monitoring Center**.

To add a monitoring center, complete the following steps.

- Add a Standard Monitoring Center
- Add a Custom Monitoring Center
- Edit Settings for Virtual Keypad
- View Communications Status

#### Add a Standard Monitoring Center

To add a standard monitoring center, complete the following steps.

1. Go to **Settings > Monitoring Center**.
2. In **Monitoring Centers**, select the Add icon.
3. Select a monitoring center. If you select Other, go to Add a Custom Integration.
4. Enter the automation username and password. A login with API level permissions is required for all features of the monitoring center for it to function properly. You may need to contact your monitoring center to generate an API login.
5. To allow users in Virtual Keypad to manage their emergency contacts list, select **Emergency Contacts**.
6. To allow users to place the system on test remotely from Dealer Admin, Tech APP, and Virtual Keypad, select **Place System on Test**.
7. Select **Save**.

#### Add a Custom Monitoring Center

If you own your monitoring center, you can request a custom monitoring center. To add a custom monitoring center, complete the following steps.

1. Go to **Settings > Monitoring Center**.
2. In **Monitoring Center**, select the Add icon.
3. In **Monitoring Center**, select **Other**.
4. Select **Send Request**.
5. After you're contacted by SecureCom, enter the code that the representative gives you in **Monitoring Center Code**, then select **Save**.
6. Enter the automation username and password for the monitoring center. A login with API level permissions is required for all features of the monitoring center for it to function properly. You may need to contact your monitoring center to generate an API login.
7. To allow users in Virtual Keypad to create an emergency contacts list, select **Emergency Contacts**.
8. To allow users to place the system on test remotely from Virtual Keypad, select **Place System on Test**.

9. Select **Save**.

### Edit Settings for Virtual Keypad

To give an app user the ability to edit contacts and place a system on test, make them an Administrator. Standard level app users can not use either of these features.

### View Communications Status

You can view the monitoring center connection status for a single system in **System Status**. You can also view the status for all of a customer's systems at once by opening the **Customer Summary**.

## 26.1.2 Configure Receivers

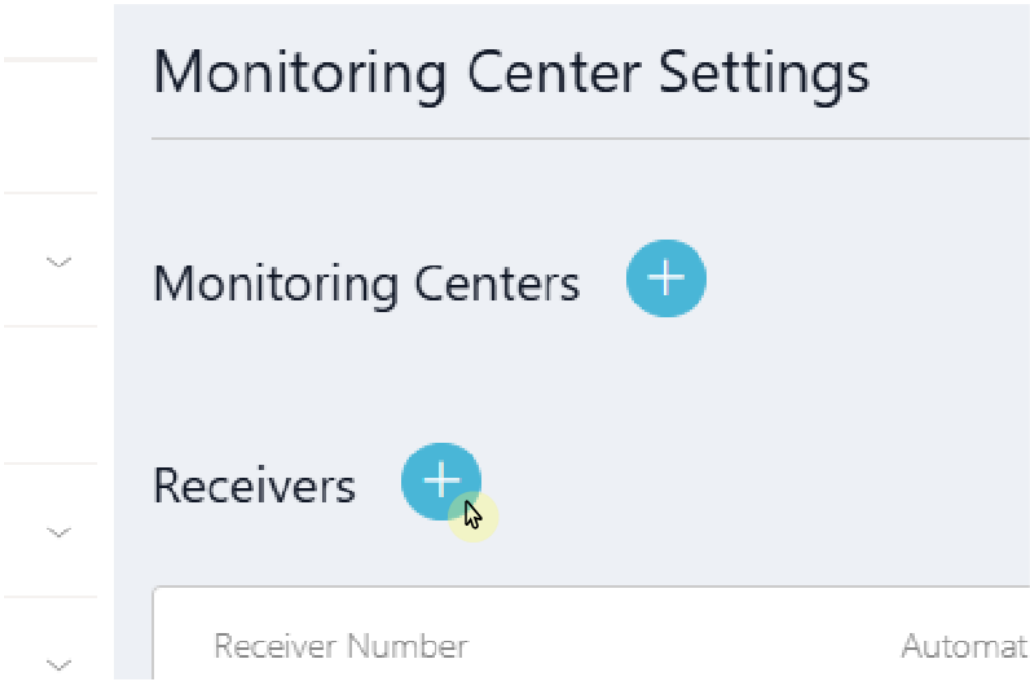
To add, edit, or delete a receiver, complete the following steps.

- Add a Receiver
- Edit a Receiver
- Delete a Receiver

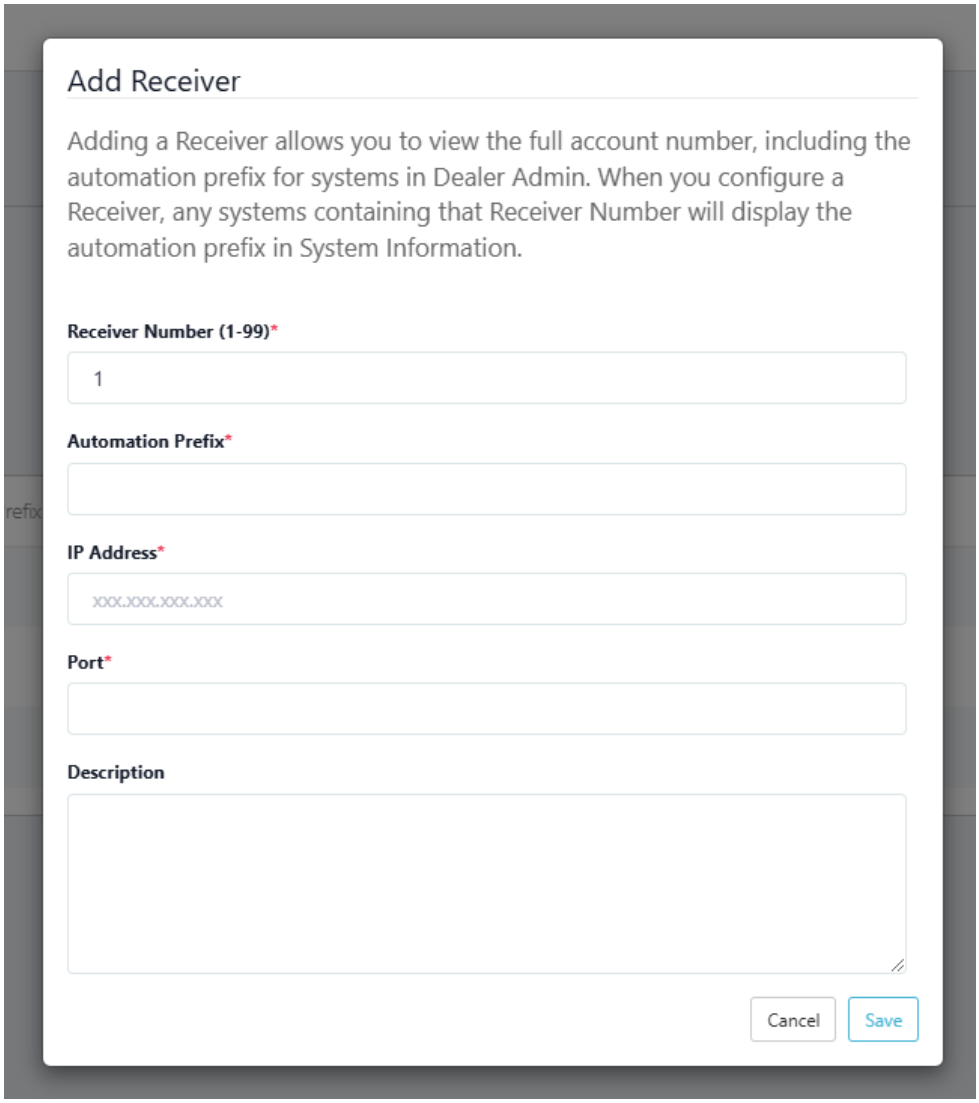
### Add a Receiver

To add a monitoring center receiver, complete the following steps.

1. In the sidebar, go to **Settings > Monitoring Center**.
2. In **Receivers**, select the Add icon.




3. Enter the receiver's **Receiver Number**, **Automation Prefix**, **IP Address**, **Port**, and **Monitoring Center**. If desired, enter a brief description about the receiver in **Description**.




4. Select **Save**.

## Edit a Receiver

To edit receiver settings, complete the following steps.

1. In the sidebar, go to **Settings > Monitoring Center**.
2. In the row of the receiver that you want to edit, select the Settings icon.
3. Edit the receiver information as needed, including the **Receiver Number**, **Automation Prefix**, **IP Address**, **Port**, **Monitoring Center**, and **Description**.
4. Select **Save**.

## Delete a Receiver

To delete a receiver, complete the following steps.

1. In the sidebar, go to **Settings > Monitoring Center**.
2. In the row of the receiver that you want to delete, select the Delete icon.
3. A dialog pops up to confirm your decision. To delete the receiver, select **OK**.

### 26.1.3 Manage Tests

When a monitoring center is configured, Dealer Admin enables you to place a system on test and take it off test. To initiate a test, complete the following steps.

- Place a System on Test
- Take a System off Test

#### Place a System on Test

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **System Status**.
4. Select **Place System on Test**, then select a duration.

> ⚠ **WARNING:** For the number of hours that you specify, the system sends signals to the monitoring center but emergency services are not contacted.

5. To start the test, select **Confirm**.

#### Take a System off Test

1. Go to **Customers**.
2. Select the system name.
3. In the sidebar, go to **System Status**.
4. Select **Take System off Test**.

## 26.2 Billing

Download SecureCom invoices directly from Dealer Admin. To download invoices, need a preset Admin or Accountant role, or a custom role with Billing & Pricing permission. To access SecureCom Billing, log in to Dealer Admin and select **Billing**. In the row of the invoice that you want to download, select PDF or CSV.

## 26.3 Tags

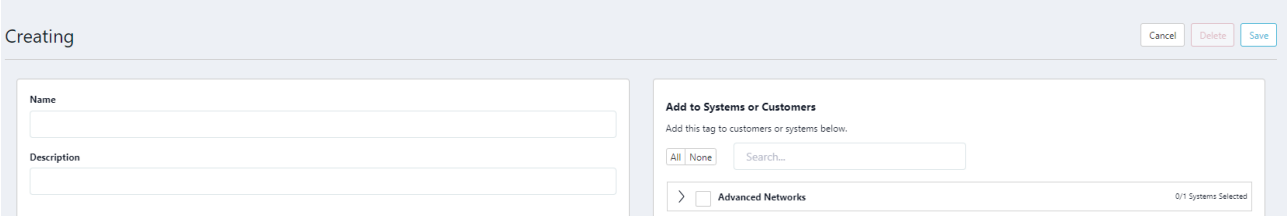
The Tags feature allows you to restrict access for personnel and organize customers and systems.

- Create a Tag
- Limit Tag Access
- Search Customers by Tag Name

### 26.3.1 Create a Tag

To create a tag for customers or systems, complete the following steps:

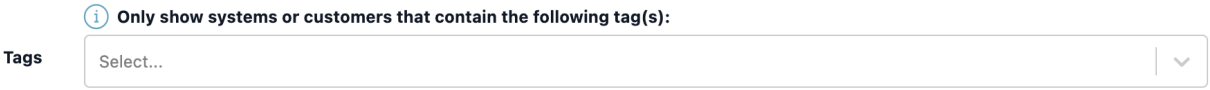
1. Go to **Settings** > **Tags**.
2. At the top of the page, select the Add icon.
3. Create a name and description for the tag.
4. Add the tag to systems or customers.




### 26.3.2 Limit Tag Access

To limit personnel to only see systems with specific tags, complete the following steps.

1. In the menu, go to **Personnel > Custom Roles**.
2. In **Custom Role List**, select an existing role or select the Add icon to create a new role.
3. In **Limit Access**, select the **Tags** dropdown menu and choose a tag to apply to the custom role.
4. At the top of the page, select **Save**.




### 26.3.3 Search Customers by Tag Name

Once you have created a tag, you can search customers using the tag name applied to them. To search customers using a tag name, complete the following steps:

1. In the menu, go to **Customers**.
2. Enter the tag name in the search bar.

## 26.4 Dealer

### 26.4.1 View and Edit Account Information

The **Dealer** page allows you to view your App Key and view or edit information about your company. To view and edit your Dealer Admin account information, complete the following steps.

1. In the menu, go to **Settings > Dealer**.
2. In the **Account** tab, you can edit your **Basic Information**, **Contact Information**, and **Security Features** as needed.
3. Select **Save**.

**Note:** Dealer Information will auto-update to any 7-Inch Touchscreen Keypads on the system.

### 26.4.2 IP Whitelisting

**IP Whitelisting** allows you to restrict connection to Dealer Admin with a list of allowed public IP addresses and a custom role option. For example, only allow panel programmers to log in to Dealer Admin when their computer is connected to your corporate network.

**Note:** Do not add dynamic IP addresses to the list of allowed addresses.

To restrict connection to certain IP addresses, complete the following steps:

1. In the menu, go to **Settings > Dealer**.
2. In the **Security Features** section, select **IP Whitelist**, then select **Add**.
3. Select the Add icon. Enter the **Location Name** and **IP Address**. To add your current IP address, select **Current IP**.
4. Select **Save**.
5. Go to **Personnel > Custom Roles** and select the role that you want to restrict to allowed IP addresses.
6. In the **Limit Access** section, select **Only allow access to Dealer Admin from whitelist IP addresses**.
7. At the top of the page, **select** Save.

## 26.4.3 Upload a Logo

**Prefer a Video?**

In this clip, we will show how to add your dealer logo on Dealer Admin.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/678926623

To upload a logo to display for your users in Virtual Keypad, complete the following steps.

**Note:** For best results, logos should be a 240 × 100 pixel PNG file with a transparent background.

1. In the menu, go to **Settings > Dealer**.
2. Open the **Web & App Logos** tab.
3. In the appropriate section, select **Upload**.
4. A file upload dialog opens. Select the logo that you want to upload and select **Open**. To preview your logo, select **Preview**.
5. Select **Save**.

To upload a logo to display for your users on 7-Inch Touchscreen Keypads, complete the following steps.

**Note:** For best results, logos should be a 270 x 110 pixel PNG file with a transparent background.

1. In the menu, go to **Settings > Dealer**.
2. Open the **8860 Private Label Settings** tab.
3. Select the **Upload** button.
4. A file upload dialog opens. Select the logo that you want to upload and select **Open**.
5. Type in the dealer information you want to display on the keypad.
6. Select **Save Contact Info**.

**Note:** If the logo is not downloading to the keypad, confirm that the panel date and time are correct, then press the DMP logo on the 8860 keypad. This triggers the keypad to reach out to Dealer Admin for the new logo.

## 26.4.4 Customer Referrals

**Note:** After customer referrals are enabled in Dealer Admin, **Refer Friend** is visible to all of your customers in the Virtual Keypad app.



**Prefer a Video?**

In this clip, we'll show you how to set up customer referrals.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/583555681

In this clip, we'll show you how to manage your customer referrals.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/584061663

### Enable and Configure Customer Referrals

To enable customer referrals, complete the following steps.

1. In the menu, go to **Settings > Dealer**.
2. Go to the **Customer Referrals** tab.
3. In **Current Customer Offer**, enter a message for existing customers who refer new customers.
4. In **New Customer Offer**, enter a message for new customers who are referred by existing customers.
5. If necessary, upload a photo for the new customer offer. For best results, images should be in landscape layout with a file size of less than 5 MB.
6. At the top of the page, select **Save**.

Existing customers can send referrals by opening Virtual Keypad, tapping **Refer Friend** in the menu, then tapping **Invite**. The customer is then prompted to compose and send a text message that contains a link to the referral form.

When the new customer opens the form, they are required to enter their name and email or phone number. When they submit the completed referral form, their contact information is populated on the **Customer Referrals** page in Dealer Admin.

### Set Up Referral Notifications

You can add up to six email addresses to be automatically notified when a new referral or email campaign response is received. To set up notifications, complete the following steps:

1. In the menu, go to **Tools > Customer Referrals**.
2. Select **Settings**.
3. Enter the email addresses of people that you want to receive notifications, then select **Save**.

## 26.4.5 Email Campaigns

The Email Campaigns feature enables you to send pre-composed emails to customers who aren't using the Virtual Keypad™ app or don't have specific features enabled on any of their systems.

Emails can be sent once per week. Your company logo, phone, and email address are automatically inserted into each pre-composed email, along with a contact button. When a customer presses the button, they are redirected to a "Thank You" page and their information automatically populates in **Customer Referrals**.

This feature automatically sends emails to all of your customers, but you can exclude specific customers. Customers can also opt out of email campaigns themselves by selecting the link to opt out in the email.

**Note:** Email campaigns are only available to users with permission to access **Dealer Settings**. For more information about permissions, refer to Personnel Roles.

- Exclude a Customer from a Campaign
- Open an Email Campaign
- Set Up Referral Notifications

**Prefer a Video?**

In this clip, we'll show you how to use email campaigns.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://vimeo.com/583431146

### Exclude a Customer from a Campaign

To exclude a customer from email campaigns, complete the following steps.

1. Go to **Customers**.
2. Select the customer name.
3. In **Customer Summary**, select **Edit**.
4. Select the checkbox next to **Exclude from Email Campaigns.**
5. Select **Save**.

### Open an Email Campaign

To open an email campaign, complete the following steps.

1. In the menu, go to **Settings > Dealer > Email Campaigns**.
2. In the row of the email that you want to preview, select **Preview**.
3. The send the email, select **Send**.
4. A dialog pops up to confirm your decision. To send the email to qualifying customers, select **Send**.

### Set Up Referral Notifications

You can add up to six email addresses to be automatically notified when a new referral or email campaign response is received. To set up notifications, complete the following steps:

1. In the menu, go to **Customer Referrals**.
2. Select **Settings**.
3. Enter the email addresses of people that you want to receive notifications, then select **Save**.

## 26.4.6 Log In as a Customer

**Note:** Log in as a customer is only available for Administrative users.

### Enable Log In As Customer

To enable the **Log In As Customer** feature, complete the following steps:

1. Go to **Settings** and select **Dealer**.
2. Go to the **Account** tab.
3. In **Security Features**, select the **Log In As Customer** checkbox.

### Dealer Login as a Customer

To log in to Virtual Keypad as a customer, complete the following steps:

1. Go to **Customers**.
2. Select the customer's name.
3. In **Systems**, find the system's row and select **Log In as Customer**.
4. A dialog box displays to confirm the request. To log in as a customer, select **Login Virtual Keypad**.

To learn how to use Virtual Keypad, refer to Virtual Keypad Help.

### Technical Support Login as a Customer

When enabled, Admin and Technician users can grant DMP Technical Support the ability to utilize Login as Customer for 30 minutes to aid in troubleshooting. DMP Technical Support cannot view customer videos at any time and all actions are audited.

**Note:** If access has not been granted, an error alert pops us.

To enable the Technical Support Login as Customer feature, complete the following steps.

1. Go to **Settings**.
2. Select **Dealer**, then go to the **Account** tab.
3. In **Security Features**, select the checkbox next to **Allow Tech Support Login as Customer**.

To grant a DMP Support Technician access to a system as a customer, complete the following steps.

1. Go to **Customers**.
2. Select the customer's name.
3. In **Systems**, find the system you want to log into.
4. Click the More icon and select **Get Support**.
5. A pop-up window displays to confirm your decision. Select **Authorize Access**.

## 26.4.7 Deactivate Cellular Communicators

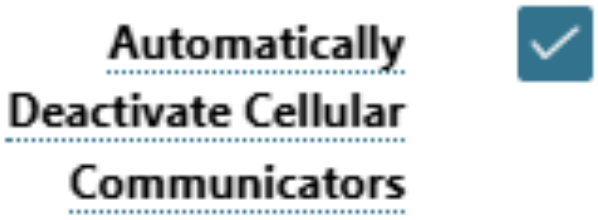
This security feature allows you to automatically deactivate cellular communicators or keep them active after deleting any **Customers** or **Systems**. Deactivating cellular communicators stops all alarm messages and signals from transmitting over cellular network. This feature is disabled by default.

To use this feature, complete the following steps:

1. Go to **Settings**, then select **Dealer**.

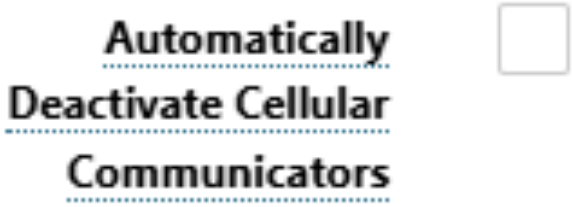
2. In **Security Features**, go to **Automatically Deactivated Cellular Communicators** and complete one of the following actions:

- **Enable** — Select the checkbox to automatically deactivate cellular communicators after deleting **Customers** or **Systems**.




**18 Automatically Deactivate Cellular Communicators**

- **Disable** — Leave the box unchecked to keep cellular communicators active after deleting **Customers** or **Systems**. This feature is disabled by default.




**19 Keep Cellular Communicators Active**