RAPTOR® TECHNOLOGIES

Raptor University

Raptor v6.1.5 System Administration

Instructor:

Table of Contents

This document is intended for users with Administrative permissions and provides information for performing tasks in the Admin menu.

The following topics are covered in this presentation:

- Overview of Raptor Solutions
- View Client Information
- Manage Users and Contacts
- Manage Visitor Module Settings
- Manage Contractor Module Settings
- Manage Student Module Settings
- Manage Staff Module Settings
- Manage Volunteer Module Settings
- Manage Emergency Mgmt Module Settings
- Manage Raptor Link Module Settings
- Manage General Module Settings
- Manage Alerts Settings
- Manage Kiosk Settings
- Maintenance
- Roles and Permissions

Note: The screens and instructions in this section apply to users with District Admin and Building Admin unless otherwise indicated.

RAPTOR TECHNOLOGIES

Overview of Raptor Solutions

Welcome to Raptor Technologies®, the nation's leading provider of integrated school safety technologies. Our mission is to protect every child, every school, every day.

Raptor® Visitor Management

The Raptor Visitor Management System allows you to know exactly who is coming in and out of your schools. Features include instant sex offender screening, custom custody databases, accurate visitor records, district-wide reporting, emergency panic button and more.

Raptor Contractor Module

The Raptor Contractor Module enables you to screen contractors for sex offender status, create and share an approved list of contractors at each school or district wide, view reports on contractor time, location, and hours, and more.

Raptor Student Module

The Raptor Student Module enables you to import data from your SIS, including students and approved guardians for student pick up; track late arrivals, early departures, and record one-time student pickups; conduct a sex offender check on anyone picking up a student; easily track custom alerts including custody orders, and more.

Raptor Staff Module

The Raptor Staff Module enables staff members to sign in and out of buildings, track itinerant staff, monitor staff hours, report on staff members currently in the building, and more.

Raptor Volunteer Management

The Raptor Volunteer Management System streamlines the volunteer process from application to screening and reporting.

First, volunteers apply in an easy-to-use, customizable application. They are then checked for sex offender status and criminal background. Finally, the information is compiled for easy review, approval and tracking. A variety of reports—including volunteer hours and top volunteers—can quickly be accessed and exported.

Overview of Raptor Solutions, cont.

Raptor Emergency Management

The Raptor Emergency Management System is comprised of software—including the Drill Manager tool—and a mobile application, Raptor Reunification. Together in one system, they join best practices with mobile technology to provide emergency managers with a comprehensive solution.

- Raptor Reunification

  The Emergency Management system enables you to use the Raptor Reunification™ mobile app to initiate drills and manage active emergencies, create comprehensive drill reports at the building and district levels, access real-time reports of status and location of every individual during an emergency, quickly retrieve each school's emergency action plans and building maps, and streamline the parent reunification process.

  In this guide, the features that are available with the Raptor Reunification mobile app are indicated by the **REU** icon.

- Drill Manager

  Raptor Drill Manager™ streamlines the communication and tracking of all drills for your district, and is one of many tools in the Raptor Emergency Management module. With Drill Manager, districts can create and publish a schedule of drill requirements to all schools; schools can then see the requirements, download calendar reminders, update the software to show when a drill is completed, and upload any required documentation; districts and schools can receive automated reminders and summary notifications; and districts can view a real-time dashboard of drill compliance for all schools.

  Drill Manager can also be integrated with the Raptor Reunification mobile app for real-time, automated drill satisfaction.

Raptor Link

Raptor Link provides the ability to integrate a Student Information System (SIS) with the Raptor System. This integration enables automatic synchronization of student, approved guardian, staff and roster data into the Raptor System.

In this guide, the features that are available with Raptor Link are indicated by the icon.

View Client Information

Users with Administrative permissions can view client information using these areas of the Raptor user interface under the Admin menu.

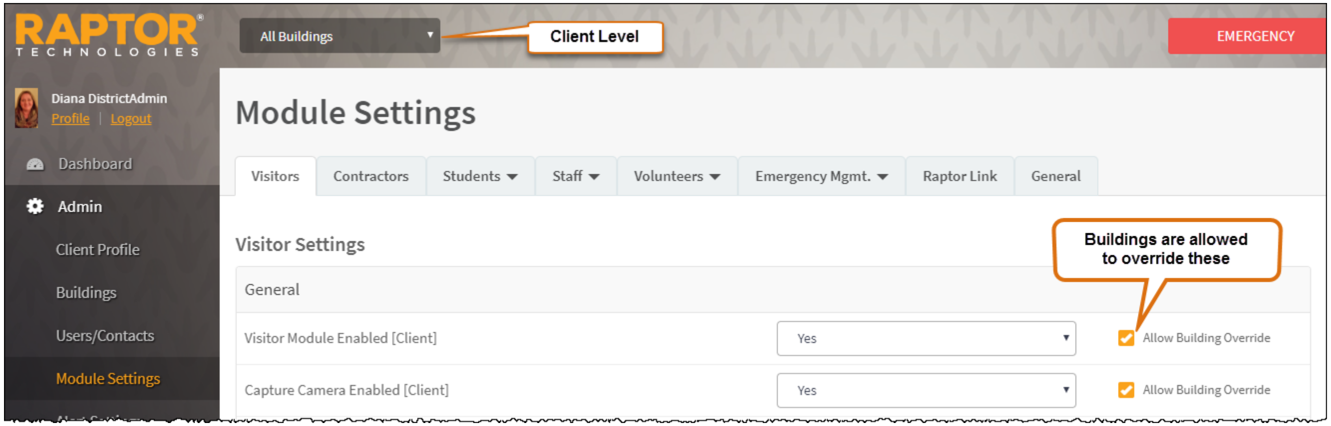
The following topics are covered in this section:

- Understanding Client Policy
- View Client Profile and Building Profile
- View Buildings
- View Logs

Client Policy

It is important to understand that users with District Admin permissions have a different view of some items in the user interface versus a user with Building Admin permissions. This is due to the concept that districts are allowed to set policy for what the individual building (schools) can do. This concept provides these advantages:

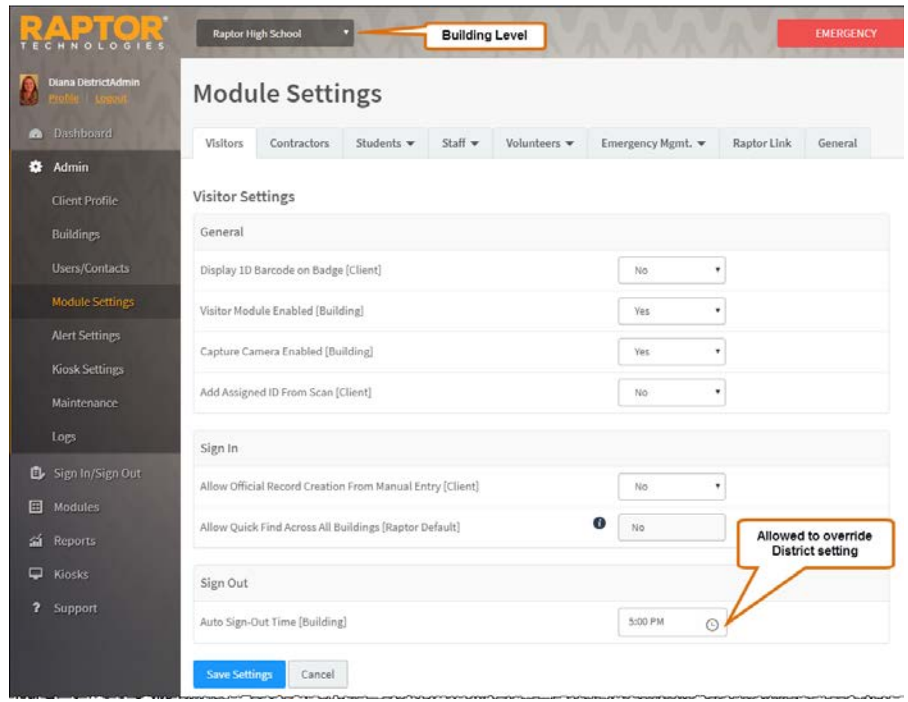
- Client has some level of control over the buildings
- Items used by all buildings can be input once and leveraged by all buildings
- Buildings can have some level of autonomy
- The default value for settings can be set at the client-level (All Buildings) and then the client can decide if the buildings should have the ability to override the default value of these settings. This is achieved by selecting the **Allow Building Override** check box.

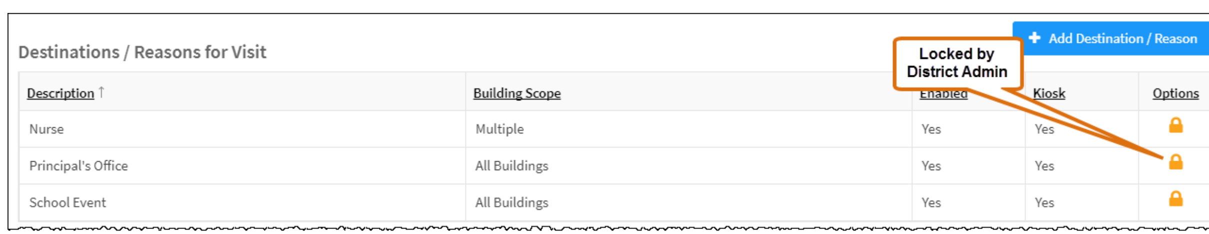


Client Policy, cont.

For example, the district wants all visitors to be automatically signed out at 5:00 p.m. However, for buildings that have classes or activities that run later into the afternoon, these buildings can adjust the auto sign-out time according to their schedule (if the District Admin has selected to Allow Building Override).

For other fields, such as **Destinations/Reasons** and **Custom** fields, the district (client level) can define these fields and they cannot be changed (as indicated by the icon at the building level). However, at the building level, new destinations/reasons can be added that are specific to the building.



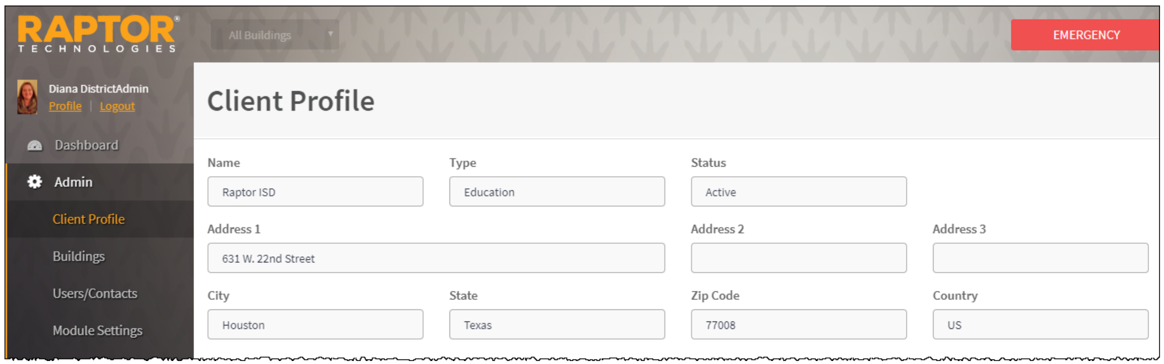


Description	Building Scope	Enabled	Kiosk	Options
Nurse	Multiple	Yes	Yes	
Principal's Office	All Buildings	Yes	Yes	
School Event	All Buildings	Yes	Yes	

View Client Profile/Building Profile

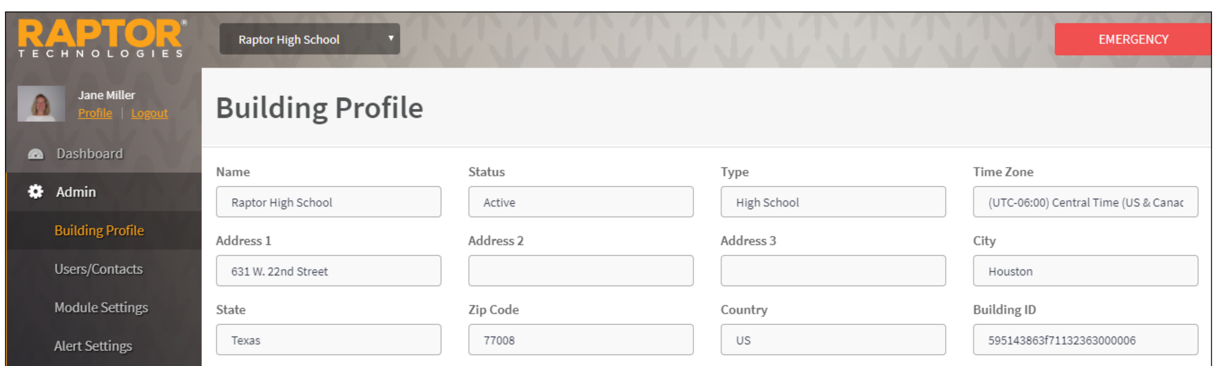
Client Profile

The Client Profile workspace is visible to District Admins to view the client information on file in the Raptor system, such as name, address, and status. You access this workspace by selecting **Admin > Client Profile** in the navigation menu.



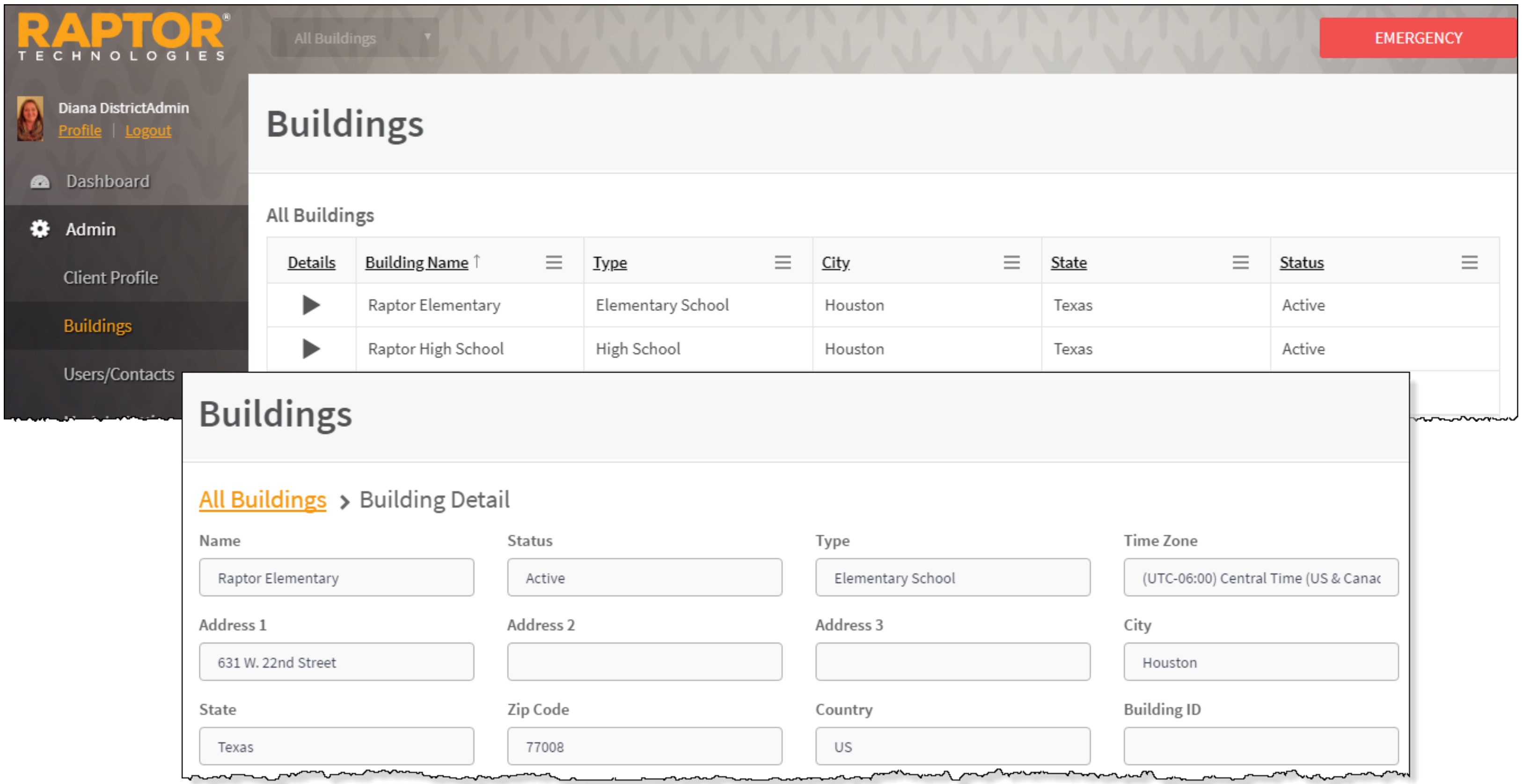
Building Profile

The Building Profile workspace is visible to Building Admins to view the information on file in the Raptor system for specific buildings, such as name, address, and status. You access this workspace by selecting **Admin > Building Profile** in the navigation menu. District Admins have a similar view using the Buildings workspace.



View Buildings

The **Buildings** workspace is visible only to District Admins to view details about the buildings in their district. To access the **Buildings** workspace, select **Admin > Buildings** in the navigation menu. Expand the Building Details to view specific information about a building.

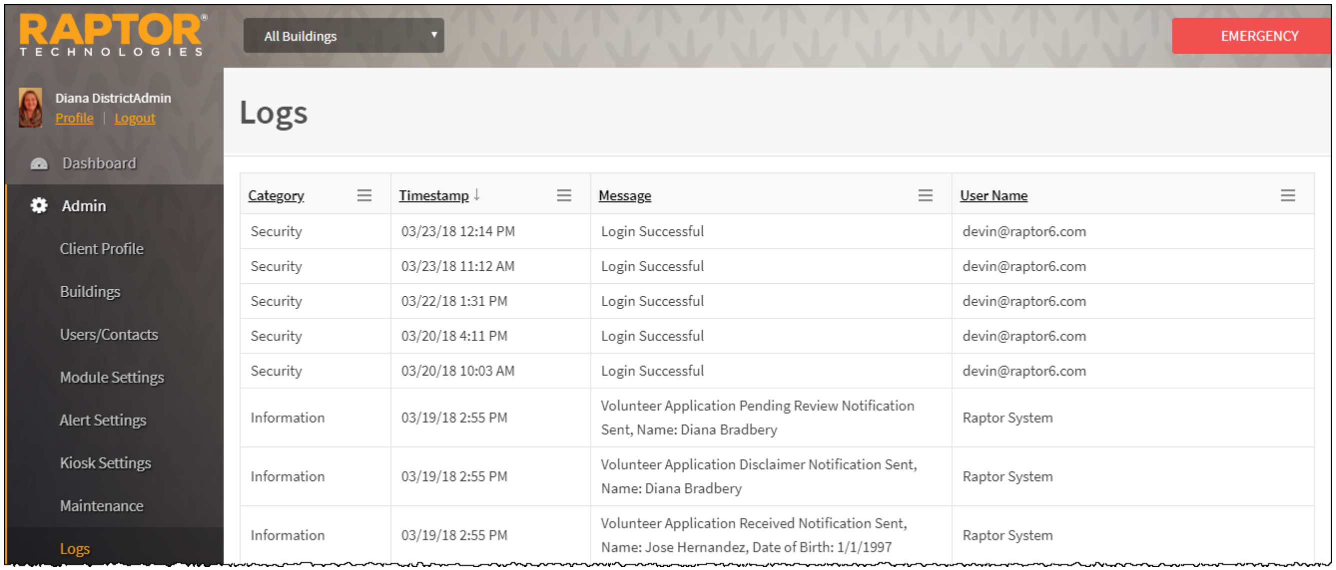


Note: Building Admins can also view the same information in the Building Profile workspace from the building selector.

View Logs

The **Logs** workspace is used by District Admins and Building Admins to view the logged information of activity in the Raptor system. You can sort and filter the information, and add or hide the columns.

To access the Logs workspace, select **Admin > Logs** in the navigation menu.



The following information displays:

- Category – Information, Security, Error or Audit
- Timestamp – Date and Time the activity occurred
- Message – Description of the activity, such as Login Successful
- User Name – Account that performed the activity

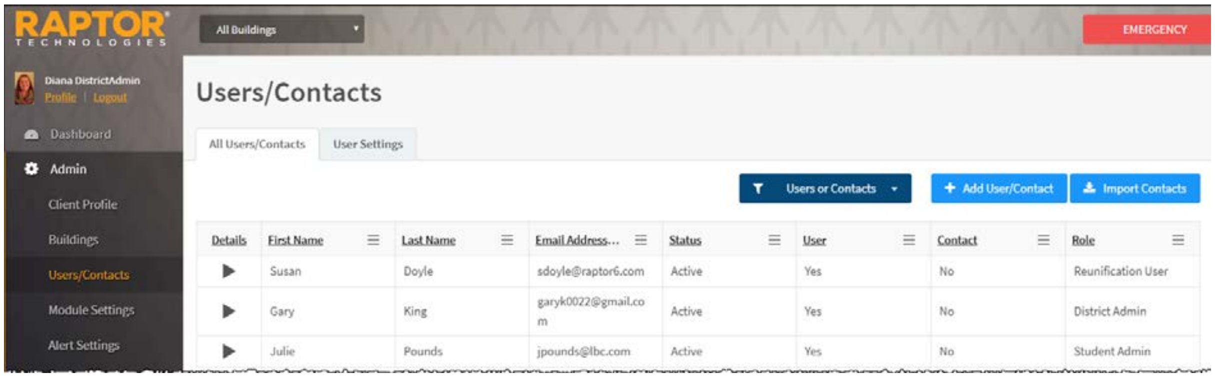
Manage Users/Contacts

You can manage the users in Raptor from the Users menu item under Admin. The following topics are covered in this section:

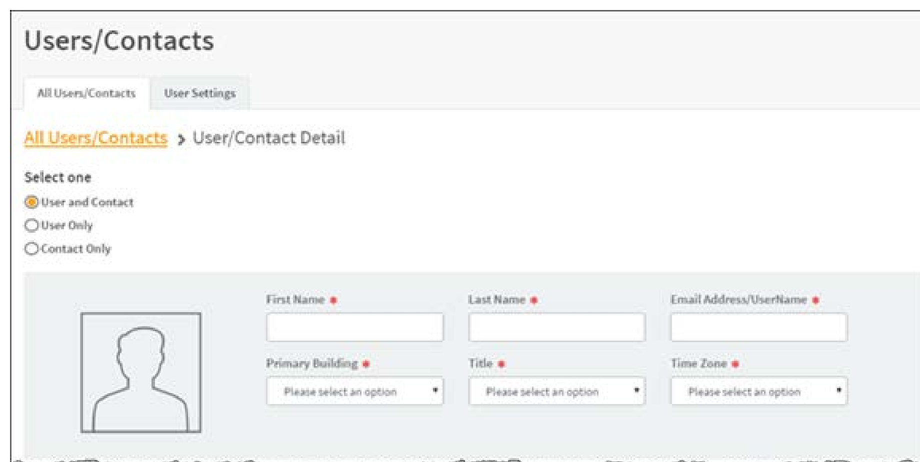
- Add Users and Contacts
- View and Modify Users and Contacts
- View User Details
- Activate and Deactivate Users
- Reset Password
- Import Contacts
- Specify Maximum Failed Logins
- Password Change Requirements

Add User and Contact

Users with the *Can Manage Users* permission can add users and contacts to the Raptor system from the **Users/Contacts** menu item under **Admin**.



1. In the navigation pane, select **Admin > Users/Contacts**.
2. On the **All Users/Contacts** tab, click **Add User/Contact**.
3. Select the **User and Contact** option.
4. On the **User/Contact Detail** workspace, specify the user information in the fields (all fields are required).



Add User and Contact, cont.

5. In the **User Detail** area, specify the **Password** and confirm it, and the **User Status**.
6. In the **Contact Detail** area, specify the **Preferred Contact Method** and the **Phone numbers**.
7. Under **Role and Permissions**, select the **Role** to assign to the user account.
8. In the **Building(s)** field, click **Add Building** and select the building from the drop-down list to specify the building to which the user has permission to view in Raptor. You can add multiple buildings if the role allows for this.

   Note: If the Role is set to *District Admin* or *District Volunteer Coordinator*, this field does not display since they can access all buildings.
9. Select the **Reunification Mobile App Primary Role** REU from the drop-down list.
10. Depending on the role that is selected, the allowable permissions display in the lower portion of the Role and Permissions section. Select the check box next to each permission you want the user to be granted. See Roles and Permissions.

    Note: If the check box has the icon next to it, the user creating the new account does not have permission to grant that specific permission.
11. Click **Save**.

You are returned to the **All Users/Contacts** workspace and a message displays indicating the new user was successfully saved.

Add User Only

1. In the navigation menu, select **Admin > Users/Contacts**.
2. On the **All Users/Contacts** tab, click **Add User/Contacts**.
3. Select the **User Only** option and enter the user information in the fields (all fields are required).
4. Under **Role and Permissions**, select the **Role** to assign to the user account.
5. In the **Building(s)** field, click **Add Building** and select the building from the drop-down list to specify the building to which the user has permission to view in Raptor. You can add multiple buildings if the role allows for this.

   Note: If the Role is set to District Admin or District Volunteer Coordinator, this field does not display since they can access all buildings.

6. Select the **Reunification Mobile App Primary Role** REU from the drop-down list.
7. Depending on the role that is selected, the allowable permissions display in the lower portion of the Role and Permissions section. Select the check box next to each permission you want the user to be granted. See Roles and Permissions.

   Note: If the check box has the icon next to it, the user creating the new account does not have permission to grant that specific permission.

8. Click **Save**.

You are returned to the **All Users/Contacts** workspace and a message displays indicating the new user was successfully saved.

Add Contact Only

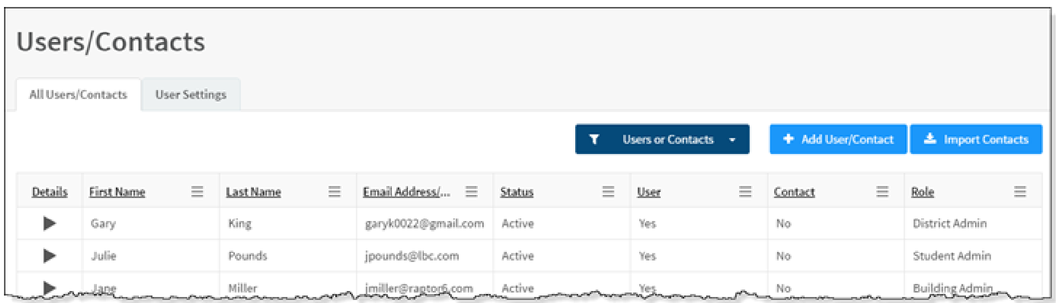
1. In the navigation menu, select **Admin > Users/Contacts**.
2. On the **All Users/Contacts** tab, click **Add User/Contacts**.
3. Select the **Contact Only** option and enter the user information in the fields (all fields are required).
4. In the **Contact Detail** area, specify the **Preferred Contact Method** and the **Phone number** to be used for notifications.
5. Click **Save**.

   You are returned to the **All Users/Contacts** workspace and a message displays indicating the new user was successfully saved.

View and Modify Users/Contacts

Users with the *Can Manage Users* permission can view all users that have been added to the Raptor system on the **All Users/Contacts** workspace.

1. In the navigation menu, select **Admin > Users/Contacts**.
2. From the Building Selector, select the **building** or select **All Buildings**.
3. On the **All Users/Contacts** tab, click **Users and Contacts** and then select one of the following options: **Users or Contacts**, **Users**, or **Contacts**.



4. Scroll to the user account or contact that you would like to view or modify and click the ▶ icon to expand the **User/Contact Detail**.
5. Modify any of the current account information, or change the account type as follows:
   - Change a *user and contact* account to only a *user account* or only a *contact* (see Modify User and Contact Account).
   - Change a *user account* to only a *contact* or to a *user and contact* (see Modify User Only Account).
   - Change a *contact* to only a *user account* or a *user account and contact* (see Modify Contact Only).
6. When you have completed your changes, click **Save**.

RAPTOR TECHNOLOGIES

View and Modify Users/Contacts, cont.

Modify User and Contact Account

If the account is currently defined as a **User and Contact**, you can change it to a **User Only** or **Contact Only** account.

1. On the **User/Contact Detail** workspace, click one of the following options:
   - **User Only** – to collapse the contact information for the user account; the user no longer receives notifications.
   - **Contact Only** – to collapse the user details, and role and permissions for the account; the user can no longer log in as a user and they will only receive notifications.
2. Click **Save**.

Note: If you change a **User and Contact** to a **User Only** or **Contact Only**, the user and/or contact information is not deleted; it is only disabled. Subsequently, if you re-enable the user or contact, that information will be reinstated except for the password, which must be re-entered and confirmed.

View and Modify Users/Contacts, cont.

Modify User Only Account

If the account is currently defined as a **User Only**, you can change it to a **User and Contact** or **Contact Only** account.

1. On the **User/Contact Detail** workspace, click one of the following options:
   - **User and Contact** – to expand the **Contact Details** and **Contact Notifications** grids on the workspace.
   - **Contact Only** – to collapse the user information for the account; the user can no longer log in as a user and they will only receive notifications.
2. If you selected **User and Contact**, complete the contact details and contact notifications for the user account and then click **Save**.

Modify Contact Only

If the account is currently defined as a Contact Only, you can change it to a User and Contact or User Only account.

1. On the **User/Contact Detail** workspace, click one of the following options:
   - **User and Contact** – to expand the **User Detail** area on the workspace.
   - **User Only** – to collapse the **Contact Detail** and **Contact Notifications** grids on the workspace, and expand the **User Detail** area.
2. Complete the user details for the user account and then click **Save**.

View and Modify Users/Contacts, cont.

View and Modify Contact Notifications

Users with the *Can Manage Client Settings* or *Can Manage Building Settings* permission can view all notifications that are associated with a contact.

1. On the **User/Contact Detail** workspace, in the **Notifications** grid, view the notifications which are associated with the contact.
2. If you would like to modify a method for notification (Email, Text or Voice), click the icon and select the appropriate check boxes, and then click the icon to save your changes.

Note: You can only select a check box for a notification method specified in the Contact Detail. For example, if Voice was not selected as a method of notification, the check box will be disabled.

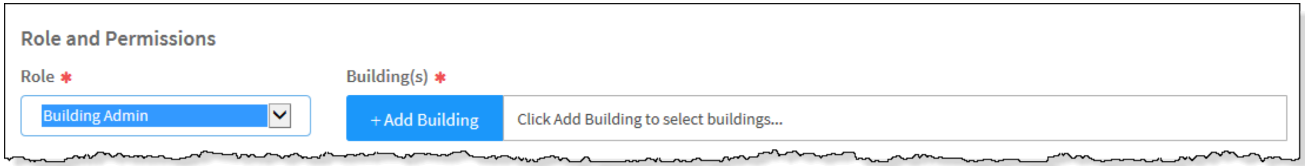
Contact Notifications

Type	Building Scope	Email	Text	Voice	Options
Sex Offender Alert	All Buildings	Yes	Yes	N/A	

Modify User Role and Permissions

When users are added to Raptor, their role and permissions are set during the account creation. Administrators can modify user roles and permissions using the following procedure.

1. In the navigation menu, select **Admin > Users/Contacts**.
2. On the **All Users/Contacts** tab, click **Users and Contacts** and then select one of the following options:
   - **Users and Contacts** – to display all users and contacts.
   - **Users** – to display only user accounts.
3. Navigate to the user account and click the ▶ icon to view the **User/Contact Detail**.
4. Under **Role and Permissions**, select the **Role** to assign to the user account. See <u>Understanding User Accounts</u>.



5. In the **Buildings** field, click **Add Building** and select the building from the drop-down list to specify the building to which the user has permission to view in Raptor. You can add multiple buildings if the role allows for this.
6. Select the check box next to each task that the user is granted permission.
7. Click **Save**.

Note: If the user is logged in when their roles or permissions have been modified, they must log out of Raptor and then log in before the new roles and/or permissions take effect.

RAPTOR TECHNOLOGIES

View User Details

You can view details about the user account, such as when it was created or modified, the number of failed login attempts, and the last time the user logged into Raptor.

1. In the navigation menu, select **Admin > Users/Contacts**.
2. From the Building Selector, select the **building** or select **All Buildings** to display all users.
3. On the **All Users/Contacts** tab, click **Users or Contacts** and then select one of the following options: **Users or Contacts** or **Users**.
4. Scroll to the user account you would like to view or modify and click the ▶ icon to expand the **User/Contact Detail**.
5. In the **User Password and Detail** area, view the following information:
   - **User Status*** – Current status of the user account. You can change the status of the user account. See Activate and Deactivate Users.
   - **Last Login** – Date and time the user last logged into Raptor.
   - **Failed Logins** – Number of times the user has attempted to log in with invalid credentials.
   - **Reset Failed Logins** – This button displays when 1 or more failed log in attempts has been recorded. Click **Reset Failed Logins** to reset the count to 0.
   - **Created Date/Time** – Date and time the user account was created.
   - **Created By** – The user who created the user account.
   - **Modified Date/Time** – Date and time the user account was last modified.
   - **Reset Password** – You can reset the password for the user account from this area. See Reset Password.

RAPTOR TECHNOLOGIES

Activate and Deactivate Users

You can activate or deactivate a user account from the **User/Contact Detail** workspace.

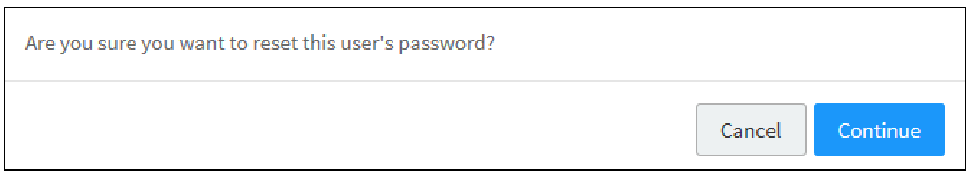
Note: If a user account has been deactivated, the user will see a message "Your account has been locked, contact your administrator" when they attempt to log in.

1. In the navigation menu, select **Admin > Users/Contacts**.
2. From the Building Selector, select the **building** or **All Buildings**.
3. On the **All Users/Contacts** tab, scroll to the user account you would like to view or modify and click the ▶ icon to expand the record.
4. In the **User Status** field, select **Active** or **Deactivated** from the drop-down menu.
5. Click **Save**.

Reset Password

Administrators can reset a user's password from the **User/Contact Detail** workspace.

1. In the navigation menu, select **Admin > Users/Contacts**.
2. From the Building Selector, select the **building** or **All Buildings**.
3. On the **All Users/Contacts** tab, scroll to the user account that you want to change the password and click the ▶ icon to expand the details.
4. In the **User Password and Detail** area, click **Reset Password**.
5. On the confirmation dialog, click **Continue** to reset the password.

   The system auto-generates a new password for the user. A drop-down message displays the changed password.
6. Click **OK**.

RAPTOR TECHNOLOGIES

Import Contacts

Administrators with the *Can Manage Users* permissions can select, map, and import a file containing one or more contact records into the system.

Note: To use this feature, you must first create an Excel spreadsheet or comma delimited file that contains the required information.

The file can contain the following contact information to be imported:

- First Name*
- Last Name*
- Email Address*
- Title*
- Notification Method*
- Text Phone – required only if defined as a notification method
- Voice Phone – required only if defined as a notification method
- Primary Building – required only if you are importing contacts for All Buildings

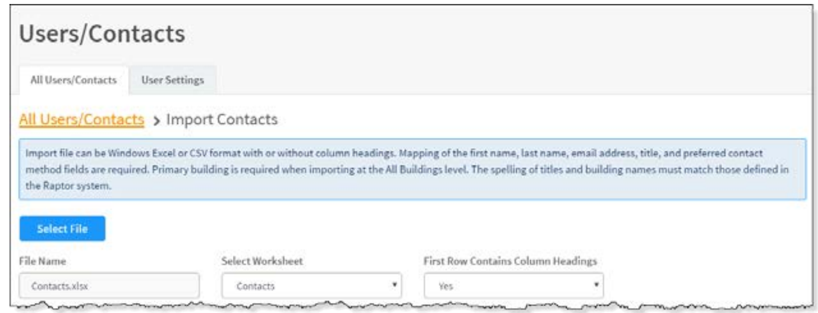
Note: Primary Building is not a field mapping option at the building level. The building in the building selector will be used.

RAPTOR TECHNOLOGIES

Import Contacts, cont.

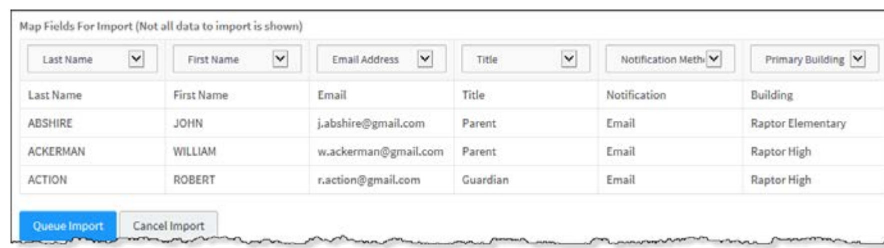
Perform the following steps to import contacts:

1. In the navigation menu, select **Admin > Users/Contacts** and then click **Import Contacts**.
2. Click **Select File**, navigate to the Excel or CSV file and click **Open**.
3. If you used Excel and the file contains multiple worksheets, select the worksheet that contains the custom alert information from the **Select Worksheet** drop-down list.



4. If the first row of the worksheet contains column headings, select **Yes** from the **First Row Contains Column Headings** drop-down list. Otherwise, select **No**.
5. Map each of the columns to be imported by selecting the appropriate fields in the drop-down menu above each column that displays.

   Note: First Name, **Last Name**, **Email Address**, **Title** and **Notification Method** are required. The columns with **Ignore** selected with not be imported.



6. Click **Queue Import**. A message displays in the lower right corner of the screen stating that the import job was successfully added to the import queue for processing.

   When the import has completed processing, an email will be sent to the email address of the user indicating the number of records successfully imported and any error that may have occurred.

Maximum Failed Logins

In Raptor, there are two thresholds for locking user accounts after failed login attempts—a threshold set by the system and a threshold specified by the user.

The system threshold allows the user five consecutive failed login attempts before they are locked out of their account for 15 minutes. After three failed login attempts, a message will display warning the user that after five failed attempts, they will be locked out of their account. If they reach the threshold of five failed login attempts, the message *Your account has been locked for 15 minutes* displays and they must wait 15 minutes before attempting to login again.

The second threshold is set on the **User Settings** tab and after the specified number of failed logins has been reached, they are locked out of their account and must contact an Administrator.

When either of the thresholds is reached, an appropriate message is written to the Logs. If a user successfully logs in before reaching either threshold, the number of failed logins is reset to 0/10.

Set Maximum Failed Logins

1. From the navigation menu, select **Admin > Users/Contacts**.
2. Click the **User Settings** tab.
3. From the **Maximum Failed Logins** drop-down list, select the number of failed login attempts that are allowed before the user account is locked and must be reset by an Administrator. By default, the number of attempts is set to 10.
4. Click **Save Settings**.

Note: If this setting is 5 or less, only the user specified threshold will be active and the user will be locked out of their account and must contact an Administrator. Also, the system will not report the number of failed login attempts in the Logs.

Manage Password Change Requirements

Users with the *Can Manage Users* permission can specify whether to require a new user to change their password after their first login to Raptor.

1. From the navigation menu, select **Admin > Users/Contacts**.
2. Click the **User Settings** tab.
3. In the **Require Password Change Upon First Login** field, select **Yes** (to enable) or **No** (to disable). The default setting is **No**.
4. Click **Save Settings**.

Manage Visitor Module Settings

Users with Administrative permissions can manage what displays in the Visitors module using the Visitors tab on the Module Settings workspace.

The following topics are covered in this section:

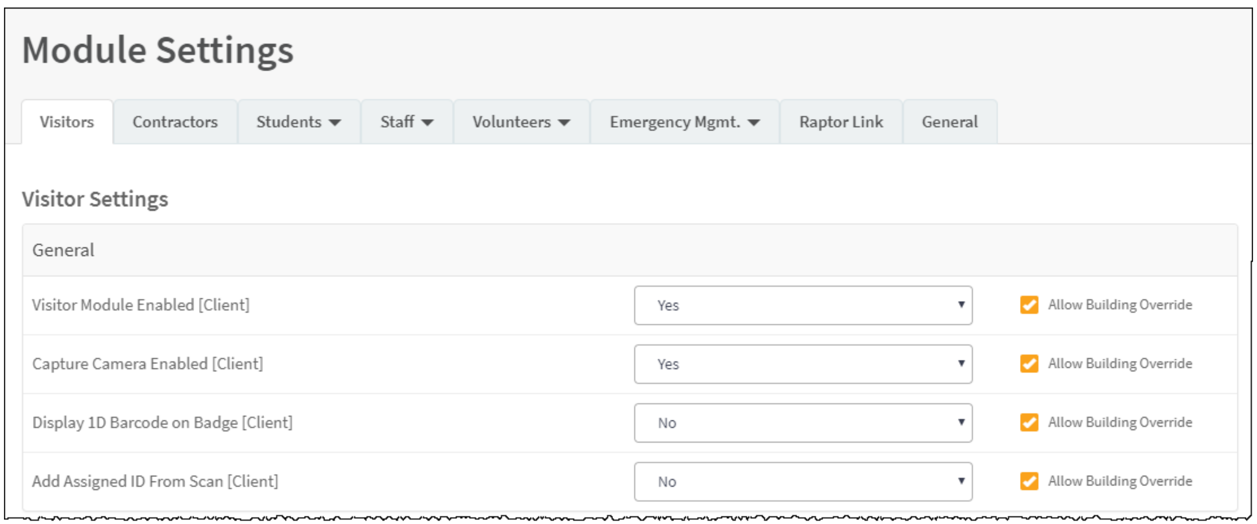
- Visitor Module Settings Workspace
- Enable/Disable Visitor Module
- Enable/Disable Capture Camera
- Display 1D Barcode on Badge
- Add Assigned ID From Scan
- Specify Sign-In Settings
- Specify Auto Sign-Out Time
- Add Destinations/Reasons for Visit
- Modify and Delete Destinations/Reasons for Visit
- Manage Custom Profile Fields
- Manage Custom Sign In Fields

Visitor Module Settings

Users with Administrative permissions can manage what displays in the Visitors module using the **Module Settings** workspace. You access this workspace by selecting **Admin > Module Settings** in the navigation menu.

On the **Visitor Module Settings** workspace, the **Allow Building Override** check box is only available when specifying settings for All Buildings (client level).

It is assumed that all procedures in this section are performed at the client level (All Buildings is selected in the Building Selector). If you want to specify settings for a specific building, select that building from the Building Selector before performing the procedure.



Enable/Disable Visitor Module

By default, Raptor is configured with the Visitors Module enabled. Users can disable this module and all Visitor options will be hidden in the navigation menu, and on the **Sign In/Sign Out** workspace and **Reports** workspace. The Visitor dashboards will also be hidden once the user logs out and logs back in after disabling the module.

1. In the navigation menu, select **Admin > Module Settings**.
2. On the **Visitors** tab, in the **Visitor Module Enabled** drop-down list, select **Yes** (to enable) or **No** (to disable).
3. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.

   Note: You must be at the client level (All Buildings) to see the **Allow Building Override** check box.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Enable Capture Camera

The capture camera feature allows the user to take a photo of the person signing in and associate that photo with the person's record in the Raptor system. This feature is useful when the person signing in does not have an official ID that can be scanned, such as a passport.

By default, Raptor is configured with the Capture Camera disabled. Users can enable this feature using the **Capture Camera Enabled** setting on the **Visitor Module Settings** workspace. When the capture camera is enabled, the Camera button displays on the **Sign In** workspace below the photo.

1. In the navigation menu, select **Admin > Module Settings**.
2. On the **Visitors** tab, from the **Capture Camera Enabled** drop-down list, select **Yes** (to enable) or **No** (to disable).
3. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Note: A camera is required to use this feature. If you are using a Windows Internet Explorer (IE) browser, you must have Adobe Flash Player installed to use the Capture Camera feature.

Display 1D Barcode on Badge

Users with Administrative permissions can control whether or not a 1D barcode is printed on the visitor badge. If the 1D barcode is printed on the badge, the visitor can simply scan the code on their badge when signing out at the front desk or kiosk.

1. In the navigation menu, select **Admin > Module Settings**.
2. On the **Visitors** tab, in the **Display 1D Barcode on Badge** drop-down list, select **Yes** (to enable) or **No** (to disable).
3. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Add Assigned ID From Scan

Users with the *Can Manage Visitors Settings* permission can specify whether to allow a 1D barcode to be captured from a visitor's ID card and populated in the **Assigned ID** field for that visitor.

1. In the navigation menu, select **Admin > Module Settings**.
2. On the **Visitors** tab, in the **Add Assigned ID From Scan** drop-down list, select **Yes** (to enable) or **No** (to disable).
3. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Specify Sign-In Settings

Users with the *Can Manage Visitor Settings* permission use the Visitor Module Settings workspace to manage visitor sign-in settings.

1. In the navigation menu, select **Admin > Module Settings**.
2. On the **Visitors** tab, in the **Sign In** area, specify the following settings:
   - **Allow Official Record Creation From Manual Entry** – Select **Yes** (to allow) or **No** (to not allow) to indicate whether the **Official Record** check box displays on the **Visitor Sign In** workspace when using manual entry.
   - **Allow Quick Find Across All Buildings** – Select **Yes** (to allow) or **No** (to not allow) to indicate whether the Quick Find feature will return the visitor if they have been scanned into any building district-wide. This feature can only be used for visitors who have an official record for at least one of the client's buildings. The default value for this setting is **No**.
   - **Allow Building Override** – Select the check box if the setting can be overridden at the building level. Otherwise, clear the check box.
3. Click **Save Settings**.
4. Log out of Raptor and then log in to see the change.

Visitor Auto Sign-Out Time

By default, Raptor is configured to automatically sign out all visitors at 5:00 PM. Users with Administrator permissions can change this time and also specify whether the setting can be overridden at the building level.

1. In the navigation menu, select **Admin > Module Settings**.
2. On the **Visitors** tab, in the **Auto Sign Out Time** field, click the icon and select the time from the drop-down list.
3. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
4. Click **Save Settings** when you have completed any changes.
5. Log out of Raptor and then log in to see the change.

Visitor Destinations/Reasons for Visit

This area of the **Visitor Module** workspace enables you to manage the destination/reasons that display in the Sign In workspace.

Destinations / Reasons for Visit

Add Destination / Reason

Details	Description ↑	Building Scope	Enabled	Kiosk	Options
▶	Nurse	Multiple	Yes	No	
▶	Principal's Office	All Buildings	Yes	No	
▶	School Event	All Buildings	Yes	No	

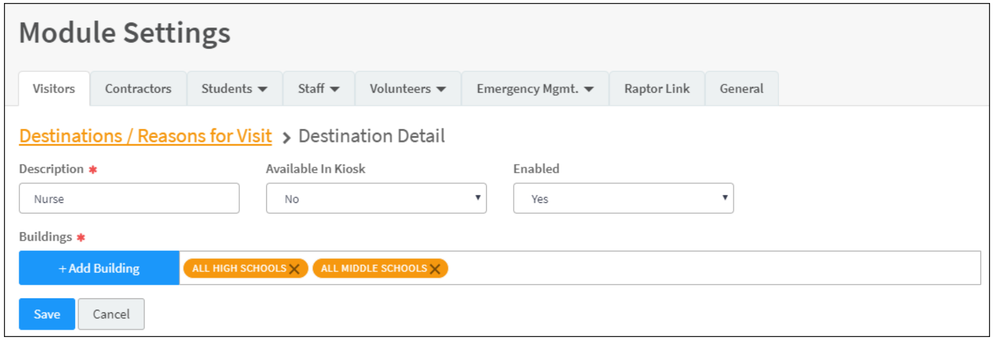
Add Destination/Reason

1. In the navigation menu, select **Admin > Module Settings**.
2. On the **Visitors** tab, in the **Destinations/Reasons for Visit** grid, click **Add Destination/Reason**.
3. Enter a name for the destination or reason in the **Description** text field.
4. If you want to disable the destination/reason for visit (it will not display on the Visitor Sign In workspace) clear the **Enabled** check box.
5. If you want to disable the destination/reason for visit in the Kiosk, clear the **Kiosk** check box.
6. Click the ✔ icon to save the new destination/reason for visit. If you want to discard your changes, click the ⊗ icon.

Modify Visitor Destinations/Reasons

You can edit destinations/reasons for visit items to the field drop-down list, enable or disable the item, or change the setting for whether it displays in the Kiosk.

1. In the navigation menu, select **Admin > Module Settings**.
2. On the **Visitors** tab, in the **Destinations/Reasons for Visit** grid, click the ▶ icon to expand the **Destination Detail**.



3. Modify the any of the information and click **Save**.

You can also click the ✎ icon in the **Options** column in the **Destinations/Reasons for Visit** grid on the **Visitor Module Settings** workspace to edit the Description name and enable/disable the Kiosk setting and the Enabled setting. Click the ✔ icon to save your changes. If you want to discard your changes, click the ✖ icon.

Delete Destinations/Reasons for Visit

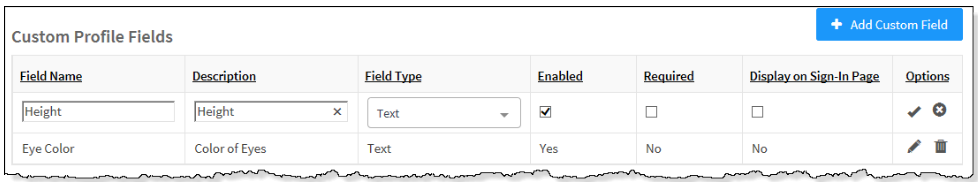
To remove a **Destinations/Reasons for Visit** item, click the 🗑 icon in the **Destinations/Reasons for Visit** grid on the **Visitor Module Settings** workspace and then click **OK** on the confirmation dialog.

Visitor Custom Profile Fields

A Custom Profile field is associated with the person being signed in (such as eye color) and displays on the **Visitor Details** workspace. It may also be configured to display on the **Sign In/Sign Out** workspace.

Note: Custom Profile fields are not available in the Kiosk.

1. In the navigation menu, select **Admin > Module Settings**.
2. On the **Visitors** tab, in the **Custom Profile Fields** grid, click **Add Custom Field**.



3. Enter the **Field Name** and **Description** in the text boxes.
4. From the **Field Type** drop-down list, select the type of field (Lookup, Text, Text Area).
5. Select or clear the **Enabled** check box.
6. If this is a required field that must be completed during sign in, select the **Required** check box.
7. Select the **Display on Sign-In Page** check box if you want the field to display on the **Sign In** workspace.

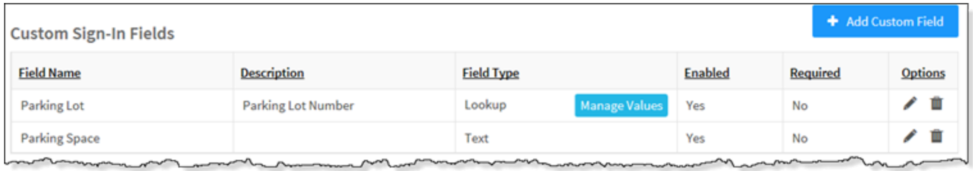
   Note: Custom Profile fields are displayed on the **Sign In** workspace only if the **Display on Sign-In Page** check box is selected. This field displays as read-only unless using the manual entry feature.
8. Click the ✔ icon to save the newly created custom field. To discard your changes, click the ✖ icon.
9. If the Lookup field type is selected, click **Manage Values** to specify the Lookup Values for the field.
10. Click **Add Lookup Value**, enter the Value in the text field and click ✔ to save it.

RAPTOR TECHNOLOGIES

Visitor Custom Sign In Fields

You can create custom sign-in fields that are associated with sign-in events (such as parking space) to display on the **Visitor Sign In** and **Visitor Delayed Entry** workspaces for all buildings or specific buildings.

1. In the navigation menu, select **Admin > Module Settings**.
2. On the **Visitors** tab, in the **Custom Sign In Fields** grid, click **Add Custom Field**.
3. Enter the **Field Name** and **Description** in the text fields.
4. In the **Field Type**, select the type of field (Lookup, Text, Text Area).
5. Select or clear the **Enabled** check box.
6. If this is a required field that must be completed during sign in, select the **Required** check box.
7. Click the icon to save the newly created custom field.
8. If the Lookup field type is selected, click **Manage Values** to specify the **Lookup Values** for the field.
9. Click **Add Lookup Value**, enter the Value in the text field and click to save it.



Note: Custom Sign In fields are not available in the Kiosk.

Modify or Delete Custom Fields

To modify either custom profile fields or custom sign-in fields, click the icon and edit the information. Click the icon to save your changes.

To delete a custom profile or custom sign-in field, click the icon and then click **OK** on the confirmation dialog.

Manage Contractor Module Settings

Users with Administrative permissions can manage what displays in the Contractors module using the **Contractors** tab on the **Module Settings** workspace.

The following topics are covered in this section:

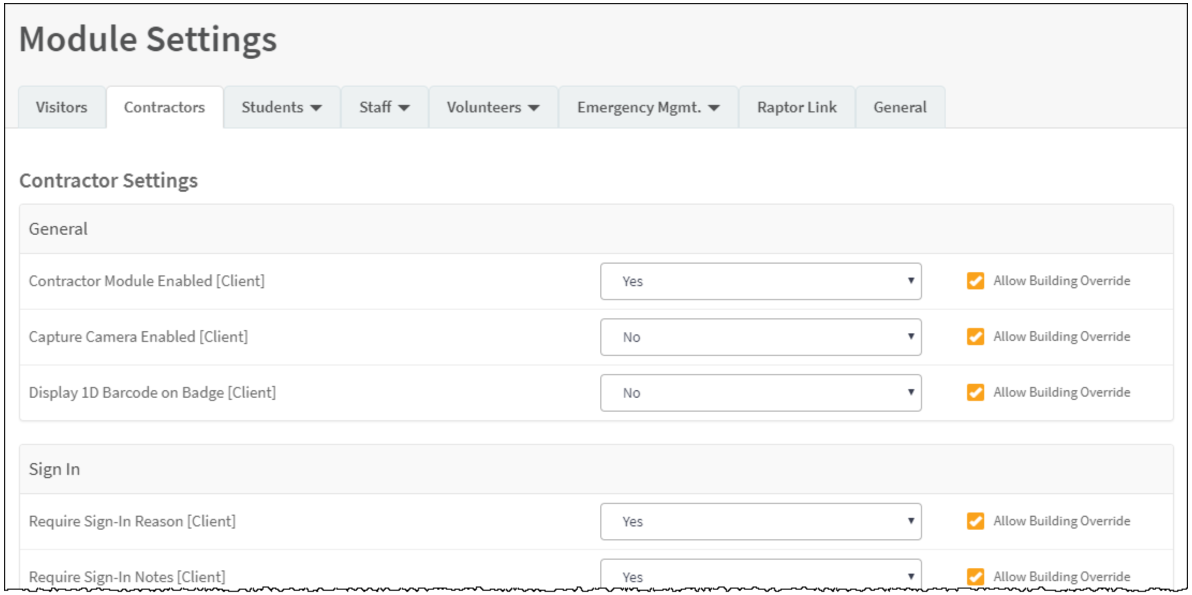
- Contractor Module Settings Workspace
- Enable/Disable Contractor Module
- Enable/Disable Capture Camera
- Display 1D Barcode on Badge
- Specify Sign-In Settings
- Specify Auto Sign-Out Time
- Add Destinations/Reasons for Visit
- Modify and Delete Destinations/Reasons for Visit
- Manage Companies
- Manage Custom Profile Fields
- Manage Custom Sign In Fields

Contractor Module Settings

Users with Administrative permissions can manage what displays in the Contractors module using the **Module Settings** workspace. You access this workspace by selecting **Admin > Module Settings** in the navigation menu.

On the **Contractor Module Settings** workspace, the **Allow Building Override** check box is only available when specifying settings for All Buildings (client level).

It is assumed that all procedures in this section are performed at the client level (All Buildings is selected in the Building Selector). If you want to specify settings for a specific building, select that building from the Building Selector before performing the procedure.



Enable/Disable Contractor Module

By default, Raptor is configured with the Contractor Module enabled. Users can disable this module and all Contractor options will be hidden in the navigation menu, and on the **Sign In/Sign Out** workspace and **Reports** workspace. The Contractor dashboards will also be hidden once the user logs out and logs back in after disabling the module.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Contractors** tab.
3. From the **Contractor Module Enabled** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if you want buildings to be able to enable or disable the Contractor module. Otherwise, clear the check box.

   Note: You must be at the client level (All Buildings) to see the **Allow Building Override** check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Enable Capture Camera

The capture camera feature allows the user to take a photo of the person signing in and associate that photo with the person's record in the Raptor system. This feature is useful when the person signing in does not have an official ID that can be scanned, such as a passport.

By default, Raptor is configured with the Capture Camera disabled. Users can enable this feature using the **Capture Camera Enabled** setting on the **Contractor Module Settings** workspace. When the capture camera is enabled, the Camera button displays on the **Sign In** workspace below the photo.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Contractors** tab.
3. From the **Capture Camera Enabled** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Note: A camera is required to use this feature. If you are using a Windows Internet Explorer (IE) browser, you must have Adobe Flash Player installed to use the Capture Camera feature.

Display 1D Barcode on Badge

Users with Administrative permissions can control whether or not a 1D barcode is printed on the contractor badge. If the 1D barcode is printed on the badge, the contractor can simply scan the code on their badge when signing out at the front desk or kiosk.

Perform the following steps to display the 1D barcode on the contractor badge:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Contractors** tab.
3. From the **Display 1D Barcode on Badge** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Contractor Sign-In Settings

Use these settings to specify whether a reason and notes are required when a contractor signs in.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Contractors** tab.
3. Specify whether the following fields are required to be completed during sign in and whether individual buildings can override these settings:
   - **Require Sign In Reason** – Select **Yes** or **No** from the drop-down list to specify whether the reason for sign in is required.
   - **Require Sign In Notes** – Select **Yes** or **No** from the drop-down list to specify whether notes must be entered during sign in.
   - **Allow Sign In For Approved Contractors Only** – Select **Yes** or **No** from the drop-down list to specify whether contractor sign in and sign out using the Find feature is restricted to contractors that have been approved by the district and have been created or imported into the Raptor System. When this setting is enabled, contractors can only sign in with operator-assisted Quick Find and Delayed Entry.
   - **Allow Building Override** – Select or clear the check box for each of the fields. If selected, the settings can be overridden at the building level. Otherwise, clear the check boxes.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Contractor Auto Sign-Out Time

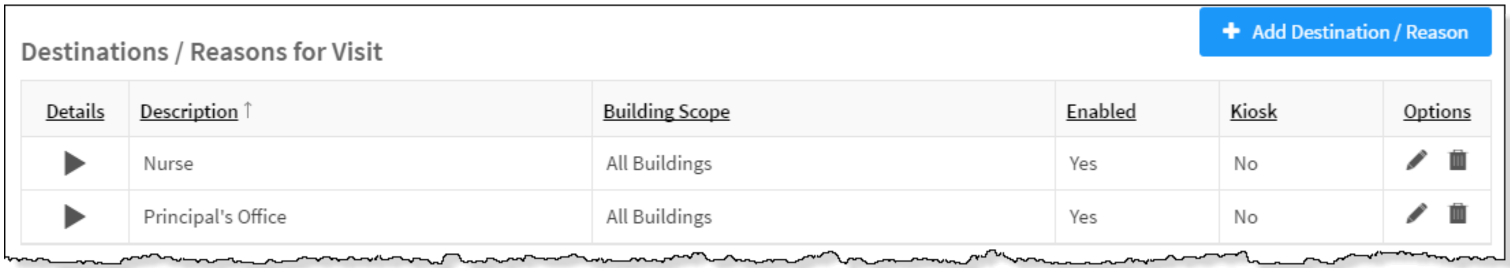
By default, Raptor is configured to automatically sign out all contractors at 5:00 PM. Users with Administrator permissions can change this time and also specify whether buildings can override this setting.

Perform the following steps to modify the auto-sign out time:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Contractors** tab.
3. In the **Auto Sign Out Time** field, click the icon and select the time from the drop-down list.
4. Select the **Allow Building Override** check box if you want buildings to be able to change this time. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Contractor Destinations/Reasons

This grid on the **Contractor Module** workspace enables you to manage the destination/reasons that display in the **Sign In** workspace.



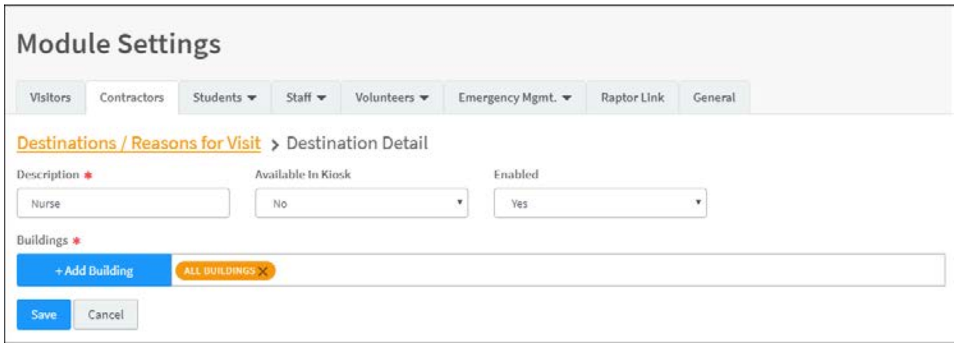
Add Destination/Reason

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Contractors** tab.
3. In the **Destinations/Reasons for Visit** grid, click **Add Destination/Reason**.
4. Enter a name for the destination or reason in the **Description** text field.
5. If you want to disable the destination/reason for visit (it will not display on the **Contractor Sign In** workspace) clear the **Enabled** check box.
6. If you want to disable the destination/reason for visit in the Kiosk, clear the **Kiosk** check box.
7. Click the ✔ icon to save the new destination/reason for visit. If you want to discard your changes, click the ⊗ icon.

Modify Destinations/Reasons

You can edit destinations/reasons for visit items to the field drop-down list, enable or disable the item, or change the setting for whether it displays in the Kiosk.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Contractors** tab.
3. In the **Destinations/Reasons for Visit** grid, click the ▶ icon to expand the **Destination Detail**.



4. Modify the any of the information and click **Save**.

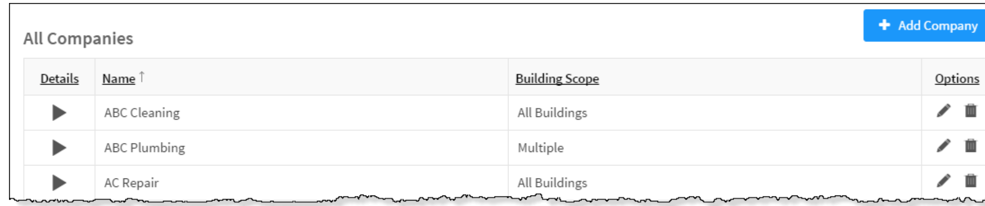
You can also click the ✎ icon in the **Options** column in the **Destinations/Reasons for Visit** grid on the **Contractor Module Settings** workspace to edit the **Description** name and enable/disable the **Kiosk** setting and the **Enabled** setting. Click the ✔ icon to save your changes. If you want to discard your changes, click the ⊗ icon.

Delete Destinations/Reasons for Visit

To remove a **Destinations/Reasons for Visit** item, click the 🗑 icon in the **Destinations/Reasons for Visit** grid on the **Contractor Module Settings** workspace and then click **OK** on the confirmation dialog.

Manage Companies

The companies who employ the contractors are listed in the **All Companies** grid on the **Contractors** workspace.



Note: When you import contractors and include the company name, the company is automatically added to the list of companies.

Add Company

1. In the navigation menu, select **Admin > Module Settings** and click the **Contractors** tab.
2. In the **All Companies** grid, click **Add Company**.
3. Enter the **Name** of the company in the text field and click the icon to save it. If you want to discard your changes, click the icon.

Modify Building Scope for Companies

Once a company is added, you can modify the buildings the contractor is associated with in the Company Details (if All Buildings is selected).

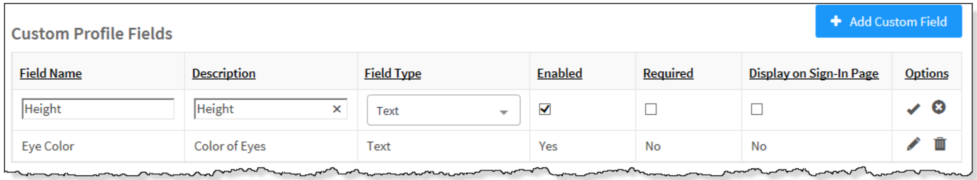
1. Click the icon to open the **Company Details**.
2. In the **Company Buildings** field, click **Add Building** and select the building or building group from the drop-down list. To delete a building, click the **X** on the building label.
3. Click **Save**.

Contractor Custom Profile Fields

A Custom Profile field is associated with the person being signed in (such as eye color) and displays on the **Contractor Details** workspace. It may also be configured to display on the **Sign In/Sign Out** workspace.

Note: Custom Profile fields are not available in the Kiosk.

1. In the navigation menu, select **Admin > Module Settings**, and click the **Contractors** tab.
2. In the **Custom Profile Fields** grid, click **Add Custom Field**.



3. Enter the **Field Name** and **Description**.
4. From the **Field Type** drop-down list, select the type of field (Lookup, Text, Text Area).
5. Select or clear the **Enabled** check box.
6. If this is a required field that must be completed during sign in, select the **Required** check box.
7. Select the **Display on Sign-In Page** check box if you want the field to display on the **Sign In** workspace.

   Note: Custom Profile fields are displayed on the **Sign In** workspace only if the **Display on Sign-In Page** check box is selected. This field displays as read-only unless using the manual entry feature.

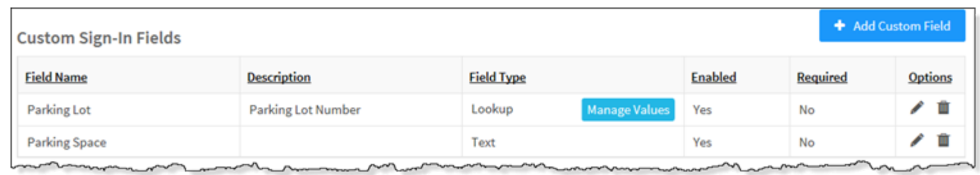
8. Click the ✔ icon to save the newly created custom field. To discard your changes, click the ⊗ icon.
9. If the Lookup field type is selected, click **Manage Values** to specify the Lookup Values for the field.
10. Click **Add Lookup Value**, enter the Value in the text field and click ✔ to save it.

Contractor Custom Sign-In Fields

You can create custom sign-in fields that are associated with sign-in events (such as parking space) to display on the **Contractor Sign In** and **Contractor Delayed Entry** workspaces for all buildings or specific buildings.

Note: Custom Sign In fields are not available in the Kiosk.

1. In the navigation menu, select **Admin > Module Settings** and click the **Contractors** tab.
2. In the **Custom Sign In Fields** area, click **Add Custom Field**.
3. Enter the **Field Name** and **Description**.
4. In the **Field Type**, select the type of field (Lookup, Text, Text Area).
5. Select or clear the **Enabled** check box.
6. If this is a required field that must be completed during sign in, select the **Required** check box.
7. Click the ✔ icon to save the newly created custom field.
8. If the Lookup field type is selected, click **Manage Values** to specify the Lookup Values for the field.
9. Click **Add Lookup Value**, enter the **Value** in the text field and click ✔ to save it.


Custom Sign-In Fields

Add Custom Field

Field Name	Description	Field Type		Enabled	Required	Options
Parking Lot	Parking Lot Number	Lookup	Manage Values	Yes	No	
Parking Space		Text		Yes	No	

Modify or Delete Custom Fields

To modify either custom profile fields or custom sign-in fields, click the ✏ icon and edit the information. Click the ✔ icon to save your changes.

To delete a custom profile or custom sign-in field, click the 🗑 icon and then click **OK** on the confirmation dialog.

Manage Student Module Settings

Users with Administrative permissions can manage what displays in the Students module using the **Students** tab on the **Module Settings** workspace.

The **Students** tab includes a drop-down menu where you can select the workspace in which you want to work:

- Student Management Settings – Use this workspace to specify student management settings, grades, custom profile fields, custom guardian fields and guardian relationships.
- Student Sign In/Out Settings – Use this workspace to specify student sign-in and sign-out settings, sign-in and sign-out reasons, and custom sign-in and sign-out fields.

RAPTOR TECHNOLOGIES

Student Management Settings

The Student Management Settings workspace is used to specify student module settings. To access this workspace, select **Admin > Module Settings** in the navigation menu and then click the **Students** tab and select **Student Management**.

From this workspace, you can perform the following tasks:

- Enable/Disable Student Management
- Specify Guardian Match Criteria for Import
- Manage Grades
- Manage Custom Profile Fields
- Manage Guardian Custom Fields
- Manage Guardian Relationships

Enable/Disable Student Management

By default, Raptor is configured with the **Student Management** feature enabled. It can be disabled to hide Student features in the navigation menu, including Student Reports, Student Sign In/Sign Out and Student dashboards.

Perform the following steps to enable or disable the **Student Management** feature:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Management** from the drop-down menu.
3. From the **Student Module Enabled** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Specify Guardian Match for Import

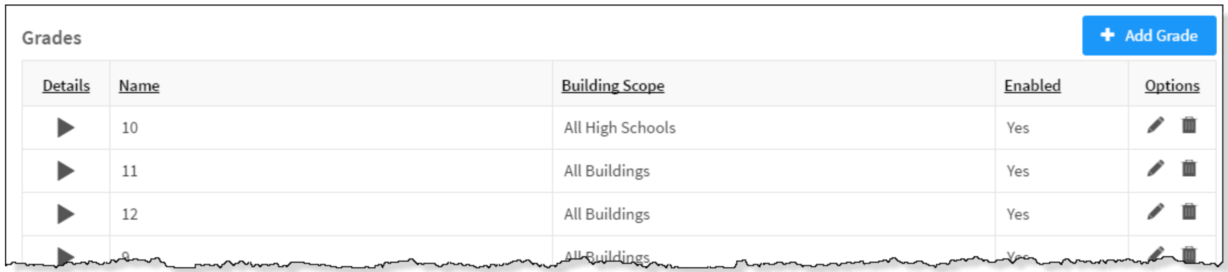
When guardian records are imported, the Raptor system uses a combination of first name, last name, and some other criteria (date of birth, email address or phone number) to determine if the imported record is already in the system. By default, this value is set to Date of Birth. The additional criteria can be specified at the client level.

Note: It is very important that you include the third type of matching criteria, such as date of birth, email address or phone number to prevent duplicate guardian records in the system.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Management** from the drop-down menu.
3. From the **Guardian Match Criteria for Import** drop-down list, select the criteria to be used in addition to first name and last name (None, Date of Birth, Phone Number, or Email Address).
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Manage Grades – Add Grade

You can define grades and then associate them with buildings so that when you are adding a student that is associated with that building, only those grades specific to the building display in the **Grades** drop-down list on the **Student Detail** workspace. This feature helps narrow the list of options in the drop-down list.



1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Management** from the drop-down menu.
3. In the **Grades** grid on the **Student Module Settings** workspace, click **Add Grade**.
4. In the **Name** text box, enter the grade number or a descriptive name.
5. If you want this field to be enabled on the Student Sign In module, keep the **Enabled** check box selected. Otherwise, clear the check box.
6. Click the ✔ icon to save the information. If you want to discard your changes, click the ⊗ icon.

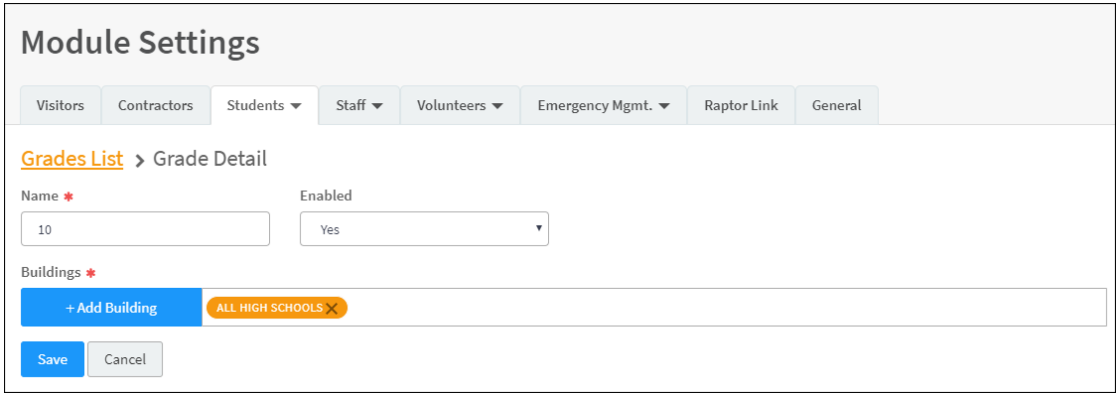
Notes:

- The Building Scope is determined by whether you are adding this setting at the client level or building level.
- When Raptor Link is used, Grades defined in the SIS will be automatically populated.

Specify Building Scope for Grades

You can specify the building or building group for specific grades if you are at the client level (All Buildings).

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Management** from the drop-down menu.
3. In the **Grades** grid, click the ▶ icon to open the **Grade Detail** workspace.



4. In the **Buildings** field, click **Add Building** and select the building or building group from the drop-down list.
5. Click **Save**.

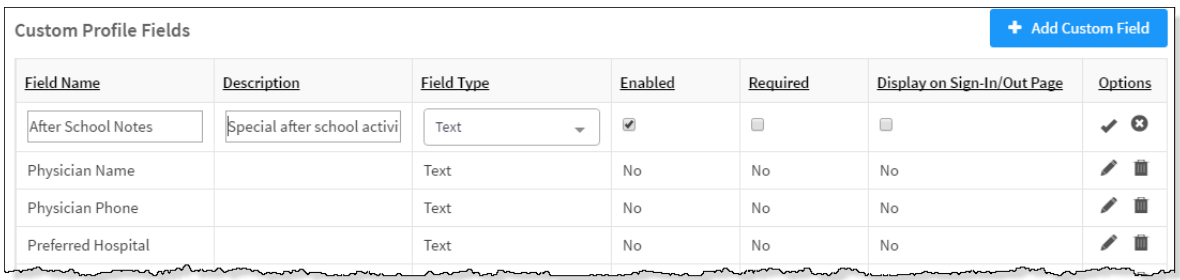
Student Custom Profile Fields

A custom profile field is associated with the student (such as Allergy Notes) and this information is displayed on the student **Details** workspace. If necessary, it may also be configured to display on the **Sign In/Sign Out** workspace.

Note: Custom Profile fields are not available in the Kiosk.

Add Custom Profile Field

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Management** from the drop-down menu.
3. In the **Custom Profile Fields** grid, click **Add Custom Field**.



4. Enter the **Field Name** and **Description** in the text boxes.
5. From the **Field Type** drop-down list, select the type of field (Lookup, Text, Text Area).
6. Select or clear the **Enabled** check box.
7. If this is a required field that must be completed during student sign in, select the **Required** check box.

Student Custom Profile Fields, cont.

8. Select the **Display on Sign-In Page** check box if you want the field to display on the **Sign In** workspace.

   Note: Custom Profile fields are displayed on the **Sign In** workspace only if the **Display on Sign-In Page** check box is selected. This field displays as read-only unless using the manual entry feature.

9. Click the ✔ icon to save the newly created custom field. To discard your changes, click the ✖ icon.
10. If the Lookup field type is selected, click **Manage Values** to specify the **Lookup Values** for the field.
11. Click **Add Lookup Value**, enter the **Value** in the text field and click ✔ to save it.

Modify or Delete Custom Profile Field

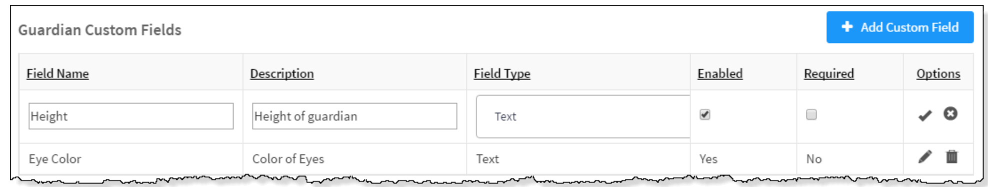
To modify a custom profile field, click the ✎ icon in the **Options** column in the **Custom Profile Field** grid on the **Student Management** workspace and edit the information. Click the ✔ icon to save your changes. If you want to discard your changes, click the ✖ icon.

To delete a custom profile field, click the 🗑 icon in the **Custom Profile Field** grid on **the Student Management** workspace and then click **OK** on the confirmation dialog.

Guardian Custom Fields

You can create custom fields to display on the **Guardian Detail** workspace.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Management** from the drop-down menu.
3. In the **Guardian Custom Fields** grid, click **Add Custom Field**.
4. Enter the **Field Name** and **Description**.
5. In the **Field Type**, select the type of field (Lookup, Text, Text Area).
6. Select or clear the **Enabled** check box.
7. If this field is a required field that must be completed during student sign in, select the **Required** check box, and then click the ✔ icon to save the newly created custom field.
8. If the **Lookup** field type is selected, click **Manage Values** to specify the Lookup Values.
9. Click **Add Lookup Value**, enter the **Value** in the text field and click ✔ to save it.



Modify Custom Guardian Fields

To modify a guardian custom field, click the ✏ icon in the **Options** column in the **Guardian Custom Fields** grid on the **Student Management** workspace and edit the information.

Click the ✔ icon to save your changes. If you want to discard your changes, click the ✖ icon.

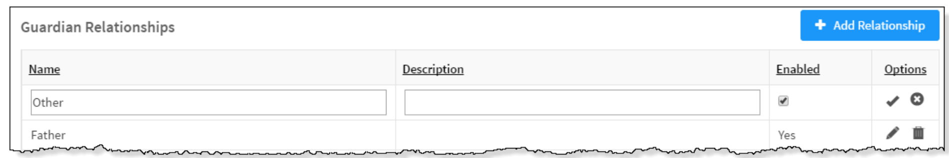
To delete a custom profile field, click the 🗑 icon in the **Guardian Custom Fields** grid on the **Student Management** workspace and then click **OK** on the confirmation dialog.

Manage Guardian Relationships

The **Guardian Relationships** grid is used to create the guardian types to be associated with students.

Add Guardian Relationship

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Management** from the drop-down menu.
3. In the **Guardian Relationships** grid on the **Student Module Settings** workspace, click **Add Relationship**.



4. Enter a **Name** and **Description**.
5. If you want this field to be enabled on the **Student Sign Out**, **Student Detail** and **Guardian Detail** workspaces, keep the **Enabled** check box selected. Otherwise, clear the check box.
6. Click the ✔ icon to save the information. If you want to discard your changes, click the ✖ icon.

Notes:

- The scope of a relationship is determined by the level (client or building) at which it was created.
- When Raptor Link is used, guardian relationships defined in the SIS will be automatically populated.

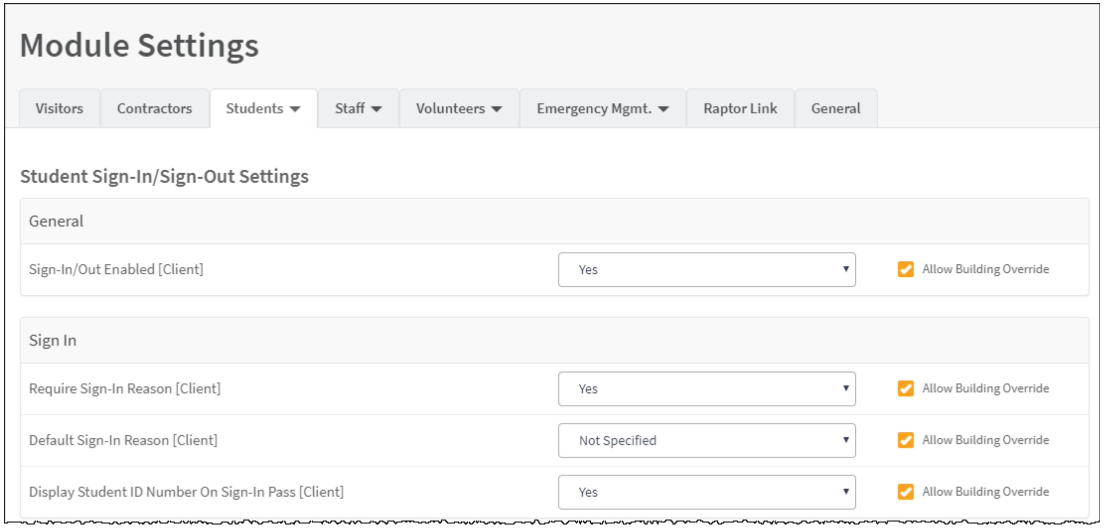
Modify or Delete Guardian Relationships

To modify a guardian relationship item, click the ✎ icon in the **Options** column and edit the information. Click the ✔ icon to save your changes. If you want to discard your changes, click the ✖ icon.

To delete a guardian relationship item, click the 🗑 icon and then click **OK** on the confirmation dialog.

Student Sign-In/Sign-Out Settings

Use the Student Sign-In/Sign-Out Settings workspace to specify sign-in and sign-out settings that display during student sign in and sign out. To access this workspace, select **Admin > Module Settings** in the navigation menu and then click the **Students** tab and select **Student Sign-In/Out**.



From this workspace, you can perform the following tasks:

- Enable/Disable Student Sign-In/Out
- Specify Student Sign-In Settings and Specify Student Sign-Out Settings
- Manage Student Sign-In Reasons and Manage Student Sign-Out Reasons
- Manage Custom Sign-In Fields and Manage Custom Sign-Out Fields
- Modify Custom Sign-In/Sign-Out Fields

Enable/Disable Student Sign-In/Out

By default, Raptor is configured with the **Student Sign In/Out** feature enabled. The feature can be disabled to hide Student Sign In and Sign Out features in the **Sign In/Sign Out** workspace.

Perform the following steps to enable or disable the Student Sign-In and Sign-Out features:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Sign-In/Out** from the drop-down menu.
3. From the **Enable Student Sign In/Out** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Specify Student Sign-In Settings

Perform the following steps to specify the fields that display during student sign in:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Sign In/Out** from the drop-down menu.
3. On the **Student Sign-In/Sign-Out Settings** workspace, specify whether the following fields are required to be completed during sign in and whether the settings can be overridden at the building level:
   - **Require Sign-In Reason** – Select **Yes** or **No** from the drop-down list to specify whether the reason for sign in is required.
   - **Default Sign-In Reason** – Select the default reason that displays when students sign in.
   - **Display Student ID Number On Sign-In Pass** – Select **Yes** or **No** from the drop-down list to specify whether the student ID displays on the sign-in pass (**Yes** is the default setting).
   - **Allow Building Override** – Select or clear the check box for each of the settings. If the check box is selected, the setting can be overridden at the building level.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

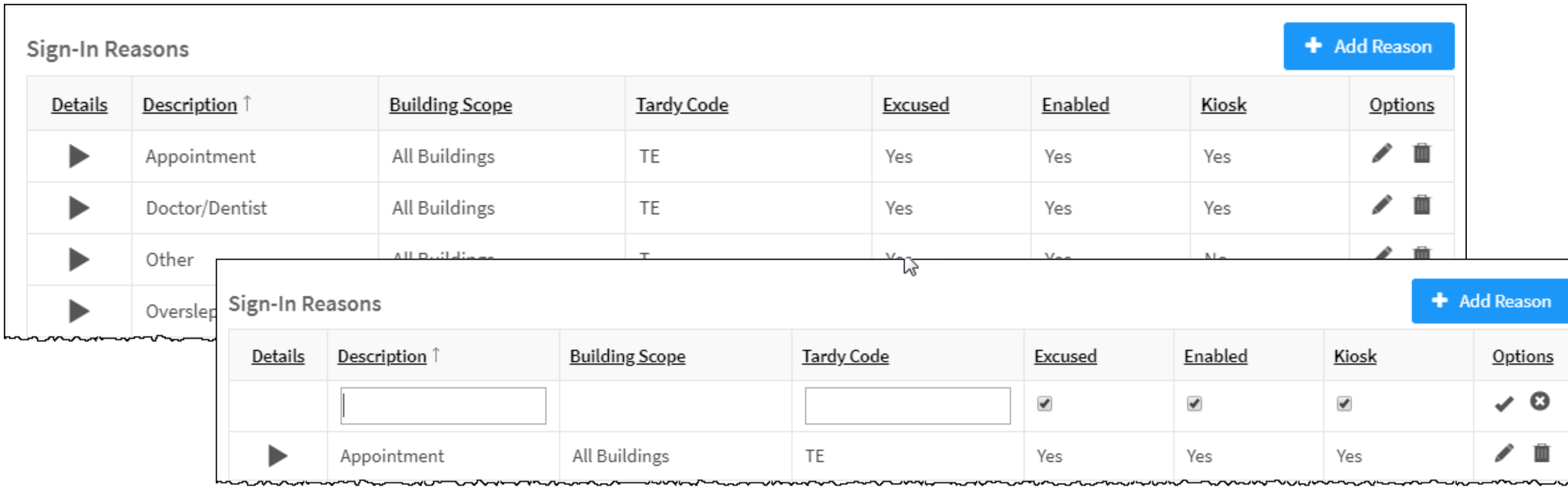
Specify Student Sign-Out Settings

Perform the following steps to specify the fields that display during student sign out:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Sign In/Out** from the drop-down menu.
3. On the **Student Sign-In/Sign-Out Settings** workspace, specify whether the following fields are required to be completed during sign out and whether the settings can be overridden at the building level:
    - **Require Sign-Out Reason** – Select **Yes** or **No** from the drop-down list to specify whether the reason for sign out is required.
    - **Default Sign-Out Reason** – Select the default reason that displays when students sign out.
    - **Display Student ID Number On Sign-Out Pass** – Select **Yes** or **No** from the drop-down list to specify whether the student ID displays on the sign-out pass (Yes is the default setting).
    - **Allow One-Time Pickup to Become an Approved Guardians** – Select **Yes** or **No** to indicate whether a one-time pickup can be added to the approved guardian list for a specific student.
    - **Allow Building Override** – Select or clear the check box for each of the settings. If the check box is selected, the setting can be overridden at the building level.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Add Student Sign-In Reasons

You can view, add, modify and delete the reasons that display during student sign in from the **Sign-In Reasons** area on the **Student Sign-In/Sign-Out Settings** workspace.



1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Sign In/Out** from the drop-down menu.
3. In the **Sign-In Reasons** grid, click **Add Reason**.

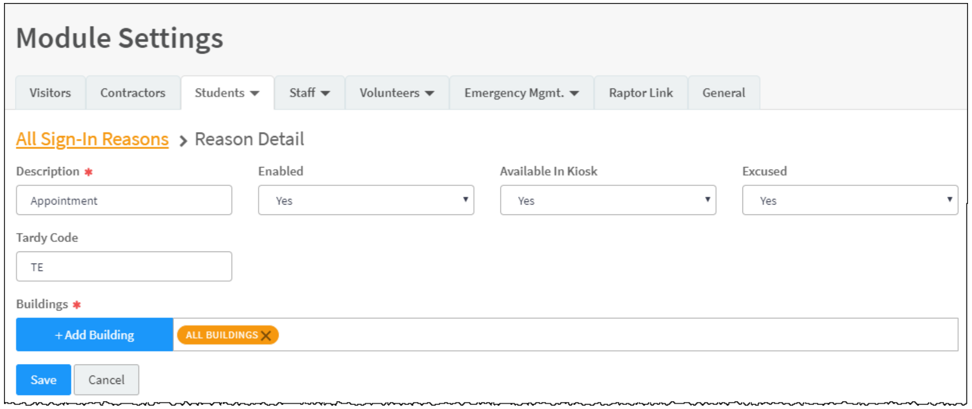
Add Student Sign-In Reasons, cont.

4. Specify the following information:
   - **Description** – Enter a description for the sign-in reason.
   - **Building Scope** – This field will be based on the building selected in the building selector when defining the sign-in reason.
   - **Tardy Code** – Enter the tardy code associated with the sign-in reason. This field only displays if you have Raptor Link enabled and the SIS Provider set to PowerSchool.
   - **Excused** – This check box is selected by default. If you want the reason to be automatically listed as an excused reason, leave the check box selected. Otherwise, clear the check box.
   - **Enabled** – This check box is selected by default. If you want the reason to display in the Sign In Reason drop-down list, leave the check box selected. Otherwise, clear the check box.
   - **Kiosk** – This check box is selected by default. If you want the sign-in reason to display on the Kiosk, keep the check box selected. Otherwise, clear the check box.
5. Click the ✔ icon to save the new reason for sign in. If you want to discard your changes, click the ⊗ icon.

Modify Student Sign-In Reasons

You can edit or remove reasons for sign in to the drop-down list, enable or disable the item, or change the setting for whether it displays in the Kiosk.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Sign In/Out** from the drop-down menu.
3. In the **Sign-In Reasons** grid, click the icon to expand the **Reason Detail**.
3. Modify the any of the information and click **Save**.



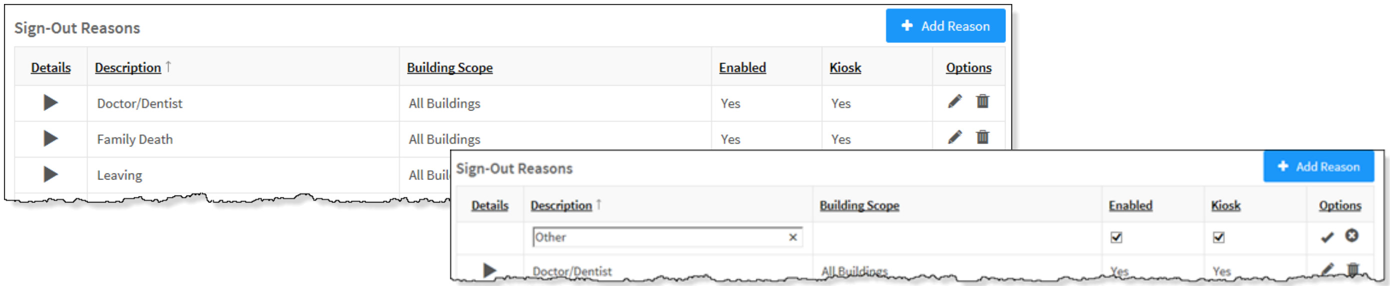
You can also click the icon in the **Options** column in the **Sign-In Reasons** grid on the **Student Sign-In/Sign-Out Settings** workspace to edit the **Description**, **Tardy Code**, and enable/disable the **Kiosk** and **Enabled** settings. Click the icon to save your changes. If you want to discard your changes, click the icon.

Delete Sign-In Reasons

To remove a reason, click the icon in the **Sign-In Reasons** grid on the **Student Sign-In/Sign-Out Settings** workspace and then click **OK** on the confirmation dialog.

Add Student Sign-Out Reasons

You can view, add, modify and delete the reasons that display during student sign out from the **Sign-Out Reasons** grid on the **Student Sign-In/Sign-Out Settings** workspace.

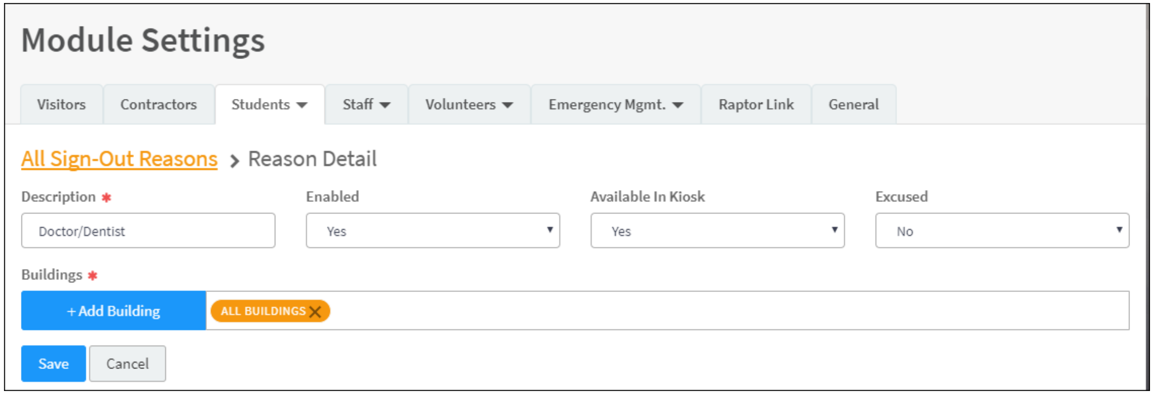


1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Sign In/Out** from the drop-down menu.
3. In the **Sign-Out Reasons** grid, click **Add Reason** and enter a **Description** for the reason.
4. The Enabled and Kiosk check boxes are selected by default. Perform the following depending on how you want the reason to display in the **Student Sign Out** workspace:
   - **Enabled** – If you want the reason to display in the Sign Out Reason drop-down list, leave the check box selected. Otherwise, clear the check box.
   - **Kiosk** – If you want the sign-in reason to display on the Kiosk, keep the check box selected. Otherwise, clear the check box.
5. Click the ✔ icon to save the new reason for sign in. If you want to discard your changes, click the ⊗ icon.

Modify Student Sign-Out Reasons

You can edit or remove reasons for sign out to the drop-down list, enable or disable the item, or change the setting for whether it displays in the Kiosk.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Sign In/Out** from the drop-down menu.
3. In the **Sign-Out Reasons** grid, click the ▶ icon to expand the **Reason Detail**.



4. Modify the any of the information and click **Save**.

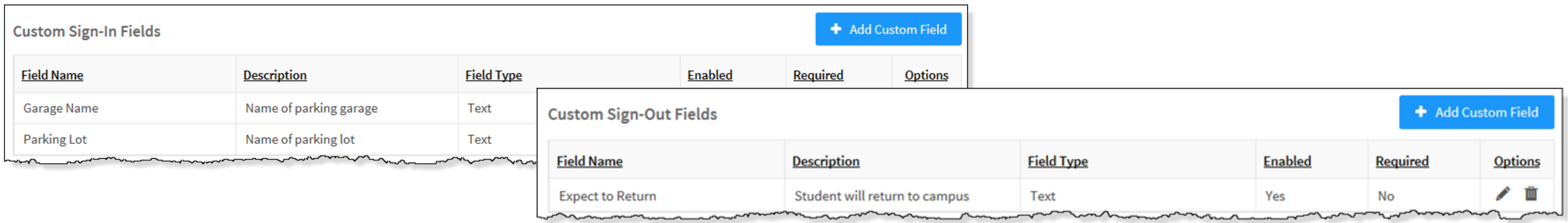
You can also click the ✎ icon in the **Options** column in the **Sign-Out Reasons** grid on the **Student Sign-In/Sign-Out Settings** workspace to edit the **Description** name, and the **Kiosk** and **Enabled** settings. Click the ✔ icon to save your changes. If you want to discard your changes, click the ✖ icon.

Delete Sign-In Reasons

To remove a reason, click the 🗑 icon in the **Sign-In Reasons** grid on the **Student Sign-In/Sign-Out Settings** workspace and then click **OK** on the confirmation dialog.

Custom Sign-In/Sign-Out Fields

You can create custom sign-in and sign-out fields that are associated with sign-in and sign-out events (such as Parking Lot and Expect to Return) to display on the **Student Sign In**, **Student Sign Out** and **Student Delayed Entry** workspaces for all buildings or specific buildings.



1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Students** tab and select **Student Sign In/Out** from the drop-down menu.
3. In the **Custom Sign-In Fields** or **Custom Sign-Out Fields** grid, click **Add Custom Field** and enter the **Field Name** and **Description**.
4. In the **Field Type**, select the type of field (Lookup, Text, Text Area).
5. Select or clear the **Enabled** check box.
6. If this is a required field that must be completed during student sign in, select the **Required** check box.
7. Click the ✔ icon to save the newly created custom field.
8. If the Lookup field type is selected, click **Manage Values** to specify the **Lookup Values** for the field.
9. Click **Add Lookup Value**, enter the **Value** in the text field and click ✔ to save it.

Modify Custom Sign-In/Out Fields

To modify a custom sign-in or sign-out field, click the icon in the **Options** column in the **Custom Sign-In Fields** or **Custom Sign-Out Fields** grid on the **Student Sign-In/Sign-Out Settings** workspace and edit the information.

Click the icon to save your changes. If you want to discard your changes, click the icon.

Delete Custom Sign-In/Sign-Out Field

To delete a custom sign-in or sign-out field , click the icon in the **Custom Sign-In Fields** or **Custom Sign-Out Fields** grid on the **Student Sign-In/Sign-Out Settings** workspace and then click **OK** on the confirmation dialog.

Manage Staff Module Settings

Users with Administrative permissions can manage what displays in the Staff module using the **Staff** tab on the **Module Settings** workspace.

The **Staff** tab includes a drop-down menu where you can select the workspace in which you want to work:

- Staff Management Settings – Use this workspace to specify staff management settings and custom profile fields.
- Staff Sign In/Out Settings – Use this workspace to specify staff sign-in and sign-out settings, sign-in and sign-out reasons, and kiosk sign-in settings.

Staff Management Settings

The **Staff Management Settings** workspace is used to specify staff module settings. To access this workspace, select **Admin > Module Settings** in the navigation menu and then click the **Staff** tab and select **Staff Management**.

From this workspace, you can perform the following tasks:

- Enable/Disable Staff Management
- Add Staff Custom Profile Fields
- Modify Staff Custom Profile Fields

Enable/Disable Staff Management

By default, Raptor is configured with the **Staff Management** feature enabled. It can be disabled to hide Staff features in the navigation menu, Reports workspace and Staff dashboards.

Perform the following steps to enable or disable the **Staff Management** feature:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Management** from the drop-down menu.
3. From the **Staff Module Enabled** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

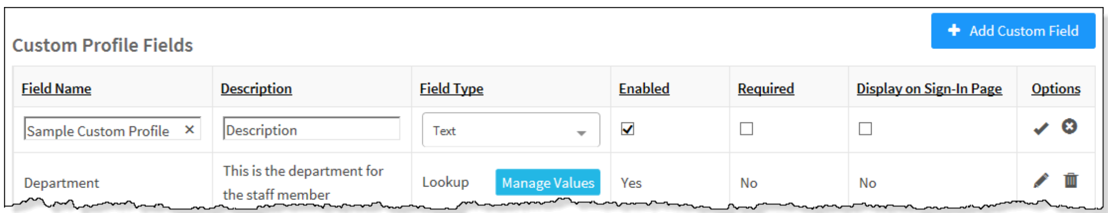
Staff Custom Profile Fields

A Custom Profile field is associated with the person being signed in (such as eye color) and displays on the **Details** workspace. It may also be configured to display on the **Sign In/Sign Out** workspace.

Note: Custom Profile fields are not available in the Kiosk.

Add Custom Profile Field

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Management** from the drop-down menu.
3. In the **Custom Profile Fields** grid, click **Add Custom Field**.



4. Enter the **Field Name** and **Description** in the text boxes.
5. From the **Field Type** drop-down list, select the type of field (Lookup, Text, Text Area).
6. Select or clear the **Enabled** check box.
7. If this is a required field that must be completed during staff sign in, select the **Required** check box.

Staff Custom Profile Fields, cont.

8. Select the **Display on Sign-In Page** check box if you want the field to display on the **Sign In** workspace.

   Note: Custom Profile fields are displayed on the **Sign In** workspace only if the **Display on Sign-In Page** check box is selected. This field displays as read-only unless using the manual entry feature.

9. Click the ✔ icon to save the newly created custom field. To discard your changes, click the ✖ icon.
10. If the Lookup field type is selected, click **Manage Values** to specify the **Lookup Values** for the field.
11. Click **Add Lookup Value**, enter the **Value** in the text field and click ✔ to save it.

Modify or Delete Custom Profile Field

To modify a custom profile field, click the ✎ icon in the **Options** column in the **Custom Profile Field** grid on the **Staff Management** workspace and edit the information. Click the ✔ icon to save your changes. If you want to discard your changes, click the ✖ icon.

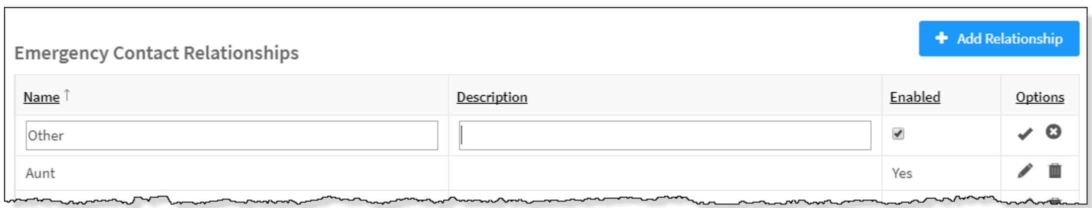
To delete a custom profile field, click the 🗑 icon in the **Custom Profile Field** grid on the **Staff Management** workspace and then click **OK** on the confirmation dialog.

Emergency Contact Relationships **REU**

Use this area on the **Staff Management Settings** workspace to specify the emergency contact relationships that are available in the **Staff Details** workspace.

Add Relationship

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Management** from the drop-down menu.
3. In the **Emergency Contact Relationships** grid, click **Add Relationship**.



4. Enter the **Name** and optional **Description** in the text boxes and select or clear the **Enabled** check box.
5. Click the ✔ icon to save the emergency contact relationship. If you want to discard your changes, click the ⊗ icon.

Staff Sign-In/Sign-Out Settings

Use the **Staff Sign-In/Sign-Out Settings** workspace to specify sign-in and sign-out settings that display during Staff Sign In and Sign Out. To access this workspace, select **Admin > Module Settings** in the navigation menu and then click the **Staff** tab and select **Staff Sign-In/Out**.

From this workspace, you can perform the following tasks:

- Enable/Disable Staff Sign-In/Out
- Specify Staff Sign-In Settings and Specify Staff Sign-Out Settings
- Specify Kiosk Settings
- Manage Staff Sign-In Destinations/Reasons and Manage Staff Sign-Out Destinations/Reasons
- Manage Staff Custom Sign-In Fields

Enable/Disable Staff Sign-In/Out

By default, Raptor is configured with the **Staff Sign In/Out** feature enabled. The feature can be disabled to hide Staff Sign In and Sign Out features in the **Sign In/Sign Out** workspace.

Perform the following steps to enable or disable the Staff Sign-In and Sign-Out features:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Sign-In/Out** from the drop-down menu.
3. From the **Enable Staff Sign In/Out** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Specify Staff Sign-In Settings

Perform the following steps to specify the fields that display during staff sign in:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Sign In/Out** from the drop-down menu.
3. On the **Staff Sign-In/Sign-Out Settings** workspace, specify whether the following fields are required to be completed during sign in and whether the settings can be overridden at the building level:
   - **Require Sign-In Reason** – Select **Yes** or **No** from the drop-down list to specify whether the reason for sign in is required.
   - **Require Sign-In Reason For** – Select **Only Non-Primary Building Staff** or **All Staff** from the drop-down list to specify who the reason for sign in is required when the staff member is signing into a building.
   - **Display Staff ID Number On Badge** – Select **Yes** or **No** from the drop-down list to specify whether the staff ID displays on the badge (No is the default setting).
   - **Allow Building Override** – Select or clear the check box for each of the settings. If the check box is selected, the setting can be overridden at the building level.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Specify Staff Sign-Out Settings

Perform the following steps to specify the fields that display during staff sign out:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Sign In/Out** from the drop-down menu.
3. On the **Staff Sign-In/Sign-Out Settings** workspace, specify whether the following field is required to be completed during sign out and whether the settings can be overridden at the building level:
    - **Require Sign-Out Reason** – Select **Yes** or **No** from the drop-down list to specify whether the reason for sign out is required.
    - **Auto Sign Out Time** – Click the icon and select the time from the drop-down list.
    - **Allow Building Override** – Select or clear the check box for each of the settings. If the check box is selected, the setting can be overridden at the building level.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

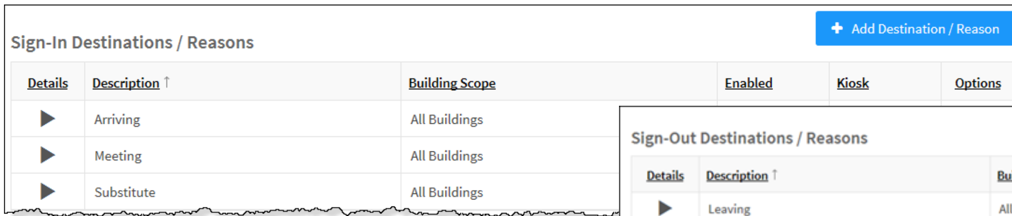
Staff Kiosk Settings

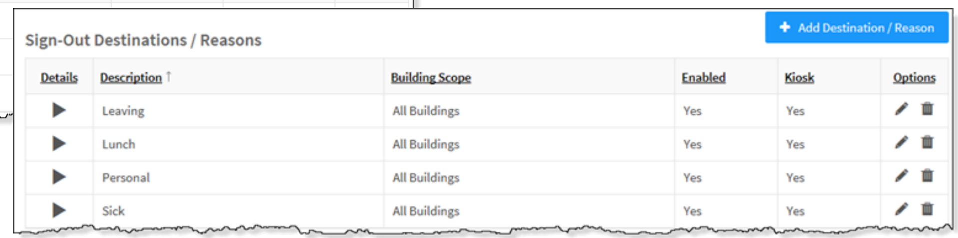
Perform the following steps to specify staff sign-in settings when using the kiosk:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Sign In/Out** from the drop-down menu.
3. Specify whether the following fields are required to be completed during staff sign in on the Kiosk and whether individual buildings can override these settings:
   - **Kiosk Require Sign In Reason** – Select **Yes** or **No** from the drop-down list to specify whether the reason for sign in is required.
   - **Kiosk Require Sign In Reason For** – Select **Only Non-Primary Building Staff** or **All Staff** from the drop-down list to specify who the reason for sign in is required when the staff member is signing into a building using the kiosk.
   - **Allow Building Override** – Select or clear the check box for each of the fields. If selected, the setting can be overridden at the building level.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Sign-In/Out Destinations/Reasons

You can view and manage the destinations/reasons that display during staff sign in and sign out from the **Sign In Destinations/Reasons** and **Sign Out Destinations/Reasons** grids on the workspace.





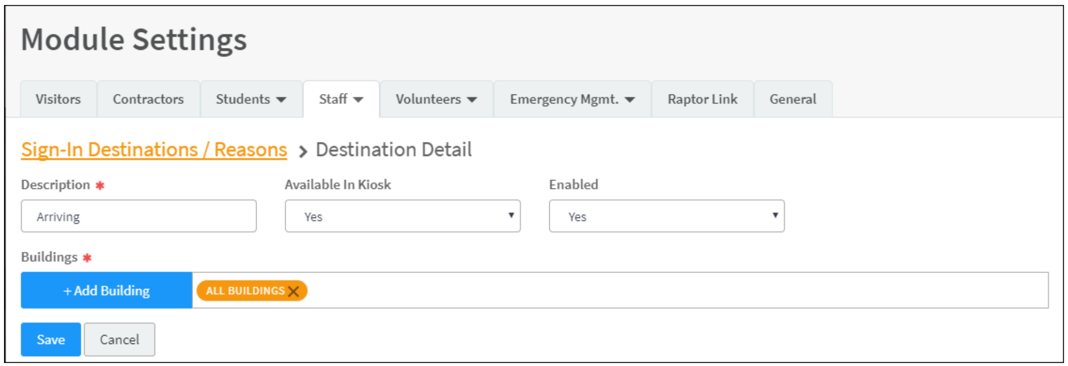
1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Sign In/Out** from the drop-down menu.
3. In the **Sign-In Destinations/Reasons** or **Sign-In Destinations/Reasons** grid, click **Add Destination/Reason** and enter a name in the **Description** text field.

4. The **Enabled** and **Kiosk** check boxes are selected by default. Perform the following depending on how you want the reason to display in the Staff Sign In workspace:
   - **Enabled** – If you want the reason to display in the **Sign In Reason** drop-down list, leave the check box selected. Otherwise, clear the check box.
   - **Kiosk** – If you want the sign-in reason to display on the Kiosk, leave the check box selected. Otherwise, clear the check box.
5. Click the ✔ icon to save the new reason for sign in. If you want to discard your changes, click the ⊗ icon.

Modify Sign-In Destinations/Reasons

You can edit or remove destinations/reasons for sign in, enable or disable the item, or change the setting for whether it displays in the Kiosk.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Sign In/Out** from the tab drop-down menu.
3. In the **Sign-In Destinations/Reasons** grid, click the icon to expand the **Destination Detail**.



4. Modify the any of the information and click **Save**.

You can also click the icon in the **Options** column in the **Sign-In Destinations/Reasons** grid on the **Staff Sign In/Sign-Out Settings** workspace to edit the **Description**, and **Kiosk** and **Enabled** settings. Click the icon to save your changes. If you want to discard your changes, click the icon.

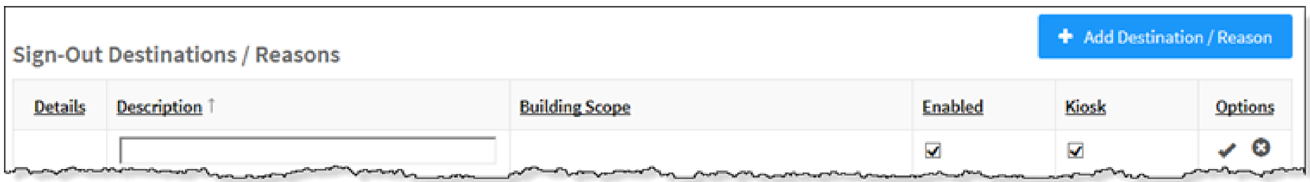
Delete Sign-In Destinations/Reasons

To remove a Sign-In Destinations/Reasons item, click the icon in the **Sign-In Destinations/Reasons** grid on the **Staff Sign-In/Out Settings** workspace and then click **OK** on the confirmation dialog.

Staff Sign-Out Destinations/Reasons

You can view and manage the destinations/reasons that display during staff sign out from the **Sign Out Destinations/Reasons** grid on the workspace.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Sign In/Out** from the drop-down menu.
3. In the **Sign-Out Destinations/Reasons** grid, click **Add Destination/Reason**.

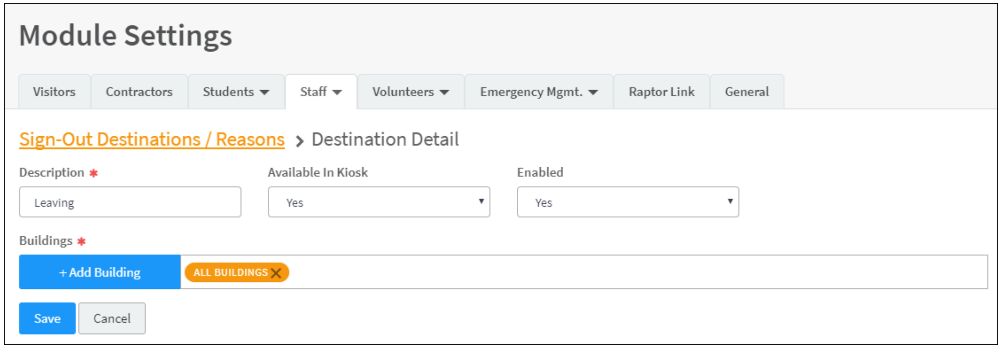


4. Enter a name for the destination or reason in the **Description** text field.
5. The **Enabled** and **Kiosk** check boxes are selected by default. Perform the following depending on how you want the reason to display in the **Staff Sign Out** workspace:
   - **Enabled** – If you want the reason to display in the Sign Out Reason drop-down list, leave the check box selected. Otherwise, clear the check box.
   - **Kiosk** – If you want the sign-out reason to display on the Kiosk, leave the check box selected. Otherwise, clear the check box.
6. Click the ✔ icon to save the new reason for sign out. If you want to discard your changes, click the ⊗ icon.

Modify Sign-Out Destinations/Reasons

You can edit or remove destinations/reasons for sign out, enable or disable the item, or change the setting for whether it displays in the Kiosk.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Sign In/Out** from the tab drop-down menu.
3. In the **Sign-Out Destinations/Reasons** grid, click the icon to expand the **Destination Detail**.



4. Modify the any of the information and click **Save**.

You can also click the icon in the **Options** column in the **Sign-Out Destinations/Reasons** grid on the **Staff Sign In/Sign-Out Settings** workspace to edit the **Description** name and enable/disable the **Kiosk** setting and the **Enabled** setting. Click the icon to save your changes. If you want to discard your changes, click the icon.

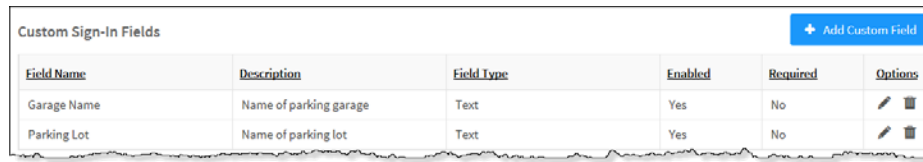
Delete Sign-Out Destinations/Reasons

To remove a **Sign-Out Destinations/Reasons** item, click the icon in the **Sign-Out Destinations/Reasons** grid on the **Staff Sign-In/Out Settings** workspace and then click **OK** on the confirmation dialog.

Staff Custom Sign-In Fields

You can create custom sign-in fields that are associated with sign-in events (such as Parking Lot) to display on the **Staff Sign In** and **Staff Delayed Entry** workspaces for all buildings or specific buildings.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Staff** tab and select **Staff Sign In/Out** from the drop-down menu.
3. In the **Custom Sign-In Fields** grid, click **Add Custom Field**.


Custom Sign-In Fields

+ Add Custom Field

Field Name	Description	Field Type	Enabled	Required	Options
Garage Name	Name of parking garage	Text	Yes	No	
Parking Lot	Name of parking lot	Text	Yes	No	

4. Enter the **Field Name** and **Description**.
5. In the **Field Type**, select the type of field (Lookup, Text, Text Area).
6. Select or clear the **Enabled** check box.
7. If this is a required field that must be completed during staff sign in, select the **Required** check box.
8. Click the ✔ icon to save the newly created custom field.
9. If the Lookup field type is selected, click **Manage Values** to specify the **Lookup Values** for the field.
10. Click **Add Lookup Value**, enter the value in the text field and click ✔ to save it.

Modify Custom Sign-In Field

Click the ✏ icon in the **Options** column and edit the information. Click the ✔ icon to save your changes. If you want to discard your changes, click the ✖ icon.

Delete Custom Sign-In Field

Click the 🗑 icon in the **Options** column and then click **OK** on the confirmation dialog.

Manage Volunteer Module Settings

Users with Administrative permissions can manage what displays in the Volunteer module using the **Volunteers** tab on the **Module Settings** workspace. The **Volunteers** tab includes a drop-down menu where you can select the workspace in which you want to navigate:

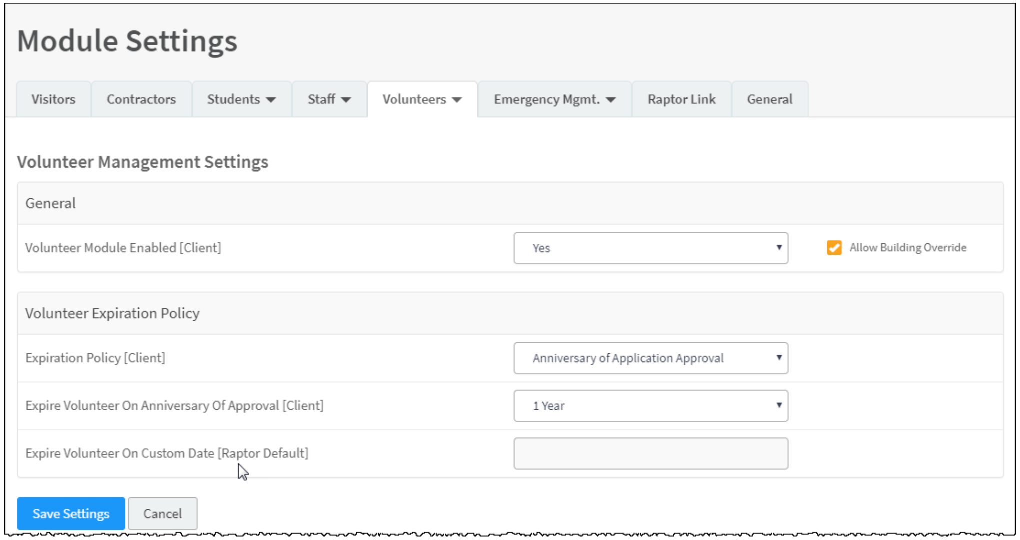
- Volunteer Management Settings – This workspace is used to manage what displays on the Volunteer workspace, including volunteer expiration policy, functions, organizations, affiliations, and custom profile fields.
- Volunteer Sign-In/Sign-Out Settings – This workspace is used manage volunteer sign-in and sign-out settings.
- Volunteer Application Settings – This workspace is used to manage volunteer application settings, notifications and online volunteer application features.
- Volunteer Portal Settings – This workspace is used to manage the volunteer portal settings.
- Event Management Settings – This workspace is used to enable volunteer event management.

Volunteer Management Settings

The Volunteer Management Settings workspace is used to specify volunteer module settings. To access this workspace, select **Admin > Module Settings** in the navigation menu and then click the **Volunteer** tab and select **Volunteer Management**.

From this workspace, you can perform the following tasks:

- Enable/Disable Volunteer Management
- Specify Volunteer Expiration Policy
- Manage Functions
- Manage Requirements
- Manage Organizations
- Manage Affiliations
- Add Custom Profile Fields
- Modify Custom Profile Fields



Enable/Disable Volunteer Management

By default, Raptor is configured with the Volunteer Management feature enabled. It can be disabled to hide Volunteer features in the navigation menu, Reports workspace and Volunteer dashboards.

Perform the following steps to enable or disable the Volunteer Management feature:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management** from the drop-down menu.
3. In the **Volunteer Module Enabled** field, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Note: If you disable the Volunteer Module, all associated features will be also be disabled (Volunteer Management, Volunteer Sign In/Out, Volunteer Application, Volunteer Events, and Volunteer Portal). Subsequently, when you enable the Volunteer Module, you will then need to enable all of the other features that were previously disabled.

Volunteer Expiration Policy

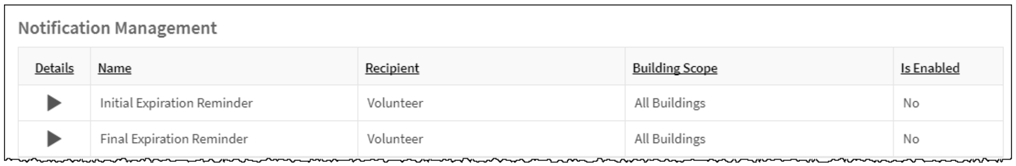
Users with Administrative permissions can specify when a volunteer's ability to volunteer for functions will automatically expire, at which time they will be required to resubmit a volunteer application.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management** from the drop-down menu.
3. In the **Volunteer Expiration Policy** area, specify the following information:
   - **Expiration Policy** – Select one of the following options from the drop-down list to specify how the expiration policy will be implemented:
     - **None** – No expiration policy will be set for volunteers. If this option is selected, the **Expire Volunteer on Anniversary of Approval** and **Expire Volunteer On Custom Date** fields will be disabled (grayed out).
     - **Anniversary of Application Approval** – If this option is selected, Volunteers will be expired on the anniversary date of application approval. You must select the anniversary year in the **Expire Volunteer On Anniversary of Approval** field.
     - **Custom Date** – Select this option to be able to select a date from the calendar in the **Expire Volunteer On Custom Date** field to specify the expiration policy.
   - **Expire Volunteer On Anniversary of Approval** – This field is enabled if the **Expiration Policy** is set to **Anniversary of Application Approval**. From the drop-down list, select the anniversary year on which to expire the volunteer. By default, the expiration is set to 1 Year.
   - **Expire Volunteer On Custom Date** – This field is enabled if the **Expiration Policy** is set to **Custom Date**. From the calendar icon, select the date on which to expire the volunteer.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Manage Expiration Notifications

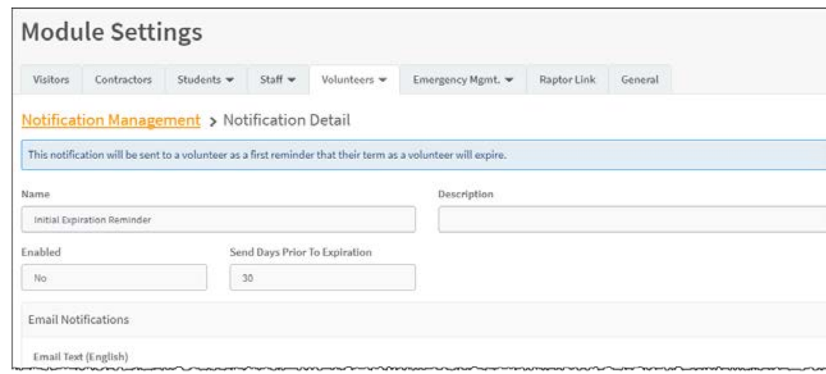
You can manage volunteer expiration notifications from **Notification Management** grid on the **Volunteer Management Settings** workspace. Notifications can only be managed at the client level (All Buildings).

- **Initial Expiration Reminder** – Sent to volunteer as first reminder that their term as a volunteer will expire.
- **Final Expiration Reminder** – Sent to volunteer as final reminder that their term as a volunteer will expire.


Notification Management

Details	Name	Recipient	Building Scope	Is Enabled
▶	Initial Expiration Reminder	Volunteer	All Buildings	No
▶	Final Expiration Reminder	Volunteer	All Buildings	No

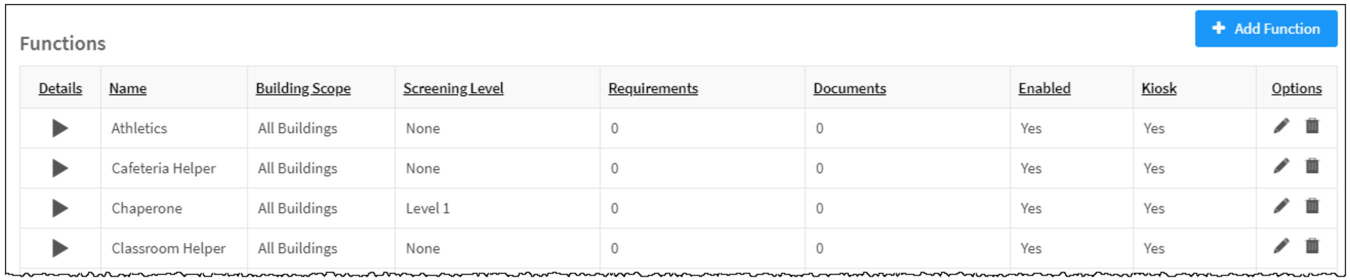
1. In the **Notification Management** area, click the ▶ icon in the **Details** column to expand the **Notification Detail**, and specify the following information:
   - **Name** – *Read-only*
   - **Description** – Optional description.
   - **Enabled** – Select **Yes** or **No** to indicate whether the notification is enabled (active).
   - **Send Days Prior To Expiration** – Select the number of days the notification is to be sent prior to the volunteer's expiration date.
   - **Email Text** – Use the default message that will be sent in an email or modify it with a custom email message.



2. Click **Save**.

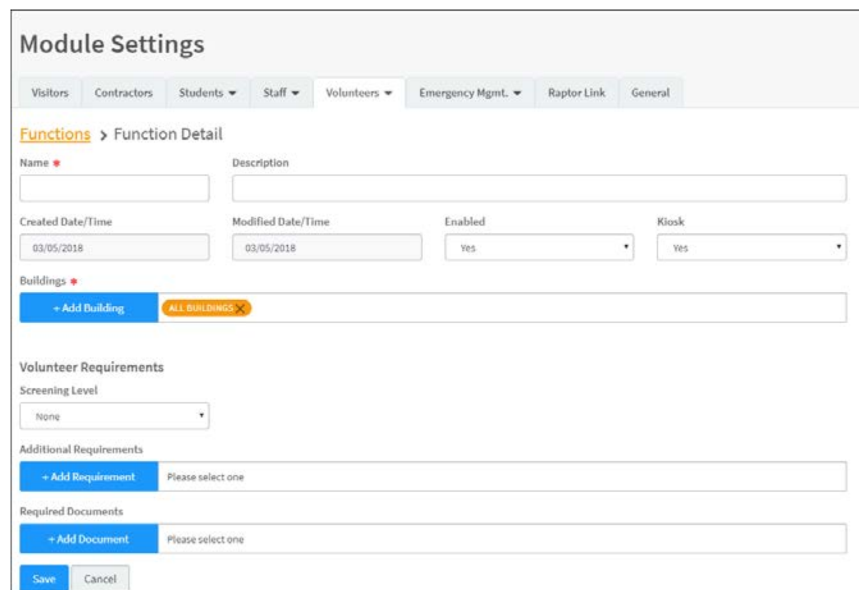
Add Functions

You can add the functions that display during volunteer sign in from the **Functions** grid on the **Volunteer Management Settings** workspace. Functions can only be managed at the client level (All Buildings).



Details	Name	Building Scope	Screening Level	Requirements	Documents	Enabled	Kiosk	Options
▶	Athletics	All Buildings	None	0	0	Yes	Yes	
▶	Cafeteria Helper	All Buildings	None	0	0	Yes	Yes	
▶	Chaperone	All Buildings	Level 1	0	0	Yes	Yes	
▶	Classroom Helper	All Buildings	None	0	0	Yes	Yes	

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management**.
3. In the **Functions** grid, click **Add Function**.
4. Enter a **Name** and **Description** and specify the following:
   - **Enabled** – Select **Yes** (to enable) or **No** (to disable).
   - **Kiosk** – Select **Yes** (to enable) or **No** (to disable).
5. Click **Add Building** and select the building or building group.
   Click the X to delete building.



Add Functions

6. Select the **Screening Level** for criminal background screening required for the function.

   Note: Criminal background screening is only done on volunteer applications received from the online volunteer application.

7. Click **Add Requirement** and select the requirement(s) associated with the function.

   Note: One or more requirements must already be created. See Add Requirements.

8. In the **Required Documents** field, click **Add Document** and select the required document(s) associated with the function.

   Note: To use this feature, one or more required documents must already be created. See Add Required Document.

9. Click **Save**.

Modify Function Details

You can modify and delete functions at the client level (All Buildings).

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management** from the drop-down menu.
3. In the **Functions** grid, click the ▶ icon to expand the **Function Detail** and modify any of the information.
4. Click **Save**.

Note: After the changes have been saved, the **Modified Date/Time** *read-only* field is updated.

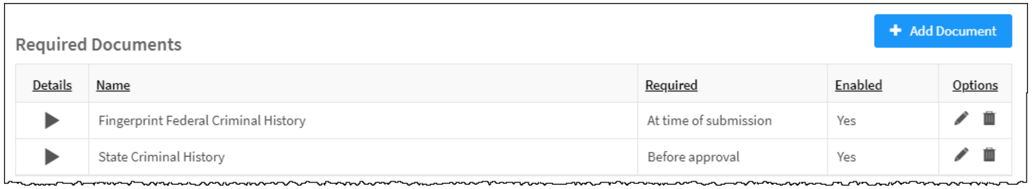
You can also click the ✎ icon in the **Options** column to perform in-line edits and then click the ✔ icon to save your changes.

Delete Function

To delete a function, click the 🗑 icon to remove the item from the list of Functions.

Add Required Document

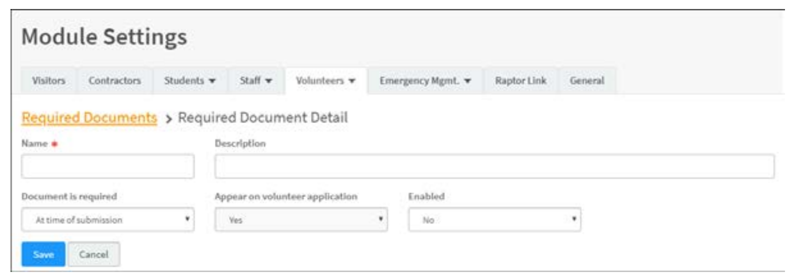
The **Required Documents** grid on the **Volunteer Management Settings** workspace is used to view and manage required documents that volunteers must provide prior to approval. The required documents can be displayed on the volunteer application and can be associated to functions.


Required Documents

Add Document

Details	Name	Required	Enabled	Options
▶	Fingerprint Federal Criminal History	At time of submission	Yes	
▶	State Criminal History	Before approval	Yes	

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management**.
3. In the **Required Documents** grid, click **Add Document** and specify the following:



   - **Name***
   - **Description** (*Optional*)
   - **Document is required** – Select when the document must be provided (At time of submission or Before approval).

     Note: When **Document is required** is set to **At time of submission**, the **Appear on volunteer application** field is set to **Yes** and cannot be changed.
   - **Appear on volunteer application** – Select **Yes** or **No** to indicate whether this required document should be displayed on the volunteer application.
   - **Enabled** – Select **Yes** (to enable) or **No** (to disable) to specify whether the required document is currently enabled or disabled.
4. Click **Save**.

Modify Required Document

You can edit the required document name, when it is required, and if the required document is enabled or disabled.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management**.
3. In the **Required Documents** grid, click the icon in the **Options** column to modify any of the following information:
   - **Name*** – Modify the name of the required document.
   - **Required** – Select when the document must be provided (At time of submission or Before Approval).
   - **Enabled** – Select **Yes** (to enable) or **No** (to disable) to specify whether the required document is currently enabled or disabled.
4. Click the icon to save your changes. If you want to discard your changes, click the icon.

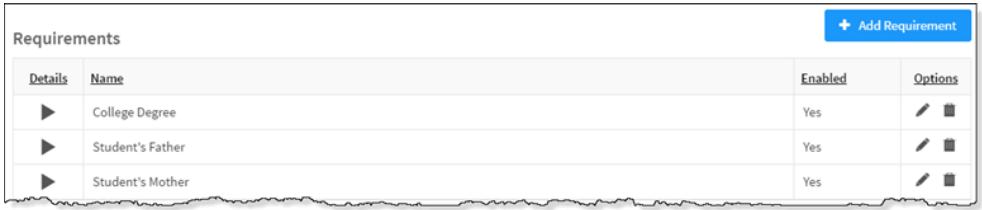
Delete Required Document

To remove a required document, click the icon in the **Required Documents** grid on the **Volunteer Management Settings** workspace and then click **OK** on the confirmation dialog.

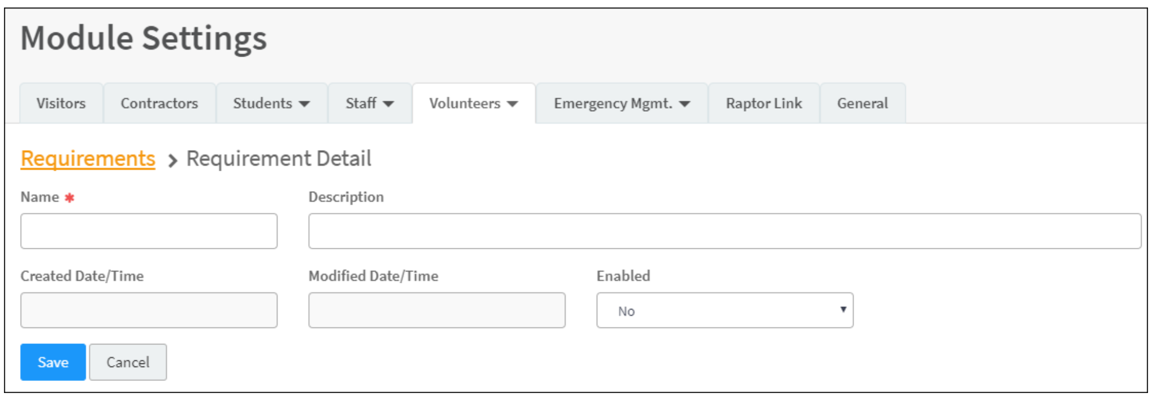
Note: A warning message displays if you attempt to delete a required document that is associated with one or more functions.

Add Requirements

You can view and manage the requirements that can be associated to functions and displayed during the application approval process from the **Requirements** grid on the **Volunteer Management Settings** workspace.



1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management**.



3. In the **Requirements** grid, click **Add Requirement** and enter a **Name** and **Description**.
4. In the **Enabled** field, select **Yes** (to enable) or **No** (to disable).
5. Click **Save**.

Modify Requirements

You can modify and delete requirements at the client level (All Buildings).

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management** from the drop-down menu.
3. In the **Requirements** grid, click the ▶ icon to expand the **Requirement Detail** and modify any of the information.
4. Click **Save**.

Note: After the changes have been saved, the **Modified Date/Time** *read-only* field is updated.

You can also click the ✎ icon in the **Options** column to perform in-line edits and then click the ✔ icon to save your changes.

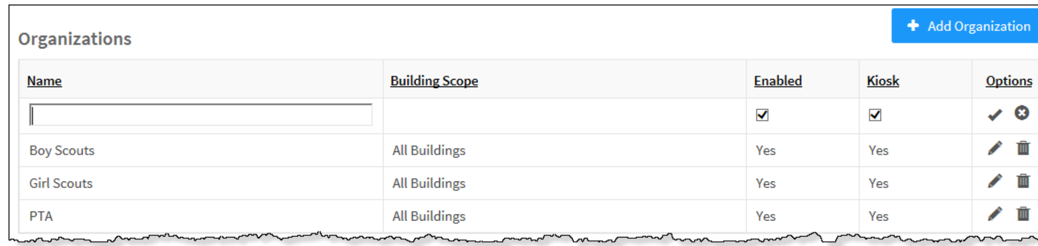
Delete Requirement

To delete a requirement, click the 🗑 icon to remove the item from the list of Requirements.

Note: A warning message displays if you attempt to delete a requirement that is associated with one or more functions.

Manage Organizations

You can manage the organizations that display during volunteer sign in from the **Organizations** grid on the **Volunteer Management Settings** workspace at the client level (All Buildings). An organization is who the volunteer is representing.



1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management**.
3. In the **Organizations** grid, click **Add Organization**.
4. Enter a **Name** and specify the following:
   - **Enabled** – If you want the organization to display on the **Sign In** workspace, leave the check box selected. Otherwise, clear the check box.
   - **Kiosk** – If you want the organization to display on the Kiosk, leave the check box selected. Otherwise, clear the check box.
4. Click the ✔ icon to save the new organization. If you want to discard your changes, click the ✖ icon.

Modify Organization

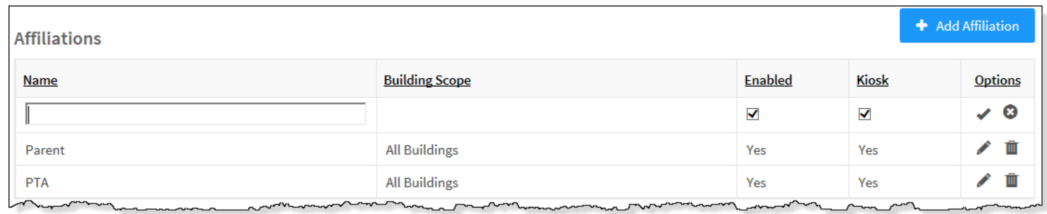
Click the ✎ icon in the **Options** column and modify the information. Click ✔ to save the organization. If you want to discard your changes, click the ✖ icon.

Delete Organization

Click the 🗑 icon in the **Options** column and then click **OK** on the confirmation dialog.

Manage Affiliations

You can manage the affiliations that display during volunteer sign in from the **Affiliations** grid on the **Volunteer Management Settings** workspace at the client level (All Buildings). An affiliation is the relationship to a student who attends the school (for example, mother, father, or uncle).



1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management**.
3. In the **Affiliations** grid, click **Add Affiliation**.
4. Enter a **Name** and specify the following:
   - **Enabled** – If you want the affiliation to display on the **Sign In** workspace, leave the check box selected. Otherwise, clear the check box.
   - **Kiosk** – If you want the affiliation to display on the Kiosk, leave the check box selected. Otherwise, clear the check box.
4. Click the ✔ icon to save the new affiliation. If you want to discard your changes, click the ⊗ icon.

Modify Affiliation

Click the ✎ icon in the **Options** column and modify the information. Click ✔ to save the affiliation. If you want to discard your changes, click the ⊗ icon.

Delete Affiliation

Click the 🗑 icon in the **Options** column and then click **OK** on the confirmation dialog.

Volunteer Custom Profile Fields

A Custom Profile field is associated with the person being signed in (such as eye color) and displays on the **Volunteer Details** workspace. It may also be configured to display on the **Sign In/Sign Out** workspace.

Note: Custom Profile fields are not available in the Kiosk.

Add Custom Profile Field

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Management** from the drop-down menu.
3. In the **Custom Profile Fields** grid, click **Add Custom Field**.


Custom Profile Fields

+ Add Custom Field

Field Name	Description	Field Type	Enabled	Required	Display on Sign-In Page	Order	Options
Height	Physical Height	Text	☑	☐	☑	2	
Eye Color	Color of Eyes	Text	Yes	No	Yes	1	

4. Enter the **Field Name** and **Description**.
5. From the **Field Type** drop-down list, select the type of field (Lookup, Text, Text Area).
6. Select or clear the **Enabled** check box.
7. If this is a required field that must be completed during staff sign in, select the **Required** check box.

Volunteer Custom Profile Fields, cont.

8. Select the **Display on Sign-In Page** check box if you want the field to display on the **Sign In** workspace.

   Note: Custom Profile fields are displayed on the **Sign In** workspace only if the **Display on Sign-In Page** check box is selected. This field displays as *read-only* unless using the manual entry feature.

9. In the **Order** column, specify the order in which the custom profile field displays on the **Volunteer Detail** workspace, the **Personal Information** page of the online volunteer application, and the **Application Detail** workspace. By default the fields appear in the order in which they were created.

   Note: You must edit each custom profile field to change the sequence order.

10. Click the ✔ icon to save the newly created custom field. To discard your changes, click the ⊗ icon.
11. If the Lookup field type is selected, click **Manage Values** to specify the **Lookup Values** for the field.
12. Click **Add Lookup Value**, enter the **Value** in the text field and click ✔ to save it.

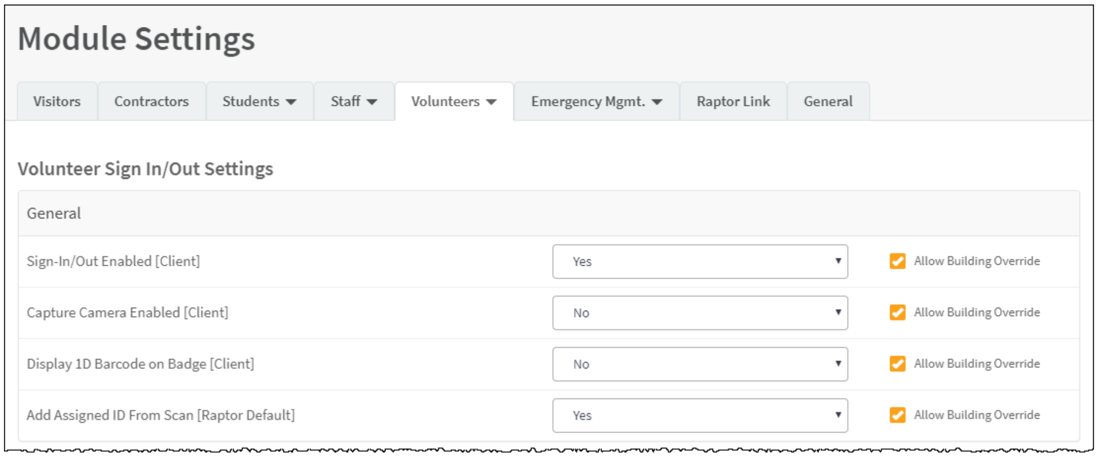
Modify or Delete Custom Profile Field

To modify a custom profile field, click the ✎ icon in the **Options** column in the **Custom Profile Field** grid on the **Volunteer Management** workspace and edit the information. Click the ✔ icon to save your changes. If you want to discard your changes, click the ⊗ icon.

To delete a custom profile field, click the 🗑 icon in the **Custom Profile Field** grid on the **Volunteer Management** workspace and then click **OK** on the confirmation dialog.

Volunteer Sign-In/Sign-Out Settings

Use the Volunteer Sign-In/Sign-Out Settings workspace to specify sign-in and sign-out settings that display during Volunteer Sign In and Sign Out. To access this workspace, select **Admin > Module Settings** in the navigation menu and then click the **Volunteers** tab and select **Volunteer Sign-In/Out**.



From this workspace, you can perform the following tasks:

- Enable/Disable Volunteer Sign-In/Out
- Enable/Disable Capture Camera
- Display 1D Barcode on Badge
- Specify Volunteer Sign-In Settings
- Add Volunteer Custom Sign-In Fields
- Specify Auto Sign-Out Time

Enable/Disable Volunteer Sign-In/Out

By default, Raptor is configured with the Volunteer Sign In/Out feature enabled. The feature can be disabled to hide Volunteer Sign In and Sign Out features in the **Sign In/Sign Out** workspace.

Perform the following steps to enable or disable the Volunteer Sign-In and Sign-Out features:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Sign-In/Out** from the drop-down menu.
3. From the **Enable Volunteer Sign In/Out** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Enable Capture Camera

The capture camera feature allows the user to take a photo of the person signing in and associate that photo with the person's record in the Raptor system. This feature is useful when the person signing in does not have an official ID that can be scanned, such as a passport.

By default, Raptor is configured with the Capture Camera disabled. Users can enable this feature using the **Capture Camera Enabled** setting on the **Volunteer Sign-In/Sign-Out Settings Settings** workspace. When the capture camera is enabled, the Camera button displays on the **Sign In** workspace below the photo.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Sign In/Out** from the drop-down menu.
3. From the **Capture Camera Enabled** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Note: A camera is required to use this feature. If you are using a Windows Internet Explorer (IE) browser, you must have Adobe Flash Player installed to use the Capture Camera feature.

Add Assigned ID From Scan

Users with the *Can Manage Volunteer Settings* permission can specify whether to allow a 1D barcode to be captured from a volunteer's ID card and populated in the Assigned ID field for that volunteer.

Perform the following steps to enable or disable this feature:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Sign In/Out** from the drop-down menu.
3. In the **Add Assigned ID From Scan** field, select **Yes** (to enable) or **No** (to disable) from the drop-down list.
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Display 1D Barcode on Badge

Users with Administrative permissions can control whether or not a 1D barcode is printed on the volunteer badge. If the 1D barcode is printed on the badge, the volunteer can simply scan the code on their badge when signing out at the front desk or kiosk.

Perform the following steps to display the 1D barcode on the contractor badge:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Sign In/Out** from the drop-down menu.
3. From the **Display 1D Barcode on Badge** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Volunteer Sign-In Settings

Use these settings to specify what is required when a volunteer signs in.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Sign In/Out** from the drop-down menu.
3. Specify whether the following field is required to be completed during sign in and whether individual buildings can override this settings:
   - **Volunteer Can Sign In to Any Building** – Select **Yes** or **No** from the drop-down list to specify whether the Find search returns the volunteers name when they sign into any building in the district; not just those buildings listed on their volunteer application.
   - **Require Sign-In Organization** – Select **Yes** or **No** from the drop-down list to specify whether an organization is required during volunteer sign in.
   - **Allow Building Override** – Select or clear the check box for each of the fields. If selected, the settings can be overridden at the building level. Otherwise, clear the check boxes.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Volunteer Auto Sign-Out Time

By default, Raptor is configured to automatically sign out all volunteers at 6:00 PM. Users with Administrator permissions can change this time and specify whether the setting can be changed at the building level.

Perform the following steps to modify the auto-sign out time:

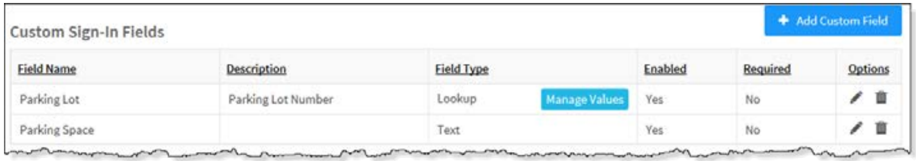
1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Sign In/Out** from the drop-down menu.
3. In the **Auto Sign Out Time** field, click the icon and select the time from the drop-down list.
4. Select the **Allow Building Override** check box if you want buildings to be able to change this time. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Volunteer Custom Sign-In Fields

You can create custom sign-in fields that are associated with sign-in events (such as Parking Lot) to display on the **Volunteer Sign In** and **Volunteer Delayed Entry** workspaces for all buildings or specific buildings.

Note: Custom Sign-In fields are not available in the Kiosk.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Sign In/Sign Out**.
3. In the **Custom Sign-In Fields** grid, click **Add Custom Field**.
4. Enter the **Field Name** and **Description**.



5. In the **Field Type**, select the type of field (Lookup, Text, Text Area).
6. Select or clear the **Enabled** check box.
7. If this is a required field that must be completed during volunteer sign in, select the **Required** check box.
8. Click the ✔ icon to save the newly created custom field.
9. If the Lookup field type is selected, click **Manage Values** to specify the **Lookup Values** for the field.
10. Click **Add Lookup Value**, enter the **Value** in the text field and click ✔ to save it.

Modify Custom Sign-In Field

Click the icon in the **Options** column and edit the information. Click the ✔ icon to save your changes. If you want to discard your changes, click the icon.

Delete Custom Sign-In Field

Click the icon in the **Options** column and then click **OK** on the confirmation dialog.

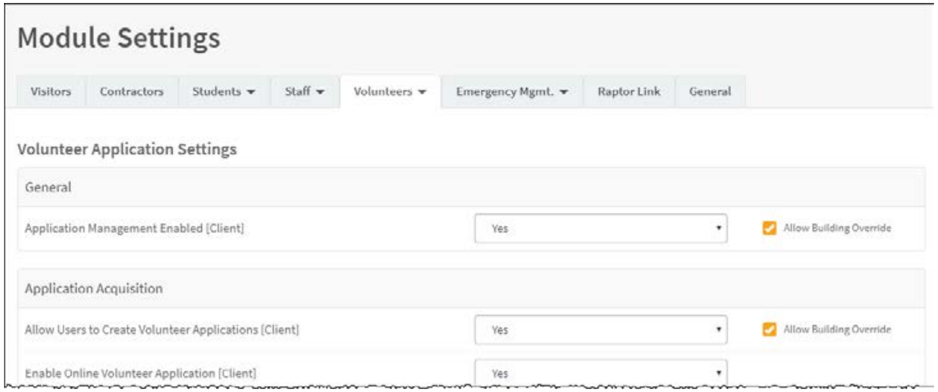
Volunteer Application Settings

The Volunteer Application Settings workspace includes settings for volunteer applications. To access this workspace, select **Admin > Module Settings** in the navigation menu and then click the **Volunteers** tab and select **Volunteer Application**.

Note: This workspace is available with both the Raptor System and Raptor Volunteer Management System, however settings are limited with the Raptor System.

From this workspace, you can perform the following tasks:

- Enable/Disable Application Management
- Specify Application Acquisition Settings
- Specify Approval Queue Settings
- Specify Application Renewal Policy
- Manage Volunteer Notifications
- Manage Online Volunteer Application Page



Enable/Disable Application Management

By default, Raptor is configured with the **Volunteer Application Management** feature enabled, however, the feature can be disabled to hide these settings.

Perform the following steps to enable or disable the Volunteer Application Management features:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Application** from the drop-down menu.
3. From the **Application Management Enabled** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Application Acquisition Settings

Users with the *Can Manage Volunteer Settings* permission can specify the settings for how volunteer applications are managed.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Application**.
3. In the **Application Acquisition** area, specify the settings (see next slide).
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Application Acquisition Settings, cont.

Specify the following settings:

- **Allow Users to Create Volunteer Applications** – Select **Yes** (to enable) or **No** (to disable) to indicate whether users can create volunteer applications in the Volunteer Module.

  Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
- **Enable Online Volunteer Application** –Select **Yes** (to enable) or **No** (to disable) to indicate whether the online application is available.
- **Application Return URL** – Enter the URL where the browser will be sent when a volunteer applicant clicks Finish on the last page of the online volunteer application.

  Note: URLs ending with a forward slash (/) are not supported.
- **Enable Spanish Localization** – If the Online Volunteer Application feature is enabled, you can also enable the application to display in Spanish. Select **Yes** (to enable) or **No** (to disable).
- **District Email Address** – Enter the email address that will be displayed on the Personal Information page of the online volunteer application to be used if the applicant does not have an email address.
- **Enable Building Groups** – Select **Yes** (to enable) or **No** (to disable) to specify whether building groups display on the online volunteer application. When enabled, the user can select a building group, such as All Elementary Schools, rather than selecting each elementary school where they want to volunteer.

Specify Approval Queue Settings

Users with the *Can Manage Volunteer Settings* permission can enable or disable the automatic approval of a volunteer application when all requirements are met, such as no matches to possible sex offender alerts, a clean criminal background screening and all custom defined requirements.

You can also enable automated notifications to the Building Volunteer Coordinator when a volunteer has been approved.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Application** from the drop-down menu.
3. Specify the following information:
   - **Automatically Approve When Requirements Satisfied** – Select **Yes** (to enable) or **No** (to disable) to enable or disable automatic approval of volunteer applications when requirements have been satisfied.
   - **Notify Building Volunteer Coordinator On Approval** – Select **Yes** (to enable) or **No** (to disable) to enable or disable automatic notifications to the Building Volunteer Coordinator associated with the same buildings selected on the application, when volunteer applications have been approved.

     Note: This feature requires the Application Approved - Internal Notification to be enabled.

     Allow Building Override – Select the check box if the setting can be overridden at the building level. Otherwise, clear the check box.
   - **Texas DPS User ID** – Enter the Texas DPS user ID to be referenced when creating a new batch of volunteer applications that are formatted specifically for Texas DPS.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Specify Application Renewal Policy

Users with the *Can Manage Volunteer Settings* permission can select the number of days prior to the volunteer's expiration date at which time the volunteer can submit a new application. The renewal options are in 30-day increments.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Application** from the drop-down menu.
3. From the **Allow Application Renewal Prior to Expiration** drop-down list, select the number of days prior to expiration that the volunteer can resubmit a volunteer application (30 Days is the default).

   To disable this feature, select **Never** from the drop-down list.
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Manage Volunteer Notifications

Use the **Notification Management** grid on the **Volunteer Application Settings** workspace to enable and disable the notifications that are automatically sent to volunteer applicants and to people who are specified in contacts during the application process.

Notification Management

Details	Name	Recipient	Building Scope	Is Enabled
▶	Application Received	Applicant	All Buildings	Yes
▶	Application Approved	Applicant	All Buildings	Yes
▶	Application Renewal Notice	Volunteer	All Buildings	No
▶	Application Approved - Internal Notification	Client Contacts	All Buildings	Yes
▶	Volunteer Application Disclaimer	Client Contacts	All Buildings	Yes
▶	Application Requires Attention	Client Contacts	All Buildings	Yes
▶	Application Denied	Client Contacts	All Buildings	Yes

- **Application Received** – Sent only to volunteer applicants upon receipt of application.
- **Application Approved** – Sent only to volunteer applicants upon approval of application.
- **Application Renewal Notice** –Sent to active volunteers when their application renewal window begins as defined by the volunteer application renewal policy.
- **Application Approved - Internal Notification** – Sent to volunteer coordinator contact(s) when application has been approved.
- **Volunteer Application Disclaimer** – Sent to the volunteer coordinator contacts when applicant has read and accepted the disclaimer on the volunteer application.
- **Application Requires Attention** – Sent to volunteer coordinator contact(s) when application needs attention.

Manage Volunteer Notifications, cont.

- **Application Denied** – Sent to volunteer coordinator contact(s) when application has been denied.
- **Criminal Background Screening Maintenance** – Sent to volunteer coordinator contact(s) to notify volunteer application service is entering maintenance mode (only customers with criminal background screening feature enabled).
- **Criminal Background Screening Funds Low Depleted or Replenished** – Sent to the specified client contact when criminal background screening low funds threshold has been met, or fund is depleted or replenished.
- **Volunteer Portal User Account Creation Failed** – Sent to volunteer coordinator contact(s) when volunteer portal user account fails to be created because the email address is already used by another user account.

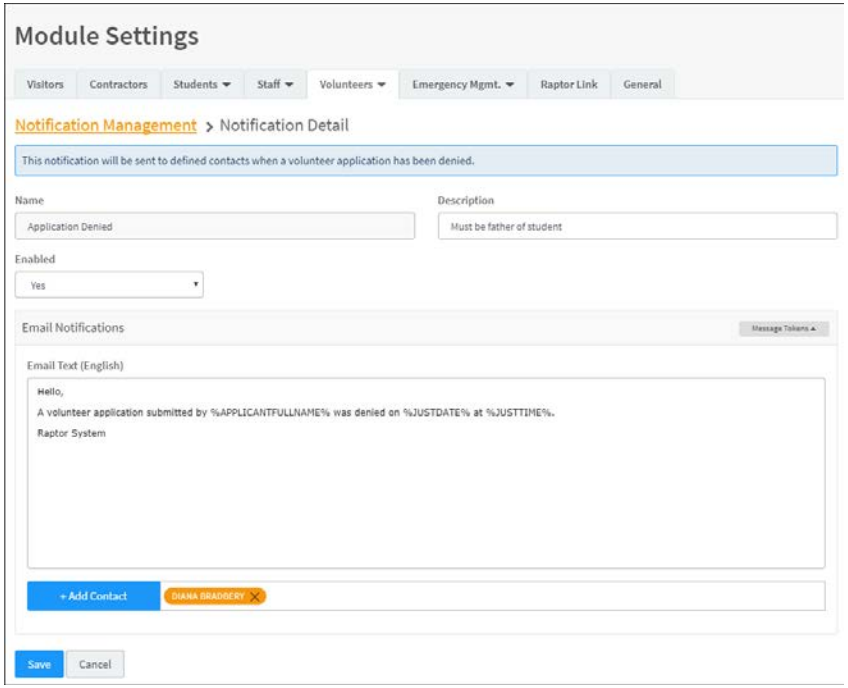
Volunteer Notifications, cont.

Note: Contacts must be defined prior to using this feature where the applicant is the recipient of the notification.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Application**.
3. In the **Notification Management** grid, click the ▶ icon in the Details column and specify the following:
   - **Enabled** – Select **Yes** (enable) or **No** (disable).
   - **Description** – Optional description.
   - **Email Text** – Message that will be sent via email. You can also use Message Tokens to compile the message.
   - **Email Contacts** – Click **Add Contact** and select the contact name.

     To remove an email contact, click the **X** in the contact label.

     Note: If the contact name is gray, it was defined at the district level and cannot be removed at the building level.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.



Note: In the **Add Contact** drop-down list, the icons that display represent the contact's preferred method of notification. If the contact has selected both Text and Email as their preferred notification method, when one method is populated with the contact name, the other method will be automatically populated.

Message Tokens for Volunteer Notifications

You can also use Message Tokens, which are variables, in the notification message so that when the message is sent, the tokens will be replaced by their associated value.

Click **Message Tokens** to view the variables that can be entered in the message.

%APPLICATIONID% - Unique Application ID Number
%CLIENTNAME% - District Name
%BUILDINGNAME% - Building Name
%JUSTDATE% - Date Logged - MM/DD/YYYY

Example:

Congratulations. Your application has been approved and you are now able to volunteer at %CLIENTNAME%.

View Online Application URLs

Use the **Online Volunteer Application Page Management** area on the **Volunteer Application Settings** workspace to manage the online volunteer application page that can be accessed from your district website.

If the **Online Volunteer Application** feature is enabled, the URLs to access the online volunteer application are generated in the **Online Volunteer Application Page Management** area in the lower portion of the **Volunteer Application Settings** workspace. You can use these URLs to display on your client website.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Application** from the drop-down menu.
3. In the **Online Volunteer Application Page Management** area on the **Volunteer Application Settings** workspace, view the URLs in the appropriate fields:
   - **English Language URL** –If Online Volunteer Application is enabled, the URL to access the English language online volunteer application displays in this field.
   - **Spanish Language URL** – If Spanish Localization is enabled, the URL to access the Spanish language online volunteer application displays in this field.

Note: If the Online Volunteer Application feature is disabled, these fields will be disabled. You must enable the feature to enable the URL fields.

Online Application Content

Users with the *Can Manage Volunteer Settings* permission can specify the text that displays on the following pages of the online volunteer application.

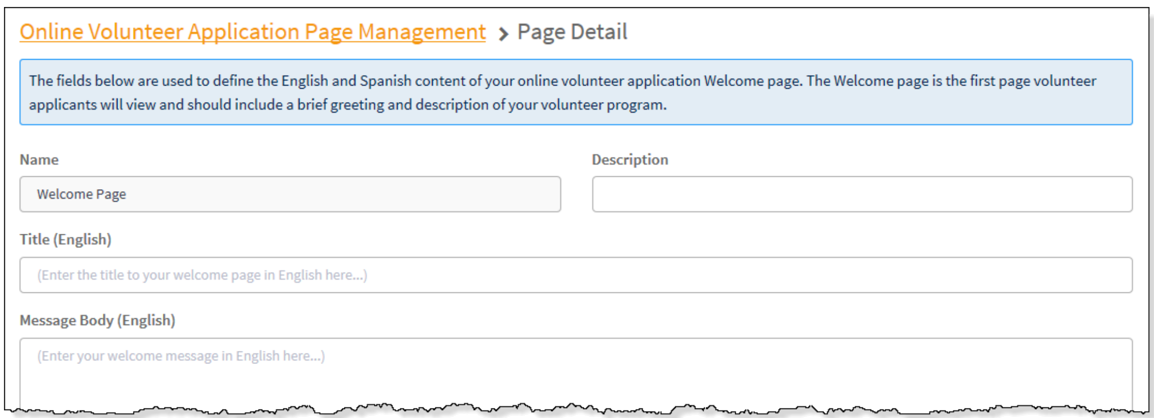
Details	Name	Building Scope
▶	Welcome Page	All Buildings
▶	Existing Volunteer Page	All Buildings
▶	Duplicate Application Page	All Buildings
▶	Documents Page	All Buildings
▶	Disclaimer Page	All Buildings
▶	Self-Serve Payment Page	All Buildings
▶	Closing Page	All Buildings
▶	Application Service Unavailable Page	All Buildings

- **Welcome Page** – First page that displays in the online volunteer application.
- **Existing Volunteer Page** – Displays for a volunteer who has already been approved and is resubmitting an online volunteer application but it is not within their renewal window.
- **Duplicate Applications Page** – Displays when a person is attempting to submit an application using the online volunteer application however that person already has an application under review.
- **Documents Page** – This page displays the required documents that applicants must provide either at time of submission or before approval.
- **Disclaimer Page** – This page displays before the application Self-Serve Payment page or the Closing page, and provides a disclaimer and signature field for the applicant.
- **Self-Serve Payment Page** – This page displays if you have selected one or more functions that require a background check that has an associated cost that will be paid by the applicant; allows applicant to provide payment information.
- **Closing Page** – Last page of the online volunteer application.
- **Application Service Unavailable Page** – Displays when the online volunteer application is down due to maintenance.

Online Application Content, cont.

Perform the following steps to specify the content that displays on the online volunteer application:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Application** from the drop-down menu.
3. In the **Online Volunteer Application Page Management** area on the workspace, click the ▶ icon in the **Details** column for the [page name].



4. On the **Page Detail** workspace, specify the **Title** (for English and Spanish) and the **Message Body** (English and Spanish).

   Note: If the Spanish language online application is disabled, you must enable it before the fields will be enabled.

5. Click **Save**.

Volunteer Portal Settings

The **Volunteer Portal Settings** workspace enables users with the *Can Manage Volunteer Settings* permission to manage the volunteer portal. To access this workspace, select **Admin > Module Settings** in the navigation menu and then click the **Volunteers** tab and select **Volunteer Portal**.

Note: This workspace is only available if the Raptor Volunteer Management System is enabled.

From this workspace, you can perform the following tasks:

- Specify Portal Management Settings
- Manage Volunteer Portal Notifications
- Access Volunteer Portal URL

Specify Portal Management Settings

Use this area on the **Volunteer Portal Settings** workspace to enable or disable the volunteer portal, and to specify whether volunteers can add hours.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Portal** from the drop-down menu.
3. Specify the following settings:
   - **Volunteer Portal Enabled** -- Select **Yes** (to enable) or **No** (to disable). By default, the volunteer portal is disabled.
   - **Allow Volunteers to Add Hours** – Select **Yes** (to allow) or **No** (to not allow).

     Note: This setting displays only when the **Enable/Disable Volunteer Portal** setting is enabled.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

Volunteer Coordinator Notifications

Use the **Notification Management** grid on the **Volunteer Portal Settings** workspace to enable and disable the email notification that is sent to the Volunteer Coordinator when a volunteer selects the **Contact Volunteer Coordinator** option in the Volunteer Portal, and to specify the contacts who receive the email notification.

Note: This grid only displays when the Enable/Disable Volunteer Portal setting is enabled.

Notification Management

Details	Name	Recipient	Building Scope	Is Enabled
▶	Email Volunteer Coordinator	Client Contacts	All Buildings	No

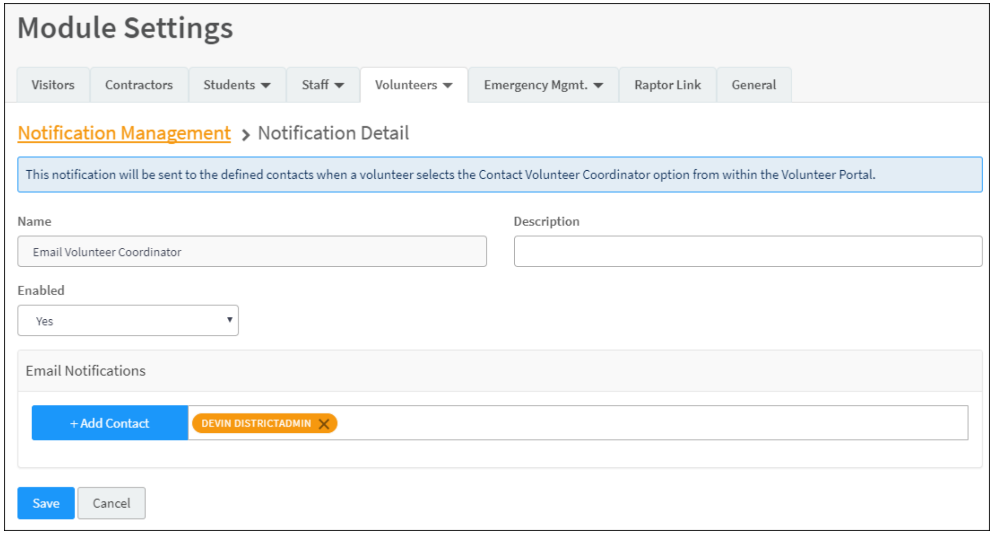
Note: Contacts must be defined prior to using this feature.

Perform the following steps to set up automatic notifications:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Portal** from the drop-down menu.
3. In the **Notification Management** grid, click the ▶ icon in the **Details** column.

Volunteer Coordinator Notifications, cont.

4. On the **Notification Detail** workspace, specify the following information:



- **Enabled** – Select **Yes** (enable) or **No** (disable) to indicate whether the notification should be enabled.
- **Email Notifications** – Click **Add Contact** and select the contact name from the drop-down list. The contact information must be added in Contacts prior to creating the email notification.

  To remove an email contact, click the **X** in the contact label.

  Note: If the contact name is gray, it was defined at the district level and cannot be removed at the building level.

5. Click **Save**.

Access Volunteer Portal URL

This feature generates a client-specific URL to access the Volunteer Portal. This URL will also be provided in the Volunteer Approval notification to applicants when the Volunteer Portal is enabled and the applicant has provided a valid email address.

Note: If the Volunteer Portal is disabled, this field will be blank.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Portal** from the drop-down menu.
3. In the **Volunteer Portal Access** list on the workspace, view the URL in the **Volunteer Portal URL** field.

4. Copy the URL into your browser to access the volunteer portal for your district. You can also include this URL on your district website for volunteers to access the volunteer portal.

Enable/Disable Event Management

The **Volunteer Event Settings** workspace enables users with the *Can Manage Volunteer Settings* permission to manage the volunteer event settings in Raptor. You use this workspace to enable or disable volunteer event management.

Note: This workspace is only available if the Raptor Volunteer Management System is enabled.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Volunteers** tab and select **Volunteer Portal** from the drop-down menu.
3. From the **Volunteer Event Management Enabled** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Manage Emergency Mgmt Module Settings

Use the **Drill Manager** or **Emergency Mgmt** tab on the **Module Settings** workspace to manage the settings specific to Drill Manager and Raptor Reunification®. The following topics are covered in this section:

- Emergency Management Module Settings
- Enable/Disable Drill Manager
- Notification Management
- Enable/Disable Drill Notifications
- Enable/Disable Reunification
- Enable/Disable Notifications
- View Emergency Types
- Manage Emergency Sub-Types
- Manage Locations/Manage Location Categories
- Manage Statuses

RAPTOR
TECHNOLOGIES

Emergency Management Module Settings

Use the **Drill Manager** or **Emergency Mgmt** tab on the **Module Settings** workspace to manage the settings specific to Drill Manager and Raptor Reunification. How the settings display in the **Module Settings** workspace depends on whether your district had Raptor Reunification enabled.

Raptor Reunification Enabled

If your district has Raptor Reunification enabled, the **Module Settings** workspace includes the **Emergency Mgmt** tab and drop-down menu where you can select the workspace in which you want to work:

- **Drill Manager** – Use this workspace to enable the Drill Manager module, and manage notifications for drills. Users must have the *Can Manage Client Settings* or *Can Manage Building Settings* permission to view the **Drill Manager** workspace.
- **Reunification** REU – Use this workspace to manage the settings specific to the reunification application. Users must have the *Can Manage Reunification Settings* permission to access the **Reunification** workspace.

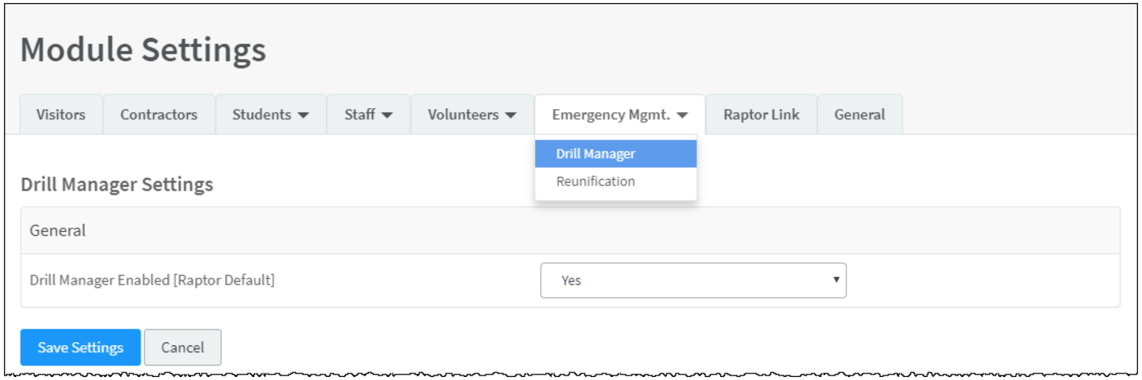
Reunification Not Enabled

If your district does not have Reunification enabled, the **Module Settings** workspace includes only the **Drill Manager** tab.

Enable/Disable Drill Manager

Drill Manager enables you to manage the drills that will be used during emergencies. Perform the following steps to enable or disable Drill Manager:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Drill Manager** tab, or click the **Emergency Mgmt** tab and select **Drill Manager**.



3. From the **Drill Manager Enabled** drop-down list, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be changed at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Notification Management

Use the **Notification Management** grid on the **Drill Manager Settings** workspace to enable and disable the notifications that are automatically sent to the specified contacts about upcoming drills and drill requirements.

Note: Contacts must be defined prior to setting up notifications.

Notification Management

Details	Name	Delivery	Recipient	Enabled
▶	Upcoming Drill Summary (Per Building)	Sent on the first day of the month	Client Contacts	Yes
▶	Drill Reminder (Per Requirement)	Sent five days prior to drill due date	Client Contacts	Yes
▶	Reminder Summary (All Buildings)	Sent five days prior to drill due date	Client Contacts	No
▶	End of Month Summary (All Buildings)	Sent on the first day of the month	Client Contacts	No

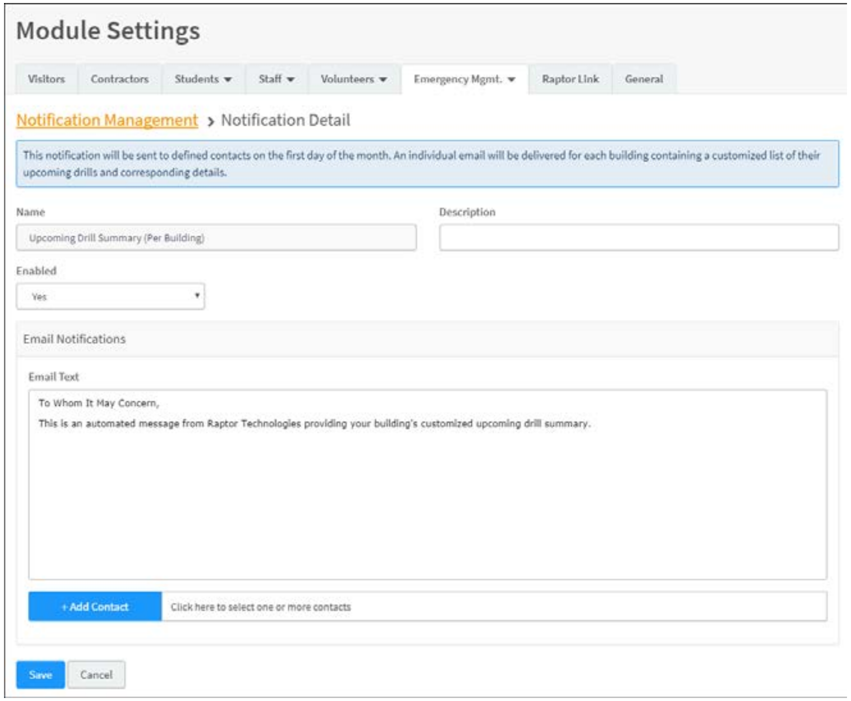
- **Upcoming Drill Summary (Per Building)** – This notification will be sent to defined contacts on the first day of the month. An individual email will be delivered for each building containing a customized list of their upcoming drills and corresponding details.
- **Drill Reminder (Per Requirement)** – This notification will be sent to defined contacts five days prior to the drill due date, only if the drill requirement has not been completed. An individual email will be delivered for each drill requirement, by building, containing the drill details that is at risk of being out of compliance.
- **Reminder Summary (All Buildings)** – This notification is only available at the All Buildings level and will be sent to defined contacts five days prior to the drill due date. The reminder summary contains a list of all buildings that have not completed a specific drill requirement and are at risk of being out of compliance. An individual email reminder summary will be delivered for each drill requirement due in five days.
- **End of Month Summary (All Buildings)** – This notification is only available at the All Buildings level and will be sent to defined contacts on the first day of the month. The End of Month Summary provides a breakdown by building of each drill requirement due during the month and their status.

Enable/Disable Notifications

Perform the following steps to enable automatic notifications:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Drill Manager** tab, or click the **Emergency Mgmt** tab and select **Drill Manager**.
3. In the **Notification Management** grid, click the ▶ icon in the Details column for the notification.
4. Specify the following information:
   - **Enabled** – Select **Yes** (enable) or **No** (disable).
   - **Description** – Optionally, enter a description.
   - **Email Text** – Enter the message that will be sent via email.
   - **Contacts** – Click **Add Contact** and select the contact name. The contact information must be added prior to creating the email notification.

     Note: In the Add Contact drop-down list, the icons that display represent the contact's preferred method of notification.



     To remove an email contact, click the **X** in the contact label.

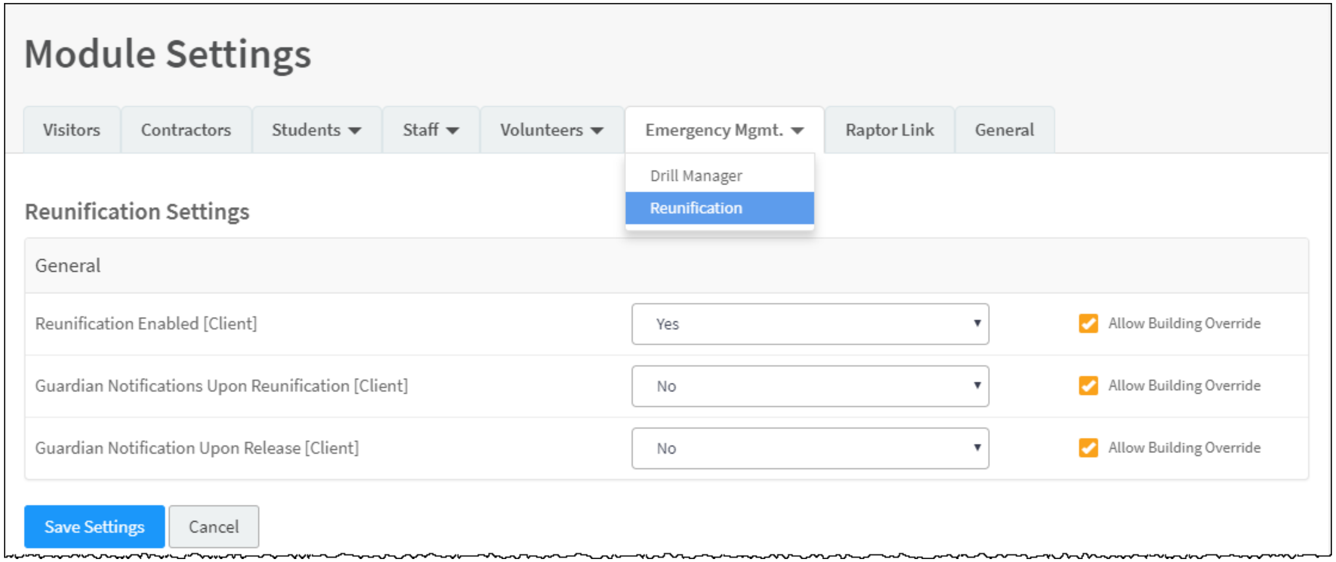
5. Click **Save**.

RAPTOR TECHNOLOGIES

Reunification Module Settings

The Raptor Reunification System helps ensure that students are tracked, accounted for, and reunited with their parents or guardians safely and as efficiently as possible during emergency events. The Raptor Reunification System can be implemented as a standalone product or integrated with the Raptor System.

When integrated with the Raptor System, users can manage the administrative tasks in Raptor from the **Emergency Mgmt > Reunification Settings** workspace.



Enable/Disable Reunification Module

By default, Raptor is configured with the Reunification application enabled. Perform the following steps to enable or disable the Reunification module:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Emergency Mgmt** tab and select **Reunification** from the drop-down menu.
3. From the **Reunification Enabled Enabled** field, select **Yes** (to enable) or **No** (to disable).
4. Select the **Allow Building Override** check box if the setting can be overridden at the building level. Otherwise, clear the check box.
5. Click **Save Settings**.
6. Log out of Raptor and then log in to see the change.

Enable/Disable Notifications

During the reunification process, guardians can be notified when the student has been reunified with another parent or guardian (Guardian Notification Upon Reunification). In addition, during a controlled release process, parents or guardians can be notified when a student has been released from school (Guardian Notification Upon Release).

Perform the following steps to enable or disable these notifications:

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Emergency Mgmt** tab and select **Reunification** from the drop-down menu.
3. Specify the following settings:
   - **Guardian Notification Upon Reunification** – Select **Yes** (to enable) or **No** (to disable).
   - **Guardian Notification Upon Release** – Select **Yes** (to enable) or **No** (to disable).
   - **Allow Building Override** – Select the check box if the setting can be overridden at the building level. Otherwise, clear the check box.
4. Click **Save Settings**.
5. Log out of Raptor and then log in to see the change.

View Emergency Types

The Emergency Types are pre-defined, system default categories that are read-only and cannot be modified. The Emergency Type categories hold user-defined sub-types that are used when initiating incidents in the product.

Note: When creating an Emergency Sub-Type, it must be categorized in one of the Emergency Types.

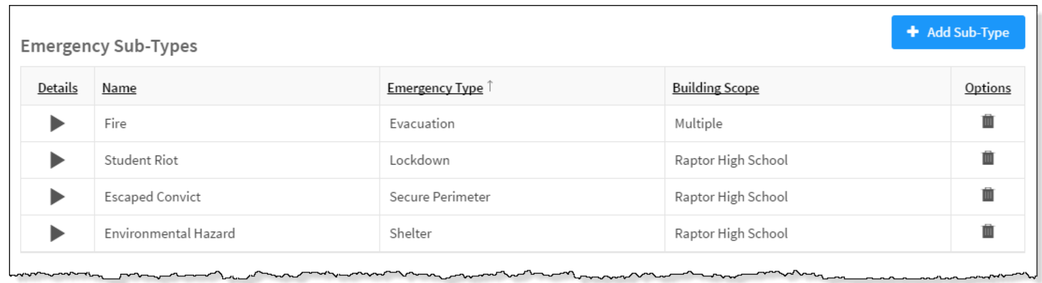
1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Emergency Mgmt** tab and select **Reunification** from the drop-down menu.
3. View the **Emergency Types** in the list. The name and building scope display.

Emergency Types

Name	Building Scope
Evacuation	All Buildings
Lockdown	All Buildings
Secure Perimeter	All Buildings
Shelter	All Buildings

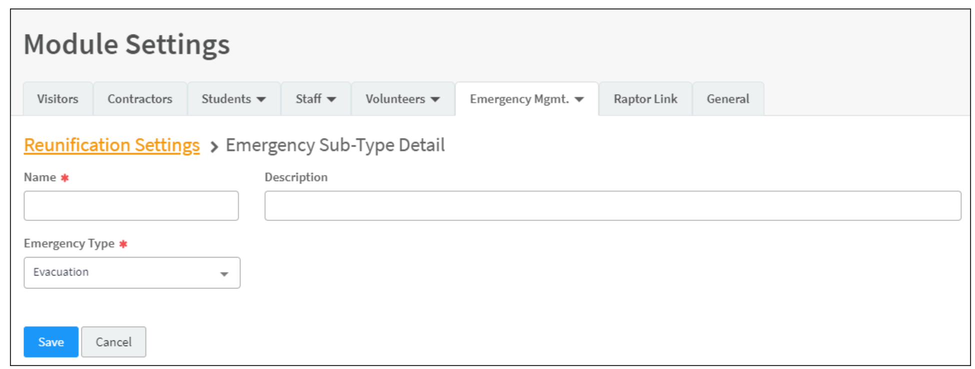
Manage Emergency Sub-Types

The **Emergency Sub-Types** area on the **Reunification Settings** workspace are user-defined and specific to a pre-defined emergency type. The Reunification module ships with out-of-the-box values to be used as an example and modified based on your district's operations plan. You can view, create, modify and delete emergency sub-types.



Add Emergency Sub-Types

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Emergency Mgmt** tab and select **Reunification**.
3. In the **Emergency Sub-Types** grid, click **Add Sub-Type**.
4. Enter a **Name*** and optional **Description**.
5. Select the **Emergency Type*** in which this emergency sub-type is categorized.
6. Click **Save**.



Modify or Delete Emergency Sub-Type

Click the icon to modify the details and then click **Save**.

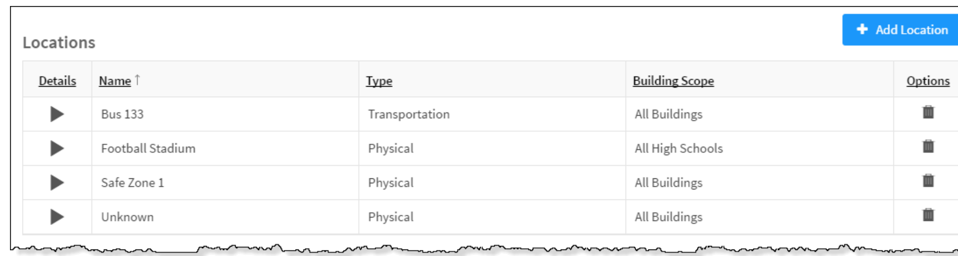
To delete an emergency sub-type, click the icon in the **Options** column and then click **OK** on the confirmation dialog.

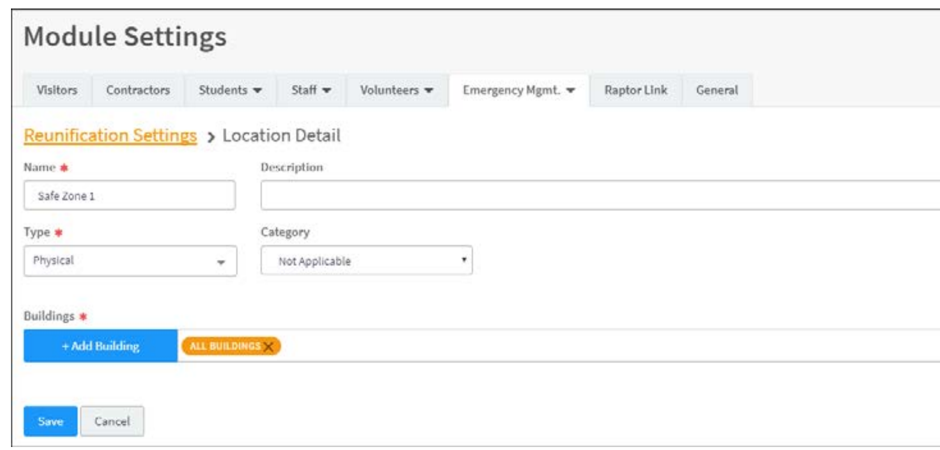
Manage Locations

The **Locations** grid on the **Reunification Module Settings** workspace is used to manage the physical and transportation locations used during a drill or live emergency. From this area, users with the *Can Manage Reunification Settings* permission can view, create, modify and delete locations.

Add Location

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Emergency Mgmt** tab and select **Reunification**.
3. In the **Locations** grid, click **Add Location**.
4. Enter a **Name*** and optional **Description**.
5. Select the location **Type*** (Physical or Transportation).
6. Click **Add Building*** and select the building, a building group, or All Buildings.
7. Click **Save**.





Modify or Delete Location

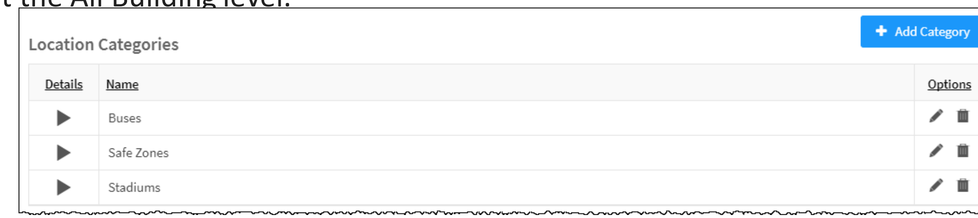
Click the icon to modify the details and then click **Save**.

To delete a location, click the icon in the **Options** column and then click **OK** on the confirmation dialog.

Manage Location Categories

The **Location Categories** grid on the **Reunification Settings** workspace is used to manage the categories that can be used when defining the locations. From this grid, users with the *Can Manage Reunification Settings* permission can view, create, modify and delete location categories.

Note: You can only create location categories at the All Building level.



Create Location Category

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Emergency Mgmt** tab and select **Reunification**.
3. In the **Locations** grid, click **Add Location Category**.
4. Enter a **Name*** and **Description** (optional) for the location category and click **Save**.

Modify Location Category

In the **Location Categories** grid, click the icon in the **Details** column to modify the information about the location category and click **Save**.

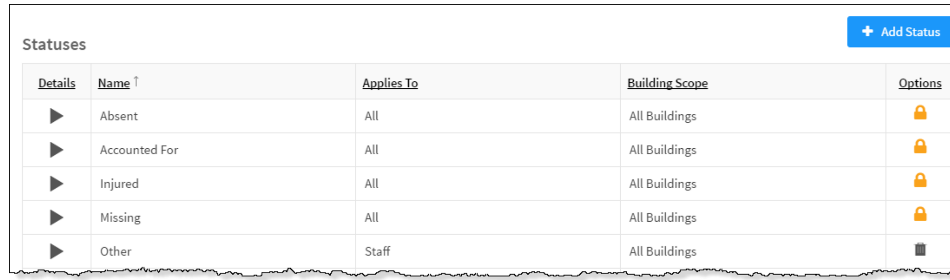
You can also click the icon in the **Location Categories** grid to modify the name of the category, and then click to save it. Click to discard your changes.

Delete Location Category

In the **Location Categories** grid, click the icon for the item to be removed and then click **OK** on the confirmation dialog to complete the process.

Manage Statuses

The **Statuses** grid on the **Reunification Settings** workspace is used to manage the various statuses that can be assigned to individuals during a drill or emergency response. From this grid, users with the *Can Manage Reunification Settings* permission can view, create, modify and delete statuses (specific to user-defined statuses).

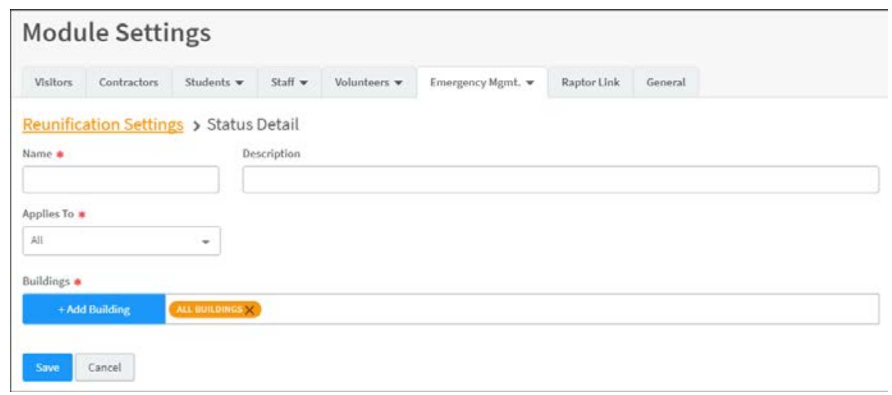


Note: The icon indicates that the status is Raptor defined and cannot be modified. If the status is locked, the fields on the Status Detail workspace are *read-only* and cannot be changed.

Add Status

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **Emergency Mgmt** tab and select **Reunification**.
3. In the **Statuses** grid, click **Add Status**.
4. Enter a **Name*** and optional **Description**.
5. Select who the status **Applies To*** during the reunification process (All, Student, or Staff).

   Note: When the status is configured to All, it can also be used for Visitors, Volunteers and Contractors; also known as *Others*.
6. Click **Add Building*** and select the building, a building group, or All Buildings.
7. Click **Save**.



Modify or Delete Status

Click the icon to modify the details and then click **Save**.

To delete a status, click the icon in the **Options** column and then click **OK** on the confirmation dialog.

Manage Raptor Link Module Settings

Raptor Link provides the ability to integrate a Student Information System (SIS) with the Raptor System. This integration enables unattended synchronization of student, guardian, staff and roster data into the Raptor System. This data is then used by Raptor Reunification and the Raptor Student and Staff modules.

Use the **Raptor Link** tab on the **Module Settings** workspace to view the read-only Raptor Link settings, manage the Raptor Link error notifications, and view Raptor Link building status.

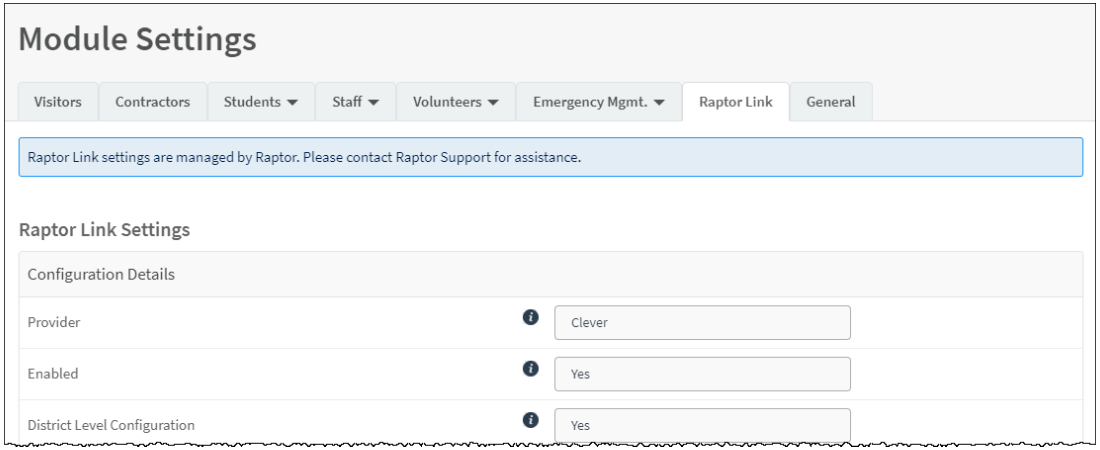
The following topics are covered in this section:

- View Raptor Link Settings
- Manage Raptor Link Notifications
- View Raptor Link Building Status

View Raptor Link Settings

The **Raptor Link Settings** area on the **Raptor Link** tab displays the configuration details for Raptor Link. These settings are managed by Raptor and are read-only.

1. In the navigation menu, select **Admin > Module Settings**, and then click the **Raptor Link** tab.
2. In the Raptor Link Settings area, view the **Configuration Details**.



The **District Level Configuration** setting determines if Raptor Link is integrated at the district level (all buildings use the same Raptor Link connection) or at the building level (each building has a discrete Raptor Link connection):

- If Raptor Link is integrated at the district level, the value is **Yes**.
- If Raptor Link is integrated at the building level, the value is **No**.

Manage Raptor Link Notifications

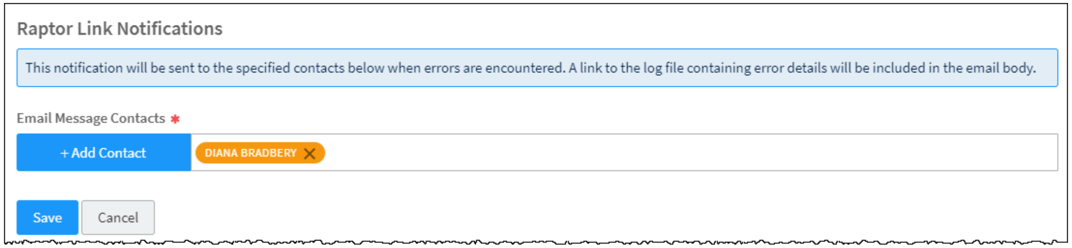
The Raptor Link Notifications area on the workspace only displays at the district level. Use this area to specify the contacts who will receive an email when Raptor Link has encountered an error.

Note: Contacts must be defined prior to using this feature where the applicant is the recipient of the notification.

1. In the navigation menu, select **Admin > Module Settings**, and click the **Raptor Link** tab.
2. In the **Raptor Link Notifications** area, click **Add Contact** and select the contact name from the drop-down list. The contact information must be added prior to creating the email notification.

   Notes:

   - In the **Add Contact** drop-down list, the icons that display represent the contact's preferred method of notification.

   - If the contact has selected both Text and Email as their preferred notification method, when one method is populated with the contact name, the other method will be automatically populated.

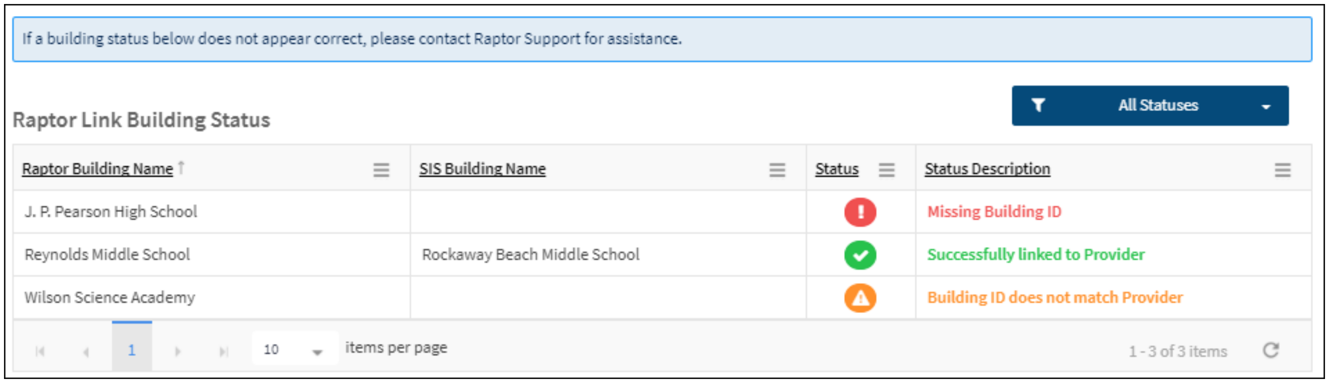
   To remove an email contact, click the **X** in the contact label.

   Note: If the contact name is gray, it was defined at the district level and cannot be removed at the building level.

3. Click **Save**.

View Raptor Link Building Status

The Raptor Link Building Status grid on the Raptor Link tab displays the building status for all buildings in the district. This grid on the workspace is only available at the district level.



Click the filter button to filter the information you want to display.

An icon displays in the **Status** column to indicate the Raptor Link status for the building and a description displays in the **Status Description** column:

- Indicates that the Raptor building is successfully linked to an SIS or SIS proxy building and is correctly functioning.
- Indicates that a value appears in the Building ID field of the building but the building is not linked to an SIS or SIS proxy building.
- Indicates that there is no value in the Building ID field.

View Tardy Code Writeback Error Log

The **Tardy Code Writeback Error Log** grid on the **Raptor Link** tab displays the errors that occur when a tardy code cannot be written back to the SIS.

- If All Buildings is selected in the building selector, all tardy codes that could not be written back display in the error log.
- If you have a specific building selected in the building selector, only those tardy codes that could not be written back for that building display in the error log.

The information that is displayed includes date/time, first and last name of the student, student ID number, building name (if all buildings is selected) and the error message.

Manage General Module Settings

Use the **General** tab on the **Module Settings** workspace to manage cross-module settings that are used throughout the product but are not specific to a module.

The following topics are covered in this section:

- View Documents REU
- Add Documents REU
- Modify and Delete Documents REU
- Manage Titles
- Upload District Image

RAPTOR TECHNOLOGIES

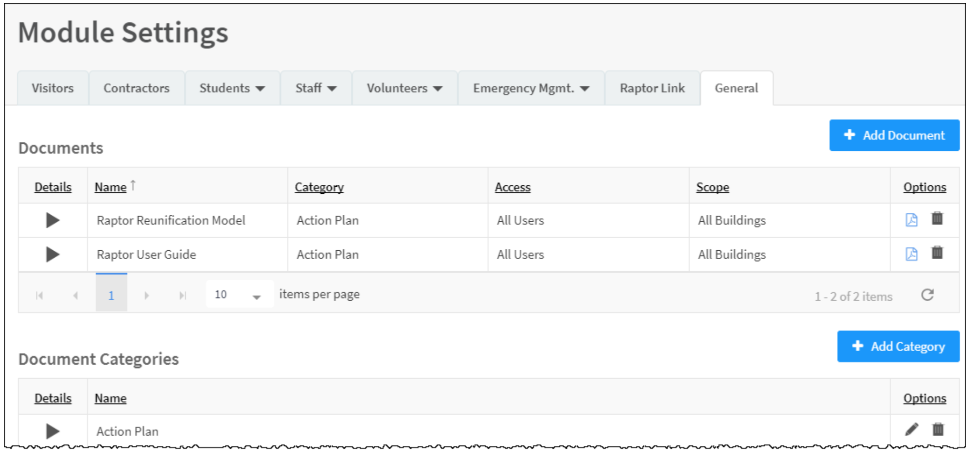
View Documents REU

If the Reunification module is enabled and depending on your permissions, you can view and manage documents related to the reunification process from the **Documents** area on the **General Module Settings** workspace.

- Users with the *Can Manage Documents* permission, can view, add, modify, and delete documents on the workspace.
- Users without the *Can Manage Documents* permission can only view the document (PDF) and document metadata.

1. In the navigation menu, select **Admin > Module Settings** and click the **General** tab.
2. Use the **Documents** grid to view the documents. The name of the document, type, who can access it and the building scope display.
3. Click the icon in the **Options** column to preview the document in PDF format.

Note: You must have Adobe Acrobat installed to view the PDF.

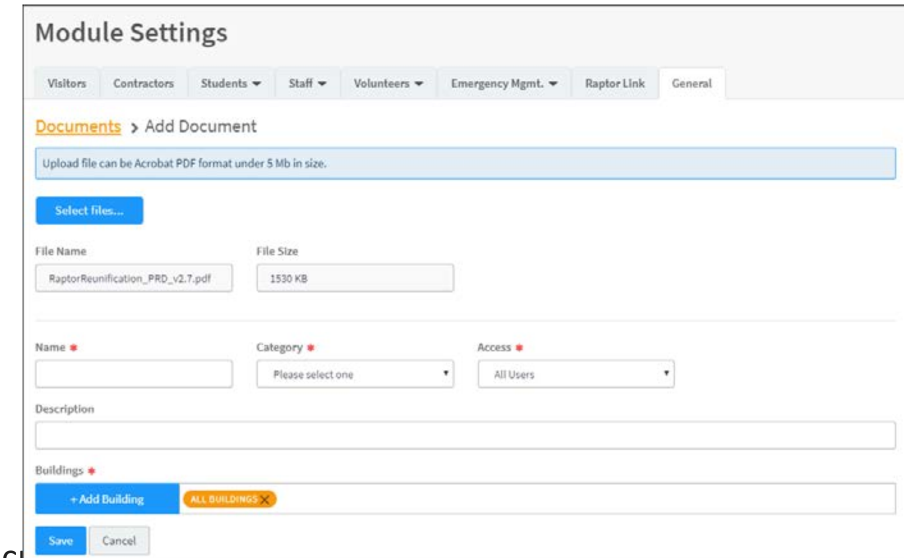


Add Documents REU

Users with the *Can Manage Documents* permission can add documents to the **Documents** grid on the **General** workspace.

Note: The document must be in Adobe Acrobat PDF format and less than 5 MB in size.

1. In the navigation menu, select **Admin > Module Settings** and click the **General** tab.
2. In the **Documents** area, click **Add Document**.
3. Click **Select File** and navigate to the location where the file is saved on your computer.
4. Complete the following information:
   - **Name*** – Enter a name for the document.
   - **Category*** –Select the document category (Action Plan, Emergency Plan, or Facility Map).
   - **Access*** – Select who has access to the document (All Users, Student Supervisor, or Incident Commander).
   - **Description** – Optionally, enter text that describes the document, for example, when it should be used.
   - **Buildings*** – Click **Add Building** and select the building or building group for the buildings where the document is available.
5. Click **Save**.



Modify and Delete Documents REU

Users with the *Can Manage Documents* permission can modify the documents that are uploaded to the **Documents** grid on the **General** workspace.

1. In the navigation menu, select **Admin > Module Settings** and then click the **General** tab.
2. In the **Documents** grid, click the ▶ icon for the document you want to modify.
3. Modify any of the fields for the existing document or upload a new version of the document.

   You can view the date the document was originally uploaded (Created Date) and by whom (Created By), and the last time it was modified (Modified Date) and by whom (Modified By) in the lower portion of the screen. These fields are *read-only* and are generated by the system.
4. Click **Save**.

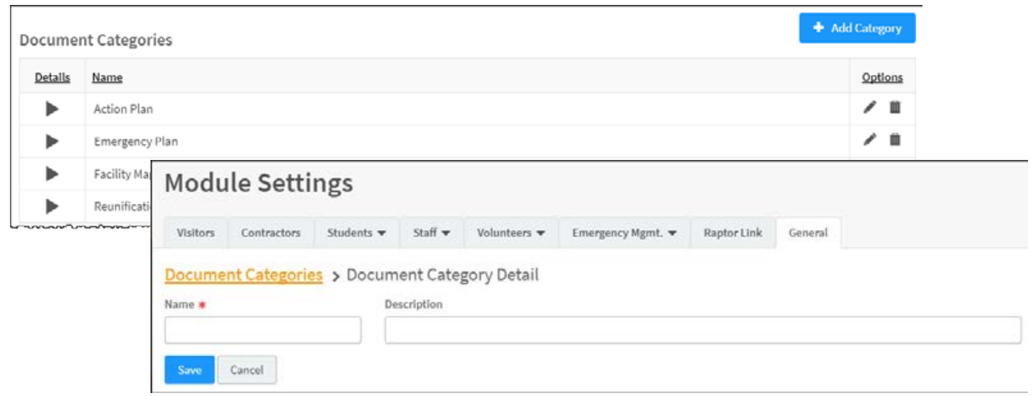
Delete Document

In the **Documents** area, click the 🗑 icon in the **Options** column and then click **OK** on the confirmation dialog.

Manage Document Categories

The **Document Categories** grid on the **General** workspace is used to manage the categories that can be used to organize documents. From this grid, users with the *Can Manage Documents* permission can view, create, modify and delete document categories.

Create Document Category



You can only create document categories at the All Building level.

1. In the navigation menu, select **Admin > Module Settings** and then click the **General** tab.
2. In the **Document Categories** grid, click **Add Category**.
3. Enter a **Name*** and **Description** (optional), and click **Save**.

Modify Document Category

In the **Document Categories** grid, click the icon in the **Details** to modify the information and then click **Save**.

You can also click the icon in the **Document Categories** grid to modify the name of the category, and then click to save it. Click to discard your changes.

Delete Document Category

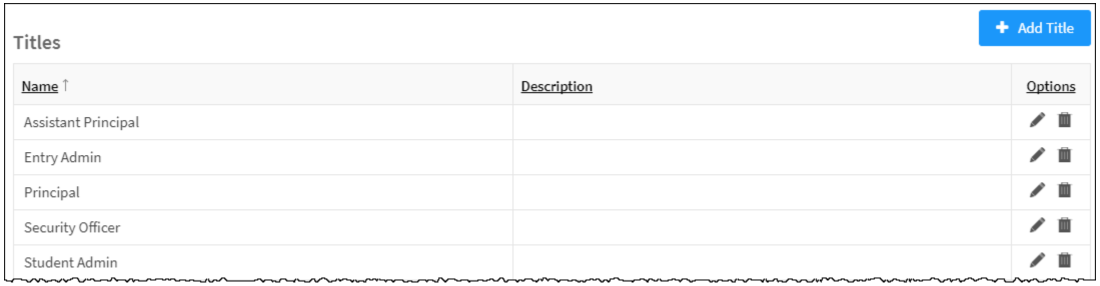
In the **Document Categories** grid, click the icon for the item to be removed and then click **OK** on the confirmation dialog to complete the process.

Manage Titles

Users with Administrative permissions can view, create, modify and delete Titles. These titles are used in the Users and Contacts features.

Note: Titles are available for use across all buildings, whether they are created at the building level or the client level.

1. In the navigation menu, select **Admin > Module Settings** and click the **General** tab.
2. In the **Titles** grid, click **Add Title** or click the icon to modify the existing title.



3. Enter the **Name** and **Description** and then click the icon to save the title.

Delete Title

Click the icon to delete a title, and then click **OK** on the confirmation dialog.

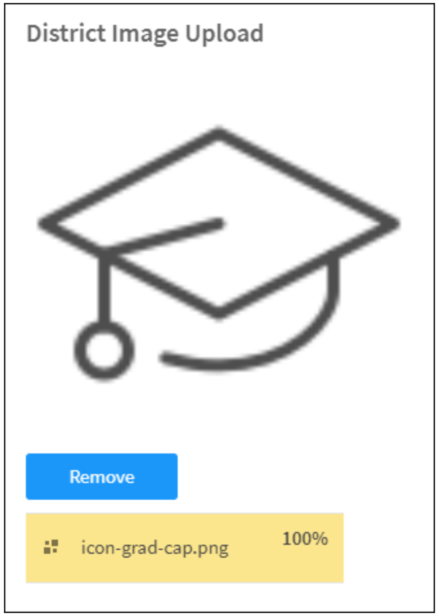
Upload District Image

Use this area on the **General Settings** workspace to upload your district's logo image to be displayed on the Volunteer Portal, Online Volunteer Application and Kiosk.

1. In the navigation menu, select **Admin > Module Settings**.
2. Click the **General** tab.
3. In the **District Image Upload** area, click **Select File**.
4. Navigate to the file on your computer, select it and click **Open**.

   The image is uploaded and displays in the area.

If you want to delete a district logo that has been uploaded, click **Remove**, and then click **Continue** on the confirmation dialog.



Manage Alert Settings

Alerts are used to flag specific individuals on your campus and to notify relevant response personnel. You use the **Alert Settings** workspace to manage alert notifications.

The following topics are covered in this section:

- About Alerts
- Alert Settings Workspace
- Sex Offender Alert Notifications
- Custom Alerts – Matching Criteria
- Add Custom Alert/Custom Alert Notifications
- Import Custom Alerts
- Enable/Disable Emergency Buttons
- Specify Emergency Alert Notification
- Message Tokens for Emergency Alerts
- View Instant Alerts
- Add Instant Alert/Modify Instant Alerts
- Incident Alerts
- Manage System Notifications

About Alerts

Alerts are used to flag specific individuals during the sign-in process or the student sign-out by guardian process, and to notify relevant response personnel. Use the **Alert Settings** workspace to manage alerts and notifications for the following types of alerts:

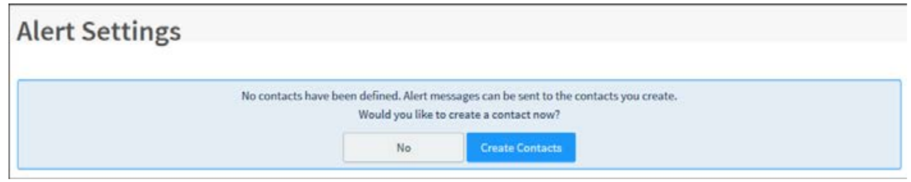
- **Sex Offender Alerts** – Each time a visitor, contractor, volunteer or guardian who is picking up a student signs into the Raptor system, their name and date of birth are compared against over 750,000 known sex offenders across all 50 states and several territories within the United States. Raptor takes the extra step of comparing all known alias names used by the sex offenders to the name of the person signing in, providing a thorough screening process.
- **Custom Alerts** – Previously known as private alerts, these alerts are customized to meet the specific needs of your school and/or district. Custom alerts are used to notify relevant personnel that a potentially unwanted person is signing in to a building. They are commonly used for custody issues, restraining orders or banned visitors.
- **Emergency Buttons** – The Emergency button displays in the upper right corner of the screen if Emergency Alerts are enabled for your school or for all schools in the district. In case of an emergency (for any reason), you can click the Emergency button to send a silent emergency message via email, text message, or voice message to a customized recipient list.
- **Instant Alerts** – Manage the instant alerts used to broadcast a message to all users that are logged into the Raptor System.
- **Incident Alerts** – Manage notifications that are used during the reunification process.

The **Alert Settings** feature allows you to configure alert notifications at the client level (All Buildings) and then modify or add items at the building level that are specific to each building. See Client Policy.

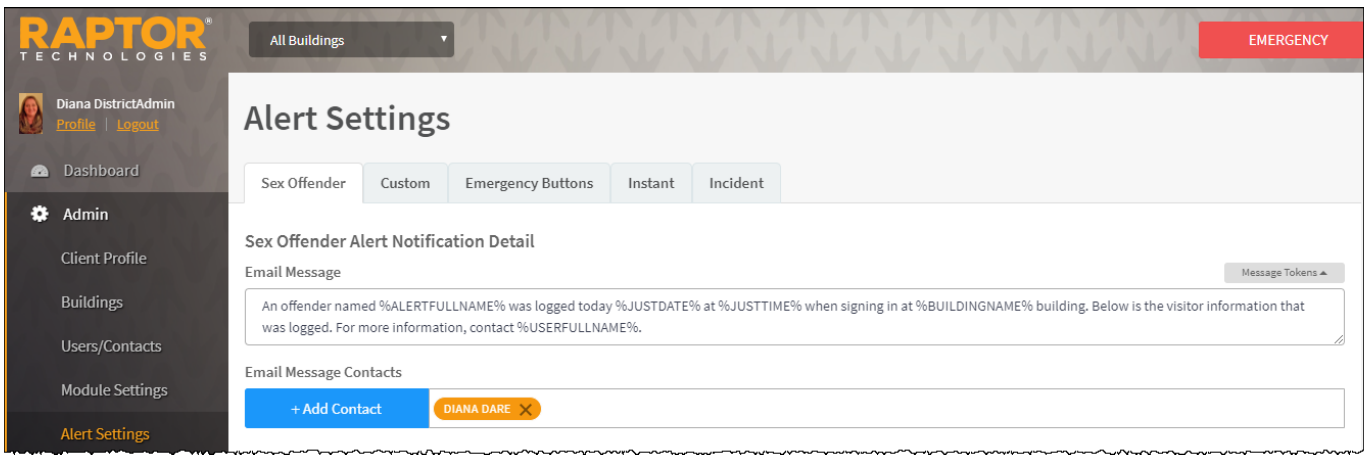
Alert Settings Workspace

You use the **Alert Settings** workspace (**Admin > Alert Settings**) to manage alert notifications. When you open the **Alert Settings** workspace, if there are no contacts defined, the following message displays.

Important: If contacts are not defined and associated to the alerts, then no one will be notified of the alert (other than the user signing in the person).



Click **Create Contacts** (see Add Contact) or click **No** to open the **Alert Settings** workspace.



Notifications can be created at the All Buildings level or for a specific building. If you define a notification message and contacts for any of the alert types at the All Buildings level, these contacts will receive the notification message when the alert is triggered in any building.

At the specific building level, the notification created at the All Buildings level can be used or a different notification message can be entered and contacts specific to the building can be entered. Notifications created at the building level do not affect the content or recipients of the notification at the All Buildings level.

Sex Offender Alert Notifications

During the sign in process, if a Possible Offender Alert displays and the match is confirmed, a silent alert is immediately sent via email and/or text message to a customized recipient list set up in the **Sex Offender Alert Notifications Detail**.

Note: Contacts must be defined prior to setting up notifications. See Manage Contacts.

1. In the navigation pane, select **Admin > Alert Settings**.
2. On the **Sex Offender** tab, specify the following information and then click **Save**.

Email Notifications

- **Email Text** – The email message is pre-populated with a default message using message tokens but you can change this message if desired. This message that is sent via email in addition to the Visitor/Offender information. You can also use Message Tokens.
- **Email Contacts** – Click **Add Contact** and select the contact name from the drop-down list. The contact information must be added in Contacts prior to creating the email notification.

  Note: In the **Add Contact** drop-down list, the icons that display represent the contact's preferred method of notification. This applies to all notifications.

  To remove an email contact, click the **X** in the contact label.

  Note: If the contact name is gray, it was defined at the district level and cannot be removed at the building level. This applies to all notifications.

Sex Offender Alert Notifications, cont.

Text Message Notifications

- **Text Message** – The optional text message is pre-populated with a default message using message tokens but you can change this message if desired. If this field is left blank, no text message is sent. You can also use Message Tokens.
- **Text Message Contacts** – For those who want to be notified via a text message, click **Add Contact** and select the contact name from the drop-down list. The contact information must be added in Contacts prior to creating the text message notification.

  To remove a text contact, click the **X** in the contact label.

District Policy Message

Users with the Can Manage Alerts permission can specify the district policy and procedures to be followed when a visitor, contractor, guardian or volunteer matches a sex offender during sign in. This message can be accessed on the Match Confirmation alert notification.

1. In the **District Policy Message** area on the **Sex Offender Alert Notification Detail** workspace, enter the message that you want displayed when **Match** is selected on the Possible Sex Offender dialog.
2. Click **Save**.

Sex Offender Alert Notifications, cont.

Message Tokens for Sex Offender Alert Notifications

You can also use Message Tokens, which are variables, in the notification message so that when the message is sent, the tokens will be replaced by their associated value. Click **Message Tokens** to view the variables that can be entered in the message.

%CLIENTNAME% - District Name
%BUILDINGNAME% - Building Name
%USERFULLNAME% - User's First and Last Name
%ALERTFULLNAME% - Visitor's First and Last Name
%JUSTTIME% - Time Logged - hh:mm: tt
%JUSTDATE% - Date Logged - MM/DD/YYYY

Example:

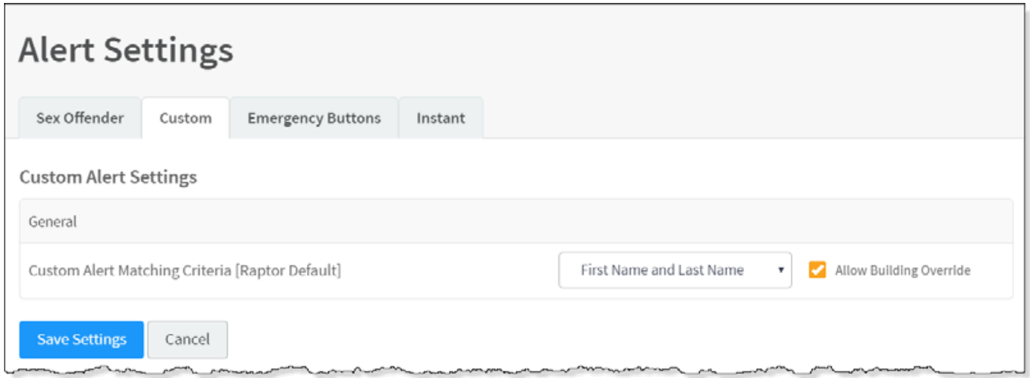
An alert has been issued by %USERFULLNAME% at %CLIENTNAME% %BUILDINGNAME% on %JUSTDATE% at %JUSTTIME%.

Custom Alerts – Matching Criteria

Custom alerts are similar to offender alerts except that the matching criteria is defined by your school and/or district. When a visitor or contractor is signed in, Raptor compares that person's first name and last name (depending on the selected matching criteria) to each of the custom alerts.

When creating custom alerts, District Admins can set the matching criteria for the possible offender alert. The more matching criteria that is required reduces the number of false positive matches.

1. In the navigation menu, select **Admin > Alert Settings** and then click the **Custom** tab.
2. From the **Custom Alert Matching Criteria** drop-down list, select the criteria that must be matched:
   - Last Name
   - First Name and Last Name
   - First Name, Last Name, and Date of Birth (best option for reducing number of false positive matches)



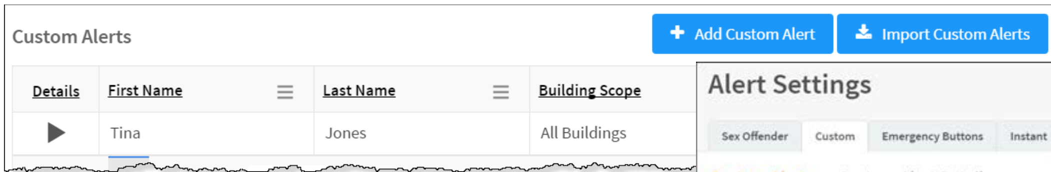
3. If you are at the client level (All Buildings), the **Allow Building Override** check box is visible. If you want to allow buildings the ability to override the Custom Alert Matching Criteria, select the check box.
4. Click **Save Settings**.

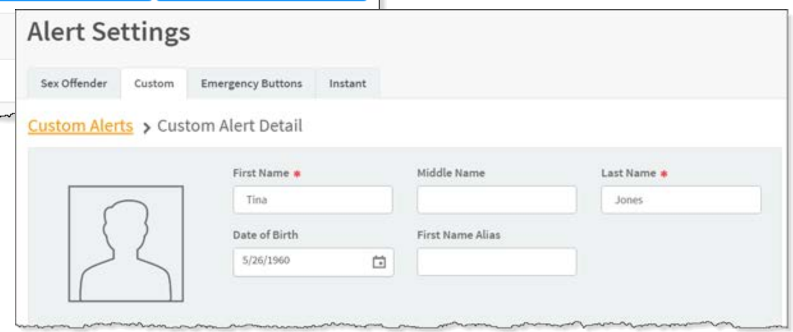
RAPTOR TECHNOLOGIES

Add Custom Alert

Note: Contacts must be defined prior to setting up notifications. See Manage Contacts.

1. In the navigation pane, select **Admin > Alert Settings** and then click the **Custom** tab.
2. In the **Custom Alerts** grid, click **Add Custom Alert**.





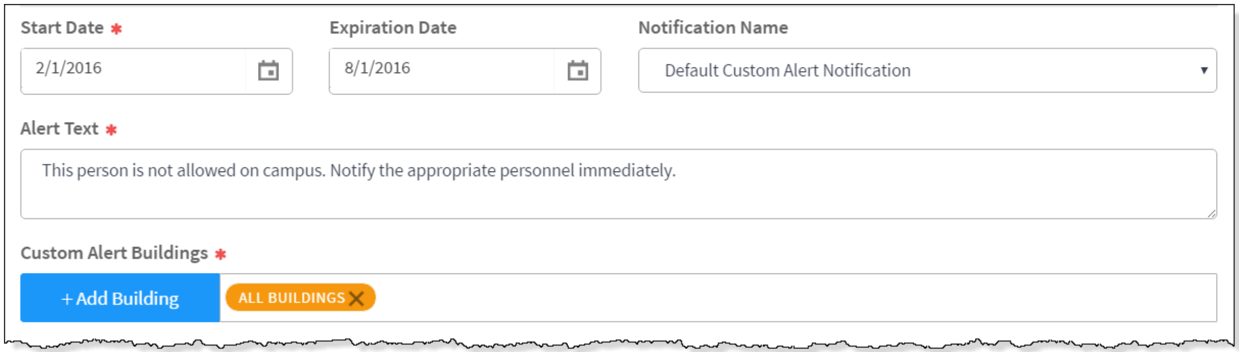
3. Use one of the following methods to specify the person in the alert:
   - **Find** – If the person has previously signed in to the building, enter their name (or a portion of their name) in the text box and click **Find**.
     If more than one record is returned, click the Select icon to display their information in a Detail view.
   - **Manual Entry** – If the person has not previously signed in to the building, manually enter the person's information in fields.

Notes:

- Required fields are determined by the Custom Alert Matching Criteria setting in Custom Alert Settings and indicated with an asterisk *.
- If the person uses a nickname instead of their first name, enter it in the First Name Alias text field.

Add Custom Alert, cont.

4. Enter the following alert information:



- **Start Date*** – Select the date from the calendar to indicate the date the alert should become active.
- **Expiration Date** – Select the date from the calendar to indicate the date the alert should become inactive. If left blank, the alert will not be expired until you enter an expiration date or delete the alert.
- **Notification Name** – Select the notification that contains the default notification message and who to notify.

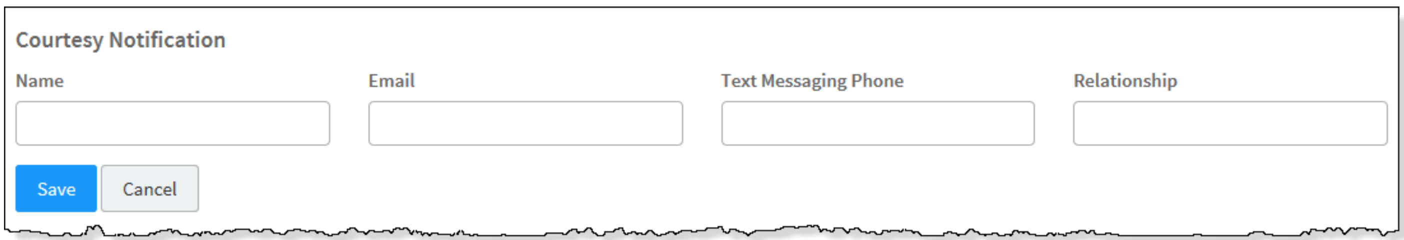
  Note: If you want notifications to be sent when the alert is issued, you must complete the information in the Custom Alert Notification prior to adding the custom alert.
- **Alert Text*** – Enter the information that displays in the **Notes** field on the Possible Custom Alert. This is the information that is visible to the Entry Admin when signing in the person.
- **Custom Alert Buildings*** – Click **Add Building** and select the buildings where the alert is active.

Add Custom Alert, cont.

5. If you want to upload and associate a document with the custom alert so that document is available to the Front Desk operator when there is a positive match, click **Select File**, navigate to the PDF document, and click **Open**. The file is uploaded and the document name displays in the **Document File Name** field.

   If the document is no longer relevant and you want to remove it, click **Delete File**.

6. In the **Courtesy Notification** area, enter the following information for external notification when the alert is triggered:

   - **Name** – First and last name of the person to be notified.
   - **Email** – If preferred method of contact is email, enter their email address.
   - **Text Messaging Phone** – If preferred method of contact is text message, enter their mobile phone number.
   - **Relationship** – Enter their relationship.

7. Click **Save**.

   A confirmation message displays in the lower right corner of the screen indicating the alert was successfully added.

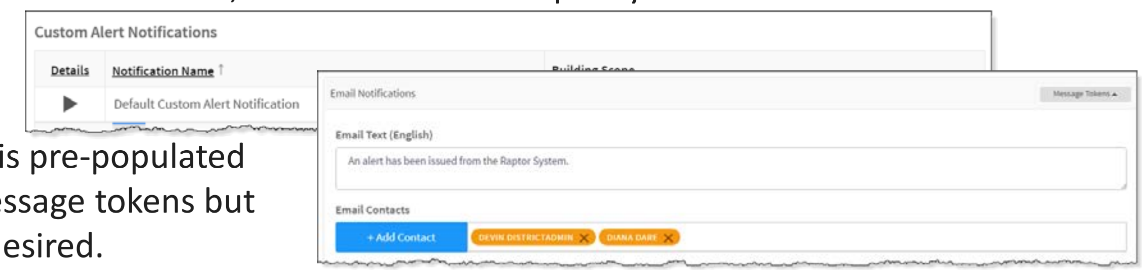
RAPTOR TECHNOLOGIES

Custom Alert Notifications

You can specify recipients of a custom alert notification and the message that is sent in the notification. This information can then be referenced in the alert detail so that the notification is sent when the custom alert is issue.

Note: Contacts must be defined prior to setting up notifications.

1. In the navigation menu, select **Admin > Alert Settings** and then click the **Custom** tab.
2. Navigate to the **Custom Alert Notification** area, click the ▶ icon to specify the information in the notification and then click **Save**.



Email Notifications

- **Email Text** – The email message is pre-populated with a default message using message tokens but you can change this message if desired.
- **Email Contacts** – Click **Add Contact** and select the contact name from the drop-down list. The contact information must be added prior to creating the email notification.

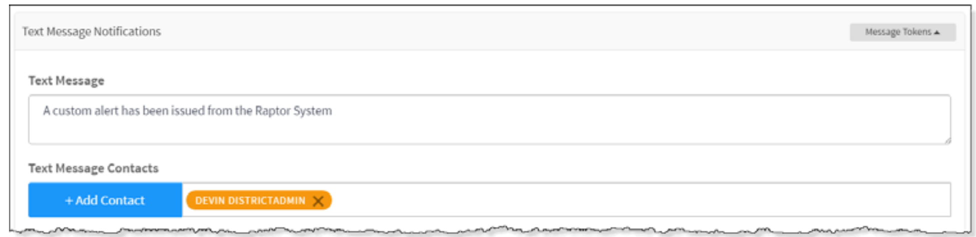
  Note: In the **Add Contact** drop-down list, the icons that display represent the contact's preferred method of notification.

  To remove an email contact, click the **X** in the contact label.

  Note: If the contact name is gray, it was defined at the district level and cannot be removed at the building level. This applies to all notifications.

Custom Alert Notifications, cont.

Text Message Notifications



- **Text Message** – The text message is pre-populated with a default message using message tokens but you can change this message if desired.
- **Text Message Contacts** – For those who want to be notified via a text message, click **Add Contact** and select the contact name from the drop-down list. The contact information must be added prior to creating the text message notification.

  To remove a text contact, click the **X** in the contact label.

  Note: If the contact has selected both **Text** and **Email** as their preferred notification method, when one method is populated with the contact name, the other method will be automatically populated.

Message Tokens

You can use Message Tokens, which are variables, in the notification message so that when the message is sent, the tokens will be replaced by their associated value.

%CLIENTNAME% - District Name
%BUILDINGNAME% - Building Name
%USERFULLNAME% - User's First and Last Name
%CUSTOMALERTTEXT% - First 90 characters of the Custom Alert text
%ALERTFULLNAME% - Visitor's First and Last Name
%JUSTTIME% - Time Logged - hh:mm: tt
%JUSTDATE% - Date Logged - MM/DD/YYYY

Click **Message Tokens** to view the variables that can be entered in the message.

Example:

An alert has been issued by %USERFULLNAME% at %CLIENTNAME% %BUILDINGNAME% on %JUSTDATE% at %JUSTTIME%.

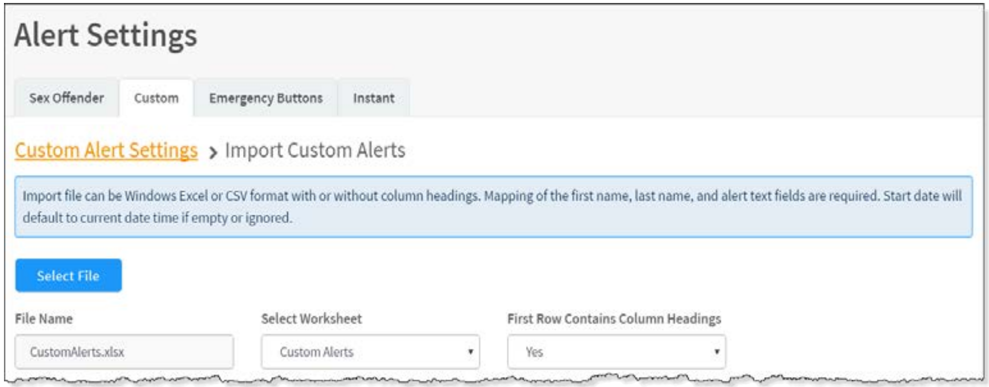
RAPTOR TECHNOLOGIES

Import Custom Alerts

Administrators with the *Can Manage Alerts* permission can also import custom alerts, which provides the flexibility to configure multiple custom alerts in one process. The import utility also includes the ability for unattended import of custom alerts by creating a manifest file that includes information about the field mapping and file to be imported.

1. In the navigation menu, select **Admin > Alert Settings**.
2. Click the **Custom** tab and then click **Import Custom Alerts**.

3. On the **Import Custom Alerts** workspace, click **Select File** and navigate to the location where the file is saved on your computer. Select the **Excel** or **CSV** file and click **Open**.



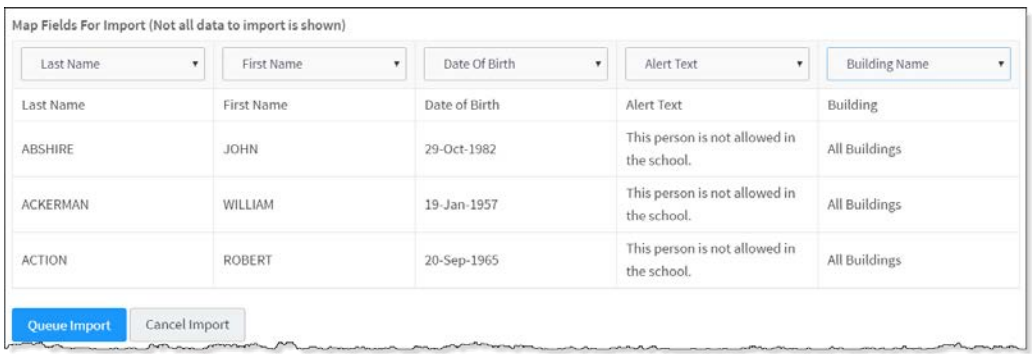
Note: You must first create an Excel spreadsheet or comma delimited file that contains the required information (*). The following can be imported:

- First Name*
- Middle Name
- Last Name*
- Date of Birth
- First Name Alias
- Start Date
- Expiration Date
- Alert Text*
- Building Name (If you are importing at the All Buildings level.)
- Courtesy Notification – Name
- Courtesy Notification – Email
- Courtesy Notification – Text Messaging Phone
- Courtesy Notification – Relationship

Import Custom Alerts, cont.

4. If you used Excel and the file contains multiple worksheets, select the worksheet that contains the custom alert information from the **Select Worksheet** drop-down list.
5. If the first row of the worksheet contains column headings, select **Yes** from the **First Row Contains Column Headings** drop-down list. Otherwise, select **No**.
6. Map each of the columns to be imported by selecting the appropriate fields in the drop-down menu above each column that displays.

   Note: First Name, Last Name, and Alert Text are required columns. The columns with **Ignore** selected with not be imported.



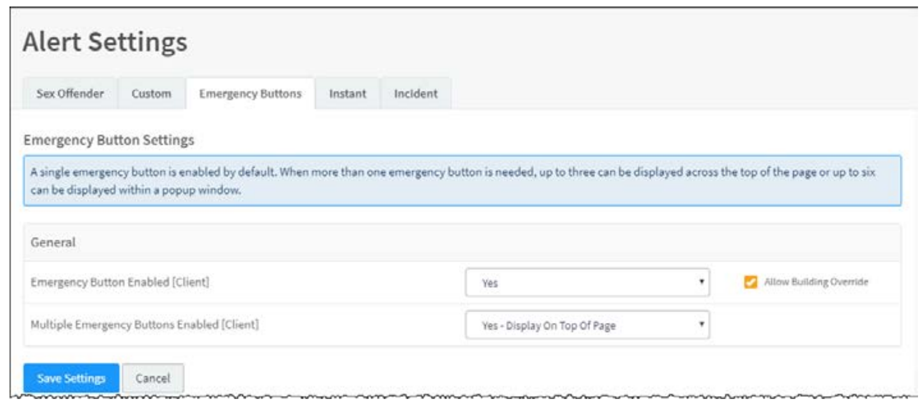
7. If you want to create a manifest file to schedule automatic imports, click **Save Manifest** and save the file. You can then schedule the imports using a scheduling utility. See the User Guide for details.
8. Click **Queue Import**. A message displays in the lower right corner of the screen stating that the import job was successfully added to the import queue for processing.

   When the import has completed processing, an email will be sent to the email address of the user indicating the number of records successfully imported and any error that may have occurred.

Enable/Disable Emergency Buttons

When enabled, the **Emergency** button is always displayed on the screen. In an emergency at your campus, clicking this button will dispatch a silent emergency message via email, text message, or voice message to a customized recipient list.

You can also enable multiple emergency buttons to quickly notify the appropriate contacts about specific emergencies. When enabled, up to three buttons can be displayed across the top of the page, or up to six buttons can be displayed within a popup window.



1. In the navigation pane, select **Admin > Alert Settings** and then click the **Emergency Buttons** tab.
2. In the **General** settings, specify the following information:
   - **Emergency Button Enabled** – Select **Yes** (to enable) or **No** (to disable).
   - **Multiple Emergency Buttons Enabled** – Select **Yes – Display On Top of Page** or **Yes – Display In Popup Window** (to enable), or **No** (to disable).
   - Select or clear the **Allow Building Override** check box. If selected, this setting can be overridden at the building level.
3. Click **Save Settings**.

Specify Emergency Button Details

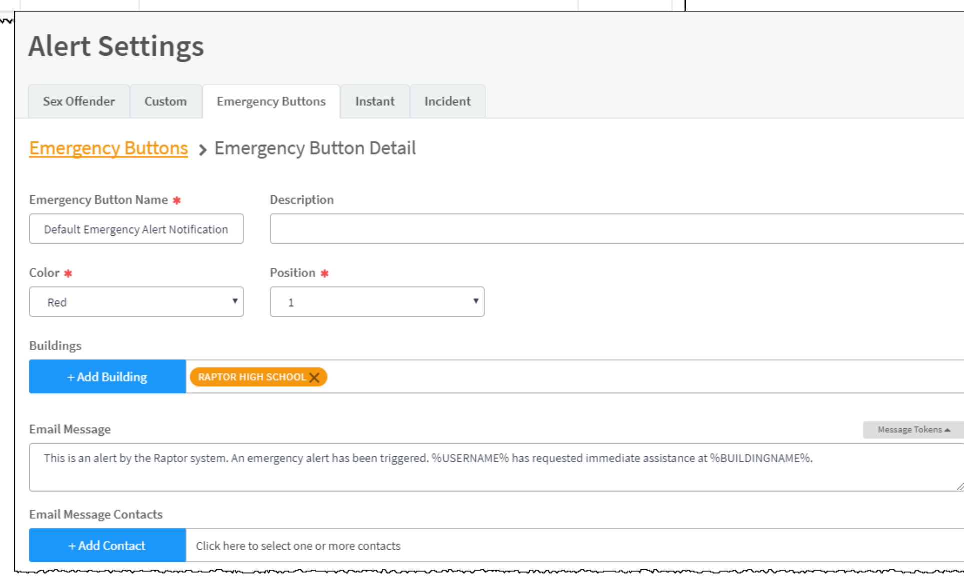
You can specify the emergency button name, message and the contacts who will receive a notification using the Emergency Button Detail workspace. The contacts specified in the notification will be notified whenever an emergency alert is issued.

Note: Contacts must be defined prior to setting up notifications.

1. In the navigation menu, select **Admin > Alert Settings**.
2. Click the **Emergency Buttons** tab and navigate to the **Emergency Buttons** grid.

3. If you want to modify the **Default Emergency Alert Notification**, click the ▶ icon to expand the **Emergency Button Detail**.

   If you want to create a new emergency button, click **Add Emergency Button**.



Specify Emergency Button Details, cont.

4. Specify the following information:
    - **Emergency Button Name*** – This name displays on the button at the top of the page or in a popup window. The name is limited to 18 characters.
    - **Description** – Optionally, enter a description for the button.
    - **Color** – Select the background color for the button.
    - **Position** – Select the position (order) of where the button displays in relevance to other buttons.
    - **Buildings** – Click **Add Building** and select the building where the emergency button will be implemented. When **All Buildings** is selected, the notification is enabled for all schools in the district. The All Buildings option is only available at the district level.

      Note: If All Buildings is selected, and a user views this field for a specific school, only the school's name appears in the Buildings field.
    - **Email Message/Email Message Contacts** – Accept the default message or enter a custom message and select the contacts who should receive the message. Click the **X** to remove a contact.
    - **Text Message/Text Message Contacts** – Accept the default message or enter a custom message and select the contacts who should receive the message. Click the **X** to remove a contact.
    - **Voice Message/Voice Message Contacts** – Accept the default message or enter a custom message and select the contacts who should receive the message. Click the **X** to remove a contact.
5. Click **Save**.

Notes:

- In the **Add Contact** drop-down list, the icons that display represent the contact's preferred method of notification.
- If the contact has selected both Text and Email as their preferred notification method, when one method is populated with the contact name, the other method will be automatically populated.
- If the contact name is gray, it was defined at the district level and cannot be removed at the building level.

Message Tokens for Emergency Alerts

You can also use Message Tokens, which are variables, in the notification message so that when the message is sent, the tokens will be replaced by their associated value.

Click **Message Tokens** to view the variables that can be entered in the message.

%CLIENTNAME% - District Name
%BUILDINGNAME% - Building Name
%USERFULLNAME% - User's First and Last Name
%EMERGENCYBUTTONNAME% - Emergency Button Name
%JUSTTIME% - Time Logged - hh:mm: tt
%JUSTDATE% - Date Logged - MM/DD/YYYY

Example:

This is an alert by the Raptor system. An emergency alert has been triggered. %USERNAME% has requested immediate assistance at %BUILDINGNAME%.

View Instant Alerts

Instant alerts provide the ability for an administrator with the *Can Manage Alerts* permission to broadcast a message to all users that are until the expiration date and time have elapsed, or the administrator disables the alert.

Typically, instant alerts are used to notify users of an early dismissal of students (for example, due to weather) or to immediately inform front desk employees of a special situation.

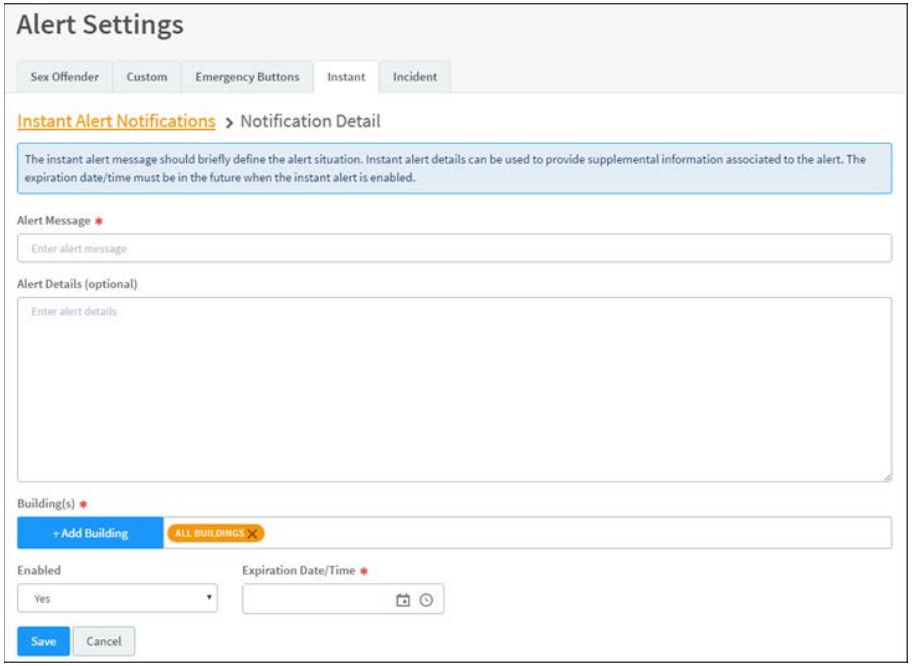
1. In the navigation menu, select **Admin > Alert Settings** and click the **Instant** tab.
2. In the **Instant Alert Notifications** grid, view the **Instant Alerts**.

   The alert message, the buildings where it is applicable, the expiration date and time, and whether the alert is enabled display in the data grid.

Add Instant Alert

1. In the navigation menu, select **Admin > Alert Settings** and then click the **Instant** tab.
2. In the **Instant Alert Notifications** grid, click **Add Instant Alert**.
3. On the **Notification Detail** workspace, enter the **Alert Message** and optional **Alert Details**.

   Note: The Alert Message field should contain a short message that displays in the instant alert at the bottom of the screen. More details and supporting information can be entered in the Alert Details field.



4. In the **Buildings** field, click **Add Building** and select the buildings where the alert is active.
5. In the **Enabled** field, select **Yes** or **No** to indicate whether the alert is enabled immediately after saving it.
6. In the **Expiration Date/Time** field, select the date and time when the instant alert will expire. If you leave this field blank, the alert never expires.
7. Click **Save**. A confirmation message displays in the lower right corner of the screen indicating the alert was successfully added.

Modify Instant Alerts

You can modify the instant alert details:

1. In the **Instant Alert Notifications** grid, click ▶ icon for the alert to be modified.
2. On the **Notification Detail** workspace, modify the alert details and click **Save**.

You can also modify the Expiration Date/Time or Enable/Disable an instant alert from the **Instant Alert Notifications** data grid.

1. In the **Instant Alert Notifications** grid, click ✎ icon for the alert to be modified.
2. Modify the date and time in the **Expires** column, or select or clear the **Enabled** check box.
3. Click the ✔ icon to save your changes.

Delete Instant Alert

In the **Instant Alert Notifications** grid, click 🗑 icon for the alert to be deleted, and click **OK** on the confirmation dialog.

Incident Alerts REU

The **System Notifications** workspace is used manage predefined system notifications that ship with the Raptor Reunification system. These notifications are used when incidents are initiated and closed, and when students have been released or reunified with an approved guardian.

Users with the *Can Manage Alerts* permission can manage these notifications from the **Incident** tab on the **Alert Settings** workspace.

The following notifications are available for All Buildings:

- **Incident Initiation** – This notification is sent when a drill or live emergency from the Reunification mobile app is triggered. It is sent to all users tied to the building where the incident has occurred.
- **Incident Closure** – This notification is sent when a drill or incident is completed and has been closed. It is sent to all users tied to the building where the incident has occurred.
- **Released Student** – This notification is sent when a student has been released during a drill or live emergency. The notification is sent to all configured guardians for the student.
- **Reunified Student** – This notification is sent when a student has been reunified with an approved guardian.

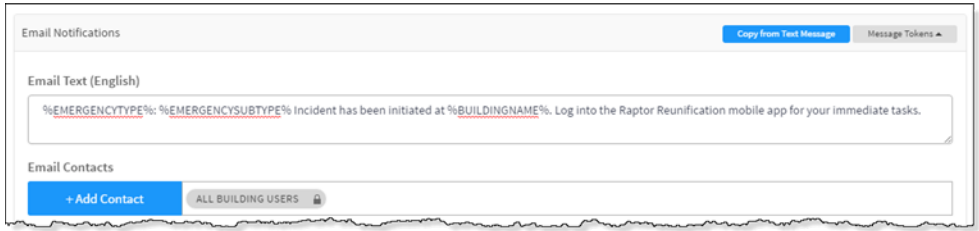
Note: Contacts must be defined prior to setting up notifications.

Manage System Notifications REU

You can specify the notification message and recipients for each of the system notifications.

Note: Contacts must be defined prior to setting up notifications.

1. In the navigation menu, select **Admin > Alert Settings**, and then click the **Incident** tab.
2. Click the ▶ icon to specify the following information and then click **Save**.



Email Notifications

- **Email Text** – The email message is pre-populated with a default message using message tokens but you can change this message if desired.

  If you want to use the same message as that used in the Text Message notification, click **Copy from Text Message**.

  To use message tokens to compile the message, see Message Tokens for Incident Notifications.

- **Email Contacts** – Click **Add Contact** and select the contact name from the drop-down list. The contact information must be added prior to creating the email notification.

  Note:

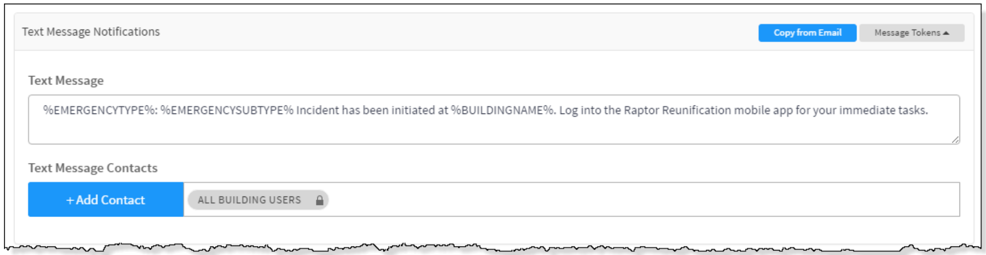
  - In the **Add Contact** drop-down list, one or more icons display next to the contact's name that represent their preferred method of notification. This applies to all notifications.
  - If the contact has selected both Text and Email as their preferred notification method, when one method is populated with the contact name, the other method will be automatically populated.

  To remove an email contact, click the **X** in the contact label.

  Note: If the contact name is gray, it was defined at the district level and cannot be removed at the building level. This applies to all notifications.

Manage System Notifications, cont.

Text Notifications



- **Text Message** – The text message is pre-populated with a default message using message tokens but you can change this message if desired.

  If you want to use the same message as that used in the Email notification, click **Copy from Email**.

  To use message tokens to compile the message, see Message Tokens for Incident Notifications.

- **Text Message Contacts** – For those who want to be notified via a text message, click **Add Contact** and select the contact name from the drop-down list. The contact information must be added prior to creating the text message notification. Only those contacts that provided a text message phone can be selected from the list.

  Note:

  - In the **Add Contact** drop-down list, one or more icons display next to the contact's name that represent their preferred method of notification. This applies to all notifications.
  - If the contact has selected both Text and Email as their preferred notification method, when one method is populated with the contact name, the other method will be automatically populated.

  To remove a text contact, click the **X** in the contact label.

  Note: If the contact name is gray, it was defined at the district level and cannot be removed at the building level.

Message Tokens for Incident Notifications

REU

You can also use Message Tokens, which are variables, in the notification message so that when the message is sent, the tokens will be replaced by their associated value.

Click **Message Tokens** to view the variables that can be entered in the message.

%CLIENTNAME% - District Name
%BUILDINGNAME% - Building Name
%INCIDENTCATEGORY% - Identifies if the incident is a drill or an emergency
%USERFULLNAME% - User's First and Last Name who initiated the incident
%EMERGENCYTYPE% - Emergency type tied to the incident initiated for the school
%EMERGENCYSUBTYPE% - Emergency sub-type tied to the incident initiated for the school

Example:

[%INCIDENTCATEGORY%] %EMERGENCYTYPE% - %EMERGENCYSUBTYPE% has been initiated at %BUILDINGNAME%. Log into the Raptor Reunification mobile app now for your immediate tasks.

Manage Kiosk Settings

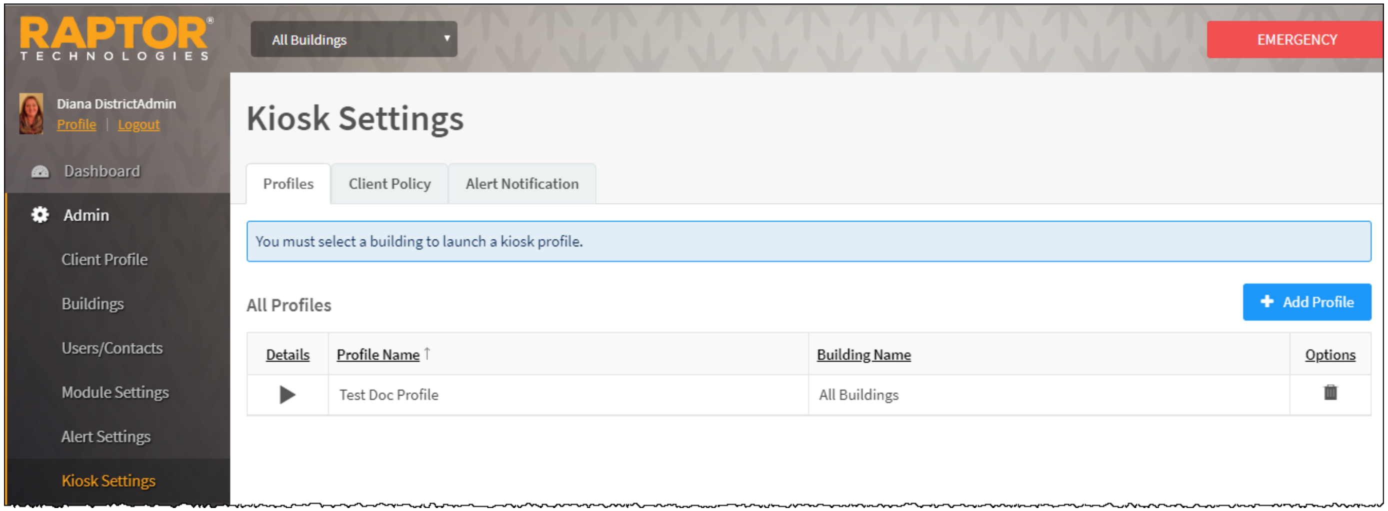
The **Kiosk Settings** workspace is used to add profiles that determine what displays on the Kiosk, manage client policy for kiosks, and launch a Kiosk. The following topics are covered in this section:

- Kiosk Settings Workspace
- Add Kiosk Profile
- Kiosk Sign In/Sign Out Custom Message
- Launch Kiosk
- Manage Client Policy
- Manage Kiosk Alert Notifications
- Message Tokens for Kiosk Notifications

Kiosk Settings Workspace

Users with the *Can Manage Kiosks* permissions can manage what displays in the Kiosks at the building level or for all buildings (client level). You access this workspace by selecting **Admin > Kiosk Settings** in the navigation menu.

From this workspace, you can add profiles that determine what displays on the Kiosk, manage client policy for kiosks, and launch the Kiosk.



Add Kiosk Profile

The **Profiles** tab is used to add a profile and launch the Kiosk. A specific building must be selected to be able to launch a Kiosk.

1. In the navigation menu, select **Kiosk Settings**.
2. On the **Profiles** tab, click **Add Profile** and enter a name in the **Profile Name** text box.

   The name assigned to the kiosk profile often describes where it is located and the available capabilities to simplify for the user; for example Students Only – South Entrance.

Notes:

- For students/staff to use the barcode reader, the Student ID/Staff ID field must be completed in their record (Student Detail/Staff Detail) and the ID number must be encoded in the 1D barcode.
- For visitors/contractors/volunteers to use the barcode reader, the Assigned ID field must contain the 1D barcode value. The 1D barcodes must be a minimum of 4 characters.

3. In the **All Modules** list, specify the following:
   - **Enable 1D and 2D Barcode Support** – Select or clear the check box to enable or disable the use of 1D and 1D/2D barcode scanners in the kiosk. Currently, Raptor supports the CipherLab 1D Barcode Reader, Motorola 2D Barcode Reader and Symbol Technologies 1D/2D Barcode Reader. This feature must be enabled to activate secure kiosk.
   - **Activate Secure Kiosk (Disables Keyboard Input Option for Visitors, Contractors, and Volunteers)** – Select or clear the check box to enable or disable the secure kiosk, which automatically requires visitors, contractors and volunteers to use either the 1D or 2D barcode scanner when signing in or signing out of a building using the kiosk. This setting disables type-in.

Add Kiosk Profile, cont.

4. For the **Visitors** module, select the check boxes for the options you want enabled. Clear the check boxes for options you do not want enabled in the Kiosk.
   - **Visitor Sign In** – Select or clear the check box to enable or disable visitor sign-in capabilities.
   - **Visitor Sign Out** – Select or clear the check box to enable or disable visitor sign-out capabilities.
   - **Enable Visitor Sign In Printing** – Select or clear the check box to enable or disable printing a badge during sign in.
5. For the **Contractors** module, select the check boxes for the options you want enabled. Clear the check boxes for options you do not want enabled in the Kiosk.
   - **Contractor Sign In** – Select or clear the check box to enable or disable contractor sign-in capabilities.
   - **Contractor Sign Out** – Select or clear the check box to enable or disable contractor sign-out capabilities.
   - **Enable Contractor Sign In Printing** – Select or clear the check box to enable or disable printing a badge during sign in.

Add Kiosk Profile, cont.

7. For the **Students** module, select the check boxes for the options you want enabled. Clear the check boxes for options you do not want enabled in the Kiosk.

    - **Student Sign In** – Select or clear the check box to enable or disable student sign-in capabilities.
    - **Student Sign Out By Parent** – Select or clear the check box to enable or disable the ability for parents to sign out student.
    - **Student Self-Sign Out** – Select or clear the check box to enable or disable the ability for students to sign themselves out.
    - **Enable Student Sign In Printing** – Select or clear the check box to enable or disable printing a tardy pass during sign in.
    - **Enable Student Sign Out Printing** – Select or clear the check box to enable or disable printing an early dismissal pass during sign out.
    - **Mask Student ID Number** – Select or clear the check box to enable or disable hiding the student ID number on the screen.
    - **Enable Student Sign In and Sign Out By Full Name** – Select or clear the check box to enable or disable allowing a student to sign in or sign out of the Kiosk for entering their first and last name.

Add Kiosk Profile, cont.

8. For the **Staff** module, select the check boxes for the options you want enabled. Clear the check boxes for options you do not want enabled in the Kiosk.
   - **Staff Sign In** – Select or clear the check box to enable or disable staff sign-in capabilities.
   - **Staff Sign Out** – Select or clear the check box to enable or disable staff sign-out capabilities.
   - **Enable Staff Sign In Printing** – Select or clear the check box to enable or disable printing a badge during sign in.
   - **Mask Staff ID Number** – Select or clear the check box to enable or disable hiding the staff ID number on the screen.
   - **Confirm Staff Member Identity** – Select or clear the check box to enable or disable displaying the Confirmation dialog during staff sign in and sign out using the 1D barcode reader.
     - When selected (enabled), the confirmation dialog displays the staff members name and they continue the sign-in process.

       If signing in using the 1D barcode from the Welcome page, and the staff member has additional personas (for example, visitor and volunteer) a confirmation dialog is displayed, and the user must select the persona.
     - When cleared (disabled), the confirmation dialog will not display and one of the following occurs:
       - If the staff member is located, the sign-in or sign-out successful message displays.
       - If no staff member is returned as a match, a warning message is displayed.

Add Kiosk Profile, cont.

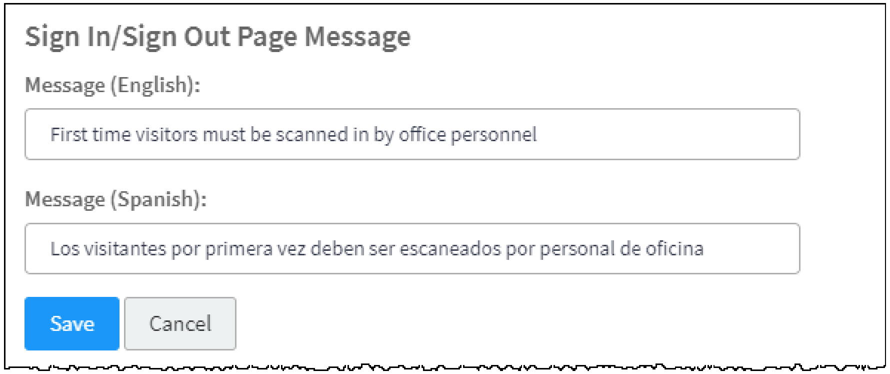
9. For the **Volunteer** module, select the check boxes for the options you want enabled. Clear the check boxes for options you do not want enabled in the Kiosk.
   - **Volunteer Sign In** – Select or clear the check box to enable or disable volunteer sign-in capabilities.
   - **Volunteer Sign Out** – Select or clear the check box to enable or disable volunteer sign-out capabilities.
   - **Enable Volunteer Sign In Printing** – Select or clear the check box to enable or disable printing a badge during sign in.
   - **Mask Volunteer ID Number** – Select or clear the check box to enable or disable hiding the volunteer ID number on the screen.
10. Click **Save**.

    A message displays in the lower right corner indicating the Profile was successfully saved.

Kiosk Sign In/Sign Out Custom Message

Users with the *Can Manage Kiosks* permission can specify a custom message to be displayed on the Kiosk Sign In/Sign Out page. You must be at the All Buildings level to specify the Sign In/Sign Out Page Message.

1. In the navigation menu, select **Kiosk Settings**.
2. On the **Profiles** tab, click the ▶ icon to expand the **Profile Detail** workspace.

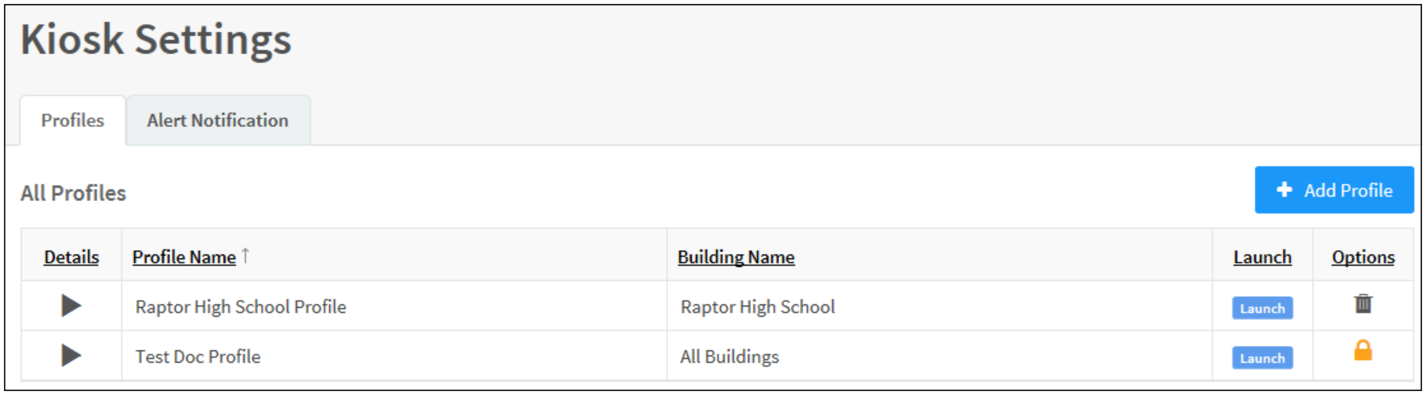


3. In the **Sign In/Sign Out Page Message** area, enter the message you want to be displayed on the Kiosk Sign In/Sign Out page. You can specify the text in English and/or Spanish.
4. Click **Save**.

Launch Kiosk

Users with the *Can Manage Kiosks* permission can use the **Profiles** tab on the **Kiosk Settings** workspace to launch a Kiosk.

Note: You must have a specific building selected in the Building Selector to be able to launch the Kiosk.



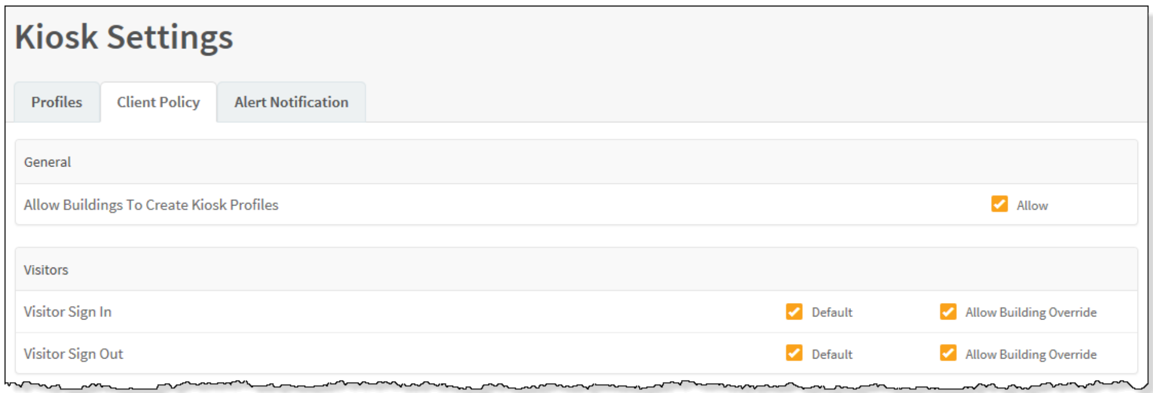
1. In the navigation menu, select **Admin > Kiosk Settings**.
2. In the **All Profiles** grid on the **Profiles** tab, click the **Launch** icon to open the Kiosk.

   A confirmation dialog displays asking you to confirm that you want to launch the Kiosk. The Kiosk will open in a new browser window tab and it is recommended that you close the Raptor Console browser window tab after the Kiosk launches.
3. Click **Continue** to launch the Kiosk.

Note: Users with the *Can Launch Kiosks* permission can also select **Kiosk** in the navigation menu to launch a Kiosk.

Manage Client Policy

The **Client Policy** tab displays on the **Kiosk Settings** workspace if **All Buildings** is selected. District Admins can use this workspace to control various settings such as whether Kiosk Profiles can be created at the building level and if the kiosk capabilities can be set for individual buildings.



The **Default** check box indicates whether an option is going to be selected by default when a new profile is created. If the **Default** check box is selected and the **Allow Override** check box is not selected, every kiosk profile created at the client or building level will inherit this setting and it cannot be turned off.

Example:

If Building Admins are allowed to create Kiosk Profiles, the district may have a policy that only Staff and Volunteers can sign-in using the kiosk.

In this scenario, the District Admin would use the **Client Policy** tab to set this policy for Students and Visitors by clearing the **Default** check boxes and **Allow Override** check boxes in the Student settings area and the Visitor settings area.

Manage Client Policy, cont.

Specify the following settings and then click **Save**.

General Settings

- **Allow Building to Create Kiosk Profiles** – Select or clear the **Allow** check box to indicate whether Building Admins are allowed to create Kiosk Profiles at the building level

Module Settings

Select or clear the **Default** check box to indicate if the option will or will not be automatically included in every kiosk profile created. Select the **Allow Building Override** check box to indicate if the setting can be overridden at the building level.

- Visitor Sign In/Visitor Sign Out
- Contractor Sign In/Contractor Sign Out
- Student Sign In/Student Sign Out/Student Sign Out by Parent
- Staff Sign In/Staff Sign Out
- Volunteer Sign In/Volunteer Sign Out/Volunteer Application

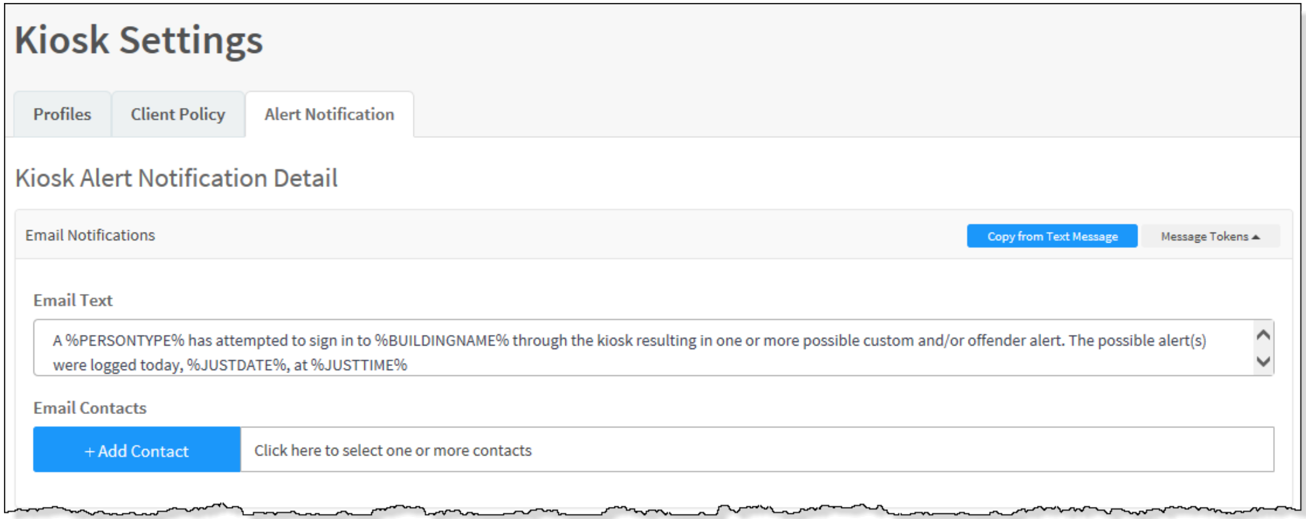
Note: Volunteer Application (the ability to apply to become a volunteer) is currently not supported through the kiosk.

Manage Kiosk Alert Notifications

The **Alert Notification** tab is used to manage the alert notifications that are sent when someone signing into the kiosk generates a possible offender or custom alert. Use the **Kiosk Alert Notification Detail** workspace to specify the message that is sent and the contacts who should receive the notification.

Note: Contacts must be defined prior to setting up notifications.

1. In the navigation menu, select **Admin > Kiosk Settings**.
2. Click the **Alert Notification** tab.
3. Specify the information and then click **Save**.



Kiosk Alert Notifications, cont.

Email Notifications

- **Email Text** – The email message is pre-populated with a default message using message tokens but you can change this message if desired. This text is sent in addition to the Visitor/Offender or Visitor/Custom Alert information so if this email message field is left blank, the Visitor/Offender or Visitor/Custom Alert information is still sent.

  If you want the same text as that specified in the Text Message Notification, click **Copy from Text Message**.

  To use message tokens to compile the message, see Message Tokens for Kiosk Notifications.

- **Email Contacts** – Click **Add Contact** and select the contact name from the drop-down list. The contact information must be added prior to creating the email notification.

  Note: In the Add Contact drop-down list, the icons that display represent the contact's preferred method of notification.

  To remove an email contact, click the **X** in the contact label.

  Note: If the contact name is gray, it was defined at the district level and cannot be removed at the building level.

Kiosk Alert Notifications, cont.

Text Message Notifications

- **Text Message** – The text message is pre-populated with a default message using message tokens but you can change this message if desired. Note that no information on the visitor or offender is sent in the text message. If this field is left blank, no text message is sent.

  To use message tokens to compile the message, see Message Tokens for Kiosk Notifications.

  If you want the same text as that specified in the Email Notification, click **Copy from Email**.

- **Text Message Contacts** – For those who want to be notified via a text message, click **Add Contact** and select the contact name from the drop-down list. The contact information must be added prior to creating the text message notification. Only those contacts that provided a text message phone can be selected from the list.

  Note: In the Add Contact drop-down list, the icons that display represent the contact's preferred method of notification.

  To remove a text contact, click the **X** in the contact label.

  Note: If the contact name is gray, it was defined at the district level and cannot be removed at the building level.

Message Tokens for Kiosk Notifications

You can also use Message Tokens, which are variables, in the notification message so that when the message is sent, the tokens will be replaced by their associated value.

Click **Message Tokens** to view the variables that can be entered in the message.

%CLIENTNAME% - District Name
%BUILDINGNAME% - Building Name
%JUSTTIME% - Time Logged - hh:mm: tt
%JUSTDATE% - Date Logged - MM/DD/YYYY
%PERSONTYPE% - Type of Person [attempting kiosk sign in] (e.g., Visitor, Volunteer, etc.)

Example:

A %PERSONTYPE% has attempted to sign in to %BUILDINGNAME% through the kiosk resulting in one or more possible custom and/or offender alert. The possible alert(s) were logged today, %JUSTDATE%, at %JUSTTIME%

Maintenance

The **Maintenance** workspace enables users to manage various aspects of the product.

- ➢ Merge Duplicate Records

Merge Duplicate Records

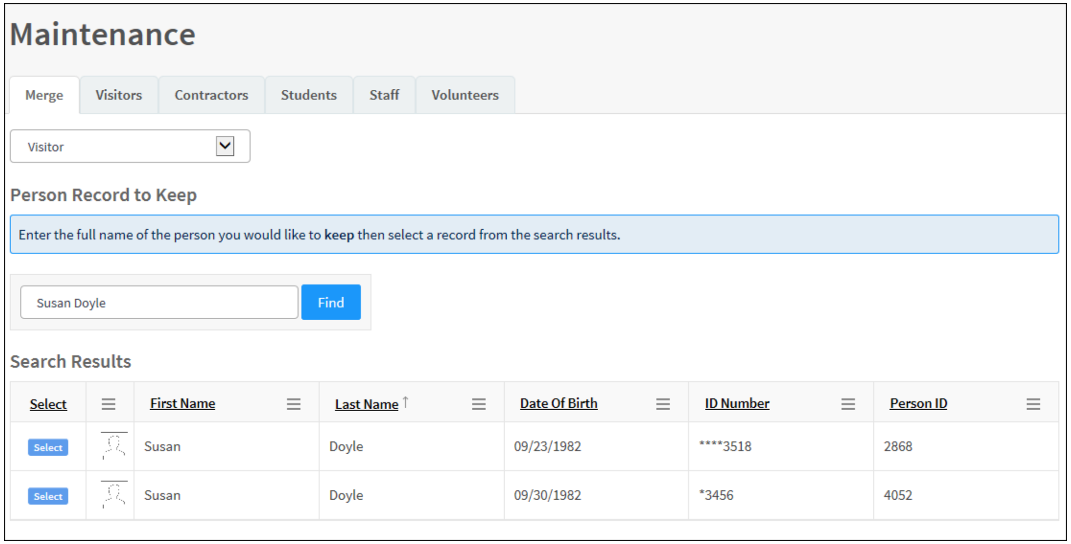
The Merge feature enables Administrators to merge duplicate person records for the same visitor. You must have the *Can Perform Maintenance* permission to view this tab.

This feature is used when a visitor was signed in twice, however the second time they were scanned in, the scanner may have incorrectly scanned their first name, last name, ID number or DOB which caused the system to create a new person record rather than using the existing visitor record.

The merge feature allows an Administrator to pull all the information for both records into a single record.

Perform the following steps to merge two records:

1. From the navigation menu, select **Admin > Maintenance**.
2. On the **Merge** tab, select **Visitor** from the drop-down list.
3. In the **Person Record to Keep** area, enter the first and last name of the person you would like to keep and then click **Find**.
4. Click **Select** for the record you want to keep.



Merge Duplicate Records, cont.

4. In the **Person Record to Merge** area, enter the first and last name of the person you would like to keep and then click **Find**.

   The icon displays next to the record you have selected to keep.

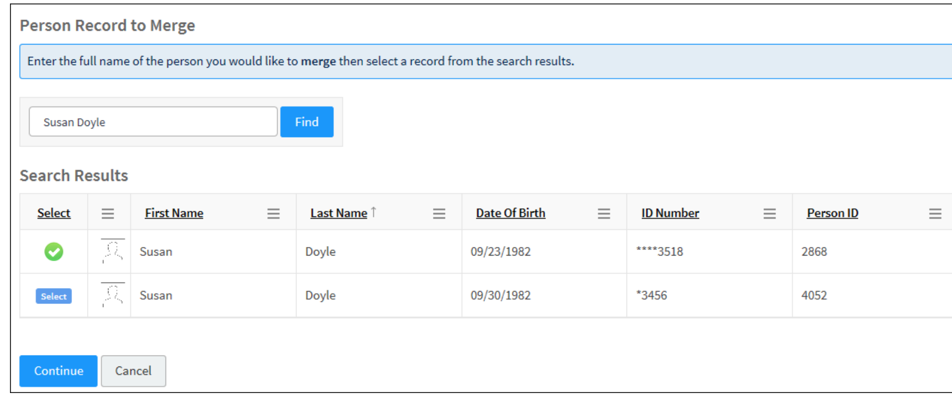
5. Click **Select** next to the record you want to merge and then click **Continue**.

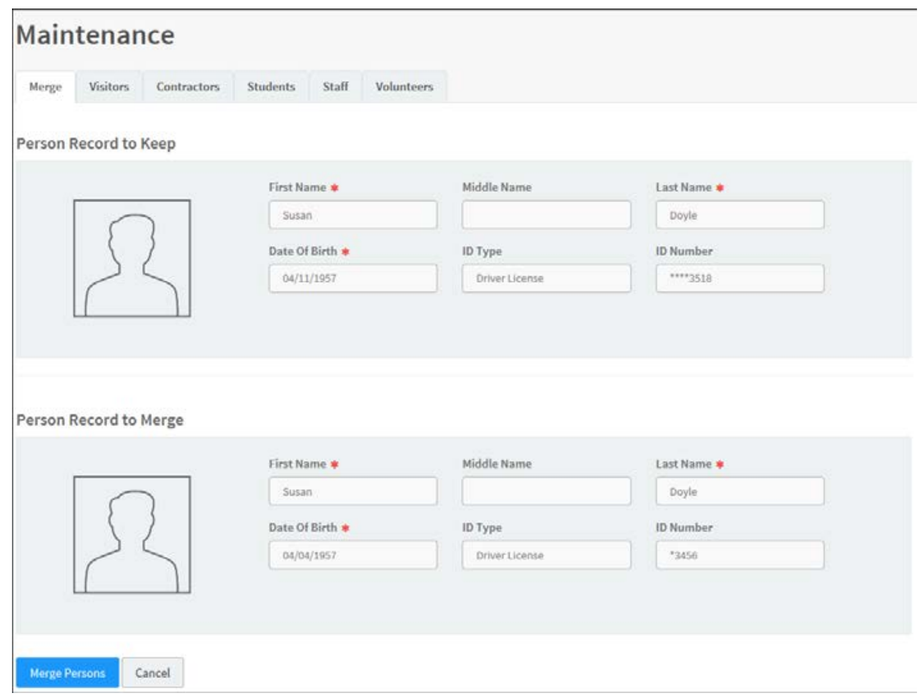
   Note: You will not be able to merge a visitor record that was scanned into Raptor with a visitor record that was not scanned. In this case the merge (official) record will display the icon instead of the **Select** button.

6. Review the information to confirm these are the records to be merged, and then click **Merge Persons**.

7. On the **Merge Confirmation** dialog, click **Submit**. If you want to discard the changes, click **Cancel**.

A confirmation message displays indicating your merge was successfully submitted to the queue and will be completed at 8:00 PM CST.





Roles and Permissions

Raptor users have a unique set of permissions assigned to them based on the type of user account (role) that they have been assigned. The permissions assigned to the account determine what they can see and do in Raptor.

The following topics are covered in this section:

- Understanding User Accounts (Roles)
- Understanding Permissions

RAPTOR TECHNOLOGIES

Understanding User Accounts (Roles)

Raptor users have a unique set of permissions assigned to them based on the type of user account (role) that they have been assigned. The following types of user accounts can be created in Raptor.

Role	Description
District Admin	The District Admin role has the highest level of permissions and is frequently assigned to district administrators. This role has full access to all schools or buildings within the district.
Building Admin	The Building Admin role is assigned to users who perform administrative functions at the school level. This type of user account is typically assigned to school secretaries, principals and assistant principals. Building Admins can be associated with more than one building.
Student Admin	The Student Admin role is assigned to users who perform student-related tasks, such as signing in and signing out students, monitoring tardy count, resetting tardy and temporary ID count, running student reports, importing students and their associated guardians, and adding, modifying and deleting students and guardians. Student Admins can be associated with more than one building. Note: The Student Module must be enabled to be able to create Student Admin accounts.
Entry Admin	The Entry Admin role is assigned to users who are responsible for signing in and signing out visitors, students, volunteers, staff and contractors who enter and leave the building. This role is typically assigned to front-desk personnel. Entry Admins can be associated with more than one building.

User Accounts, cont.

Role	Description
District Volunteer Coordinator	The District Volunteer Coordinator role is assigned to users who manage volunteers and events, and are automatically assigned to all schools and buildings within the district. Users with this role can sign in and sign out volunteers, search volunteers and run volunteer reports. Typically, a volunteer coordinator is also responsible for adding volunteers, approving volunteers, and coordinating volunteer events. Note: The Volunteer Module must be enabled to create District Volunteer Coordinator accounts.
Building Volunteer Coordinator	The Building Volunteer Coordinator role is assigned to users who manage volunteers and events at the school level. Users with this role can sign in and sign out volunteers, run volunteer reports, and approve volunteers for only the schools to which they are assigned. Note: The Volunteer Module must be enabled to create Building Volunteer Coordinator accounts.
Security Officer	The Security Officer role is assigned to District or School Resource Officers and is automatically assigned to all schools or buildings within the district. Users with this role can manage alerts and run offender reports.

User Accounts, cont.

Role	Description
District Reunification Admin REU	The District Reunification Admin role is assigned to users who manage reunification at the client level. This user can initiate and end incidents, manage reunification settings, import rosters and run reunification reports for all buildings in their district.
Building Reunification Admin REU	The Building Reunification Admin role is assigned to users who manage reunification at the building level. This user can initiate and end incidents, manage reunification settings, import rosters and run reunification reports for their specific buildings.
Reunification User REU	The Reunification role is assigned to staff members who will be granted the Reunification Mobile App permissions.
Incident Commander REU	*Mobile App User Account*. The Incident Commander role is assigned to users who are responsible for managing and overseeing a drill or live emergency. This role provides elevated access to live incident dashboards and secure documents.
Student Supervisor REU	*Mobile App User Account*. The Student Supervisor role is assigned to users who are responsible for supervising and accounting for students during a drill or live emergency.

Understanding Permissions

Each user is assigned a role that has specific permissions associated with it, and the permissions can be enabled or disabled. Typically, permissions are selected when the user account is created.

When creating a user account, the user can only grant permissions that their account includes. For example, if you are a District Admin and do not have the *Can Manage Logs* permission, you cannot create user accounts and grant the *Can Manage Logs* permission.

Refer to the following tables to understand the permissions that are available for each role.

Administration Permissions

Permission	Description	Role
Can View Logs	Provides access to the Log menu item under the Admin menu.	District Admin Building Admin District Reunification Admin Building Reunification Admin
Can Manage Client Settings	Provides access to Client Profile, Buildings, and Module Settings under the Admin menu. Provides access to Client Profile, Buildings, and Module Settings under the Admin menu. With this permission, a user can define drill schedules, update drill requirements and access the drill compliance dashboard.	District Admin
Can Manage Building Settings	Provides access to the Building Profile and Module Settings and under the Admin menu. With this permission, a user can update drill requirements and access a building’s drill schedule.	Building Admin
Can Manage Users	Provides access to the Users/Contacts menu item under the Admin menu. With this permission, a user can view, create, modify, active and deactivate Raptor user accounts, and reset the password for the account. The role of the user creating the user accounts restricts the type of user account role they can create: • District Admin – can create any user account • Building Admin – can create only Building Admin, Student Admin and Entry Admin user accounts • District Volunteer Coordinator – can create other District Volunteer Coordinators, Building Volunteer Coordinators and Volunteers. In addition, the user creating the user accounts can only assign the buildings their own account is associated with to the new user accounts.	District Admin Building Admin District Volunteer Coordinator Building Volunteer Coordinator District Reunification Admin Building Reunification Admin

Administration Permissions, cont.

Permission	Description	Role
Can Manage Alerts	Provides access to the Alert Settings menu item under the Admin menu. With this permission, a user can view and modify notification templates associated with sex offender alerts, custom alerts, the Emergency button, and instant alerts. They can also view, create, and modify custom and instant alerts, and import custom alerts.	District Admin Building Admin Security Officer District Reunification Admin Building Reunification Admin
Can Manage Kiosks	Provides access to the Kiosk Settings menu item under the Admin menu. With this permission, a user can view, create, modify per module kiosk settings, modify client kiosk policy, and launch Kiosk Profiles.	District Admin Building Admin
Can Launch Kiosks	Provides the ability to launch a kiosk.	District Admin Building Admin Entry Admin
Can Perform Maintenance	Provides access to the Maintenance menu item under the Admin menu. With this permission, a user can merge duplicate records and perform other maintenance tasks.	District Admin Building Admin District Reunification Admin Building Reunification Admin

Administration Permissions, cont.

Permission	Description	Role
Can Manage Documents	Provides access to the Documents area on the General Settings workspace under Admin. With this permission, a user can add, modify or delete documents used for reunification. This feature is not yet available in the product.	District Admin Building Admin District Reunification Admin
Can Run System Reports	Provides access to the Raptor Link Dashboard and future system reports.	District Admin Building Admin District Reunification Admin Building Reunification Admin
Can Manage Report Subscriptions	Provides access to the Subscriptions tab on the Reports page. With this permission, you can add, modify and delete report subscriptions.	District Admin Building Admin Student Admin Entry Admin District Volunteer Coordinator Building Volunteer Coordinator Security Officer

Visitor Permissions

Permission	Description	Role
Can Sign In Visitors	User can sign in visitors and access the Delayed Entry and Batch Printing features.	District Admin Building Admin Entry Admin
Can Sign Out Visitors	User can sign out visitors (single or multiple sign out), view who is signed in, reprint visitor badge, change the visitor's Destination/Reason for Visit, and the Notes field.	District Admin Building Admin Entry Admin
Can Run Visitor Reports	User can view, create, manipulate and export reports related to visitors; can access the Visitor Dashboard.	District Admin Building Admin Entry Admin
Can Manage Visitors	Provides access to the All Visitors tab in the Visitors workspace. Users can view and modify visitors with "official records" and view a visitor's sign in/sign out history.	District Admin Building Admin
Can Manage Visitor Settings	Provides access to the Visitor Module settings (Admin > Module Settings > Visitors tab). User can change Visitor Module settings, manage destination/reasons, and custom fields.	District Admin Building Admin

Contractor Permissions

Permission	Description	Role
Can Sign In Contractors	User can sign in contractors and access the Delayed Entry feature.	District Admin Building Admin Entry Admin
Can Sign Out Contractors	User can sign out contractors (single or multiple sign out), view who is signed in, reprint contractor's badge, change the contractor's Destination/Reason for Visit, and the Notes field.	District Admin Building Admin Entry Admin
Can Run Contractor Reports	User can view, create, manipulate and export reports related to contractors; can access the Contractor Dashboard.	District Admin Building Admin Entry Admin
Can Manage Contractors	Provides access to the All Contractors tab in the Contractors workspace. Users can view and modify contractors with official records, view a contractor's sign in/sign out history, and add contractors.	District Admin Building Admin
Can Manage Contractor Settings	Provides access to the Contractor Module settings (Admin > Module Settings > Contractors tab). User can change Contractor Module settings, manage destination/reasons, companies, and custom fields.	District Admin Building Admin
Can Import Contractors	User can import contractors into the Raptor system. This permission requires Can Manage Contractors permission to access the All Contractors tab.	District Admin Building Admin

Student Permissions

Permission	Description	Role
Can Sign In Students	User can sign in students and access the Delayed Entry feature.	District Admin Building Admin Student Admin Entry Admin
Can Sign Out Students	User can sort and filter the list of students, and sign out students.	District Admin Building Admin Student Admin Entry Admin
Can Run Student Reports	User can view, create, manipulate and export reports related to students; can access the Student Dashboard.	District Admin Building Admin Student Admin Entry Admin
Can Manage Students	User can view all students, sort and filter the list of students, review a student's sign in/sign out history, add students and their associated guardians, and reset tardy and temporary ID counts.	District Admin Building Admin Student Admin District Reunification Admin Building Reunification Admin

Student Permissions, cont.

Permission	Description	Role
Can Manage Student Settings	Provides access to the Student Module settings (Admin > Module Settings > Students tab). User can change Student Module settings, manage destination/reasons, and custom fields.	District Admin Building Admin Student Admin District Reunification Admin Building Reunification Admin
Can Import Students	User can import students, student photos, and guardians associated with students. Note: This permission requires that the user also have the Can Manage Students permission.	District Admin Building Admin Student Admin District Reunification Admin Building Reunification Admin
Can Manage Student Tardy Workflow	User can configure the tardy settings for the client or building. This feature is not yet available in the product.	District Admin Building Admin Student Admin

Staff Permissions

Permission	Description	Role
Sign In Staff	User can sign in staff and access the Delayed Entry feature.	District Admin Building Admin Entry Admin
Can Sign Out Staff	User can view staff and sign out staff (single or multiple sign out).	District Admin Building Admin Entry Admin
Can Run Staff Reports	User can view, create, manipulate and export reports related to staff members; can access the Staff Dashboard.	District Admin Building Admin Entry Admin
Can Manage Staff	User can search staff, import staff information, manually add staff, and purge staff details.	District Admin Building Admin

Staff Permissions, cont.

Permission	Description	Role
Can Manage Staff Settings	Provides access to the Staff Module settings (Admin > Module Settings > Staff tab). User can change Staff Module settings, manage destination/reasons, and custom fields.	District Admin Building Admin District Reunification Admin Building Reunification Admin
Can Import Staff	User can import staff members into the Raptor system. Note: This permission requires that the user also have the Can Manage Staff permission.	District Admin Building Admin District Reunification Admin Building Reunification Admin

RAPTOR TECHNOLOGIES

Volunteer Permissions

Permission	Description	Role
Can Sign In Volunteers	User can sign in volunteers and access the Delayed Entry and Batch Printing features.	District Admin Building Admin Entry Admin District Volunteer Coordinator Building Volunteer Coordinator
Can Sign Out Volunteers	User can view volunteers and sign out volunteers (single or multiple sign out).	District Admin Building Admin Entry Admin District Volunteer Coordinator Building Volunteer Coordinator
Can Run Volunteer Reports	User can view, create, manipulate and export reports related to volunteers; can access the Volunteer Dashboard.	District Admin Building Admin Entry Admin District Volunteer Coordinator Building Volunteer Coordinator

RAPTOR TECHNOLOGIES

Volunteer Permissions, cont.

Permission	Description	Role
Can Manage Volunteers	User can search volunteers, add volunteers, and delete volunteer details.	District Admin Building Admin District Volunteer Coordinator Building Volunteer Coordinator
Can Manage Volunteer Settings	User can change Volunteer Management settings and manage functions, requirements, required documents, organizations, affiliations, and custom fields; change Sign-In/Out settings; change Volunteer Application settings and manage notifications, and online application page content; change Volunteer Portal settings and manage notifications; and change Event Management settings.	District Admin Building Admin District Volunteer Coordinator Building Volunteer Coordinator
Can Import Volunteers	User can import volunteers and volunteer applications. Note: This permission requires that the user also have the Can Manage Volunteers permission.	District Admin Building Admin District Volunteer Coordinator Building Volunteer Coordinator

Volunteer Permissions, cont.

Permission	Description	Role
Can Manage Events	User can view, create, update, disable, and delete events, sign up volunteers or remove volunteers from events, and email volunteers.	District Admin Building Admin District Volunteer Coordinator Building Volunteer Coordinator
Can Approve Volunteers	User can view and approve volunteer applicants.	District Admin Building Admin District Volunteer Coordinator Building Volunteer Coordinator
Can View Events	User (volunteer) can view upcoming events and the events for which they have signed up.	Volunteer
Can Sign Up Events	User (volunteer) can sign up for events.	Volunteer
Can Edit Volunteer Hours	User (volunteer) can edit the hours they entered in the Volunteer Portal.	Volunteer
Can Access Volunteer Portal	User (volunteer) can log in to the Volunteer Portal.	Volunteer

Other Permissions

Permission	Description	Role
Can Run Offender Reports	User can view, create, manipulate and export reports related to offender and custom alert matches and mismatches.	District Admin Building Admin Security Officer

RAPTOR TECHNOLOGIES

Reunification

Permission	Description	Role
Can Import Rosters	User can import staff rosters. **Note:** This permission requires that the user also have the *Can Manage Staff* permission.	District Admin Building Admin Student Admin District Reunification Admin Building Reunification Admin
Can Perform Reunification Tasks	User can reunify student with guardians and releasing students from the incident from within the Reunification Mobile Application.	District Admin Building Admin Student Admin Entry Admin District Volunteer Coordinator Building Volunteer Coordinator Security Officer District Reunification Admin Building Reunification Admin

Reunification, cont.

Permission	Description	Role
Can Run Reunification Reports	User can view, create, manipulate, and export reports related to reunification incidents.	District Admin Building Admin Security Officer District Reunification Admin Building Reunification Admin

Reunification Mobile App

Permission	Description	Role
Can Initiate and End Incident	User can initiate and end incidents from within the Reunification Mobile Application.	District Admin Building Admin Student Admin Entry Admin District Volunteer Coordinator Building Volunteer Coordinator Security Officer District Reunification Admin Building Reunification Admin
Can Manage Reunification Settings	Provides access to the Reunification Module settings (Admin > Module Settings > Reunification tab). User can change Reunification Module settings, view emergency types, and manage emergency sub-types, locations, and statuses. Provides access to the Reunification Module settings (Admin > Module Settings > Reunification tab). User can change Reunification Module settings, view emergency types, and manage emergency sub-types, locations, and statuses. It also provides access to the Drill Schedules and Drill Compliance Dashboard. **Note:** Requires Can Manage District Settings to access the Reunification module settings.	District Admin Building Admin District Reunification Admin Building Reunification Admin

Contact Us

Raptor Technologies Support

Email: support@raptortech.com

Call: 877-7RAPTOR (877-772-7867) Option #2