Client Training HQ

Guardian Administration Guide (G2)

Table of Contents

Administration Module ... **3**
Employee Records ... **3**
- Adding Custom Fields ... 3
- Editing Custom Fields ... 5
- Manage Group Structure ... 5
- Employee Groups ... 6
- Adding New Employee Groups ... 6
- Assigning Managers to Employee Groups ... 7
- Grant Access to All Employees ... 7
- Grant Access to Some Employees ... 8
- How to Purge I-9 Forms ... 9

Users and Roles ... **10**
- Manage Users ... 10
- Adding New Users ... 11
- General Information Tab ... 11
- Group Access Tab ... 12
- Login Information Tab ... 13
- Single Sign-On ... 15
- Manage Roles ... 15
- Permissions ... 16
- Permissions Definitions ... 16
- E-Verify Permissions ... 16
- I-9 Permissions ... 17
- Reporting Permissions ... 17
- Employee Permissions ... 17
- Remediation Permissions ... 17
- Support Permissions ... 18

Locations & E-Verify ... **19**
- Location Map View versus Location List View ... 19
- Creating New Locations ... 20

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

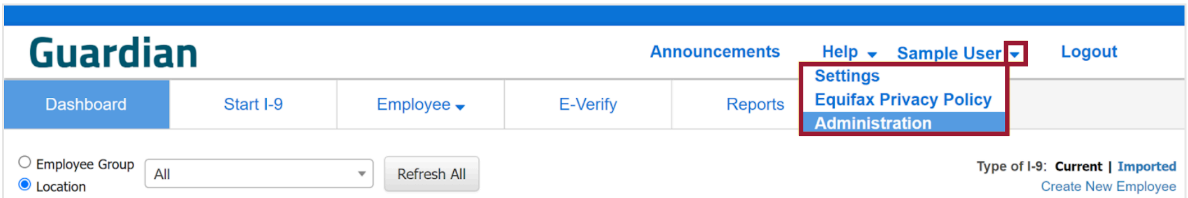
Viewing and Editing Existing Locations........ 21
Legal Entities........ 22
Creating New Legal Entities........ 22
E-Verify........ 23
I-9 Policy........ 23
New I-9 Settings........ 23
Section 1 New Hire Experience........ 24
Section 2 New Hire Experience........ 24
Document Retention........ 25
Document Retention Workflow........ 25
Employee Supporting Document Capture........ 25
Define Document Types........ 26
I-9 Management........ 26
Dashboard and Announcements........ 27
Correcting I-9s & Advanced........ 27
Portals and Remote Processing........ 28
Remote Hire Preferences........ 29
Security........ 29
User Settings........ 30
Miscellaneous Settings........ 30
Employee Access Settings........ 31
Secondary Authentication........ 31
Custom Messages for English- or Spanish-speaking employees........ 32
Communication........ 33
Email Settings........ 33
Email/Receipt Templates........ 33
Editing Email/Receipt Templates........ 34
Custom Notifications........ 35
Creating Custom Notifications........ 35
Notification Types........ 36
Creating New Notification Messages........ 41
Announcements........ 42
Creating New Announcements........ 42
Announcement Example........ 43
Customizing Help Text........ 44
Integrations........ 45
Column Header Identifier Descriptions:........ 45
Reviewing Data Feed Log........ 46
Data Feed Manual File Upload........ 46
Return to Main Application........ 47
Guardian Customer Support........ 47
More Training Available!........ 47

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Administration Module

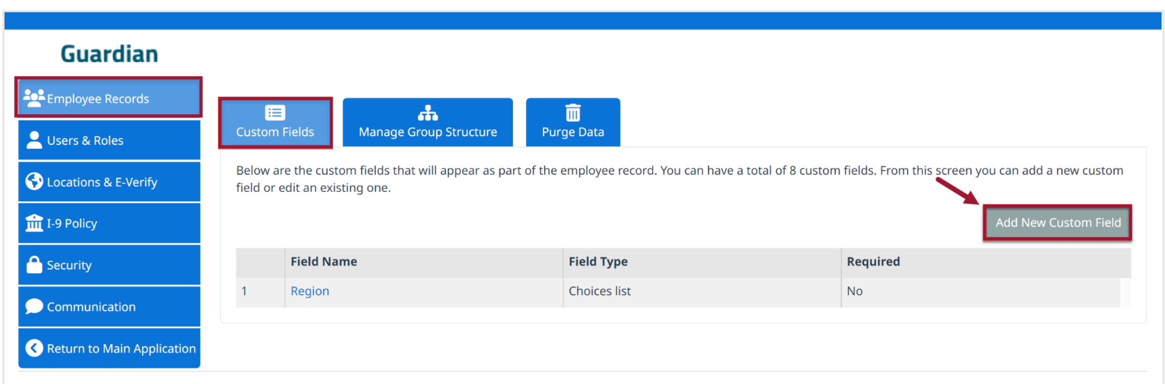
The Administration Module allows Guardian users (with Administrative permissions) to access the settings that will allow customization options. This guide will provide a step-by-step outline for each of the sections within the Administrative Module for users that are configured on the **Hierarchical structure of the Guardian system (G2).**

Users with Administrator permissions can access the Administration Module. From the Guardian dashboard or homescreen, click the caret symbol next to your name to reveal the menu options available. Click on the **Administration** option that appears in the drop-down menu to access the Administration module.



Employee Records

The first tab of the Administration Module is the **Employee Records** tab. This tab contains settings related to the management of Employee Records in Guardian, including storing employee information within Custom Fields, defining how your employees will be organized within your Group Structure, and the option to Purge Data that is no longer required to be retained.

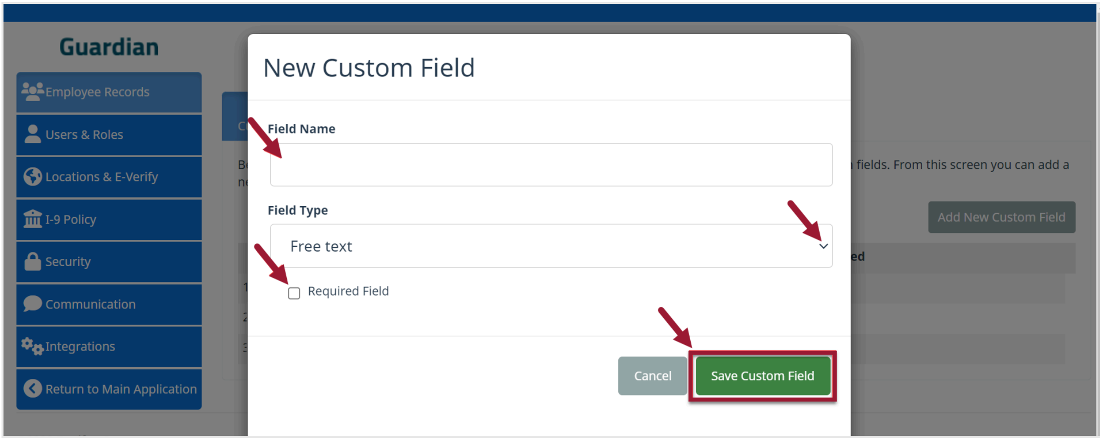


Adding Custom Fields

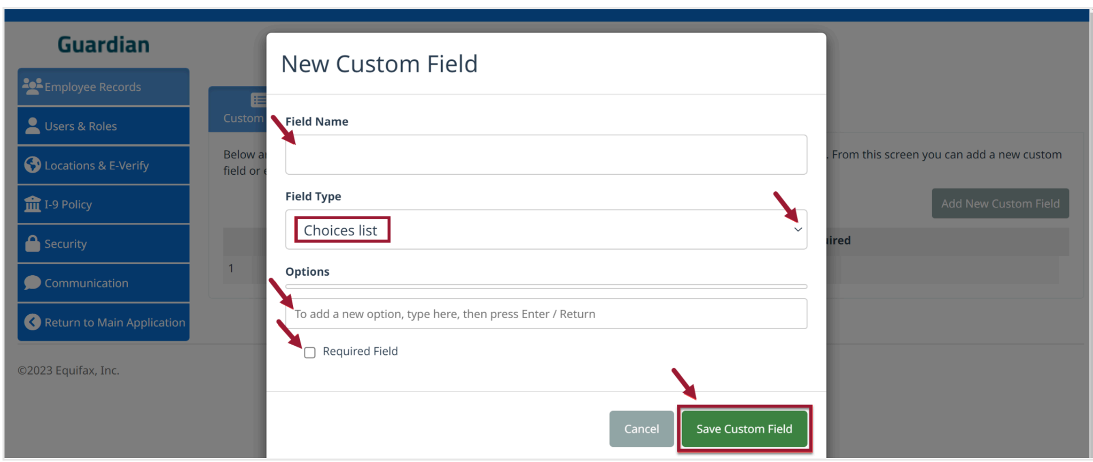
Organizations often need to track and report on employee information that is not captured on the Form I-9 itself. Guardian allows for the creation of up to eight custom fields to store additional employee information, beyond what is typically captured during the Form I-9 process. Information may be entered into a Custom Field when an employee is first created, as well as any time afterwards, from within the Employee Record.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

1) Click **Add New Custom Field**.
2) Start by entering a **Field Name**. Then, specify the **Field Type**. Custom Fields can be either **Free Text** or a **Choice List**.



3) If creating a **Choice List**, enter in a value and press **Enter**. Repeat for all desired values.



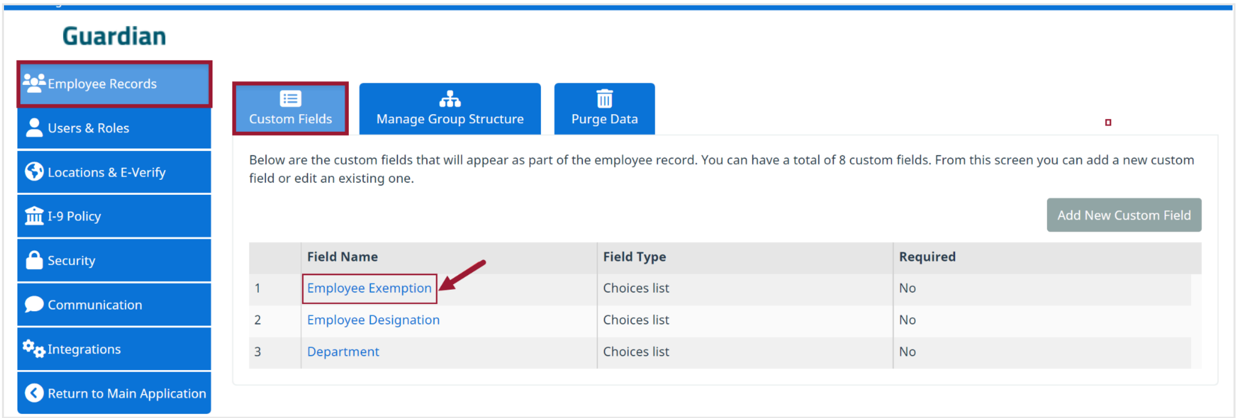
Note: Choice List values will appear in the order they are entered, and cannot be resorted without removing and reentering the values. Take care when building your Choice List. Custom Fields can be edited at a later time, but cannot be deleted once created.

4) If desired, select **Required Field** to require the field be completed when Employee Records are created. The Required Field checkbox determines if the custom field is required or not when the employee is created in Guardian. If checked, the employee will not be able to be created unless the Custom field is completed by the user. When finished, click **Save Custom Field**.

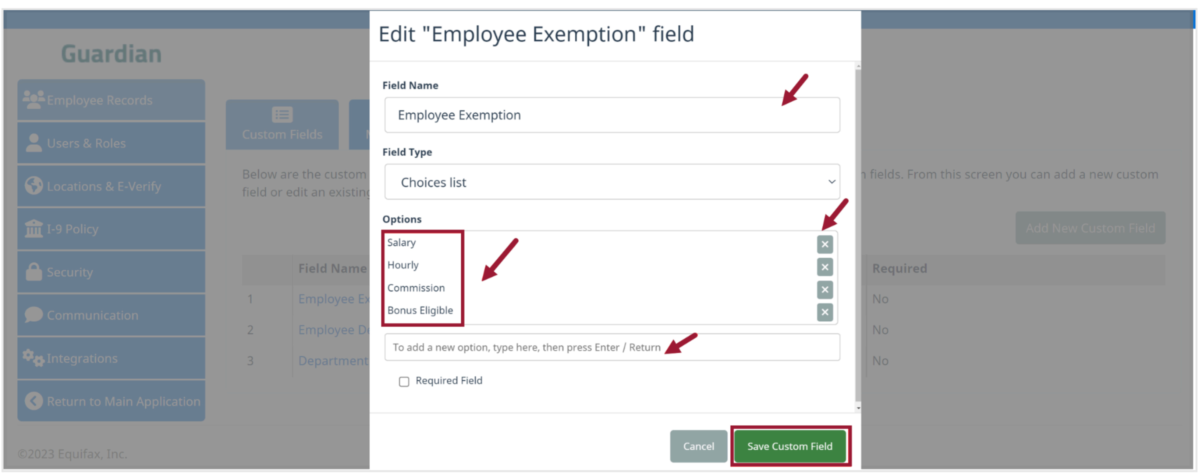
Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Editing Custom Fields

1) Edit the Custom Field as desired. To edit a Custom Field, click on the **Field Name**.



2) For **Choice Lists**, values can be removed by clicking the **X** button, and additional values can be entered. Click **Save Custom Field** when finished.

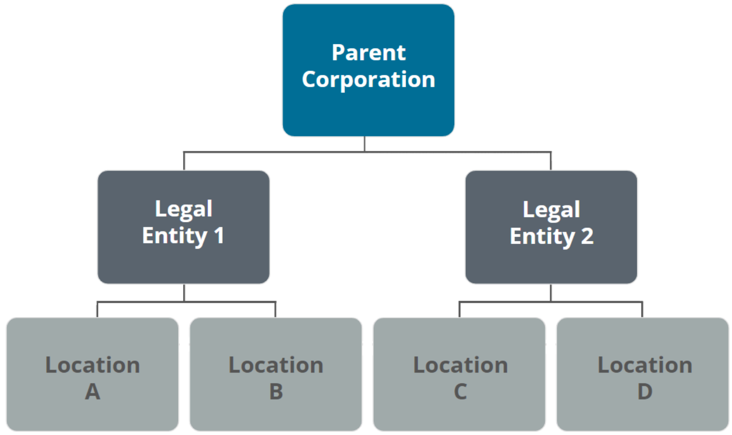


Manage Group Structure

The **Group Structure** is a customizable hierarchy that represents the various layers of your organization and groupings of employees. A common Group Structure is **Parent Organization** > **Legal Entities** > **Locations**, although your organization's Group Structure may differ. While additions can be made to the various layers (additional legal entities and locations), the structure itself cannot be modified once your Guardian site has been deployed.

An example Group Structure is shown below that includes the **Parent Organization** as the top level, two **Legal Entities** as the second level, and four **Locations** as the third and lowest level of the structure.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.



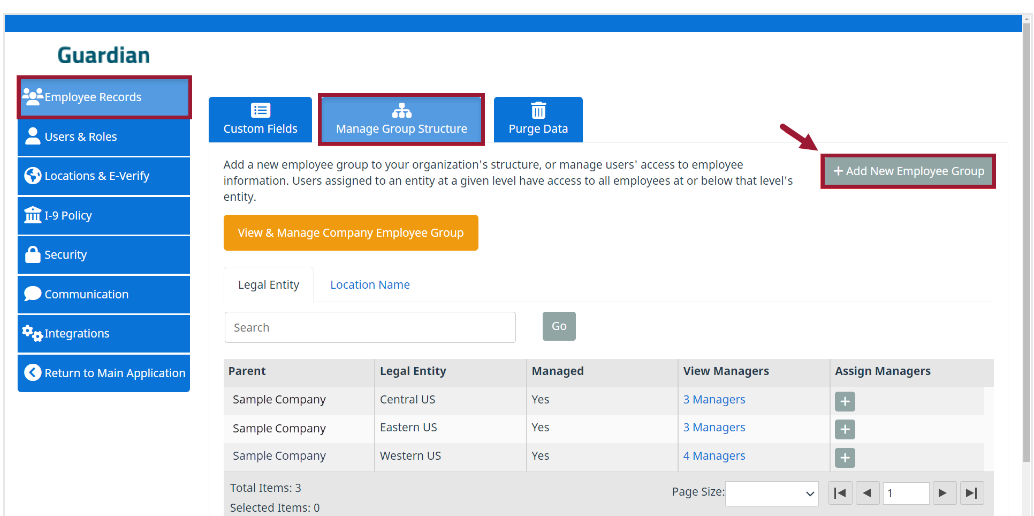
Employee Groups

The various layers of the Group Structure are used to create **Employee Groups** which are used to organize employees for reporting purposes, as well as to determine which Guardian Users will have access to their data. Employees are assigned to one Employee Group at any one time and is based on their location assignment, although their assigned Employee Group can be changed, for example in the event the employee is transferred to another part of the organization. Guardian Users may have access to one, multiple, or all Employee Groups, as defined by a Guardian Administrator.

Adding New Employee Groups

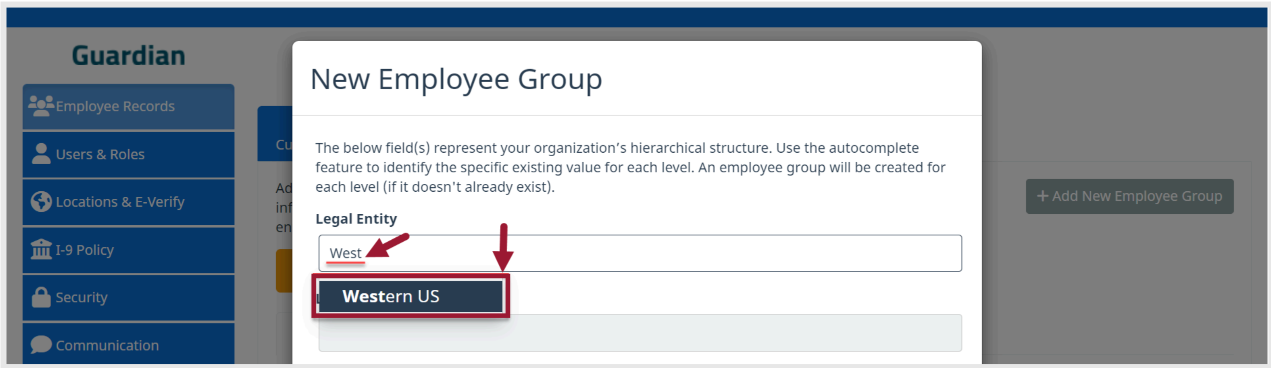
Before adding new Employee Groups, ensure the necessary components of the groups have been established, such as the legal entities and locations that will comprise the Employee Group. If a new legal entity or location must be created, refer to the Locations & E-Verify procedures in this guide. Then, after all necessary legal entities and locations have been established, a new Group can be created as follows:

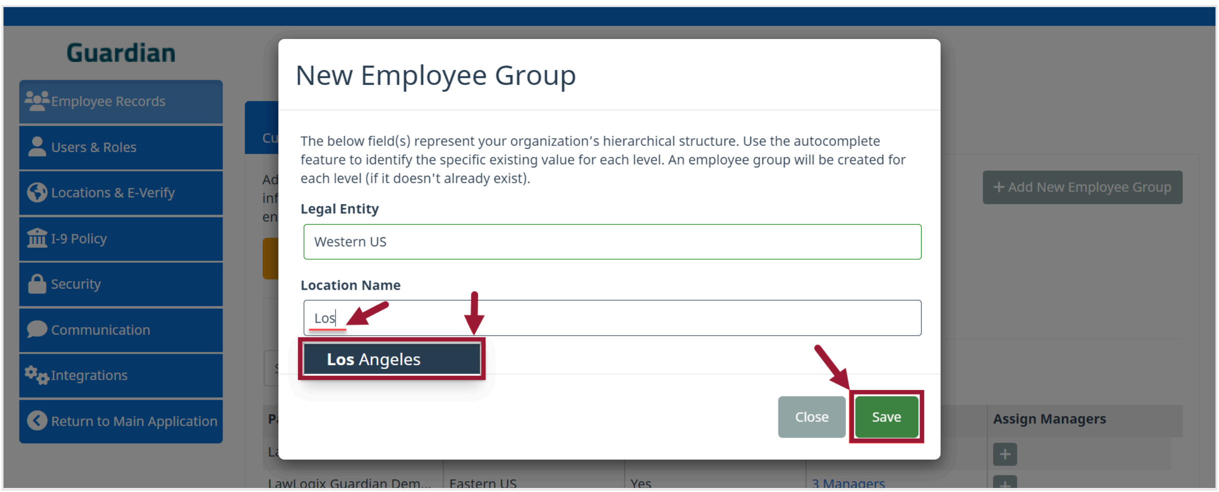
1) Click Add New Employee Group.



Images are examples and for information purposes only. They may vary across platforms and are subject to change.

2) On the New Employee Group screen that appears, type the first few characters in each field presented to define the parts of the **Group Structure** that will comprise this new **Employee Group**. From the search result(s) that appear, select the desired value.





3) Once the values have been entered and appear in the fields, click the **Save** button and then the **Close** button, which will link the location and legal entity to the Group. Remember to assign one or more users to the new Employee Group.

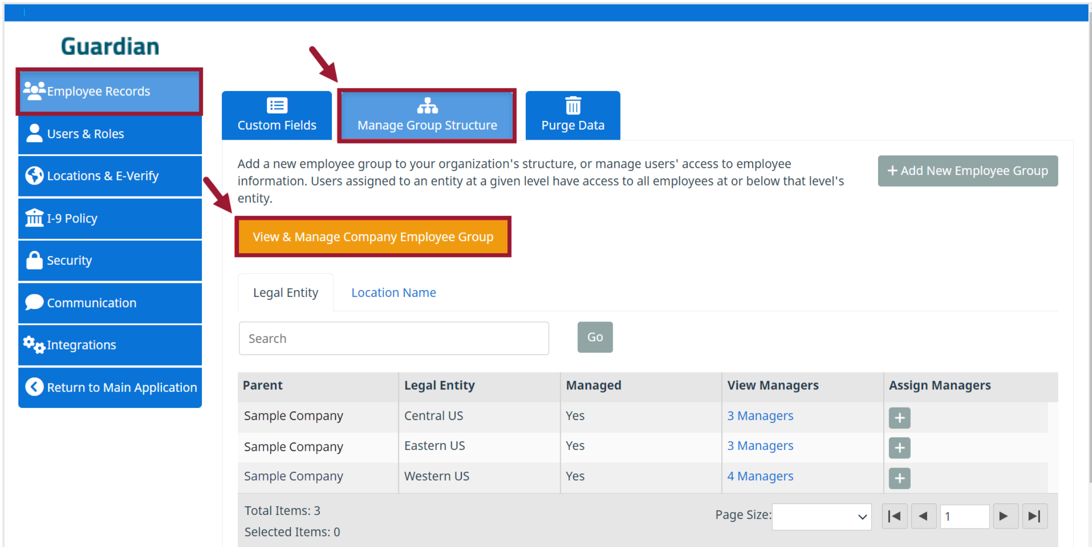
Assigning Managers to Employee Groups

For Guardian users to have access to employee data within Guardian, they must be assigned to one or more levels within your Group Structure. Users may be assigned at any level within your structure, although it is recommended that at least one user be assigned to each Employee Group at the lowest level of your Group Structure (typically the **Location** level). These assignments are used to determine who will receive certain notification emails for employees of that group.

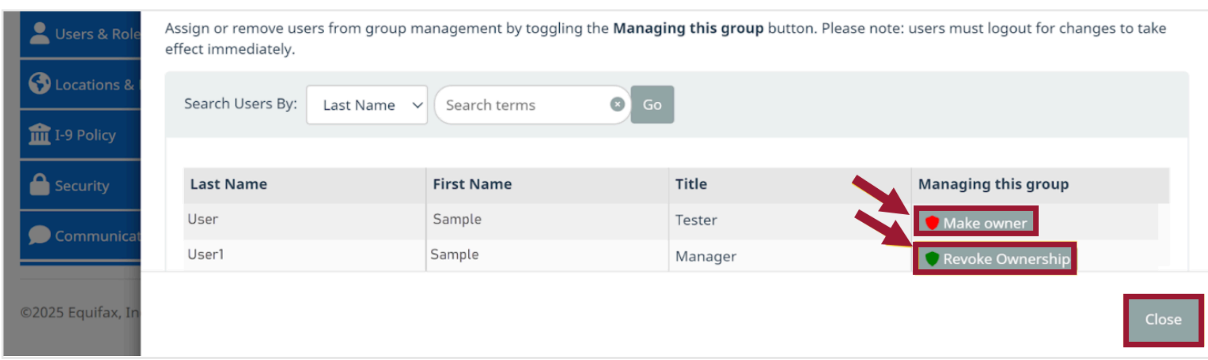
Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Grant Access to All Employees

1) A user can be given access to all employee data by clicking **View & Manage Company Employee Group**, which represents the top level of your Group Structure.



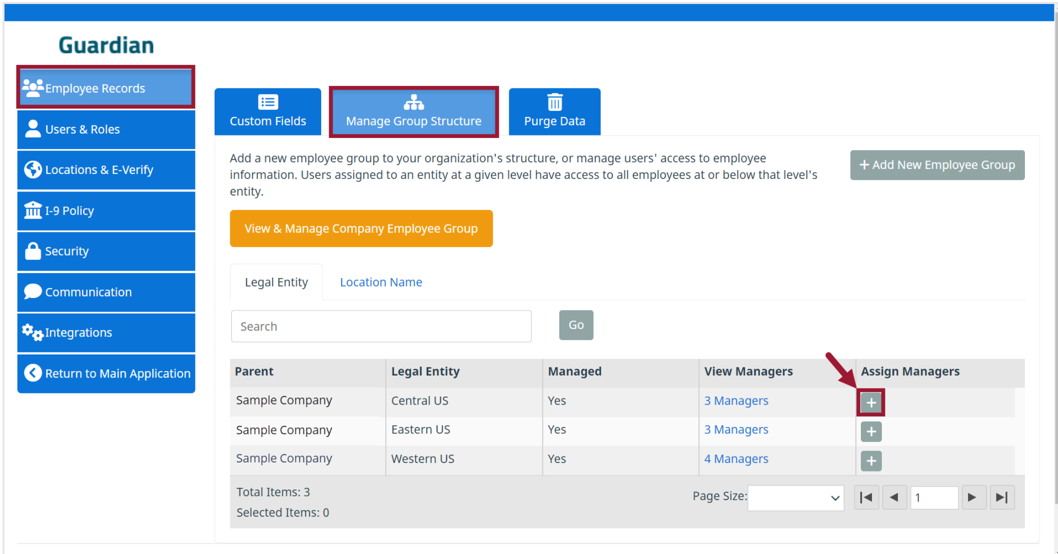
2) From the **Managing this Group** column, **Revoke Ownership** indicates that the user is already assigned to this level of the Group Structure. To assign additional users to this level, click **Make owner** next to their name. When finished, click the **Close** button at the bottom right.



Grant Access to Some Employees

3) A user can be given access to only the employees within a certain segment of your Group Structure, such as a particular legal entity. If assigned at this level, the user will have access to all Employee Groups that fall underneath. From within the desired level of your Group Structure, click the **plus** button under the **Assign Managers** column.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.



Purge Data

Organizations may choose to purge Forms I-9 that they are no longer legally required to retain. As any I-9 currently being retained by an employer may be subject to audit, periodically purging I-9's may help reduce an organization's liability in the event of a **Notice of Inspection** (NOI). An I-9 becomes purgeable when the employee is separated from the organization and the following conditions are met:

1. The employee has been terminated for at least 1 year.
2. The employee's most recent hire date is at least 3 years in the past.

Within Guardian, the **Date Purgeable** is automatically calculated using an employee's most recent period of employment. An employee with multiple I-9s will only appear as purgeable if all their I-9s meet the above criteria. For more information on USCIS retention rules for Form I-9, view Retention and Storage | USCIS.

In order to report on which I-9s are purge-eligible, an interactive report can be generated. This should be completed before the purge is complete in order to identify those I-9s that have an upcoming eligible purge date.

The **Interactive Report** should begin with the **Employee** Base Table and choose the following filters: **Tables -** *Employee* > **Field Name** - *Employee Name* > *Date Hired* > *Date Terminated* > *Purge Eligibility Date* > *Location*.

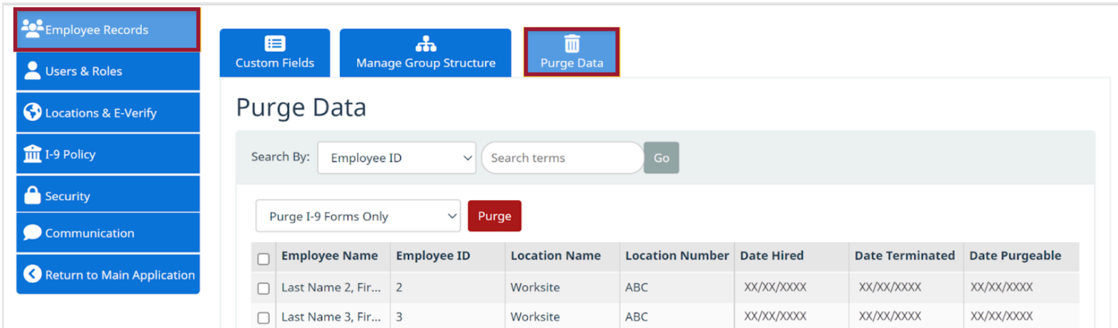
For more details on how to run Guardian Reports, visit our Connections site to view the **Guardian Reports Overview** video.

How to Purge I-9 Forms

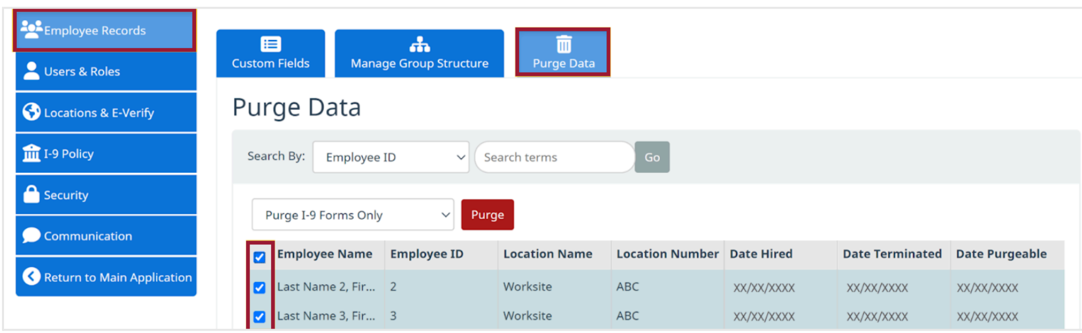
Purging data from Guardian is optional, and must be initiated by a Guardian Administrator. Guardian will not automatically purge an organization's data.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

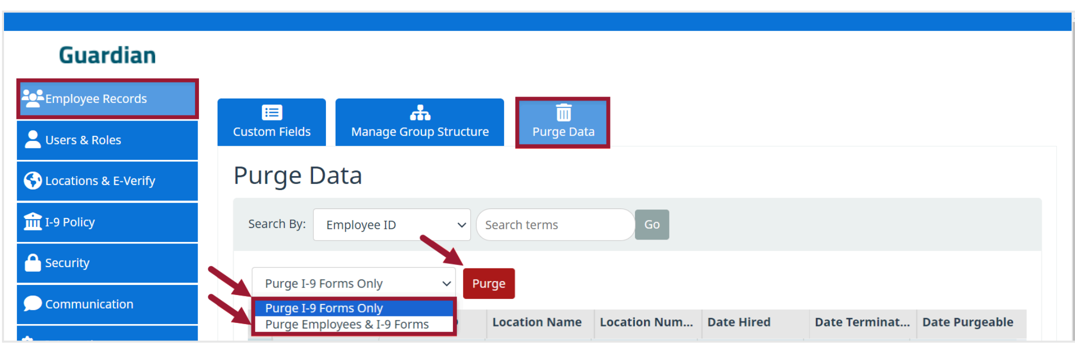
1. From **Employee Records** > **Purge Data**, review the employees who Guardian has calculated are purgeable.



2. Select one or more employees to be purged using the checkboxes next to **Employee Name**.



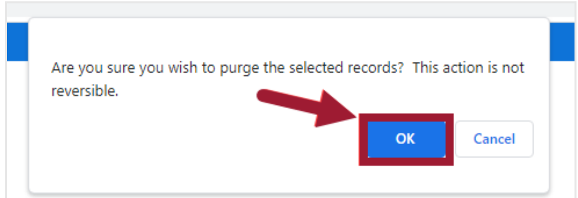
3. With the desired employee(s) selected for purging, choose whether to **Purge I-9 Forms Only** or **Purge Employees & I-9 Forms**. Click the **Purge** button.



Note: Purging only the I-9 Forms will retain the Employee Record within Guardian, including the employee's personal information, employment history dates, and anything stored in OnDocs at the employee level. Employers who commonly rehire employees may wish to use this option if they want to maintain the employee's previous hire and termination dates for future reference and to reduce the amount of data entry required if the employee is rehired.

4. A window will open with a confirmation when the **Purge** button is clicked. Click **OK** on the window (this window may look slightly different depending on the web browser being used).

Images are examples and for information purposes only. They may vary across platforms and are subject to change.



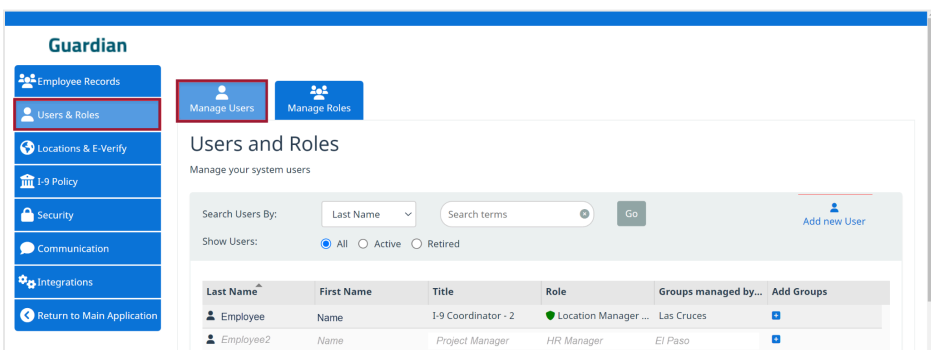
Users and Roles

This tab contains all your Guardian **Users** and their assigned **Roles**. Use this tab to edit existing users, retire existing users, and create new users. Roles, which are sets of security permissions, can be defined and assigned to users to efficiently manage user security in bulk.

Manage Users

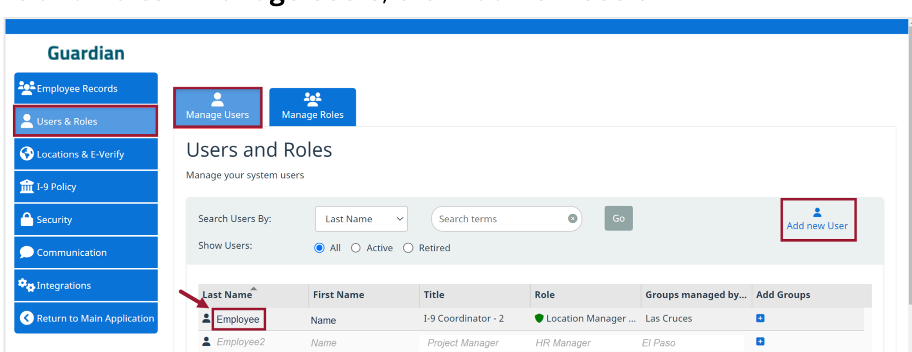
The Manage Users tab will display all users of your Guardian system. Search filters are provided to quickly find a specific user, as well as filters to view only **Active** or **Retired** users. Existing users can be edited by clicking their **Last Name**, and new users can be added by clicking **Add new User**.
The **Role** and the **Employee Groups** that a user is assigned to can be viewed from this screen and users can be assigned to additional Employee Groups by clicking the ⊞ **plus** button under the **Add Groups** column.

Once the user is added (by following the steps below), the user profile can be accessed by clicking the last name of the user in the **Last Name** column.



Adding New Users

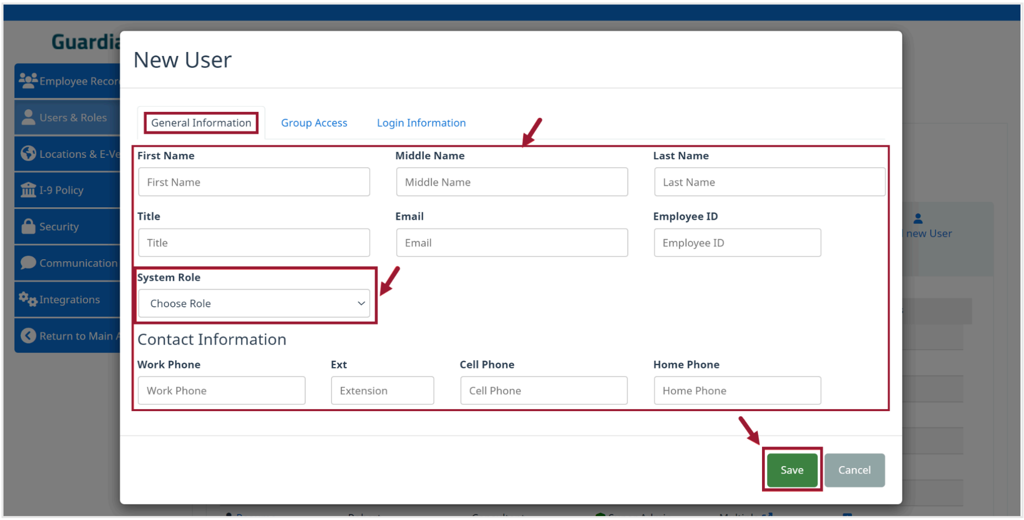
1) From **Users and Roles** > **Manage Users**, click **Add new User**.



Images are examples and for information purposes only. They may vary across platforms and are subject to change.

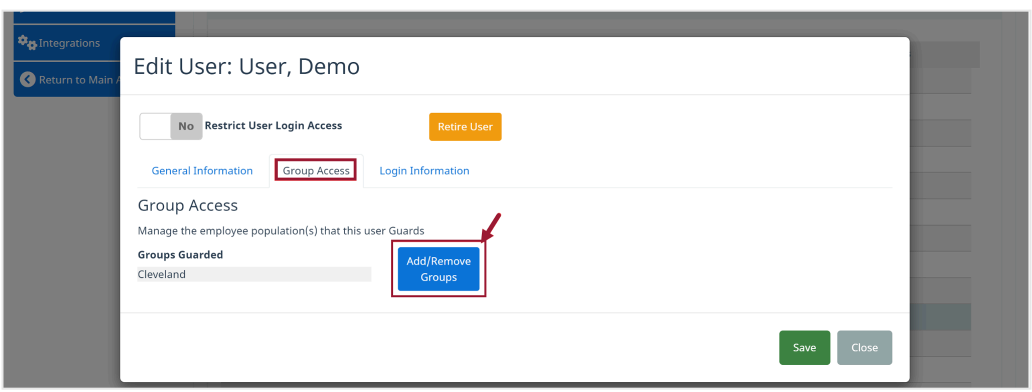
General Information Tab

2) Enter the user's information in the General Information tab and assign them to a **System Role**, which will determine their permissions. When completed, click the **Save** button. The **Group Access** tab will be active.



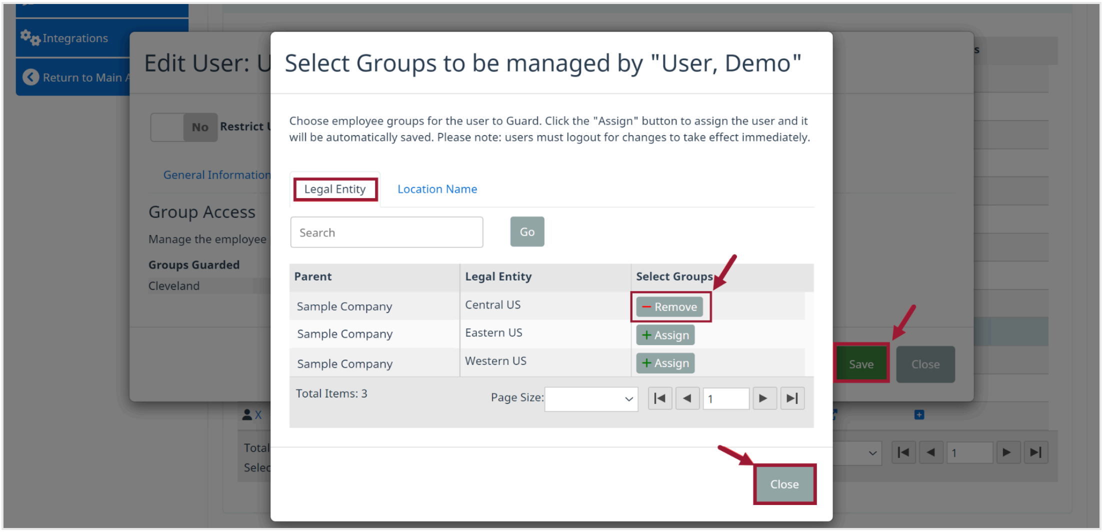
Group Access Tab

3) From the **Group Access** tab, click **Add/Remove Groups** to assign the user to one or more **Employee Groups**.

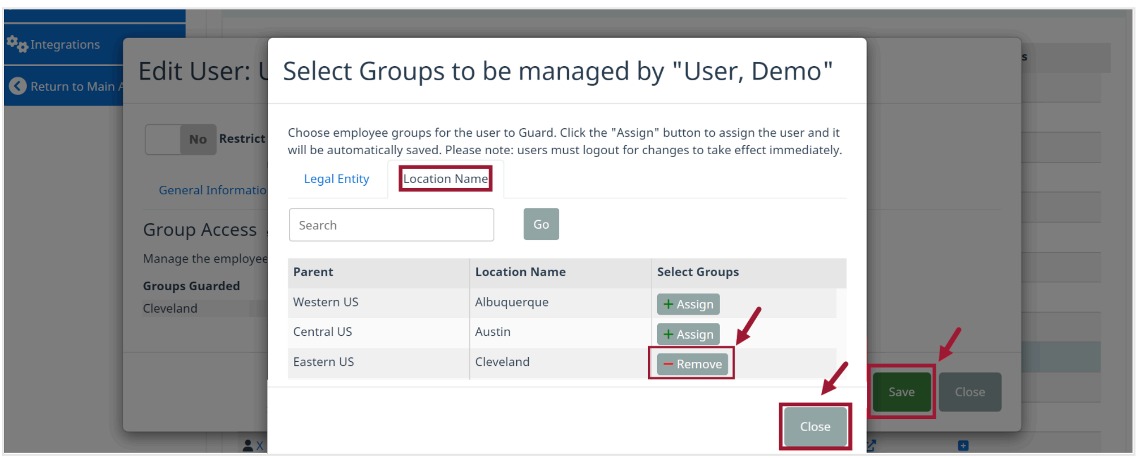


4) Select the Groups that the user should have access to. On the **Legal Entity screen**, clicking the green **+Assign** button will assign the user to that legal entity. The button will then read **– Remove**. If a user is assigned to a legal entity and no locations are needed, click the **Close** button and then the **Save** button.

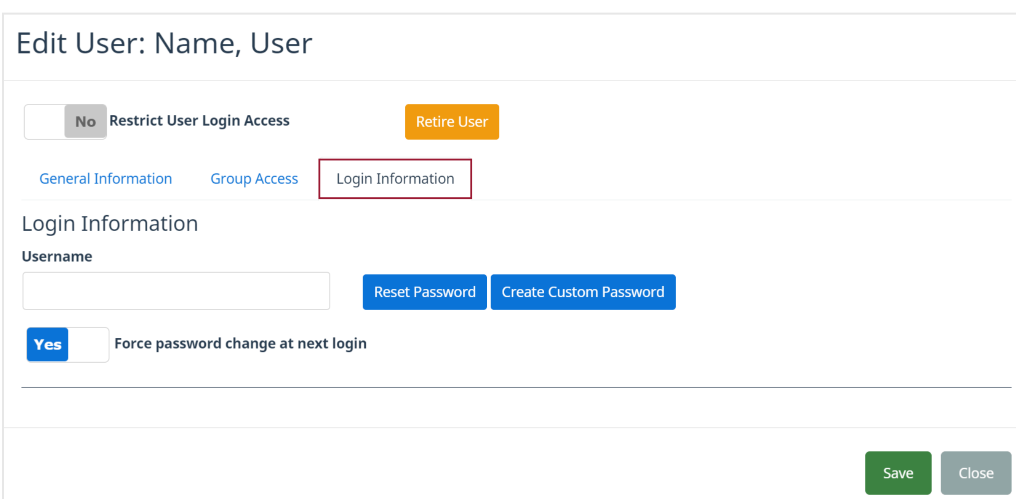
Images are examples and for information purposes only. They may vary across platforms and are subject to change.



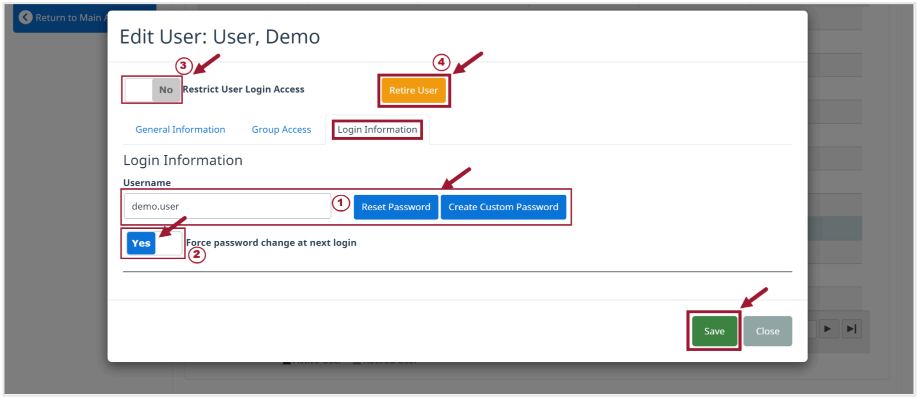
5) If individual locations should be assigned to the user as opposed to a legal entity, proceed to the **Location Name** tab, and click the green **+Assign** button to each location desired. This will assign the user to those location(s), and the button will then read **– Remove**. Once completed, click the **Close** and **Save** buttons.



Login Information Tab

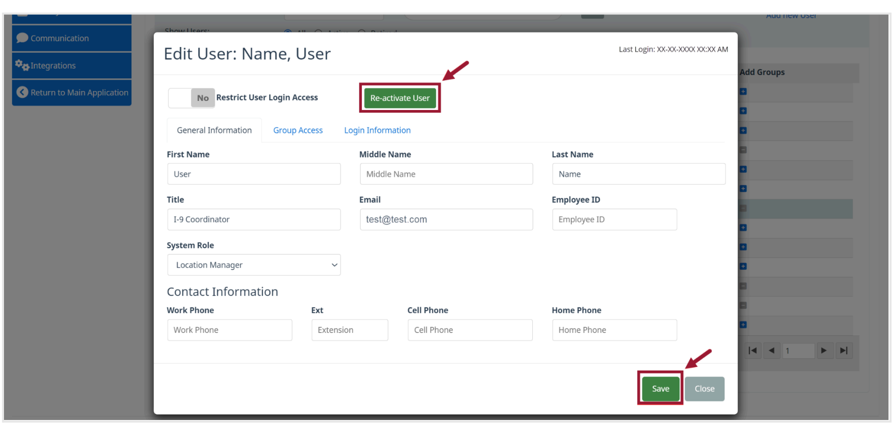


Images are examples and for information purposes only. They may vary across platforms and are subject to change.



1) **User Name** field: From the **Login Information** tab, enter a unique username into the **Username** field, and then click **Reset Password** to email the user their username and password. Alternatively, click **Create Custom Password** to enter in a password manually. If desired, the **Username** may also be customized. The user can change their own username and password after logging in.
2) **Force Password change at next login:** If set to Yes, the user will be prompted to change their password.
3) **Restrict User Login Access:** If a user is locked out, Restrict User Login Access will be set to **Yes**. This is mostly used for retired users, or if the user has accidentally locked themselves out of the system. If a user attempts to log in with an incorrect password five times in a row, their account will be locked, and they will be unable to log in until an Administrator unlocks their account. If the user does not know their current password, navigate to the **Login Information** tab and click **Reset Password** to email them a new password, or click **Create Custom Password** to manually enter a new password for them. Toggle this setting to **No** to unlock the user's account. Click **Save** at the bottom-right.
4) **Retire User** button: When a user no longer needs access to Guardian, their account should be **Retired**. Retired users will appear in italic, grayed-out text in the user listing in the **Manage Users** tab. To retire a user, click the **Retire User** button at the top of the window.

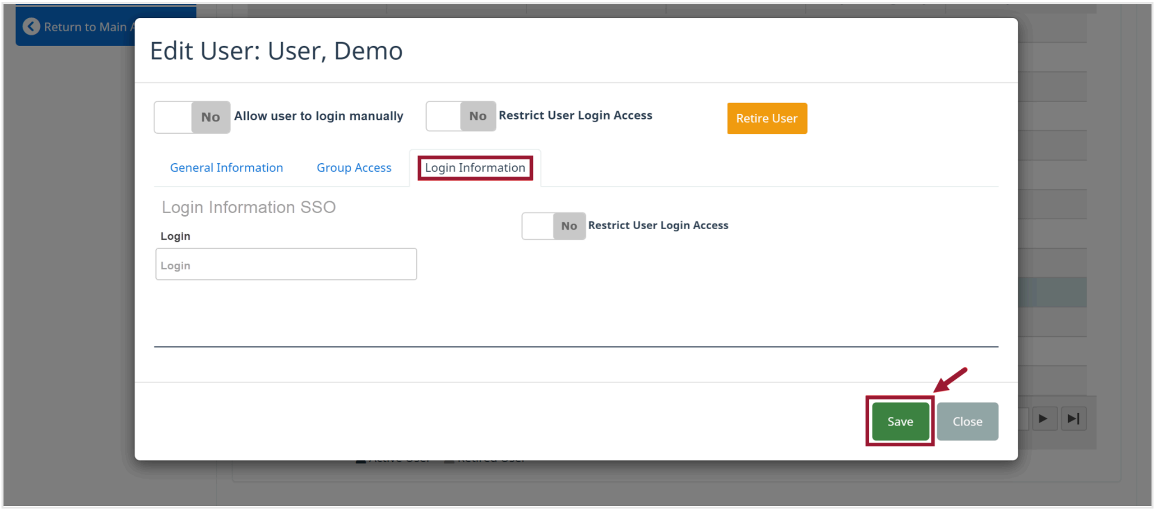
A user who is retired may not log into Guardian; however, their account may be reactivated in the future if needed. To reactivate a user, click the **Re-activate User** button as shown below:



Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Single Sign-On

Note: For organizations using **Single Sign-On** (SSO), the user's SSO ID should be entered into the **Login** field. For users without an SSO ID, enable the *Allow user to login manually* option, and configure the user with a username and password as shown in the previous steps.

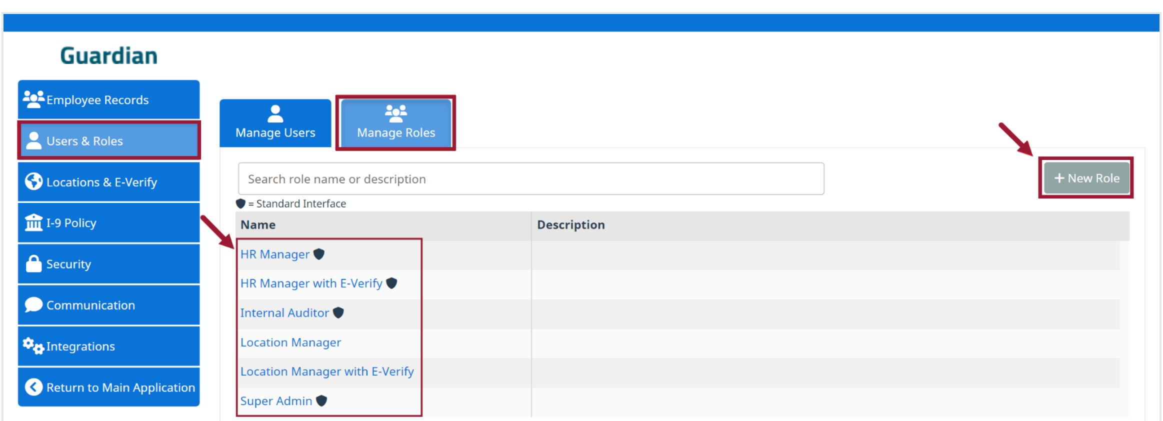


Manage Roles

Roles are sets of security permissions that are assigned to the users to efficiently manage user security in bulk. Guardian comes with six default roles. Organizations may rename the default roles, edit their permission sets, and create additional custom roles as needed.

Roles also determine whether a user will access Guardian through the **Standard Interface** or the **Location Manager Interface**. Roles with a shield next to their name utilize the Standard Interface, and roles without the shield utilize the Location Manager Interface. The interface a role utilizes is dependent on what permissions are enabled for that specific role.

Click a role in the Name column to edit a role's **Name**, **Description** or **Permissions**, or click **New Role** to create a new custom set of permissions.

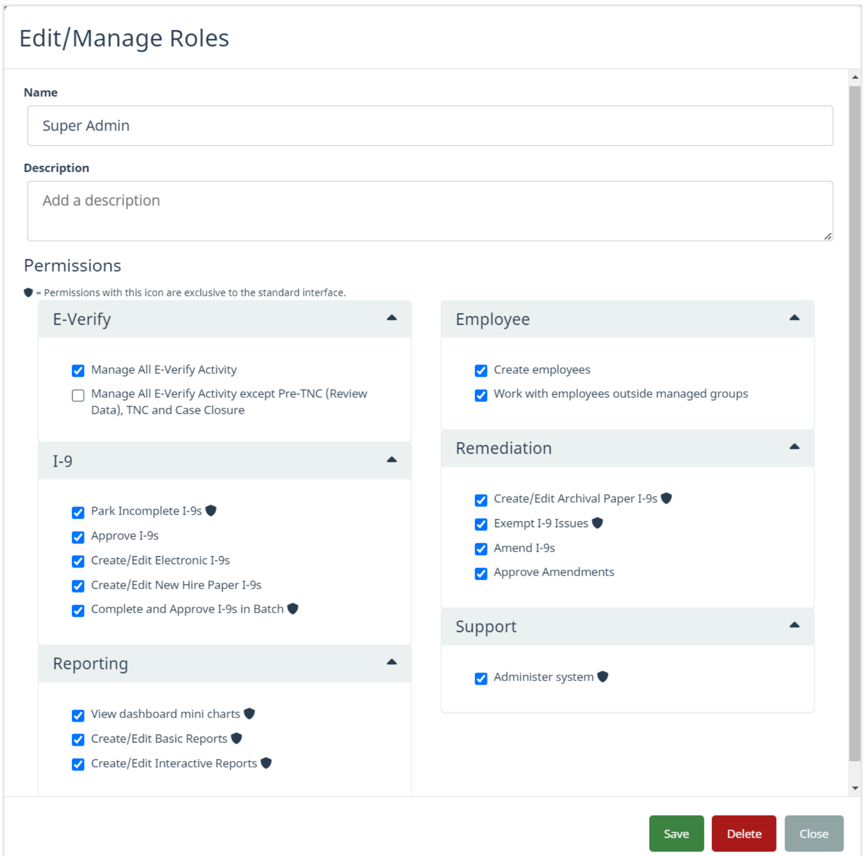


Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Permissions

Guardian provides 20+ separate permissions within a role, allowing for great flexibility in defining security for a variety of user types and responsibilities. Changing the permissions for a role will change the permissions for all users assigned to that role, allowing for efficient security management for organizations with many users.

Permissions with the shield icon identifies a function that is only accessible from the **Standard Interface**. If one or more shield permissions are enabled for a role, all users assigned to that role will be presented with the Standard Interface upon login. If all shield permissions are *disabled*, users assigned to that role will be presented with the **Location Manager** Interface upon login.



Permissions Definitions

E-Verify Permissions

- **Manage E-Verify Cases:** The user is able to access the details of the employee's E-Verify case submitted through Guardian. Additionally, they are able to process and close E-Verify cases, including Tentative Non-Confirmation (TNC).
- **Batch Close E-Verify:** The user may access the Batch Close E-Verify tool to close in bulk those E-Verify cases that returned an Employment Authorized result.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

I-9 Permissions

- **Park Incomplete I-9s:** The user is able to park an I-9 record, thereby locking an incomplete I-9 record. This differs from approval and is used in instances in which the I-9 could not be completed, but must be retained by the organization (in instances in which the new hire is unable to produce the necessary documents for Section 2 completion within three days of hire and is subsequently terminated). This permission does require the associated I-9 Policy to be enabled for the organization.
- **Complete and Approve I-9s in Batch:** The user may access the I-9 Review Queue tool to Complete/Approve I-9s in bulk.
- **Create/Edit Electronic I-9s:** The user is able to work with electronic I-9 records.
- **Create/Edit New Hire Paper I-9s:** The user is able to create I-9s of type "New Hire Paper". This type of I-9 record is used when access to Guardian was not available at the time of hire, and the I-9 was completed using the paper form.
- **Approve I-9s:** The user is able to mark the I-9 Approved, thereby locking the record from further editing, and where applicable, sending the I-9 data to E-Verify (note: the user does not need the Manage E-Verify Case permission to send the data to E-Verify).

Reporting Permissions

- **Create/Edit Interactive Reports:** The user can create, update, and run custom reports.
- **View dashboard mini charts:** The user has access to graphical reports accessible from the dashboard.
- **Access Charts & Graphs:** The user has access to graphical reports.
- **Create/Edit Charts & Graphs:** The user can create, update, and run graphical reports.
- **Access Interactive Reports:** The user has access to dynamic reports.
- **Access Basic Reports:** The user has access to a select list of pre-loaded reports in Guardian.
- **Create/Edit Basic Reports:** The user can create, update, and run the pre-loaded reports.

Employee Permissions

- **Access all employee records:** The user accessing the Standard Interface has access to all employee records regardless of whether the user is assigned to an employee's group.
- **Create employees:** The user accessing the Location Manager Interface has the ability to create new employee records (when they don't already exist).
- **Work with employees outside managed groups:** The user accessing the Location Manager Interface has access to all employee records regardless of whether the user is assigned to an employee's group.

Remediation Permissions

- **Create/Edit Archival Paper I-9s:** The user is able to create I-9's of type "Archival Paper". This type of I-9 record is used to represent historical (existing employee) Forms I-9.
- **Amend I-9s:** The user is able to create amendments for approved I-9 records (of any type). Those using the Location Manager Interface have limited functionality and can only act on pending amendments (fields previously nominated for amendment by a user of the Standard Interface), or when necessary for E-Verify purposes.

- **Approve Amendments:** The user is able to approve amendments, thereby making the change permanent. The amendment approval step is the electronic equivalent of initialing and dating the amendment. The approver's initials and date will appear on the amended I-9 PDF.
- **Exempt I-9 Issues:** The user is able to mark issues found by Guardian as exempt. This feature is primarily used when remediating historical paper I-9 records. Exemption is a form of acknowledgement that no actions will be taken to correct the issue. An exempted issue remains associated with the I-9 record, but is no longer counted in the I-9 issue count.

Support Permissions

- **Administer system:** The user has access to managing the Administration module

This table outlines the various permissions associated with Guardian Roles.

User Permissions	Guardian HR Manager Role ***Contract: Standard User****	Guardian HR Manager with E-Verify Role ***Contract: Standard User****	Guardian Location Manager Role ***Contract: Basic User****	Guardian Location Manager with E-Verify Role ***Contract: Basic User*****	Guardian Super Admin Role ***Contract: Premium User****
E-Verify: Manage E-Verify Case		X		X	X
E-Verify: Manage All E-Verify Activity except Pre-TNC (Review Data), TNC and Case Closure		Can restrict		Can restrict	
I-9: Approve I-9s	X	X	X	X	X
I-9: Create/Edit Electronic I-9s	X	X	X	X	X
I-9: Create/Edit New Hire Paper I-9s	X	X	X	X	X
I-9: Park Incomplete I-9s	X	X			X
I-9: Create/Edit Archival Paper I-9s	X	X			X
I-9: Complete and Approve I-9s in Batch	X	X			X
I-9: Create *Remote Section 1 or Remote Agent I-9*	X	X			X
Reporting: View Dashboard Mini Charts	X	X			X
Reporting: Create/Edit [basic/interative] Reports	X	X			X
Employee: Create Employees	X	X	X	X	X
Employee: Work with employees outside of managed groups	X	X	X	X	X
Employee: Access all employee records	X	X	Limited - PII blocked	Limited - PII blocked	X
Employee: Edit employee record	X	X			X
Employee: View employee record	X	X	Limited - PII blocked	Limited - PII blocked	X
Employee: Terminations, Start Date / Location changes	X	X			X
Remediation: Exempt I-9 Issues	X	X			X
Remediation: Amend I-9s	X	X	Limited - only if action pending	Limited - only if action pending	X
Remediation: Approve Amendments	X	X	Limited - only if action pending	Limited - only if action pending	X
Remediation: Create/Edit Archival Paper I-9s	X	X			X
I-9: Complete I-9s (Section 2s)	X	X	X	X	X
Admins: Can manage user permissions					X
Admins: Can update organization settings					X
Support: Administer System					X

****Standard and Premium Users: may have a set number of users included in some contracts***

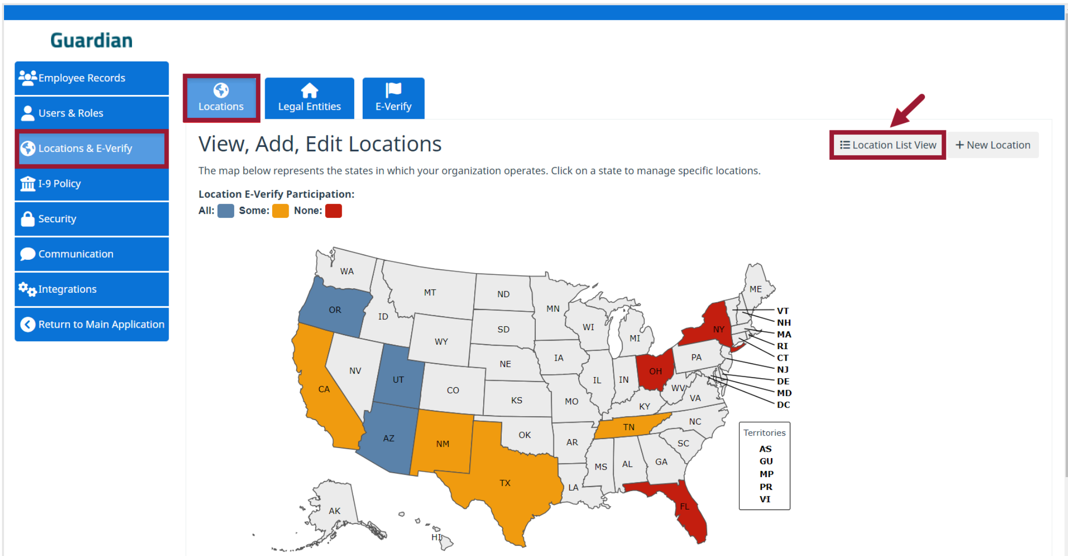
*****Basic Users: may have an unlimited number of users included in some contracts***

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Locations & E-Verify

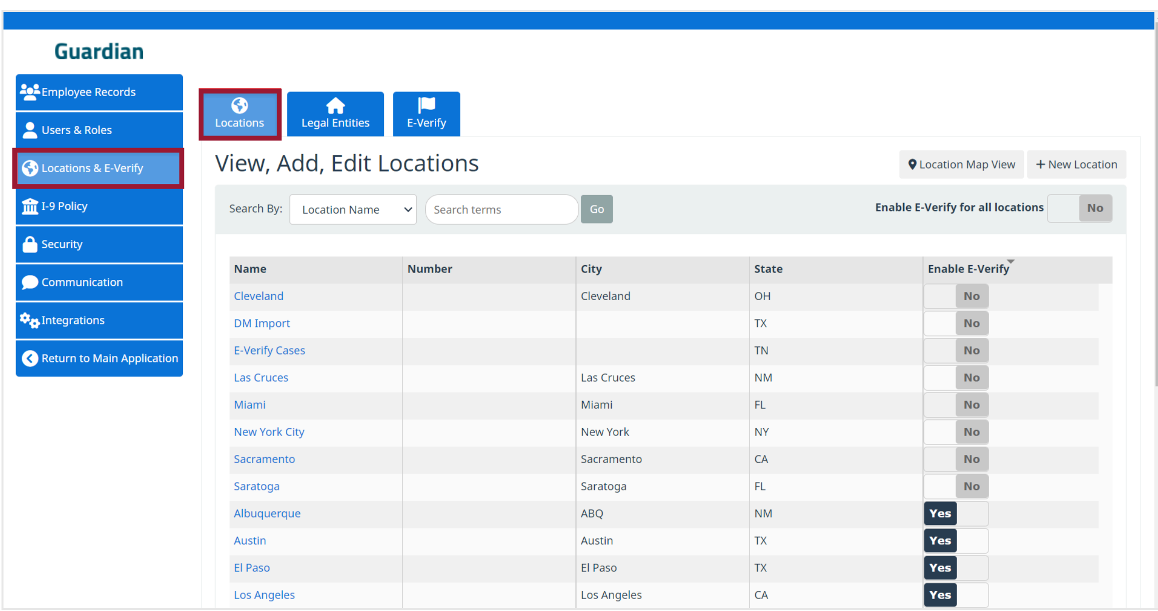
The Locations tab displays your locations and settings for each and allows additions or edits. The default view displays a map of your locations with the following colors:

- **Blue -** All locations in this state participate in E-Verify.
- **Yellow -** Some locations in this state participate in E-Verify, and some do not.
- **Red -** No locations in this state participate in E-Verify.



Location Map View versus Location List View

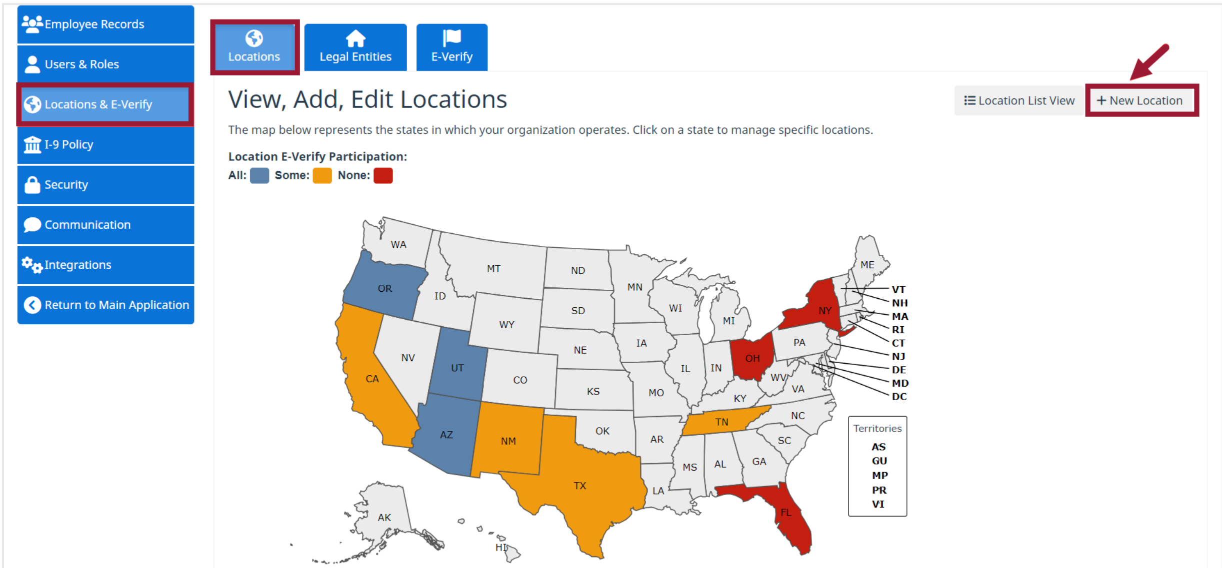
The map view of the locations as shown is the default view for the Guardian locations. To view a list view of the locations, click the **Location List View** button. The List view will then appear as the following:



Images are examples and for information purposes only. They may vary across platforms and are subject to change.

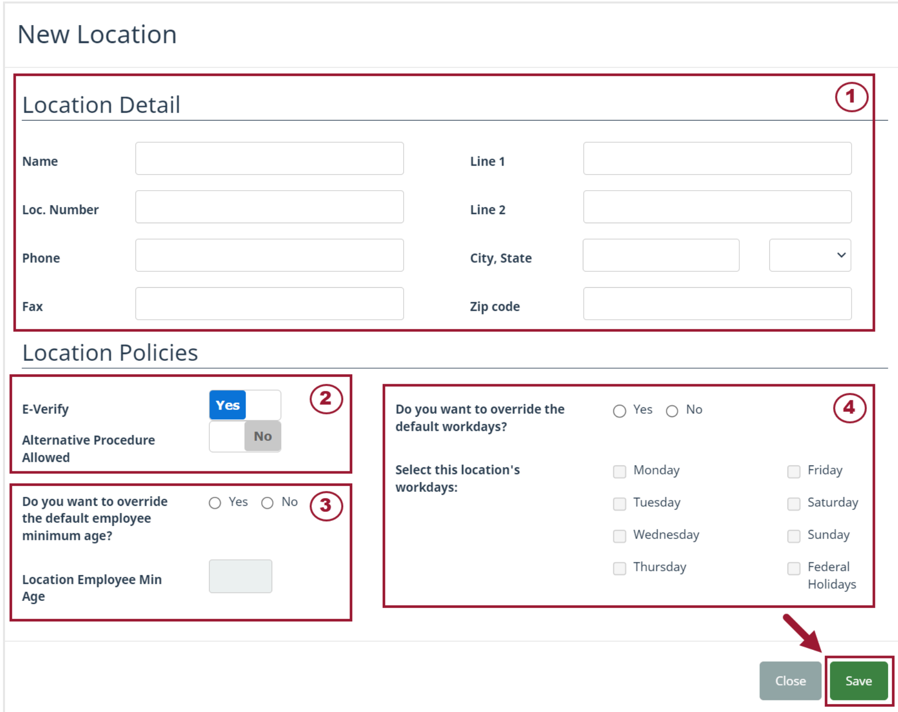
Creating New Locations

Creating a new **location** is the first step in defining a new **Employee Group**. A location is typically the lowest level within your **Group Structure**, and usually represents a physical location, such as a particular store or office building. Click the **+New Location** button (this button will appear on both the **List view** and the **Map view**).



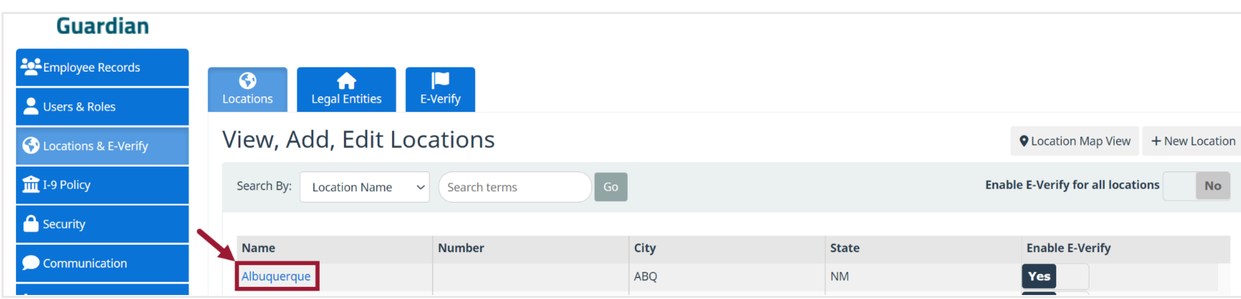
1) Enter a **Name** and **Address** for the location. The **Loc. Number** field is required for certain integrations/data feeds. The Address information will be used to automatically populate the **Section 2 Employer Address**.
2) Specify whether this location participates in **E-Verify**.
   Optionally, specify whether this location will participate in the Alternative Procedure for virtual I-9 completion. (If this is the case, ensure that the Admin setting on the **I-9 Policy > New I-9 Settings** tab **>** *Enable Alternative Procedure to Remotely Examine Documents* is set to **Yes**, as well as ensuring that all other organizational requirements have been met. Please also refer to the **USCIS Remote Examination of Documents** page for other qualifying requirements and more information).
3) If the organization has a default minimum age to work and the age is specified in the **I-9 Policy > New I-9 Settings** tab **>** *Employee default minimum age* field, select **Yes** and enter the minimum hiring age for this location in the field. This will override the global setting. If a new hire's date of birth as entered on Section 1 violates the **Minimum Age** specified in the Admin settings, they will be unable to sign Section 1.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.



4) The **Workdays** setting is used to determine the Section 2 deadline. If the organization has default workdays for this location that differ from other locations, and those workdays are specified in the **I-9 Policy > I-9 Management** tab > *Default Workdays* setting, select **Yes** and enter the workdays for this location. This will override the global setting.
5) When done, click the **Save** button. Guardian will notify you that you must now create one or more **Employee Groups** that incorporate this new location before any new hires can be associated with it. Users can also add locations to an existing group. Refer to the **Adding New Employee Groups** section of this guide for more information on this process.

Viewing and Editing Existing Locations



The View, Add, Edit Locations menu will allow Admins to make changes to the location specifics at any time. This menu will also appear when selecting the location from clicking the **Location Name** link while on the **List view** or by clicking on the colored state on the **Map view**, and then the **Location Name link**.

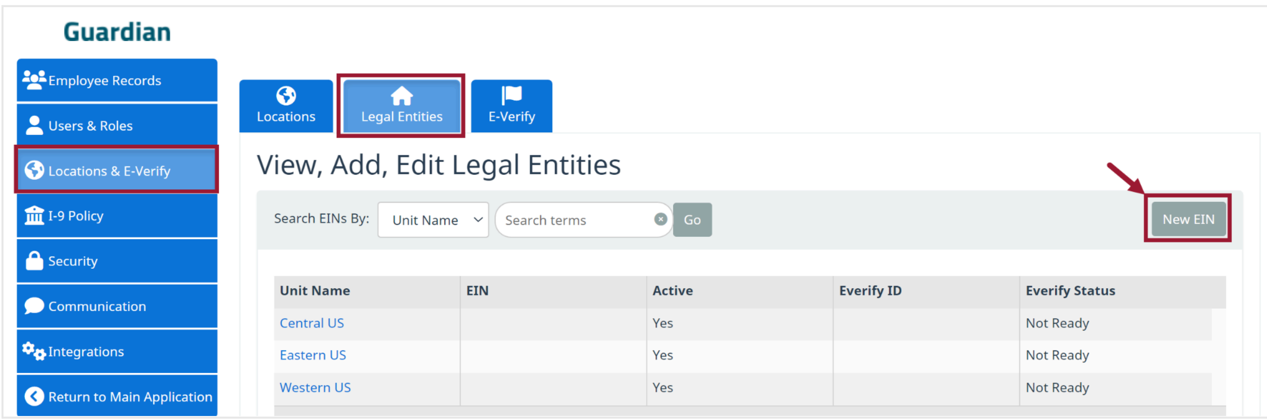
Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Legal Entities

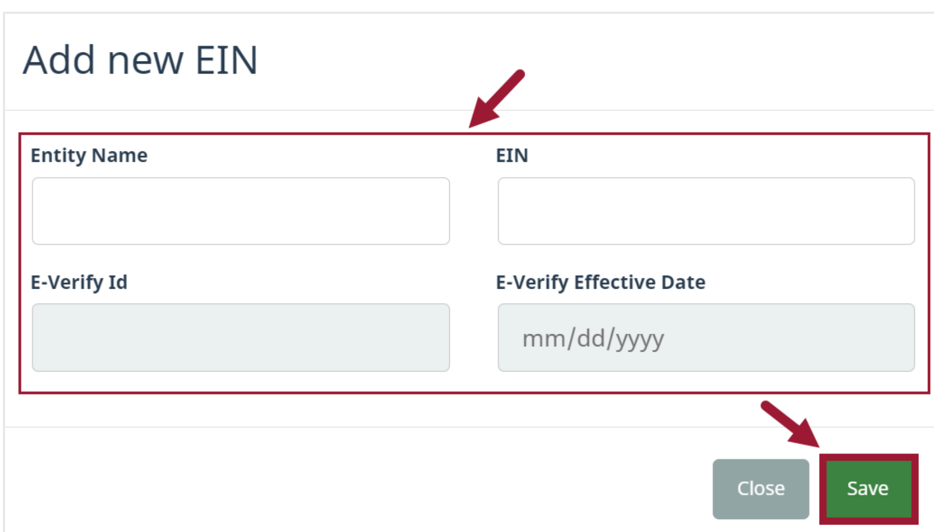
The **Legal Entities** tab displays a list of your organization's legal entities (if applicable). One or more legal entities (aka "*Business Units*") is required for **E-Verify** participation, although organizations not participating in E-Verify may still leverage legal entities for tracking and reporting purposes, if desired. Depending on how your Guardian site was initially configured, legal entities may either be integrated into your **Group Structure**, or may act as a **Custom Field** that is defined separately each time a new employee is created.

Creating New Legal Entities

1) Click the **New EIN** button.



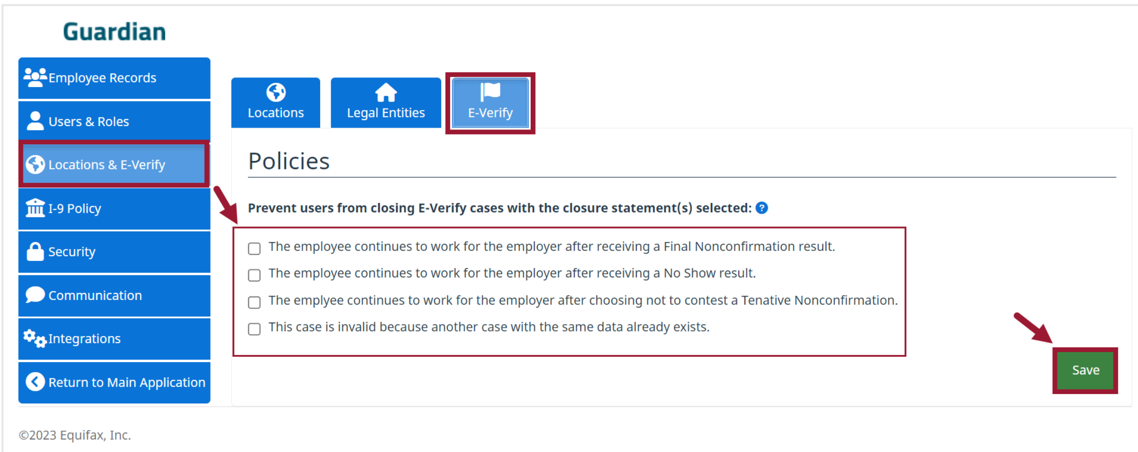
2) Enter the **Entity Name**. If the legal entity participates in E-Verify, also enter the **EIN**, **E-Verify ID**, and **E-Verify Effective Date**. If needed, contact GuardianSupport@equifax.com to enroll the legal entity in E-Verify, which involves generating and signing a new E-Verify Memorandum of Understanding (MOU). Admin users may open a Support Case by clicking the **Help** button in this scenario. Click **Save** when done.



Images are examples and for information purposes only. They may vary across platforms and are subject to change.

E-Verify

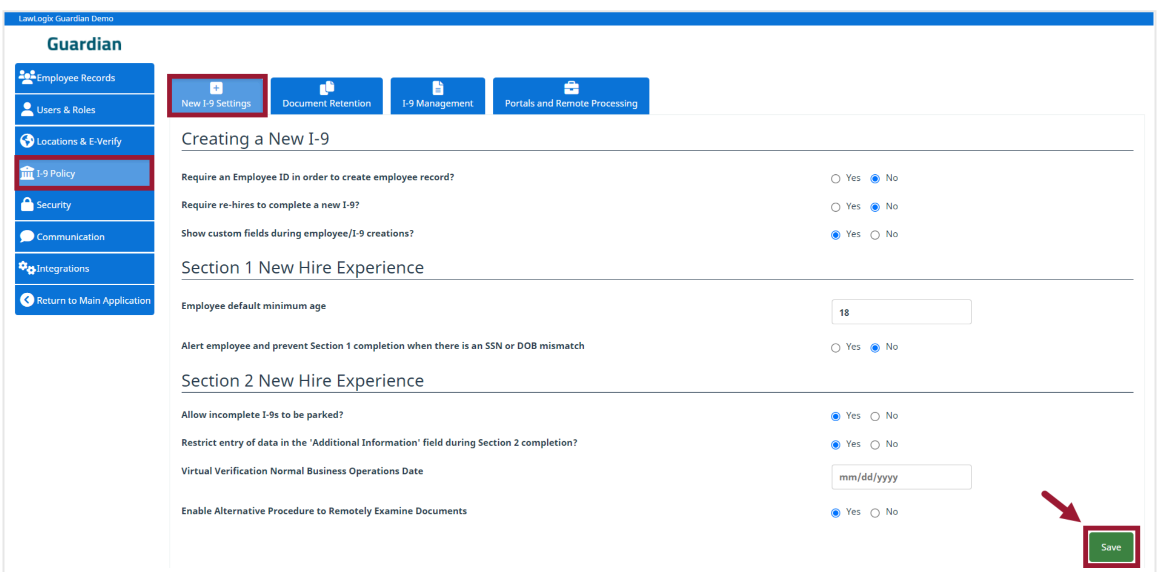
The E-Verify tab contains a group of settings used to hide certain **E-Verify Case Closure Statements**. These particular closure statements are not commonly needed, and are sometimes inadvertently selected by users. If desired, disable one or more to prevent them from being displayed to any user when closing an E-Verify case. The closure statements can be re-enabled in the future. For more information on E-Verify Case Closure Codes, please refer to the E-Verify User Manual.



I-9 Policy

This tab contains settings that impact the overall I-9 experience within Guardian. Organizations may make changes based on their internal policies relating to the I-9 processes and E-Verify.

New I-9 Settings



- **Require an Employee ID to create the employee record:** When yes, employee records cannot be created without an Employee ID.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

- **Require re-hires to complete a new I-9:** When yes, all re-hires must complete a new I-9; completing a Supplement B/Section 3 for rehires is not allowed.
- **Show custom fields during employee/I-9 creations:** When yes, custom fields are displayed on the Start I-9 and Add New Employee pages. Regardless of this setting, custom fields can always be viewed and edited from within an employee record.

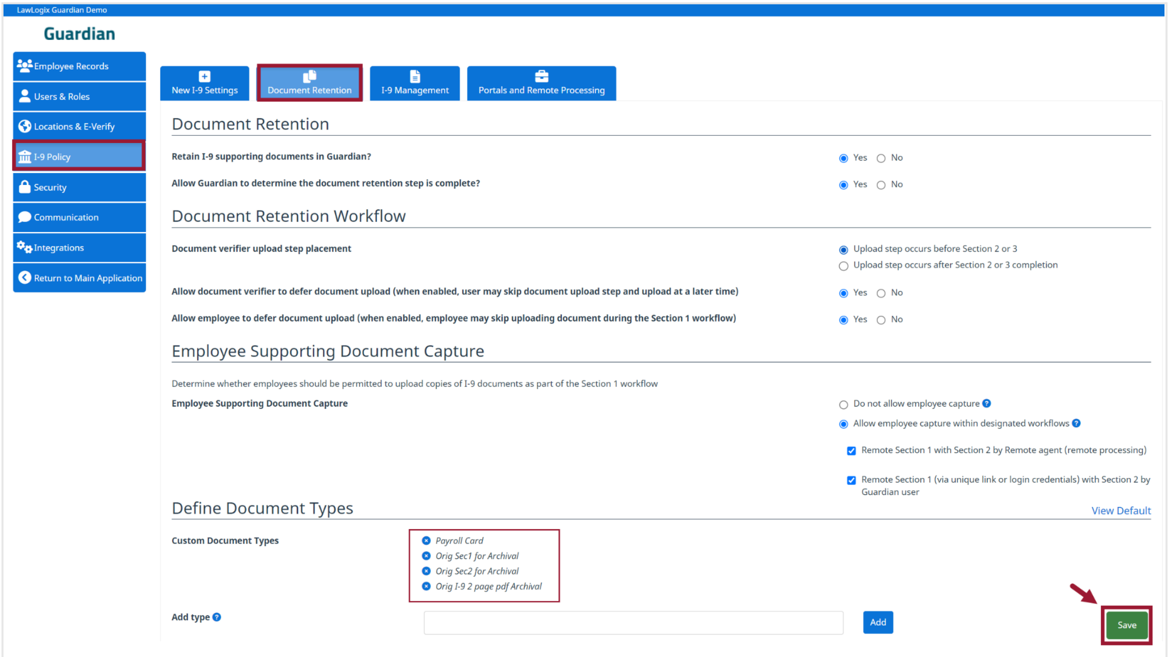
Section 1 New Hire Experience

- **Employee default minimum age:** Date of birth entered in Section 1 will be compared to this policy; Section 1 cannot be completed if the employee is younger than the minimum age requirement.
- **Alert employee and prevent Section 1 completion when there is an SSN or DOB mismatch:** When yes, the SSN and DOB entered in Section 1 are compared to the SSN and DOB values on file in the Guardian employee record. If there is a discrepancy, an error will display during Section 1 processing and prevent electronic signature. Use this option when an external source is the system of record and that record must be resolved prior to I-9 completion.

Section 2 New Hire Experience

- **Allow incomplete I-9s to be parked:** When set to **Yes,** an incomplete I-9 can be 'Parked' or saved in the incomplete status for future reference. Once Parked, the I-9 can't be modified, amended, or used again. Use this option if an employee cannot produce Section 2 documents within three days, and is terminated. ***Note:*** global setting. If this is enabled, the user must have the associated **Role Permission** to leverage this feature.
- **Restrict entry of data in the 'Additional Information' field during Section 2 completion?:** When enabled, users are unable to enter information into the Section 2 'Additional Information' field of an electronic I-9. System generated information will continue to populate.
- **Virtual Verifications Normal Business Operations Date:** When a date is present, I-9s flagged for 'virtual verification' during the Temporary Flexibility of Form I-9 Requirements Related to COVID-19 for Remote Employees that was available from 03/20/2020 to 7/31/2023.
- **Enable Alternative Procedure to Remotely Examine Documents:** When enabled, E-Verify locations may be updated to allow the alternative document examination method for I-9s and reverifications.

Document Retention



- **Retain I-9 supporting documents in Guardian?:** When yes, Guardian will prompt users to upload a copy of all Section 2 supporting documents used to complete an employee's Form I-9. When no, Guardian will only prompt for retention of documents required by E-Verify (if participating).
- **Allow Guardian to determine the document retention step is complete?:** When yes, Guardian determines when document retention requirements have been met rather than the user manually confirming via the checkbox.

Document Retention Workflow

- **Document verifier upload step placement:** Admins will choose whether the document upload step for the verifier occurs **before** Section 2 or Supplement B/Section 3 completion, or, if the document upload step for the verifier should occur **after** Section 2 or Supplement B/Section 3 completion.
- **Allow document verifier to defer document upload** *(when enabled, user may skip document upload step and upload at a later time):* When set to Yes, the user may opt not to upload supporting documents during workflow step and upload documents at a later time.
- **Allow employee to defer document upload** *(when employee may skip uploading document during the Section 1 workflow):* When set to Yes, the employee may opt to not upload supporting documents during the Section 1 workflow.

Employee Supporting Document Capture

Admins will choose the appropriate settings to determine whether employees should be permitted to upload copies of I-9 documents as part of the Section 1 workflow by selecting one of the following:

1. Do not allow employee capture **- OR -**
2. Allow employee capture within designated workflows

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

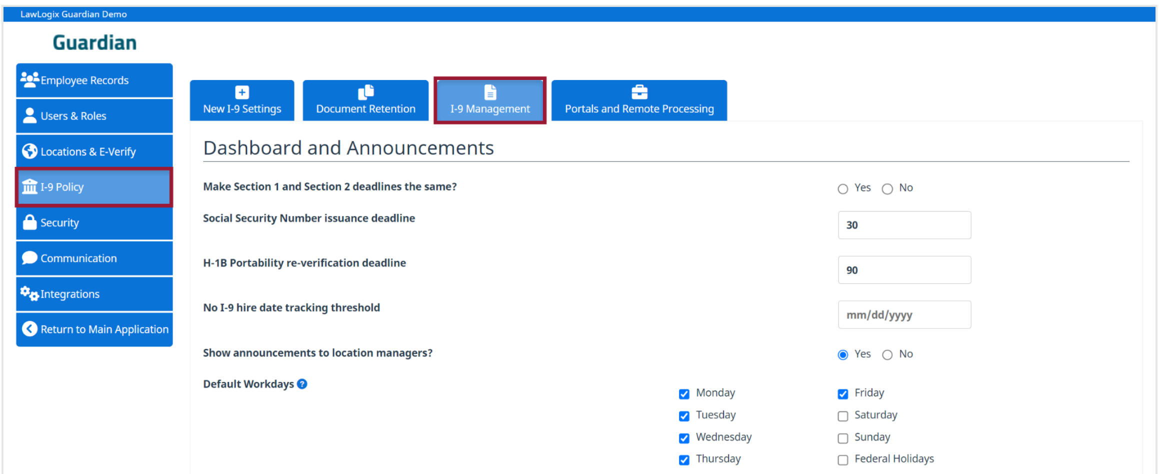
Admins will then choose one of the following depending on the workflow:

- Remote Section 1 with Section 2 by Remote Agent (remote processing).
- Remote Section 1 (via unique link or login credentials) with Section 2 by Guardian user.

Define Document Types

- **Custom Document Types:** Add customized document type names. These are used within the employee record as file references for uploaded documents. Custom document names will be available choices in addition to the system defaults. Click the **Add** button to add the 'type' and enter the custom name of the document in the field. *(The document names shown are samples only).*

I-9 Management



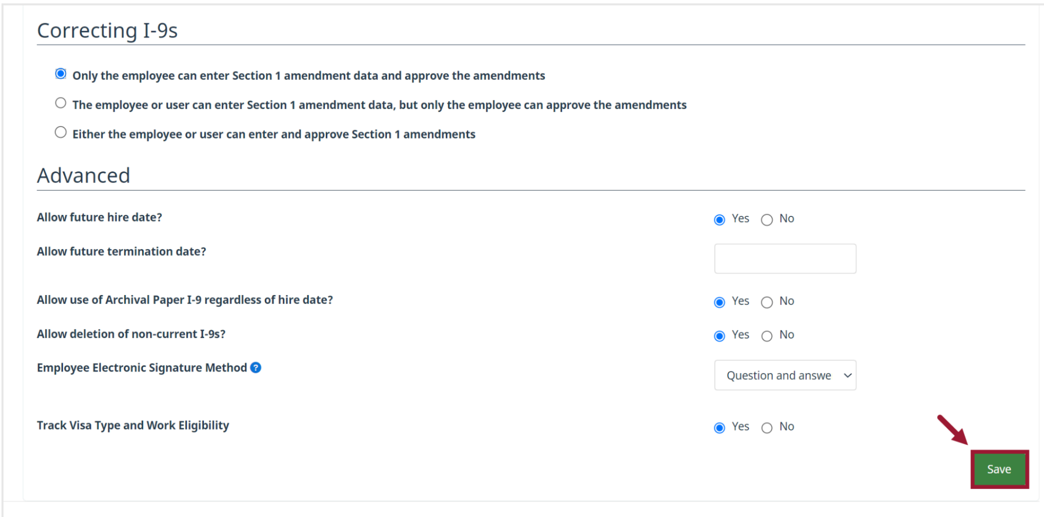
Dashboard and Announcements

- **Make Section 1 and Section 2 deadlines the same:** When yes, the Section 1 deadline will also be used as the Section 2 deadline for the "Top Pending I-9s" dashboard panel.
- **Social Security Number issuance deadline:** E-Verify employers are required to include the employee's Social Security Number in Section 1. When the SSN is not available at hire, the value entered in this field is used to determine a deadline/tickler to follow-up with the employee to update the Section 1 SSN field. The reminder will be determined based on the hire date plus the defined value, and the derived deadline will appear in the "Top I-9s Needing Further Action" dashboard.
- **H-1B Portability re-verification deadline:** Used when foreign national H-1B holders can start work for a new employer once USCIS has received the H-1B transfer petition. When this situation is true, the value entered in this field is used to determine the deadline/tickler to follow-up on the I-129 petition approval and reverification.
- **No I-9 hire date tracking threshold:** Employees with a hire date on or before the date specified will not be reported on the "Employees without I-9" dashboard, and will not generate similar notifications. This can be useful if an organization has imported employee record data, but has yet to import the associated I-9 records. In that event, this setting helps keep the users focused on processing Form I-9 for new hires.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

- **Show announcements to location managers:** When yes, the Announcement module will be visible in the Location Manager Interface.
- **Default Workdays:** Regulations require your organization to process I-9s in a timely manner. The “Three Day Rule” is dependent upon the actual days of the week your organization is open and doing business. Indicate when the organization is conducting business by checking the days of the week business is conducted. Select the “Federal Holidays” option if your business is open on federal holidays as well.

Correcting I-9s & Advanced

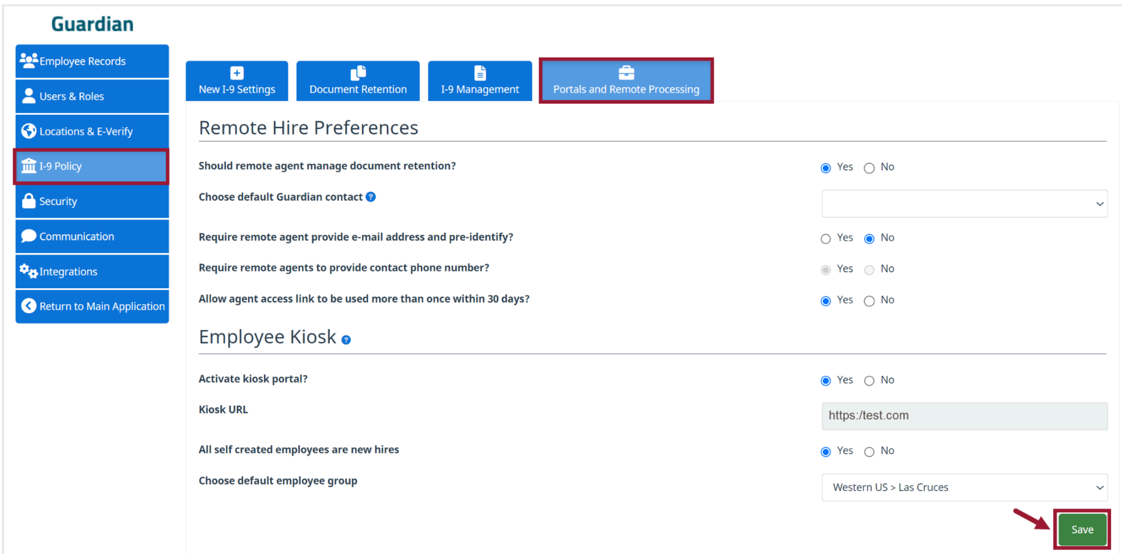


- **Only the employee can enter Section 1 amendment data and approve the amendments:** When selected, only the employee can enter amendment values for Section 1 and approve the changes *(Note: a user will first designate which fields the employee is to correct).*
- **The employee or the user can enter Section 1 amendment data, but only the employee can approve the amendments**: When selected, either the employee or HR user can enter amendment values for Section 1, but only the employee can approve the changes *(Note: a user will first designate which fields the employee is to correct).*
- **Either the employee or the user can enter and approve Section 1 amendments:** When selected, either the employee or HR user can enter amendment values for Section 1 and approve the changes.
- **Allow future hire date:** When yes, the users will be able to create employees with hire dates in the future.
- **Allow future termination date:** If you wish to allow future termination dates, enter the maximum number of days into the future allowed. Leave value of zero to not allow future termination dates.
- **Allow use of Archival Paper I-9 regardless of hire date:** When yes, the users will be able to enter archival paper I-9 records for employees with a start date up through the current date.
- **Allow deletion of non-current I-9s:** When yes, Admin users can delete I-9 records that are not marked as the ‘primary’ (current) I-9.
- **Employee Electronic Signature Method -** Admins will choose one of the two signature options:
  - **Question and answer:** Employee provides a memorable response to one of the questions

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

from a set of system-provided questions. Responses are not validated, and Guardian will never prompt an employee to recall the details of a previous electronic signature. Responses are logged in the audit trail in the event such information is requested by an auditor.
    - **Employee-generated PIN:** Employee provides a numeric PIN of at least 4 digits long.
- **Track Visa Type and Work Eligibility:** When yes, users are able to capture within the I-9 workflow, class of admissions and employment authorization category information for employees with temporary work authorization.

Portals and Remote Processing



Remote Hire Preferences

- **Should remote agents manage document retention:** When yes, the remote agent will be prompted to retain I-9 supporting documents in one of the manners defined in the "Remote Hire Document Retention Options" section.
- **Choose default Guardian contact:** Select a system user to be the default contact for the remote agent I-9 workflow. Contact information will be provided to the employee and Remote Agent in the event of questions. A contact **must** be defined to create I-9's and instructions for remote processing.
- **Require remote agent to provide e-mail address and pre-identify:** When yes, the Remote Agent must pre-identify before accessing a remote I-9 record, including providing his/her name, title, and email address. An access code is sent to the email address provided and used by the agent to gain access to the portal.
- **Require remote agents to provide contact phone number:** When yes, in addition to providing his/her name, title, and email, the Remote Agent must provide a telephone number.
- **Allow agent Access Link to be used more than once within 30 days?:** When yes, the agent may use the provided link more than once to access Guardian and complete the assigned task.

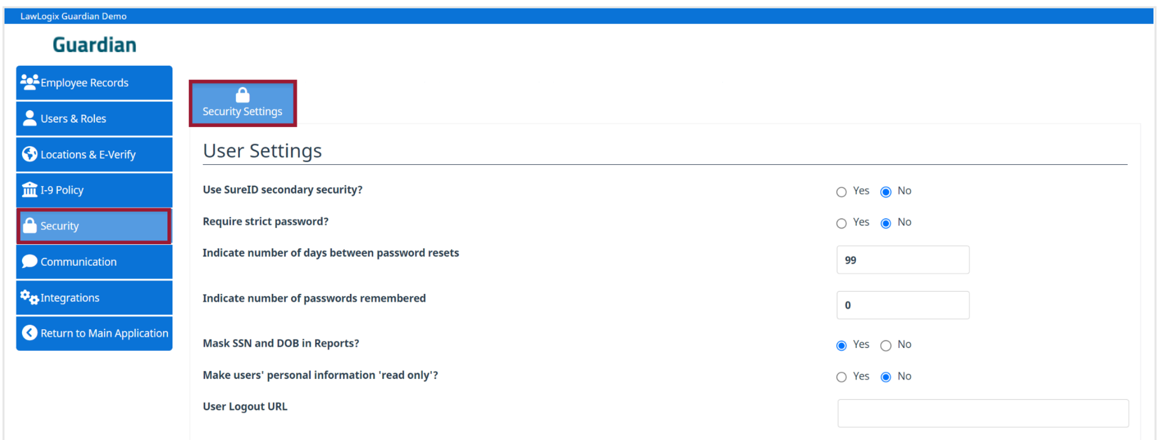
Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Employee Kiosk

- **Activate kiosk portal:** This feature provides a method for employees to "self-create" their I-9 and/or complete Section 1 by accessing a static, organization-specific URL.
- **All self-created employees are new hires:** When yes, if the new hire is eligible for E-Verify based on the kiosk default(s) then Guardian will require that the employee provide his/her Social Security Number in Section 1.
- **Choose default employee group:** If the Kiosk has been activated, select the employee group that self-created employees will be initially assigned to by default.

Security

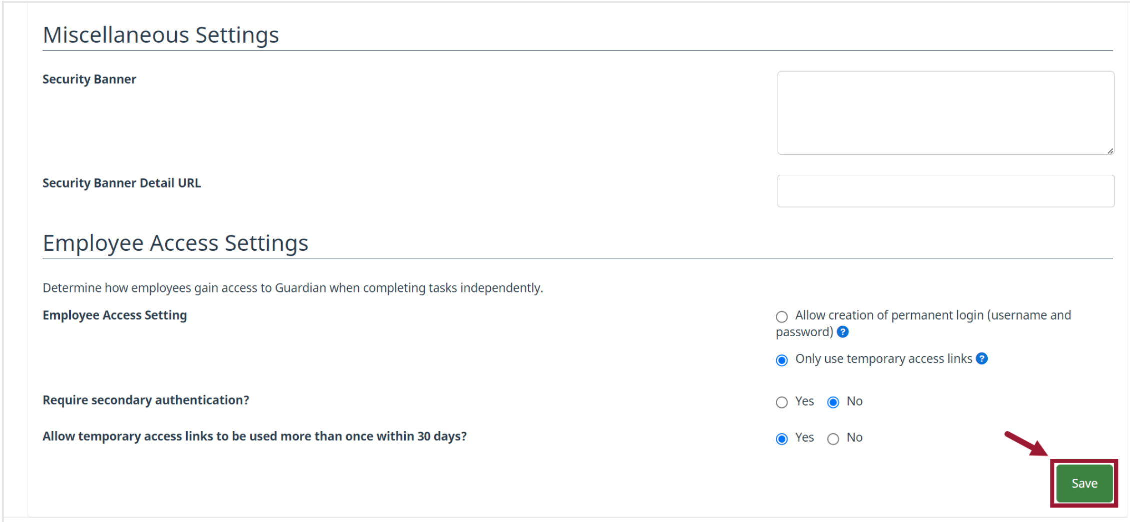
This tab contains a variety of security settings, such as password requirements, privacy settings, and security messages.



User Settings

- **Use SureID secondary security:** When yes, secondary authentication will be activated for HR users. Users define three unique faces from a set of 16. For each successive login, after providing login credentials, users must successfully select the three defined faces from a group in order to gain access to Guardian. The order of the faces are randomized during each login attempt.
- **Require strict passwords:** When yes, passwords must contain: one upper case letter, one lower case letter, one number, one special character, and be at least eight characters in length.
- **Indicate number of days between password resets:** Specify the number of days between requiring users to reset their password. Leave the field blank to not require password resets.
- **Indicate number of passwords remembered:** If requiring password resets, indicate how many prior passwords will be remembered. Passwords cannot be reset to any remembered passwords previously used.
- **Mask SSN and DOB in Reports:** When yes, Social Security Number and date of birth values are masked in reports. Data will appear as ***-**-#### and **/**/yyyy, respectively.
- **Mark users' personal information 'read only'?:** When yes, users are unable to edit information in their user profile, such as name and email.
- **User Logout URL:** Enter the URL users will be directed to after system logout. The URL must be complete, starting with 'http://' or 'https://'.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.



Miscellaneous Settings

- **Security Banner:** This short message will appear on the user interface (at the top of the screen).
- **Security Banner Detail URL:** If **Security Banner** is enabled, optionally enter a link to the organization's full Security Information page. Must start with 'http://' or 'https://'.

Employee Access Settings

This section allows Admins to determine how employees gain access to Guardian when completing tasks independently.

- **Employee Access Setting:** Select one of the below options to determine how employees (new hires, non users) will access Guardian to complete Section 1 and perform other I-9 related tasks.
    - **Allow creation of permanent login** (username and password)
    - **Only use temporary access links**
    - **Allow temporary links to be used more than once:** (Choose Yes or No). If using the **temporary access link** method, this setting allows access links to be used more than once (links will expire after 30 days).

Secondary Authentication

Whenever an Employee, Remote Agent, or HR uses a one-time access link, **Secondary Authentication** is required, simplified and replaces previous security options. **All** of the questions below for which the answers have been entered in Guardian will be presented to the user to confirm their identity. ***Note:*** If none of the choices below have data in the system the user will not be able to access the system.

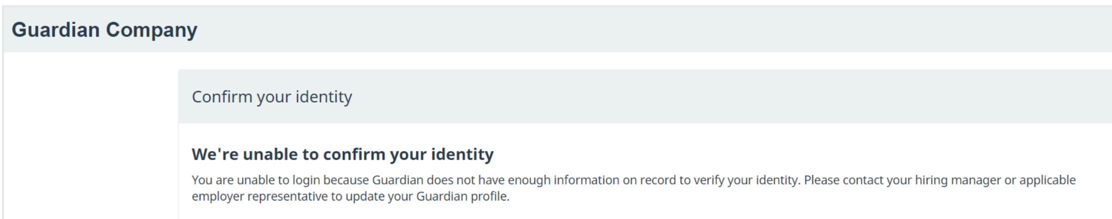
If only one challenge question has a known answer, the user must answer it correctly. Guardian will require at least two questions to be answered when there are at least three known answers. Having four or more known questions will make it easier for the user to authenticate in the event the system has incorrect values stored.

- What is the zip code of your home address?
- What is your 10-digit home phone number (###) ###-####?

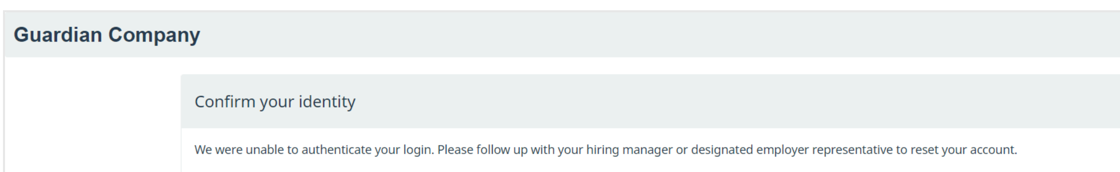
Images are examples and for information purposes only. They may vary across platforms and are subject to change.

- What is the employee ID that you were issued?
  - Include this question? (will not be included unless checked)
    ***Note*:** Some employees may not have their employee ID number in advance of hire.
- What is the name of the city of your home address?
- What are the last 4 digits of your Social Security Number?
- What is your date of birth (mm/dd/yyyy)?
- What is your last name (family name)?

If the employee does not have the necessary information on file for at least one of the chosen authentication questions, they will be unable to access their I-9 and will receive the notification when attempting to log in.

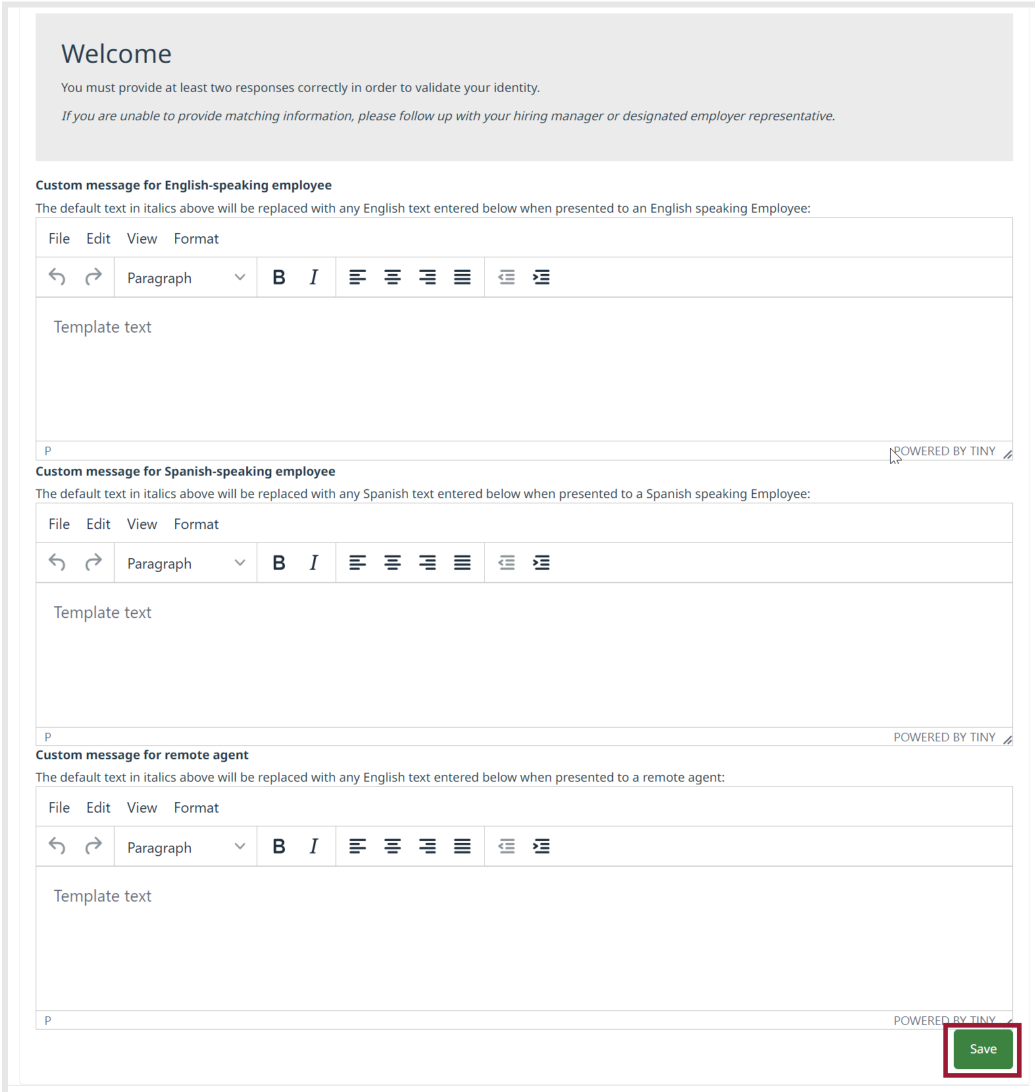


If an employee fails the secondary authentication questions five times in a row, their login will be disabled, and they will receive the below notification. In that event, a user will need to navigate to the **Login Info** tab of their employee record and create a new login for the employee. A new login link will be generated, and the previous one will be disabled.



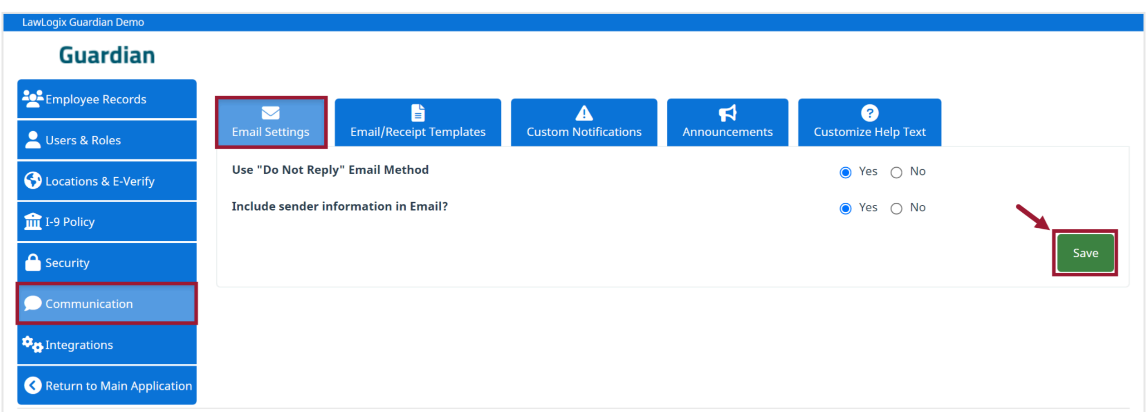
Custom Messages for English- or Spanish-speaking employees
Admins may enter custom text in each of the fields to replace the **default text** that appears in the top gray banner reading: *"If you are unable to provide matching information, please follow up with your hiring manager or designated employer representative".* The options include the Remote Agent workflow. Click the **Save** button after entering any desired custom text:

Images are examples and for information purposes only. They may vary across platforms and are subject to change.



Communication

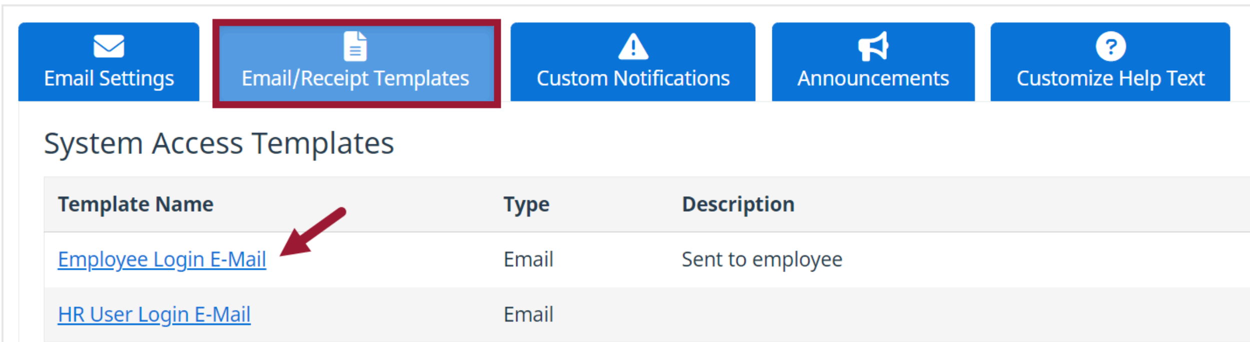
This tab allows for the customization of various system-generated messages, such as emails to new employees or users, notification emails concerning I-9 deadlines, custom announcements to system users, and the help text found throughout the system and the Form I-9 itself.



Images are examples and for information purposes only. They may vary across platforms and are subject to change.

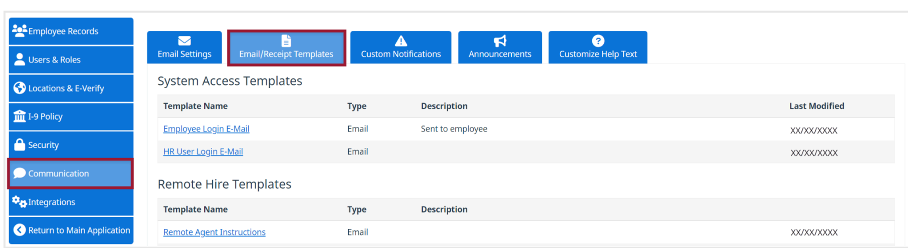
Email Settings

- **Use "Do Not Reply" Email Method:** When yes, all emails sent to the users and employees will have a from address of donotreply@lawlogix.com. When no, the From address will appear as the Guardian user who initiated the email (known as "Email spoofing"), allowing for the recipient of the email to directly reply to the sender.
- **Include sender information in Email?:** If using the "**Do Not Reply**" method, include the following line at the top of emails: *"Please Note: This E-Mail was sent by [User]. Please do not reply to this email as this mailbox is not monitored. To respond to this message please send an email to [User's Email Address]".*



Email/Receipt Templates

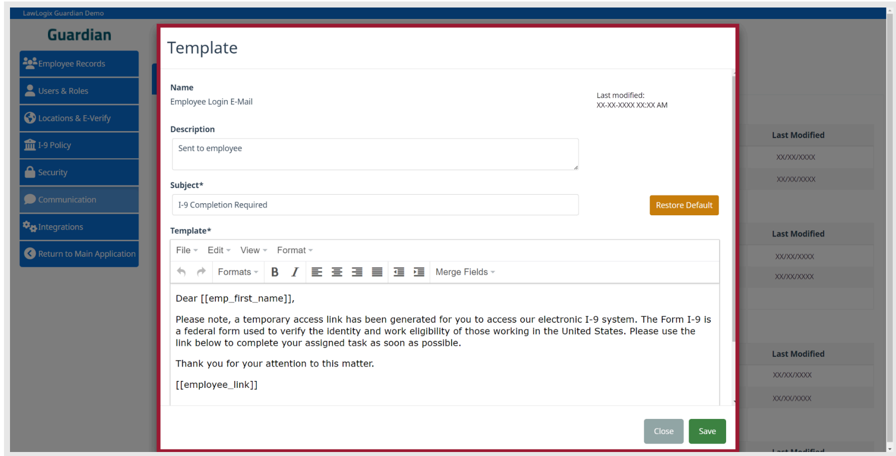
Guardian may send emails to employees and Guardian users at various stages of the Form I-9 and E-Verify workflow, such as the email containing a person's login information to Guardian.
There are also two "receipts" generated for new hires completing Section 1 remotely, or in the event a preparer/translator was used to assist an employee with Section 1. Use this tab to customize these various email and receipt templates.



Editing Email/Receipt Templates

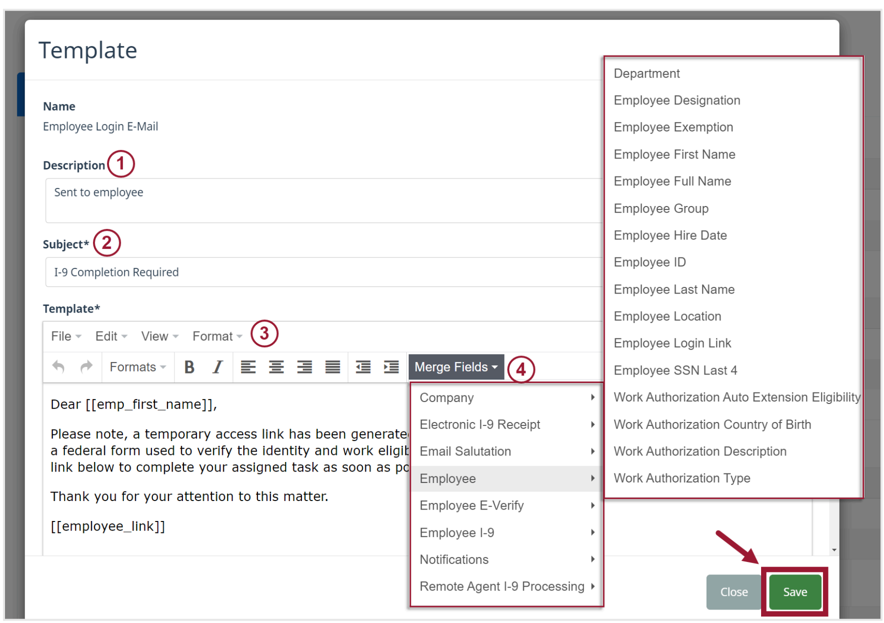
Click the **Template Name** for the template you want to edit.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.



Use the provided template editor to make any desired changes.

1. **Description** visible on the **Email/Receipt Templates** tab within the **Admin** area.
2. **Subject** line of the email.
3. **Text Editor tools**, such as bold, italic, text alignment, and bulleted and numbered lists.
4. **Merge Fields**, information of Guardian field. **Custom Fields** will also be available here.



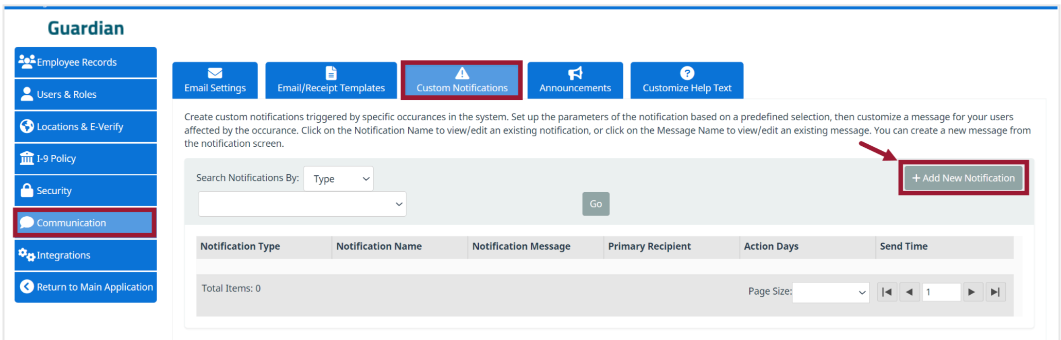
Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Custom Notifications

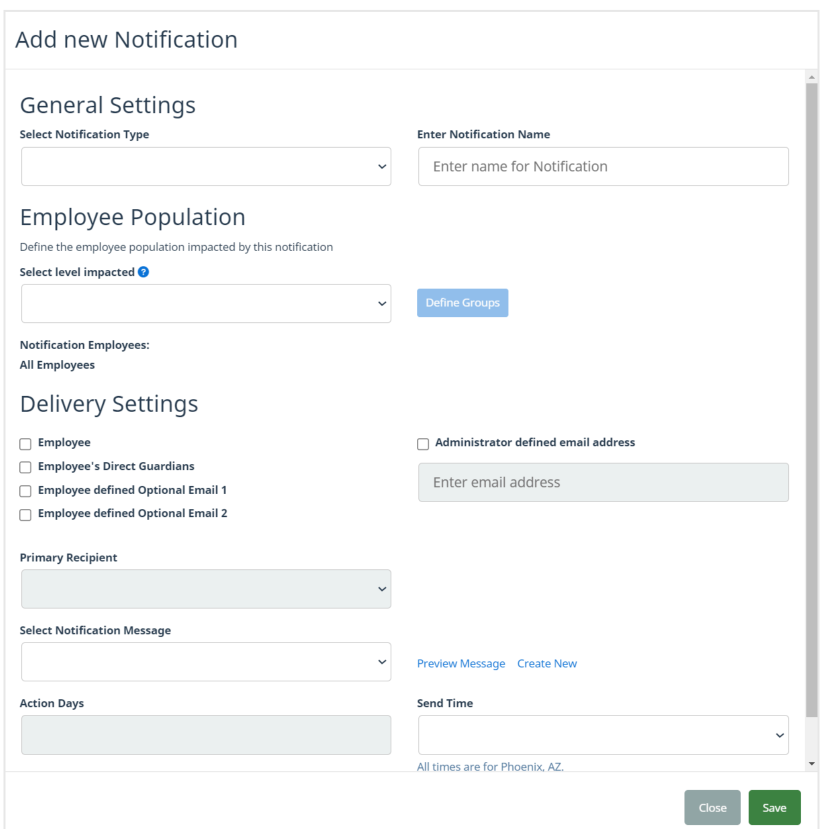
This tab allows for the creation of custom notification emails that are automatically triggered by specific occurrences in the system, such as an approaching I-9 deadline. By default, none of the available notification types are enabled. An organization may choose to use none, some, or all of the available notification types. Use this tab to create the notifications as desired by your organization, specify which employee populations a notification may trigger for, and who will receive the notification emails.

Creating Custom Notifications

Click the **Add New Notification** button.



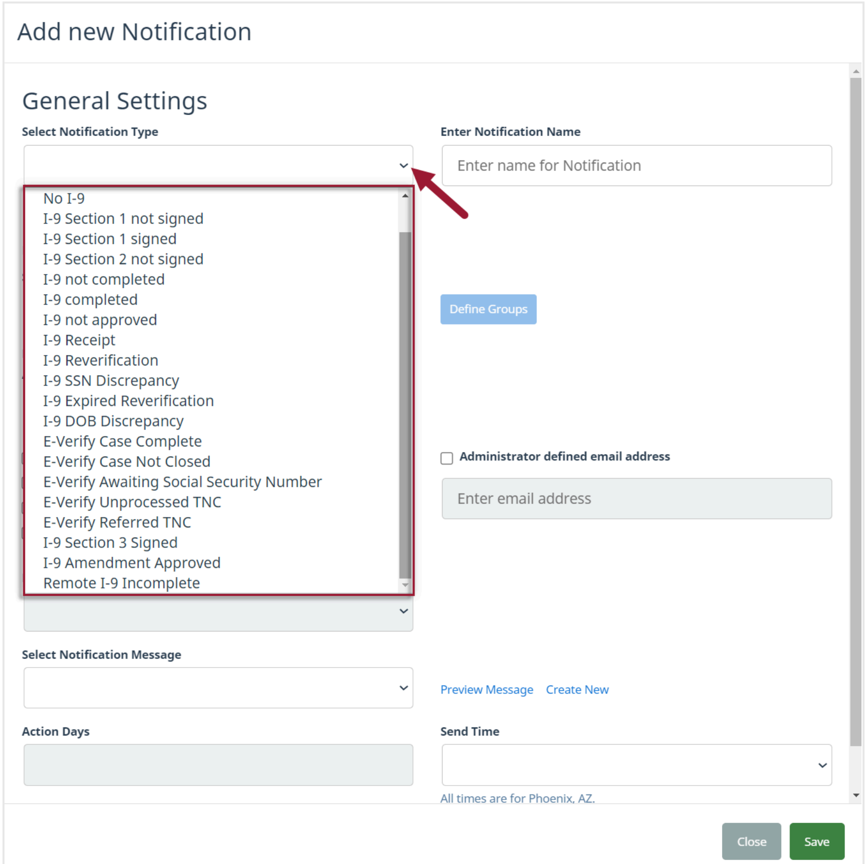
The **Add new Notification** menu will appear.



Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Notification Types

In the General Settings section, choose the **Notification Type**.



Notification Types:

- **No I-9:** Employee records created after advanced notifications have been configured trigger a notification on the employee hire date. If the employee hire date is in the past then a notification will trigger 30 minutes after record creation, or at the scheduled notification time, whichever is later. Subsequent notifications are generated daily until the I-9 record has been created. If the employee hire date is changed after record creation, then the rule is re-evaluated and the notification prepared for the updated hire date. If the hire date is advanced to the future, then a notification is sent only after that date is reached.
- **I-9 Section 1 not signed:** Electronic and New Hire Paper I-9 records that have been created, and Section 1 has not been signed trigger a notification on the I-9 hire date. If the employee hire date is in the past, then a notification will trigger 30 minutes after I-9 record creation, or at the scheduled notification time, whichever is later. Subsequent notifications are generated daily until Section 1 has been signed. If the I-9 hire date is changed after I-9 creation, then the rule is re-evaluated and the notification prepared for the updated I-9 hire date. If the I-9 hire date is advanced to the future, then a notification is sent only after that date is reached. If Section 1 is un-signed, then the rule is re-triggered and a notification sent 30 minutes after un-signing, or at the scheduled notification time, whichever is later.
- **I-9 Section 1 signed:** This event type is a one-time immediate event that triggers after the employee has signed Section 1.

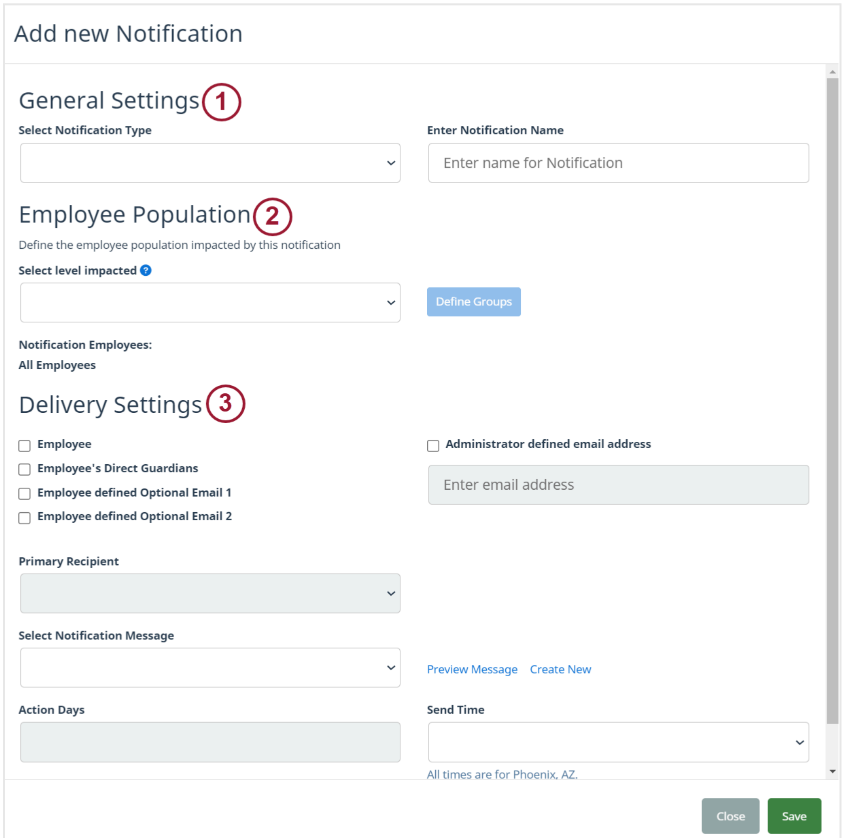
Images are examples and for information purposes only. They may vary across platforms and are subject to change.

- **I-9 Section 2 not signed:** Electronic and New Hire Paper I-9 records that have been created, and Section 2 has not been signed trigger a notification on the hire date, 30 minutes after Section 1 has been signed, or at the scheduled notification time, whichever comes first. Subsequent notifications are generated daily until Section 2 has been signed. If the I-9 hire date is changed after I-9 creation, then the rule is reapplied and the notification prepared for the updated I-9 hire date. If the I-9 hire date is advanced to the future, then a notification is sent only after that date is reached. If Section 2 is un-signed, then the rule is re-triggered and a notification sent 30 minutes after un-signing, or at the scheduled notification time, whichever is later.
- **I-9 not completed:** Electronic and New Hire Paper I-9 records that have been created, Section 2 signed, and the I-9 has not been marked “Completed” trigger a notification on the hire date, 30 minutes after Section 2 has been signed, or at the scheduled notification time, whichever is later. Subsequent notifications are generated daily until the I-9 has been marked completed. If the I-9 hire date is changed after I-9 creation, then the rule is reapplied and the notification prepared for the updated I-9 hire date. If the I-9 hire date is advanced to the future, then a notification is sent only after that date is reached.
- **I-9 completed:** This event type is a one-time immediate event that triggers after the I-9 is completed.
- **I-9 not approved:** Electronic and New Hire Paper I-9 records that have been created, marked completed, but the I-9 record has not been marked “Approved” trigger a notification on the hire date, 30 minutes after the record has been marked completed, or at the scheduled notification time, whichever is later. Subsequent notifications are generated daily until the I-9 has been marked approved. If the I-9 hire date is changed after I-9 creation then the rule is reapplied and the notification prepared for the updated I-9 hire date. If the I-9 hire date is advanced to the future then a notification is sent only after that date is reached.
- **I-9 Receipt:** Electronic and New Hire Paper I-9 records that have been created, a receipt for lost, stolen, or replacement document noted in Section 2, and the I-9 has been marked completed trigger a notification at the time (number of days prior to the needed receipt update) specified by the organization. Subsequent notifications are generated based on the organization’s notification setup (i.e. additional notifications will trigger at the intervals designated by the organization’s alert rule). If the I-9 hire date (and I-9 receipt expiration date) is changed after the I-9 was marked completed then the rule is re-applied and the notification prepared for the updated receipt expiration date.
- **I-9 Reverification:** Approval of Electronic, New Hire Paper, and Archival Paper I-9 records in which an I-9 expiration date for the employee’s work authorization exists, or the changing of the I-9 expiration date for an approved I-9 (reverification) trigger a notification at the time (number of days prior to the needed update) specified by the organization. Subsequent notifications are generated based on the organization’s notification setup (additional notifications will trigger at the intervals designated by the organization). If the I-9 expiration date changes (reverification), then the rule is reapplied and the notification prepared for the updated expiration date. The field 'Action Days' should be configured in ascending order starting with the earliest number of days prior to expiration to be notified. Separate each numeric value with a comma, 90, 60, 45, 30, 15. To trigger a notification on the date of the work authorization expiration, enter the value '0' in the 'Action Days' field.

- **I-9 SSN Discrepancy:** Signing of Section 1 of Electronic and New Hire Paper I-9 records in which the Social Security Number entered in Section 1 is different, than the Social Security Number documented within the employee's Personal tab (when present) triggers a notification 30 minutes after signing, or at the scheduled notification time, whichever is later. This notification type is exempt from the employee re-evaluation method.
- **I-9 Expired Reverification:** Approved Electronic, New Hire Paper, and Archival Paper I-9 records in which the I-9 expiration date has now passed triggers a notification when the expiration date has passed. Subsequent notifications are generated daily thereafter until the I-9 is updated with a new expiration date or the need for reverification ends (foreign national changes status). If the I-9 expiration date changes (reverification), then the rule is reapplied and the notification prepared for the updated expiration date.
- **I-9 DOB Discrepancy:** Signing of Section 1 of Electronic I-9 records in which the date of birth entered in Section 1 is different, than the date of birth documented within the employee's Personal tab (when present) triggers a notification 30 minutes after signing, or at the scheduled notification time, whichever is later. This notification type is exempt from the employee re-evaluation method.
- **E-Verify Case Complete:** A case in which E-Verify returned a final result and the case was subsequently closed with one of the available case closure statements.
- **E-Verify Case Not Closed:** A case in which E-Verify returns a final result and the case remains open in Guardian triggers a notification 60 minutes after receiving the final result, and daily until the case is closed.
- **E-Verify Unprocessed TNC:** An E-Verify case where either an SSA or DHS Tentative Nonconfirmation has been received and the employee has not indicated whether or not to contest triggers an initial notification at the time specified by the organization. Subsequent notifications are generated daily until a response to the TNC has been acknowledged and E-Verify notified of the decision to contest or not contest.
- **E-Verify Referred TNC:** An E-Verify case where either an SSA or DHS Tentative Nonconfirmation has been received, the employee contests and the user clicks the "Initiate SSA/DHS Referral" button triggers an initial notification at the time specified by the organization. Up to four subsequent notifications can be generated prior to the government response deadline based on the timing specified by the organization. Action days specified in the rule are applied based on federal working days (an action day of '4' will result in the notification being sent four federal working days before the due date).
- **I-9 Section 3 (Supplement B) Signed:** At signing of an electronic Supplement B/Section 3 record, an immediate notification is sent. No subsequent notifications are generated. However, notifications are generated for each "signing" action. This notification type is exempt from the employee re-evaluation method. However, if the Supplement B/Section 3 is unsigned and re-signed, then a new notification is triggered.
- **I-9 Amendment Approved:** At the approval of one or more pending Section 1, Section 2, or Supplement B/Section 3 amendments, an immediate notification is sent. No subsequent notifications are generated. However, notifications are generated for each approval action. This notification type is exempt from the employee re-evaluation method.

- **Remote I-9 Incomplete:** I-9 flagged for remote processing (the I-9 was created as a 'remote I-9' and includes employee/agent instructions) and Section 2 remains unsigned (the I-9 requirement is not met) triggers a notification at the designated Action Days (number of days prior to the employee's hire date) and then daily once the hire date is reached and until Section 2 is signed.

After selecting the notification type, configure the settings of the Notification:



1. **General Settings**

- **Select Notification Type:** The particular occurrence that triggers the notification email. Refer to the notification type definitions above.
- **Enter Notification Name:** Visible from the **Custom Notifications** tab in the Administration settings.

2. **Employee Population -** define the employee population impacted by this notification

- **Select Level Impacted:** the selected level will determine the pool of employees. Select the highest level that includes an attribute shared by the target population. Select either the entire organization, or a subset of your **Employee Group Structure**. For example, you may decide a particular notification is only relevant for the employees of a certain legal entity, or a specific location.
- If selecting a subset of the Group Structure, click the **Define Groups** button to define which specific Employee Groups will be impacted.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

3. **Delivery Settings**
   - **Employee:** The employee's primary email address found on their **Employee Record** > **Personal** tab > **Email.**
   - **Employee's Direct Guardians:** The Guardian users who are assigned directly to the employee's **Employee Group** (at the lowest level, typically **Location**. The users assigned only to a higher level in the **Group Structure**, such as to an entire Legal Entity, are *not* considered Direct Guardians).
   - **Employee defined Optional Email 1:** Found in the **Employee Record** > **Job Details** tab > **Notification Emails** section > **Address 1.**
   - **Employee defined Optional Email 2:** Found in the **Employee Record** > **Job Details** tab > **Notification Emails** section > **Address 2.**
   - **Primary Recipient**: If multiple recipients were defined, specify who will be the primary recipient (all others will be listed on the "**CC**" line).
   - **Select Notification Message:** The actual email to be sent when the Notification is triggered, including the email subject and body content.
   - **Action Days:** The number of days before or following an event in which the notification will trigger. For example, for the **I-9 Reverification** Notification Type, entering values of **90, 30, 0** would trigger a notification email 90 days before the expiration, 30 days before the expiration, and on the day of the expiration (assuming that the employee had not yet been reverified or terminated). See the Notification Types definitions above for additional information on how Action Days are configured for the various Notification Types.

The Action Days field is customizable for the following **Notification Types** only:

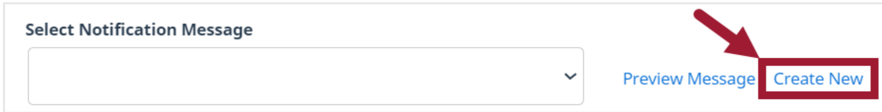
- I-9 Receipt
- I-9 Reverification
- E-Verify Unprocessed TNC
- E-Verify Referred TNC
- Remote I-9 Incomplete
- **Administrator defined email address:** A manually defined email address, such as a helpdesk group email box.
- **Send Time:** Select an alternate time (available in 15 minute increments, listed in military time, and representing **Arizona** time) to adjust when notification emails are sent. By default, notifications are sent after midnight of the day that they trigger.

The following Notification Types trigger an immediate notification email and do not allow for the customization of the Send Time:

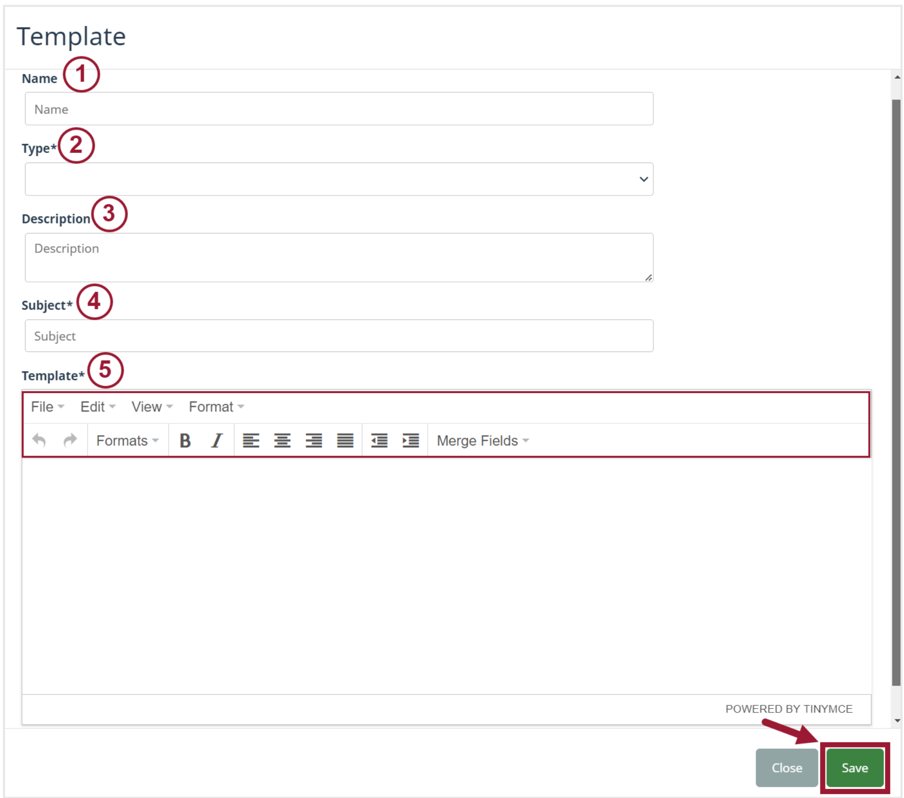
- I-9 Completed
- E-Verify Case Complete
- I-9 Section 3 (Supplement B) Signed
- I-9 Amendment Approved

Creating New Notification Messages

If creating a new **Custom Notification,** you will also need to create a new **Notification Message**, which is the actual email that will be sent to the defined **Recipients**. From the Notification settings, click the **Create New** link to the right of the **Select Notification Message** field.



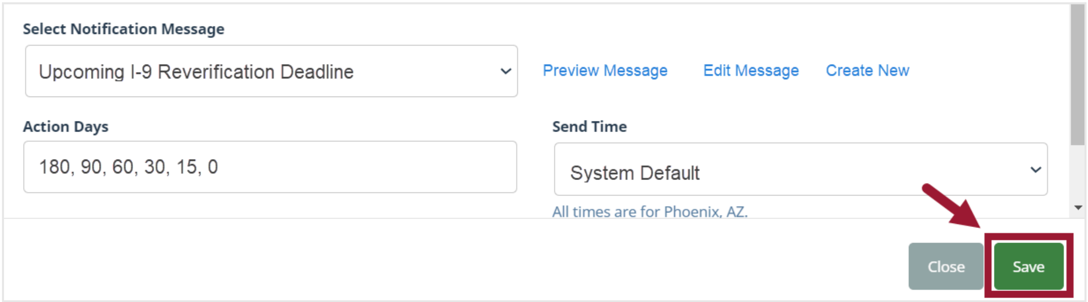
Configure the Message settings by choosing the following options:



1. **Name** of the message template, shown on the **Custom Notifications** tab within the Administration settings, for reference.
2. **Type** will be the type of notification and will be chosen from the drop-down list.
3. **Description** of the message template, shown on the **Custom Notifications** tab within the **Administration** settings, for reference.
4. **Subject** line of the email.
5. **Template** section: Admin will enter the content of the notification message. This section also includes the **Text editor** tools, such as the ability to make the text bold, italic, utilize text alignment, and create bulleted and numbered lists, and the **Merge Fields**, which will dynamically insert information based on the selected Guardian field, such as the employee's name that the email pertains to. Any **Custom Fields** created will also be available here.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

After configuring the message template, select it from the **Select Notification Message** drop-down menu, and click the **Save** button to finish configuring the Custom Notification.



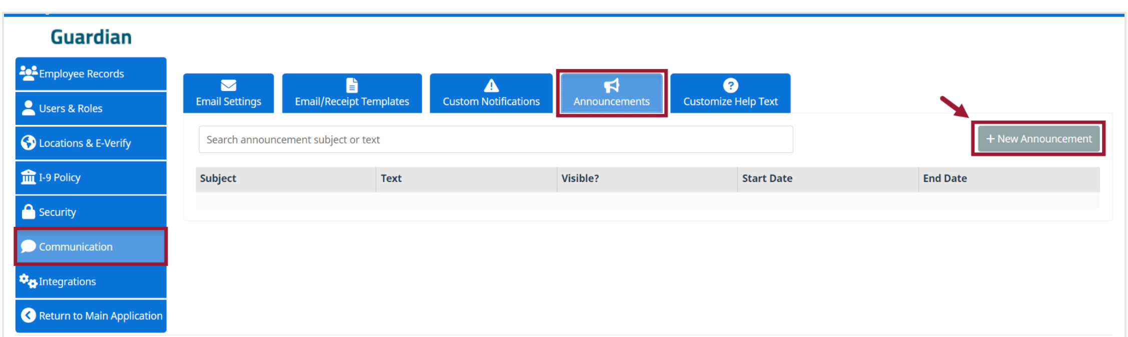
The Custom Notification will now be listed on the **Custom Notifications** tab, and can be edited in the future by clicking the **Notification Name** button.

Announcements

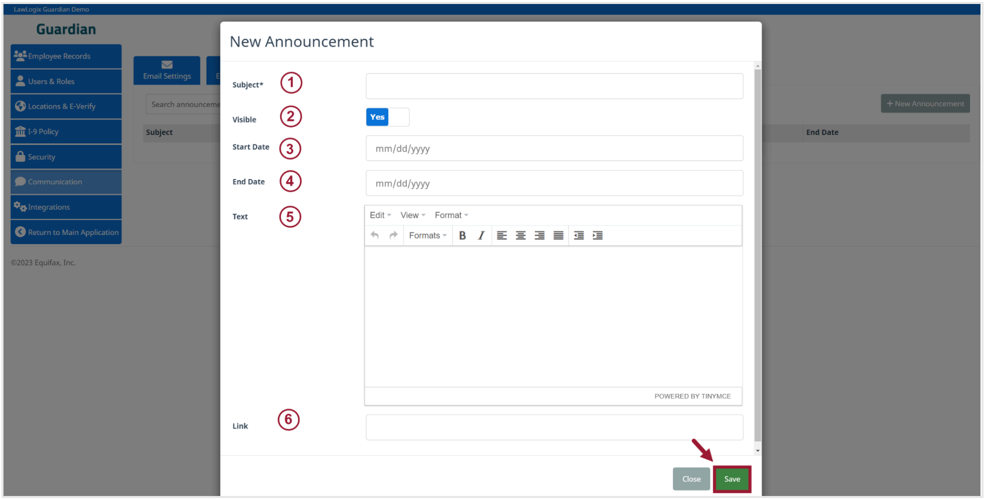
This tab allows for the creation of custom announcements that will be accessible to all **Standard Interface** users, and optionally **Location Manager** users as well (if allowed per the related **I-9 Policy** > **I-9 Management** setting). Common uses of the Announcement feature include providing users with information pertaining to internal policies and procedures, additional I-9 and E-Verify resources, and internal HR support contacts. New announcements appear once as a full-screen pop-up for each user upon login, and can be accessed again from the Announcements menu on the Guardian home page, which will appear alongside any Announcements from Guardian (see example on the following page). Announcements can be configured to be available indefinitely, or to be automatically disabled on a predetermined date.

Creating New Announcements

Click the **New Announcement** button and configure the Announcement settings.

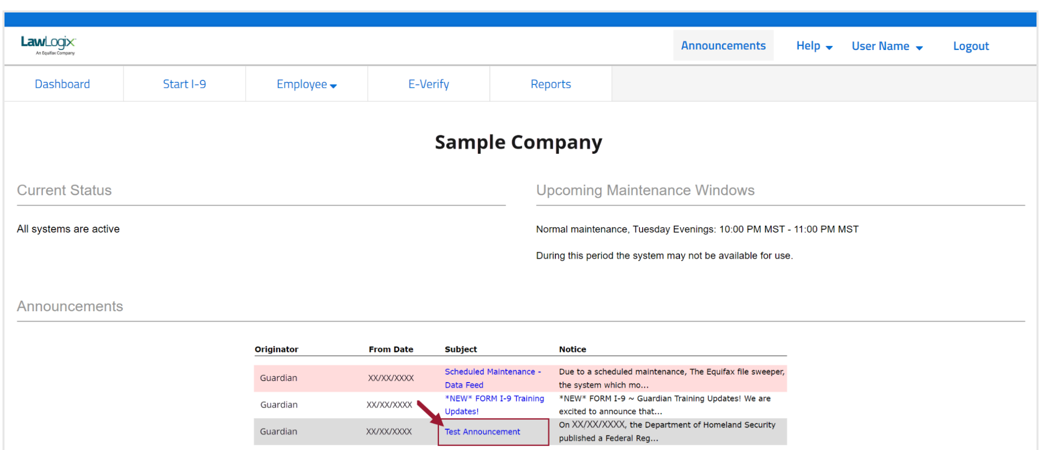


Images are examples and for information purposes only. They may vary across platforms and are subject to change.

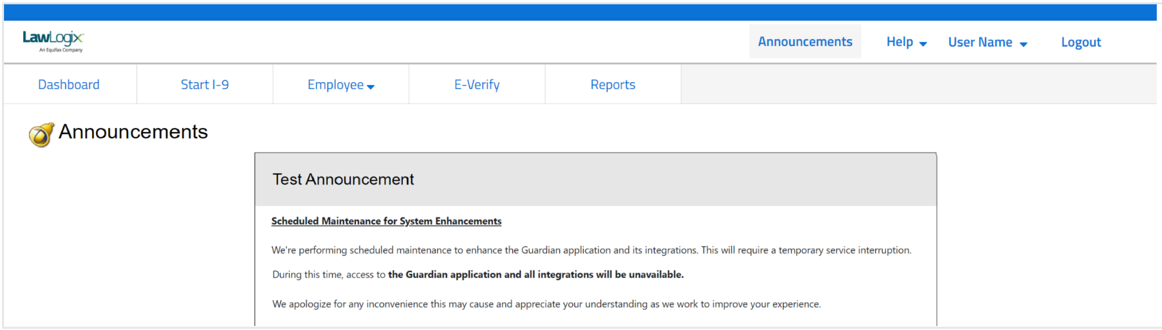


1. **Subject**, which acts as the hyperlink to open the Announcement.
2. **Visible** toggle, used to turn the Announcement on or off. To be visible, a **Start Date** value of today or in the past must also be entered. If an **End Date** of today or in the past is present, the Announcement will be disabled, regardless of the Visible setting.
3. **Start Date** (required), determines when the Announcement will become visible to users. A value of today or in the past must be entered, and the *Visible* toggle must be set to **Yes** for the Announcement to be seen by the users.
4. **End Date** (optional), determines when the Announcement will be disabled. If no End Date is provided, the Announcement will continue to be visible to the users until the *Visible* toggle is switched to **No**.
5. **Text** of the Announcement. In addition to the provided text editor tools, various HTML tags may be used to further customize your announcement.
6. **Link** (optional), provides an alternative to using HTML to create a hyperlink within your Announcement text. Provide a full URL value in the Link field, and then type [Link] anywhere in the text of your Announcement. Anywhere that [Link] is entered, a "**Click Here**" hyperlink will be inserted that links to the provided URL.

Announcement Example



Images are examples and for information purposes only. They may vary across platforms and are subject to change.

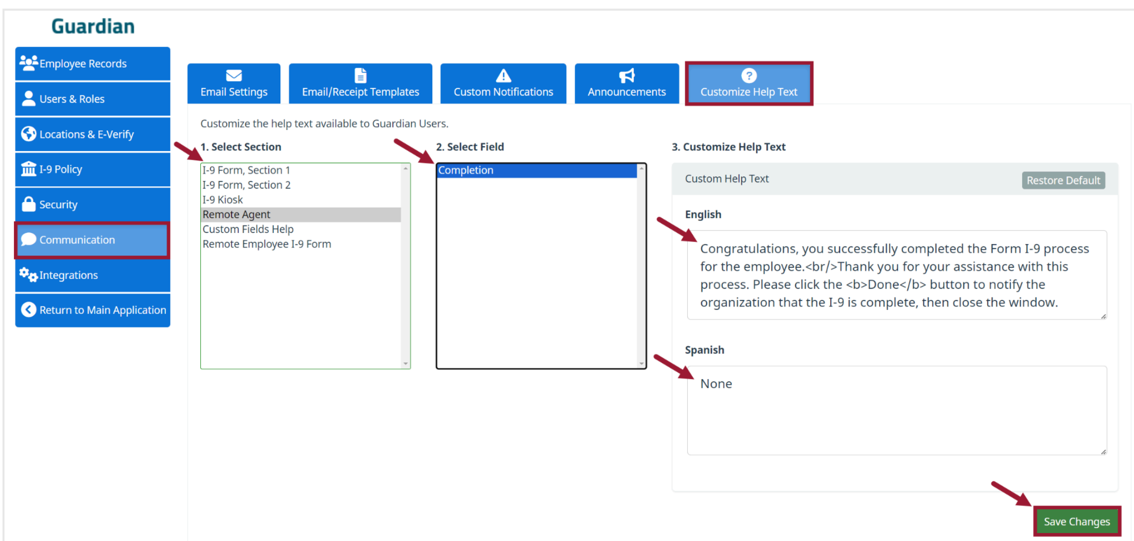


Customizing Help Text

This tab allows for the customization of the various help text that appears to employees and the users throughout the Form I-9 sections, as well as the Guardian system itself. For help text visible to employees, a customizable Spanish version is also provided when the Spanish option is selected for Section 1.

From the **Customize Help Text** tab, select the desired I-9 or Guardian section, the desired field, and then customize the English and/or Spanish help text as desired.

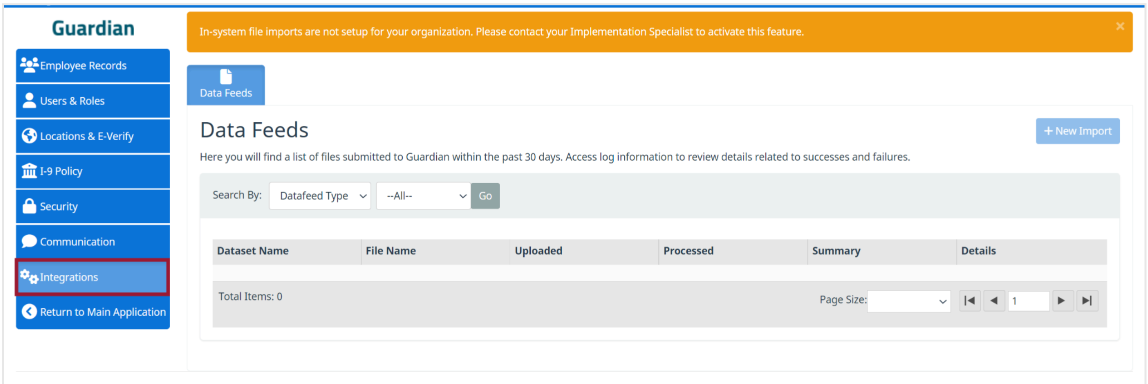
If needed, you can restore to the Guardian defaults by clicking the **Restore Default** button.



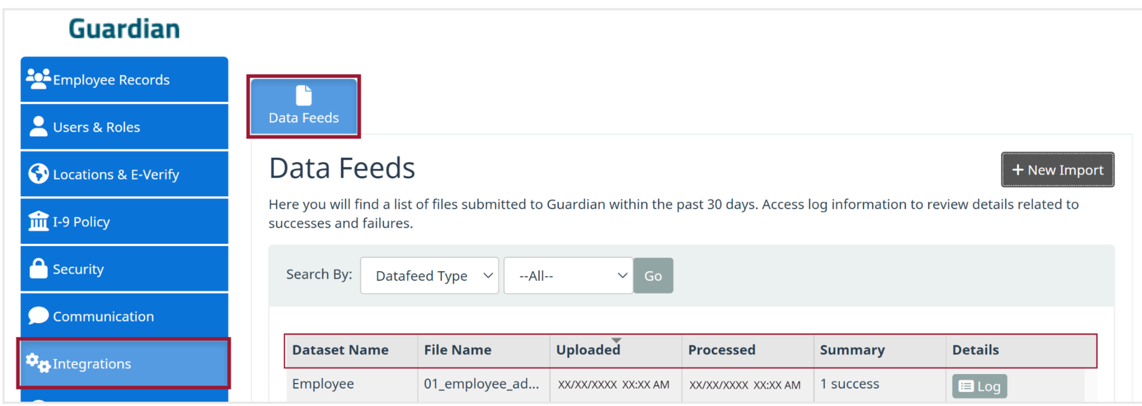
Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Integrations

This module will only appear if the organization has an active integration. Guardian provides organizations the ability to add a subscription-based service to access and deploy a host of integration options in order to maximize efficiency and compliance of the I-9 & E-Verify process.



The Integrations module will contain columns that will appear with a list of information regarding the organization's file submission. Note each column header identifiers: **Dataset Name, File Name, Uploaded Timestamp, Processed Timestamp, Summary**, and **Log Details.**



Column Header Identifier Descriptions:

Dataset Name – This item selects which database table the file is modifying. The choices are the following:

- Location
- Employee
- User
- Group
- Custom Field

Images are examples and for information purposes only. They may vary across platforms and are subject to change.

When uploading a file, the correct data set must be selected. For example, if your file is built for: **Locations**, you'll receive errors if you select **Employee** when uploading the file.
File Name – This is the name of the uploaded file. (Important to notate for troubleshooting).
Uploaded – This is the timestamp which the file was received by Guardian. (Times are in UTC - important to notate for troubleshooting).
Processed – This is the time when the file has been completely processed. (Times are in UTC)
Summary – The number of successfully processed lines ('success') and lines which failed processing ('error').
Details – Contains the 'Log' button to review which lines were successful/failed.

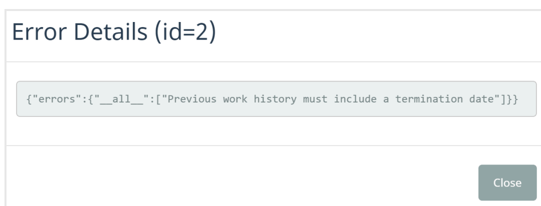
Reviewing Data Feed Log

To review the log for a specific file, click on the **Log** button on the line of the file.

The Data Feed Log page shows the following columns:
ID - The line number of the file, minus the header row. Example: ID 2 correlates to line 3 of the file.
Result - Displays whether the line resulted in an error or success.

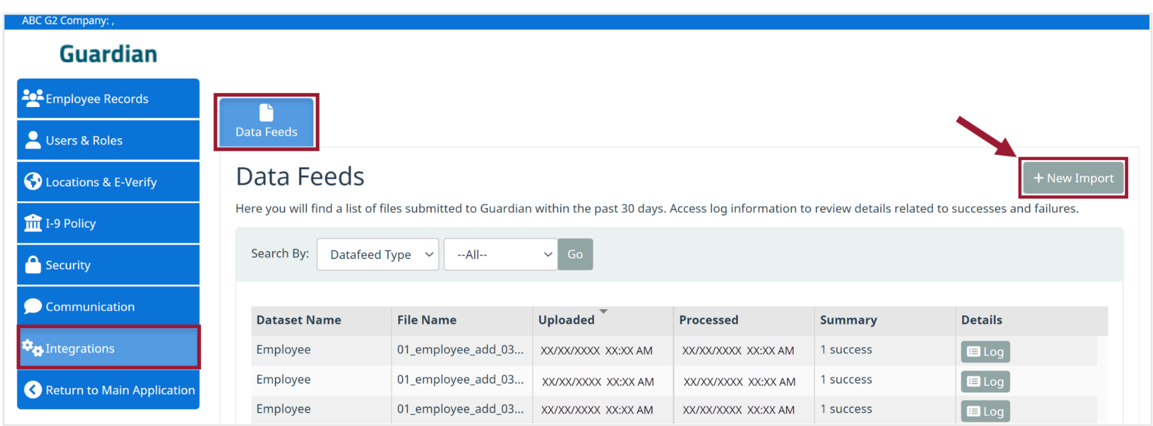
The page can be filtered to show only lines that resulted in Success or Error.

Select the **error** icon to display the detail of the line error. Most errors are displayed in plain english and describe the condition which caused the line to fail.



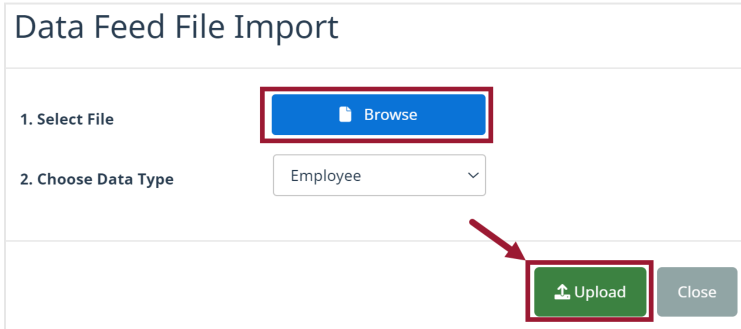
Data Feed Manual File Upload

To import a data feed file, select the **+ New Import** button.



Images are examples and for information purposes only. They may vary across platforms and are subject to change.

Click the **Browse** button to locate and select the file for upload. Choose the correct Data Type from the following: Employee, Location, User, Group, Custom Field. Click the **Upload** button.



Return to Main Application

Clicking on the **Return to Main Application** button while on any of the menus will route the Admin back to the Guardian homescreen.

Guardian Customer Support

Need additional assistance? A Guardian Administrator or full-featured/Standard User may contact our Support team at: Guardiansupport@equifax.com.

More Training Available!

Please visit our Connections site for Live and On-Demand training resources.

The information provided is intended as general guidance and is not intended to convey any tax, benefits, or legal advice. For information pertaining to your company and its specific facts and needs, please consult your own tax advisor or legal counsel.

Images are examples and for information purposes only. They may vary across platforms and are subject to change.