User Creation & Maintenance

Guardian User Creation & Maintenance

User Guide

Version 1.1

Contents

Getting Started

Guardian allows for the creation of an unlimited number of users with varying degrees of access and privileges. System administrators manage user creation and maintenance. User profiles can be created, retired, restored, and modified. Administrators may make adjustments to user profiles to restrict or further expand functionality. Each licensed user accessing Guardian must have a user profile. User profiles are created and maintained within the **Administration** module of the system.

Terms

- **Archival Paper I-9:** This is a type of I-9 record that represents those I-9s that are completed entirely on the paper form outside of Guardian for *existing* employees.
- **Administrator:** This designation refers to any Guardian user given the privilege "admin" who can access the system administration module.
- **Amendment:** This refers to electronic functionality available in Guardian that allows users to make post-completion corrections to I-9 records. Amendment changes alter the electronic data and the I-9 image.
- **Approve:** The act of locking an I-9 record from further editing. This action normally takes place after the I-9 has been completed (Section 1 and 2 signed).
- **Electronic I-9**: This is a type of I-9 record created within the system. All information on the I-9, including electronic signatures, is entered directly in Guardian.
- **E-Verify:** E-Verify is an electronic verification system that reports the work authorization status of **new hires** based on I-9 data (with the exception of Federal Contractors subject to FAR who may be required to submit existing employees).
- **FAR Queue:** Federal contractors awarded a contract on or after September 8, 2009 that includes the Federal Acquisition Regulation (FAR) E-Verify clause utilize this interface to submit existing employees (normally exempt) to E-Verify.
- **Full Featured:** User type designation that permits any or all usage of available system functionality.
- **HR:** A user of the Guardian system.
- **HR Group:** A group of one or more users of the Guardian system who share access and ownership of employee records.
- **Location:** Location normally refers to the physical sites to which employees are assigned.
- **Location Manager:** User type designation that permits limited use of key system features, namely creation and completion of electronic I-9s for new hires.
- **New Hire Paper I-9:** This is a type of I-9 record that represents those I-9s that are completed entirely on paper form outside of Guardian for *newly hired* employees).

- **Occupation Class:** Occupation class refers to a customizable designation within the database that may include one or more values and can be used to segment employee populations.
- **Park I-9:** The act of locking an *incomplete* I-9 record from further editing.
- **Responsible HR**: This is an individual user assigned to an employee record.
- **Reverify:** I-9 records for employees with temporary work authorization whose work authorization must be reverified at a certain point in order to continue working in the United States.
- **SSO:** Single sign-on (SSO) is an access control method that allows a user to login to multiple systems and applications with a single login.

Creating User Profiles

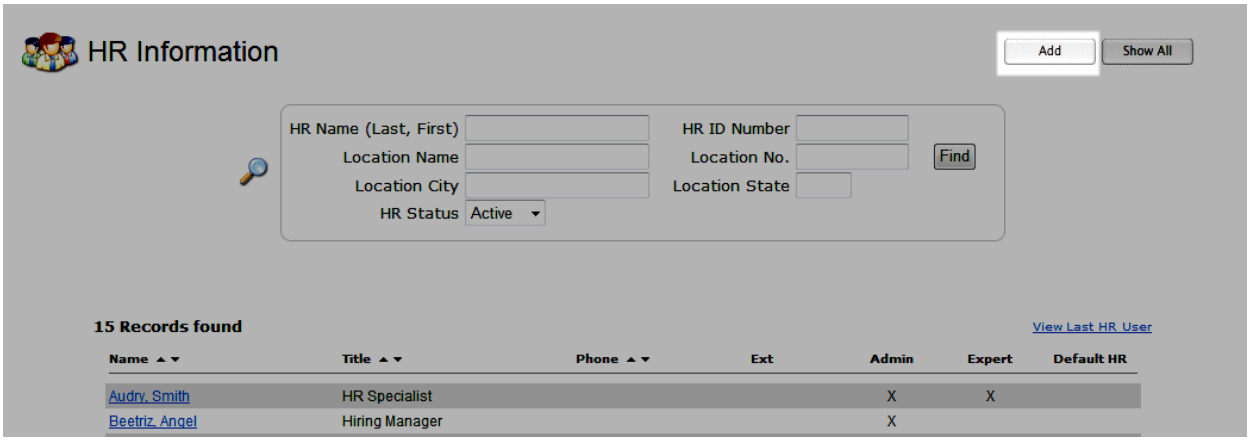
Administrators control who may access Guardian. Each licensed user interacting with the system must have a user profile. User profiles are created within the **Administration** module.

Adding the User Profile

To add the user profile:

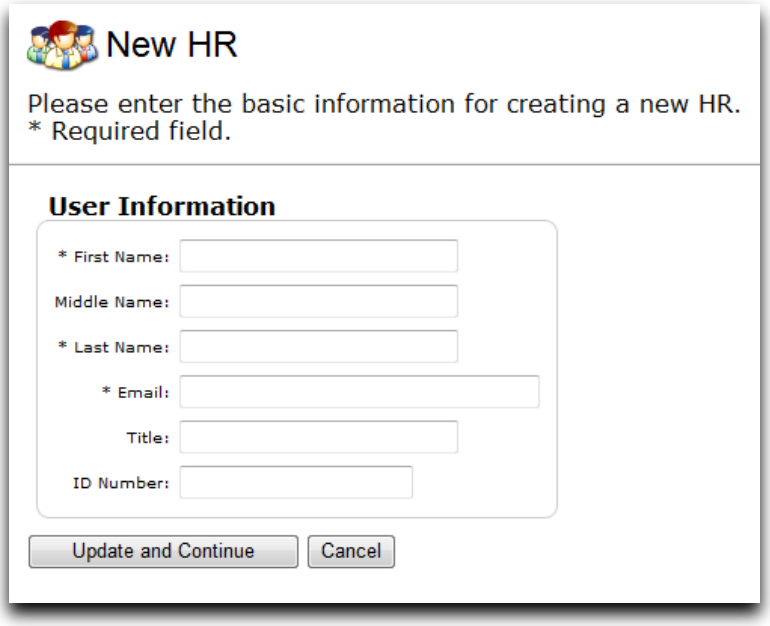
1. Access the **HR Users** link
2. On the **HR Users** page click **Add**

Figure 1: User Profile Addition



3. Enter the required new user information (at minimum: name, email, title)
4. Click **Update and Continue** to create the new profile

Figure 2: User Creation Screen



Selecting the User Type

The user profile consists of three tabs: **Personal Information**, **Privileges**, and **Permissions**. After the initial profile is added, administrators utilize the **Privileges** and **Permissions** tabs to configure the profile for use. Administrators must first decide the *user type* as this impacts the user's access to Guardian and available functionality.

User types:

Full Featured: This user type accesses the traditional Guardian interface and can be granted any or all available functionality, up to and including administrator privileges.

Location Manager: This user type accesses an alternate streamlined interface and is ideal for those users whose chief responsibility is new hire I-9 completion (some other limited functionality including E-Verify is possible). Employee and I-9 access is driven by a **To Do List** and **New Employee/New I-9** button. This user type does not have access to the traditional vertical toolbar or equivalent links (My Info, Employees, Task, I-9 Forms, Reports, etc.).

The following matrix provides an overview of the available functionality related to each user type:

Figure 3: User Access Matrix

	Can Create									Can Access							Can Edit		
Access Level	Employee	Employee Login/Email	Electronic I-9	New Hire Paper I-9	Archival I-9	Remote Agent I-9	E-Verify	Section 3	Amendments	Charts & Graphs	Administration	Reports	FAR Queue	Tasks	Calendar	Employee Record	Employment History: rehire	Employment History: terminate
Full Featured	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Location Manager	x		x	x			x	x	x*								x	

*Amendments can be created only in limited circumstances

IMPORTANT NOTES

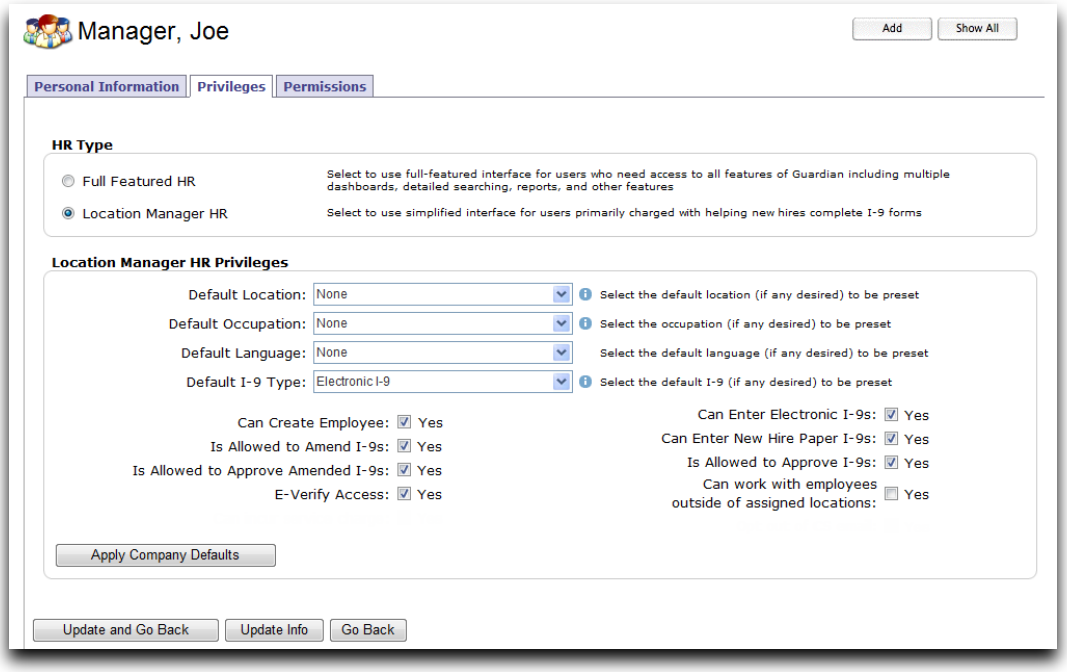
The **Location Manager** utilizes a different interface than the **Full Featured** user to complete actions. Please consult the *Location Manager Overview* tutorial for an overview of the **Location Manager** interface.

To select the user type:

1. Access the **Privileges** tab
2. In the **HR Type** section select either **Full Featured** or **Location Manager**

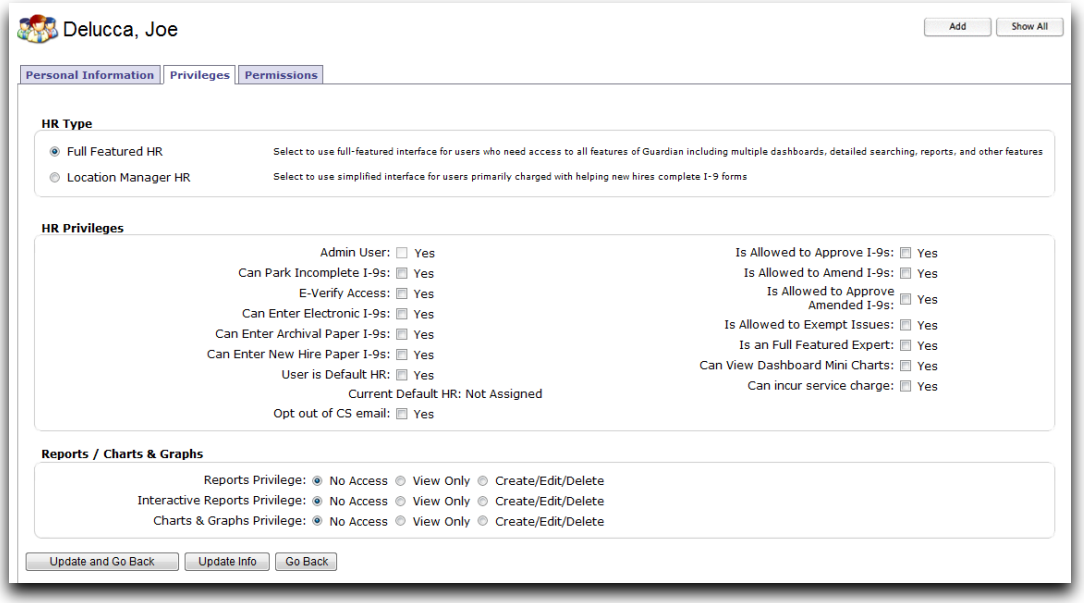
Selecting **Location Manager** as the user type limits the privilege options available to the user.

Figure 4: Location Manager User Privileges



Selecting **Full Featured** as the user type allows the user to activate all available Guardian features for the user.

Figure 5: Full Featured Privileges



Understanding User Privileges

Users may be granted individual privileges within Guardian in order to perform specific functions. The set of available privileges allows organizations to deploy a spectrum of user access levels. User privileges are set individually at the User level.

Privileges available for either user type:

Can Enter Electronic I-9s-User is able to create electronic I-9 records for employees

Can Enter New Hire Paper I-9s-User is able to create new hire paper I-9 records to represent paper I-9s completed outside of Guardian for *new* employees

Is Allowed to Approve I-9s-User is able to mark I-9s as approved, which locks the I-9 data and submits that data to E-Verify, where applicable. Once approved, changes to the I-9 record can be completed via amendment functionality only.

Is Allowed to Amend I-9s-User is able to make post I-9 completion corrections to I-9 records (corrections change the electronic data and are represented on the I-9 image in red font to denote the later adjustment); Location Manager users may only utilize the electronic amendment feature in conjunction with E-Verify submissions in which incorrect data is identified. To utilize, Location Manager users must also have the **E-Verify Access** privilege enabled.

Is Allowed to Approve Amended I-9s-User is allowed to approve and lock pending amendments (Note: approver's initials and the date of approval appear next to the correction on the I-9 image). See restrictions related to Location Manager users under **Is Allowed to Amend I-9s** privilege.

E-Verify Access-User has access to E-Verify records created for employees and can process the E-Verify cases (e.g. close cases, process Tentative Nonconfirmations). Note: this setting does not control **submission** of I-9 data to E-Verify. Data from new hire I-9s created at locations enabled for E-Verify submits to E-Verify upon I-9 **approval**.

Privileges reserved for the Full Featured user type:

Admin User-User has access to the **Administration** module to adjust system preferences, maintain location profiles, maintain user profiles, and other administrative settings as well as has access to all employee records by default.

Can Park Incomplete I-9s-User can utilize the park feature to lock and approve *incomplete* I-9s. Note, the organization must enable park functionality for the database in order to utilize (**Incomplete I-9s can be Parked** must be enabled in the **I-9 Preferences** section with **Administration**). Parking

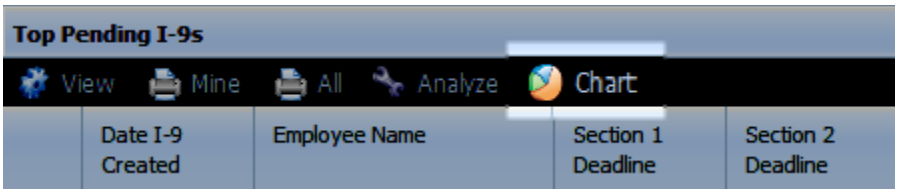
an I-9 record removes the incomplete I-9 from Dashboard view and allows the organization to create a new I-9 for the employee.

Can Enter Archival Paper I-9s-User is able to create archival paper I-9 records to represent paper I-9s that were completed outside of Guardian for *existing* employees.

Is Allowed to Exempt Issues-User is able to waive I-9 warnings and issues identified by the system. This functionality is executed on an I-9 by I-9 and issue by issue basis and usually is utilized in instances in which a correction to the I-9 is not applicable. Many times it is used in conjunction with the electronic amendment functionality, or during a remediation project of the organization's existing I-9s.

Can View Dashboard Mini Charts-User has access to mini chart functionality within select dashboard sections. Mini charts graphically represent the statistical data related to the relevant dashboard.

Figure 6: Example Dashboard Mini Chart Option



User is Default HR-A single user within the database may be assigned as the "default HR". This designation is used as a fail-safe to assign an individual to employee records in instances in which no location and/or occupation class assignment has been made. In such cases, the user identified as the default HR will appear as the responsible entity for the employee record, else Guardian selects a user in such instances that a default has not been identified.

Is an In-House Expert-User has been designated by the organization as an escalation point for I-9 questions. Note, the "escalate to expert" feature must also be enabled in order for users to utilize the feature and contact the designated "expert".

Reports Privilege-User's access to the **Reports** module and default report types can be managed with this option. Note, the organization must have **Reports Module Access** and **Reports Module Create/Edit** set to **HR by HR** in order to utilize this setting.

Interactive Reports Privilege-User's access to the **Interactive** report type can be managed with this option. Note, the organization must have **Interactive Reports Access** and **Interactive Reports Create/Edit** set to **HR by HR** in order to utilize this setting.

Charts & Graphs Privilege-User's access to the **Charts & Graphs** module can be managed with this option. Note, the organization must have **Charts & Graphs Module Access** and **Charts & Graphs Create/Edit** set to **HR by HR** in order to utilize this setting

Privileges reserved for the Location Manager user type:

Default Location-Location user has been granted permission to view/edit (for purposes of the **To Do List** population). Employee records created by the user will be assigned to this location.

Default Occupation Class-Employee records created by the user will be assigned to this occupation class. (The employee's location and occupation class assignments determine which user or group of users may access the employee record.)

Default Language-Selection of English or Spanish designates which language will appear when completing Section 1. Note, if Spanish is selected Spanish translations appear **in addition to** the Form I-9 English text).

Default I-9 Type-The type of I-9 (Electronic or New Hire Paper) selected by default when creating the I-9 record.

Default Business Unit-The default business unit in which the user will assign new employee records. Note, this option is only available to organizations who have more than one business unit (often associated with FEIN) configured within the system.

Can work with employees outside of assigned locations-When selected, the user can search and process I-9 records for employees that are not assigned to the user's location(s).

IMPORTANT NOTES

Defaults should be set when activating a Location Manager user (the Location Manager Interface does *not* have a **My Info** section for the user to access to set his/her own defaults and the Location Manger user **cannot** assign the location or occupation class when creating a new employee record through the One Minute I-9 interface).

Setting or Modifying User Privileges

To set or modify user privileges a system administrator must access the **Administration** module within the system and perform the following:

1. Access the applicable user
2. On the **Privileges** tab make the desired selections or changes
3. Click **Update Info** to save the change(s)

Note: Privilege availability changes depending on the user type selected. See section, "Understanding User Privileges" for more information on the individual settings.

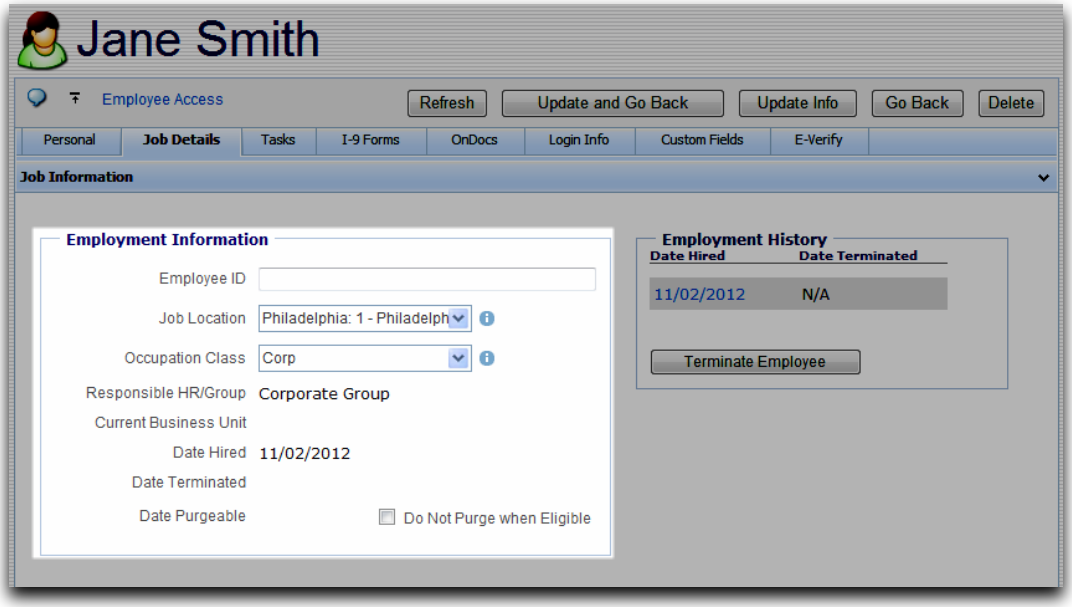
Setting or Modifying User Permissions

User permissions refer to the configuration settings that determine *which* employees the user can access or is assigned. Through settings on the **Permissions** tab users can be granted the ability to access employee records (provided visibility) and/or given ownership of employee records (assigned responsibility). Ownership refers to those users individually assigned to an employee record, or who are a member of a group assigned to an employee record. Employees can be assigned to one or more users via the **HR Group** functionality.

Users with access to employee records may be able to modify employee information and/or create and complete I-9 records (depending on permission levels and user type). Whereas users *assigned* to employee records can perform these same functions *in addition* to receiving automated outbound communications (reminder emails related to specific tasks in Guardian such as reverification).

E-mails sent from Guardian are sent to the user or users assigned to the applicable employee record (based on **Location** and **Occupation Class** assignment on the employee's **Job Details** tab). Individual user or group assignment is visible on the employee's **Job Details** tab→**Job Information** section.

Figure 7: Responsible HR/Group Assignment Example



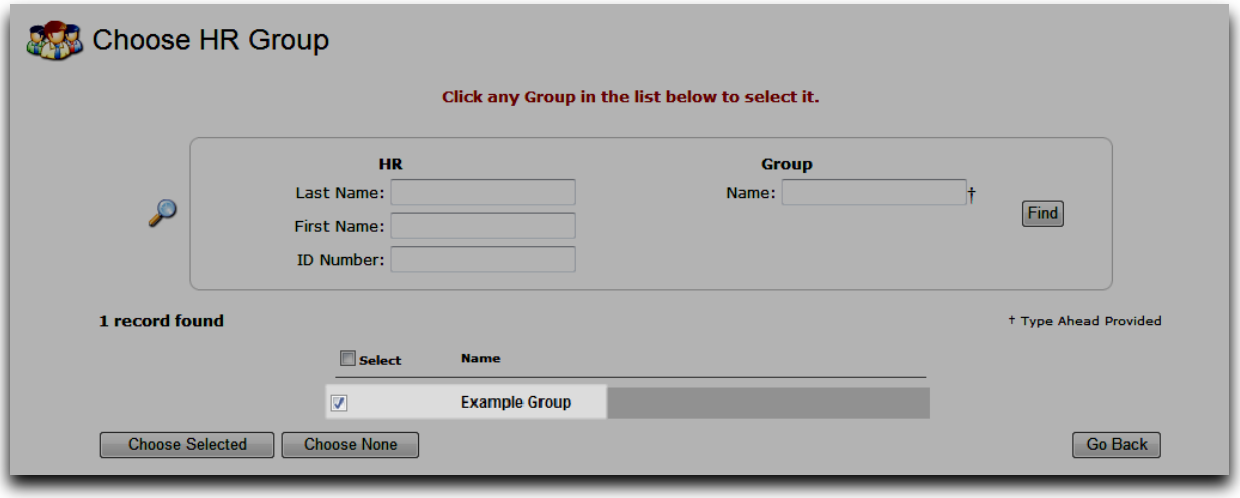
Assigning Users to Groups:

User may be granted access and responsibility to employee records based on group membership. Users may be members of one or more groups simultaneously. Usage of Groups in Guardian is not required.

To assign a user to a group:

1. Access the applicable user
2. On the **Permissions** tab click **Add Group**
3. Search for the desired group or groups (more than one can be selected at a time)
4. Click to select each desired group
5. Click **Choose Selected** to add the user as a group member to the designated group(s)

Figure 8: Example Group Selection



Assigning Location Permissions:

User location permissions play a key role in determining which employee records the user can access. Following lists the various location permission options and their impact to employee visibility.

Location Permission Options:

View/Edit All: User has access to all employees for the organization regardless of HR, Group, or location assignment. The user is not necessarily assigned to any employees.

View/Edit HR Assigned Only: User has access only to those employees assigned directly to him or her. Access or restriction by location or Group is not applied.

View/Edit HR Group Assigned Only: User has access to employees assigned directly by Group (to which the user is a member). Access or restriction by location is not applied.

View/Edit Restricted Locations Only: User has access to employees assigned directly to the user or user's Group and further restricted by location as defined within the user's profile.

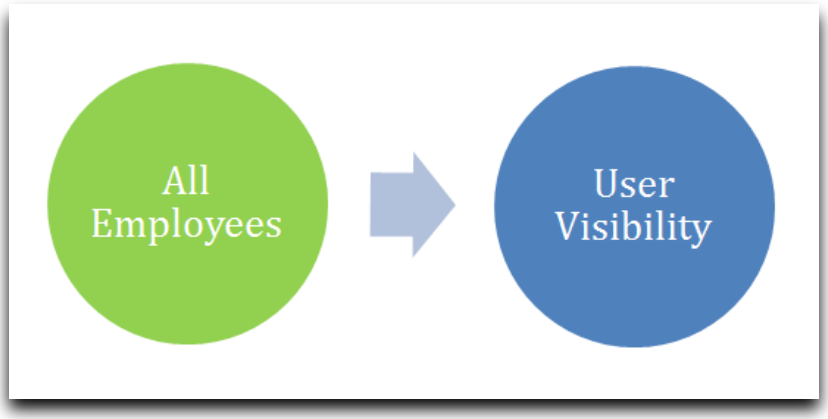
View/Edit Assigned Plus Locations: User has access to employees assigned directly to him or her or his or her Group (across locations), plus has access to **all** employees at the location(s) defined within the user's profile regardless of HR or Group Assignment.

New users are assigned the permission setting of **View/Edit Restricted Locations Only** by default.

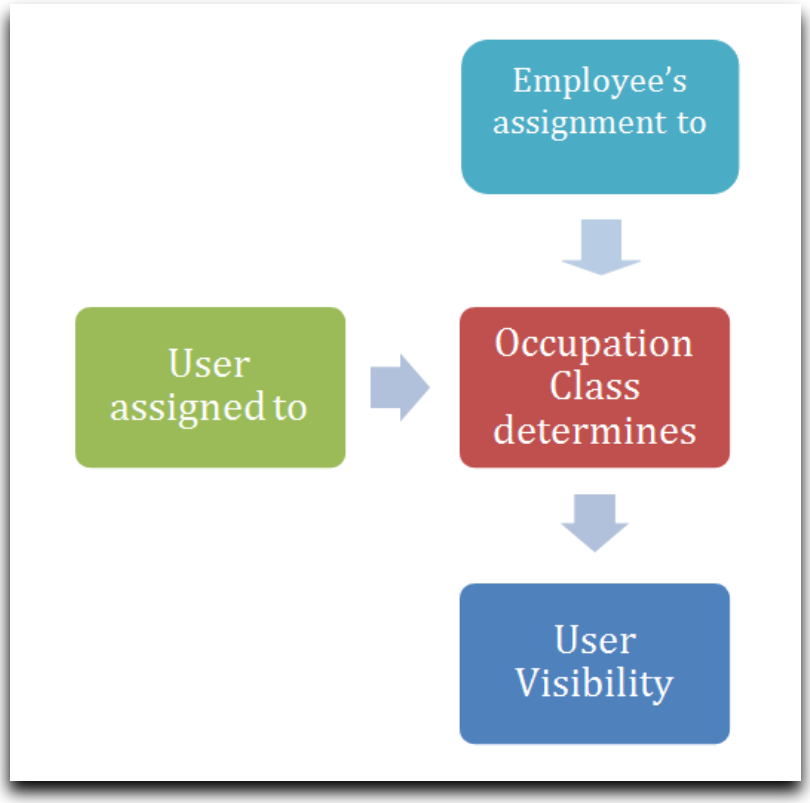
The selection of the user permission option together with location settings determines which employee records the user can access or is assigned.

Following are graphical representations of each location permission option:

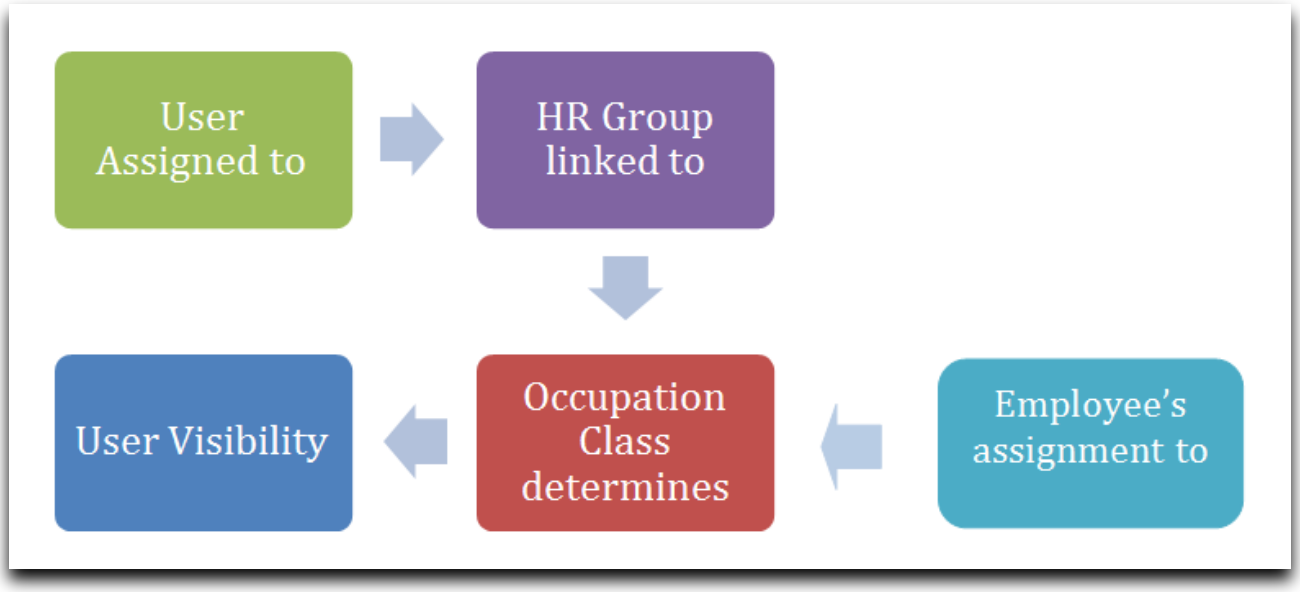
View/Edit All:



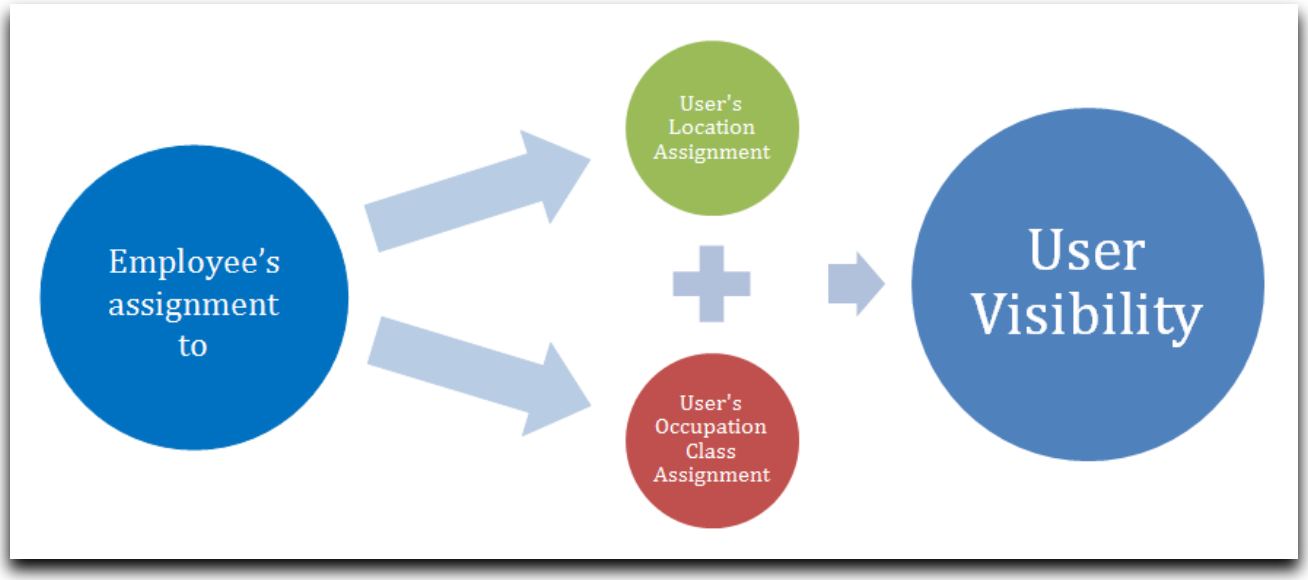
View/Edit HR Assigned Only:



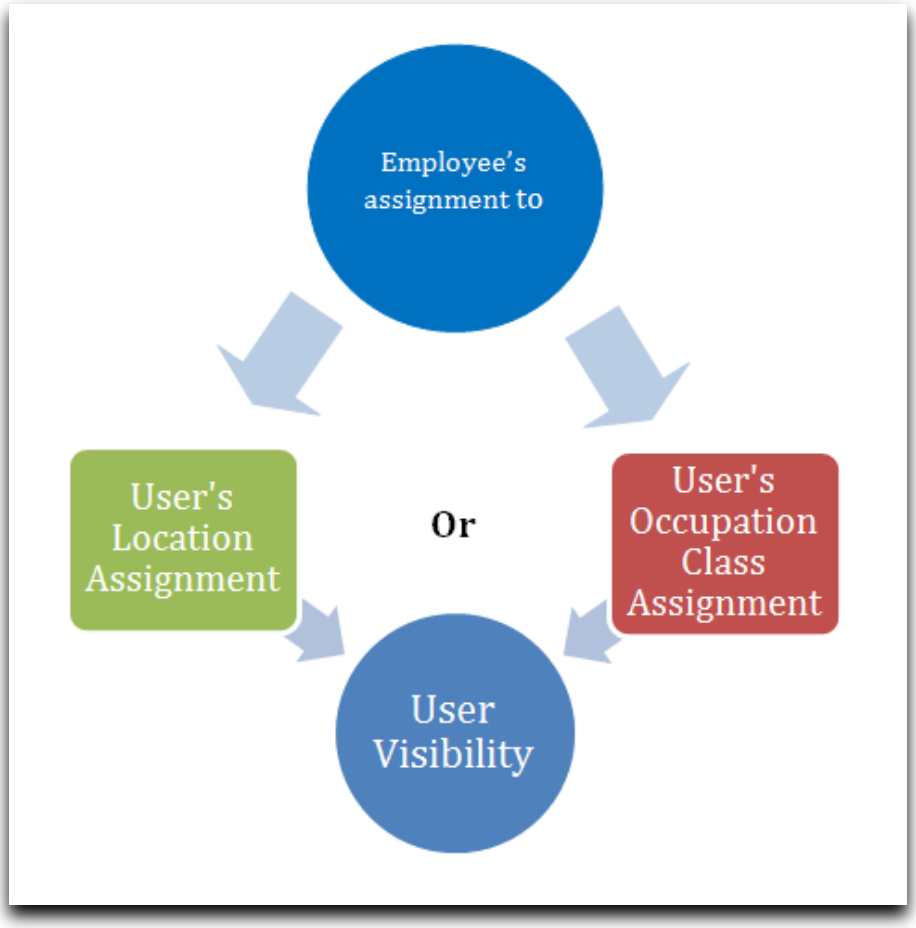
View/Edit HR Group Assigned Only:



View/Edit Restricted Locations Only:



View/Edit Assigned Plus Locations:



To assign the user's location permissions:

1. Access the applicable user
2. On the **Permissions** tab select the desired permission level
3. If **View/Edit Restricted Locations Only** or **View/Edit Assigned Plus Locations** is selected, identify which location(s)* the user may access as either **View Only** or **View/Edit**
4. Click **Update Info** to save the changes

*Note, organizations with over 125 locations defined must click **Assign Location** to search for and select the desired location(s).

Resetting User Passwords, Sending Welcome E-mails, and Restricting System Access

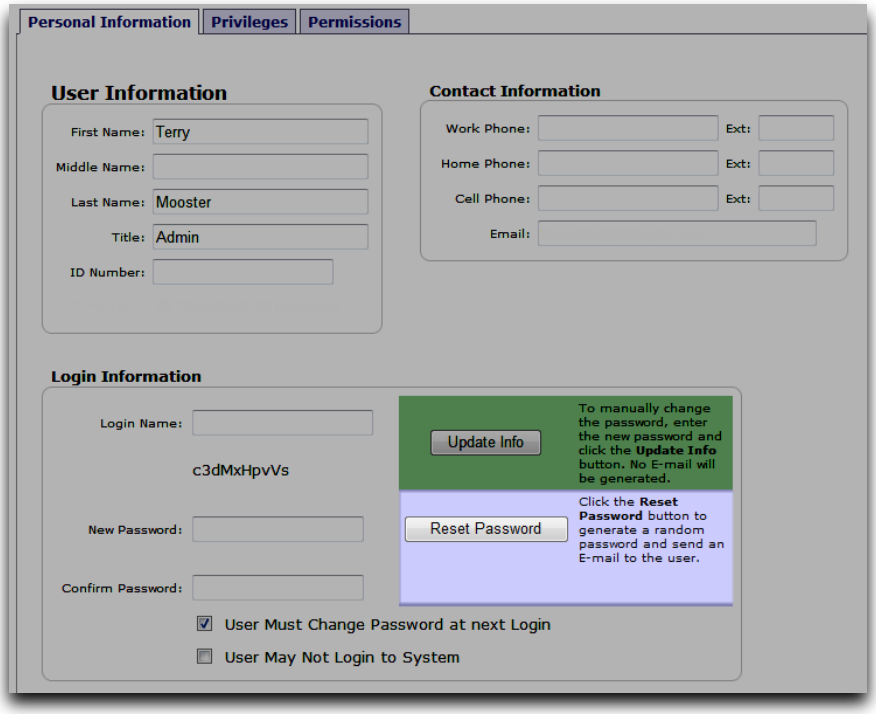
Administrators control who accesses the Guardian system. Administrators may update login information, reset login information as well as restrict system access. User login information is controlled within each user's **Personal Information** tab in the **Administration** module.

Sending the User Welcome E-mail

Upon user creation, Guardian randomly generates a username and password. The login name remains visible within the user's profile while the password remains hidden and encrypted.

To send the user login information ("welcome e-mail"):

1. Access the **HR Users** link
2. Access the applicable user
3. On the **Personal Information** tab ensure "User must change password at next login" is selected
4. Click the **Reset Password** button



Adjusting User Login Information

Administrators may customize user login names and passwords. Login information created by administrators does not generate an e-mail to the user.

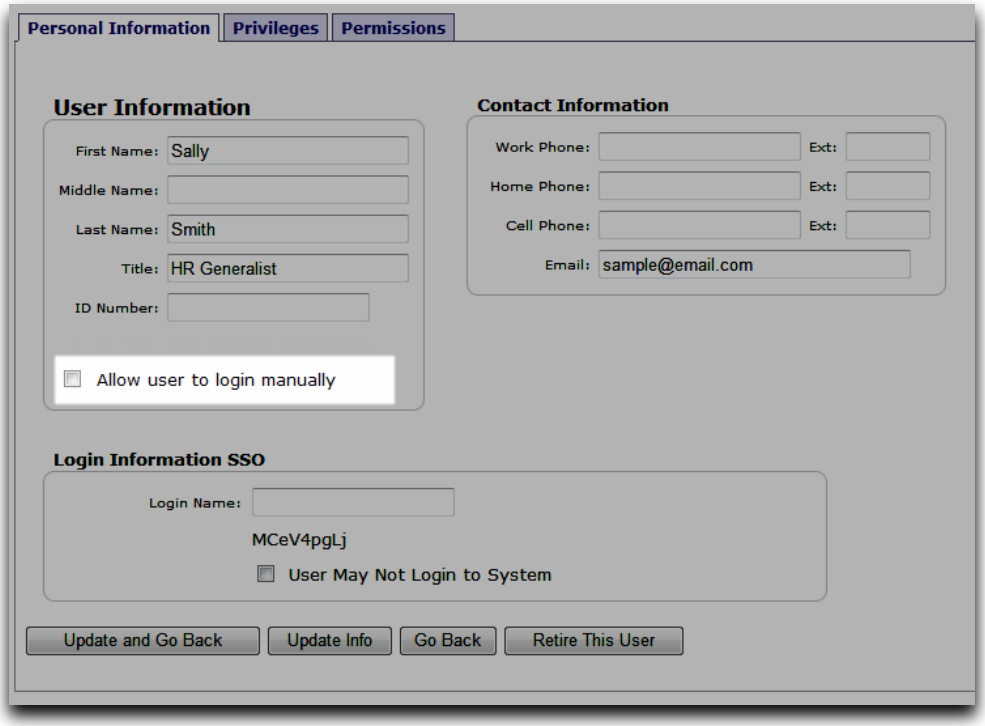
To adjust user login information:

1. Access the **HR Users** link
2. Access the applicable user
3. On the **Personal Information** tab input the desired **Login Name** and/or **New Password** (if a new password is entered the administrator must re-enter it in the **Confirm Password** field)
4. Click the **Update Info** button to save the changes

IMPORTANT NOTES

Organizations utilizing SSO functionality may only adjust the **Login Name** (used to authenticate the user via SSO) unless the option **Allow user to login manually** is selected which allows the administrator to generate a password (in order for the user to access Guardian through the traditional login means).

Figure 9: Alternate Login Option for SSO Organizations



Restricting User Access

To prevent a user from accessing Guardian:

1. Access the **HR Users** link
2. Access the applicable user
3. On the **Personal Information** tab click the **User May Not Login to System** button
4. Click the **Update Info** button to save the change

Retiring and Restoring User Profiles

Administrators may retire profiles for those users who no longer need access to Guardian. The user's profile and all related audit log entries remain within the organization's database. User profiles are retired within the **Administration** module.

Retiring the User Profile

To retire the user profile:

1. Access the **HR Users** link
2. Access the applicable user
3. On the **Personal Information** tab click the **Retire This User** button

Retired users are **unable** to login to Guardian.

Restoring the User Profile

To restore the user profile:

1. Access the **HR Users** link
2. Search for the retired user by selecting **Retired** from the **HR Status** filter dropdown
3. On the **Personal Information** tab click the **Unretire This User** button