

About User Roles

Home > eICS > Guide - Contacts > About User Roles



User roles are permission levels that are assigned to contacts within the system regardless of the person's access to eICS. There are five roles, four of which are internal roles and one that is external.

- **Domain Administrator** — Individual who establishes facilities, manages contacts, and administers libraries for the facilities within their domain.
- **Facility Administrator** — Individual who manages plans, contacts and libraries for their facility.
- **Facility Staff** — Individual who is associated with emergency management planning, response, and/or recovery at the facility level; who can manage incidents; and who may be called on to respond to an incident.
- **Facility Staff Limited** — Individual who is associated with emergency management planning, response, and/or recovery at the facility level; and who may be called on to respond to an incident. However, they are not able to start incidents.
- **External Contact** — Individual associated with a facility who may need to be notified of incidents, but who does not usually have access to eICS. For example, a vendor who delivers goods or services or the county emergency management coordinator could both be considered external contacts.

All internal roles are considered contacts and have access to the system. As such, they are assigned roles to specify and differentiate their jobs and permissions within the system.

External Contacts do not necessarily have access to the system. These are usually people or businesses that interact with facilities. They are identified to promote communication and send notifications regarding incidents.

For more information on the five main roles and their access and responsibilities, refer to [Permissions](#).

Users

Users are contacts, but contacts are not necessarily users. As an administrator, you must decide whether a new contact needs to use the eICS system. If they do, you assign a username, specify at least one phone number and email address for the contact, and assign a user role.

Domain Administrator

Domain Administrators manage information about the incident command system (ICS) and domains within the ICS. They also provide support for facilities within their domain.

Helpful Links

[Juvare.com](#)
[Juvare Training Center](#)
[Announcements](#)
[Community Resources](#)

Role	Description and Tasks
System	<p>A Domain Administrator has the highest level of access. They can:</p> <ul style="list-style-type: none">• Manage aspects of planning and create new plans that facilities can copy and use.• Add facilities to the domain.• Create incident response guides and make them available to facilities.• Manage account domain and facility roles within their specific domain.• Manage the domain library and any facility library.• Add, edit, or delete files and folders in the library.• Work with the libraries for ended and closed incidents.• Manage the content of email and voice notification templates.
Incident	<p>For incidents, Domain Administrators can add to and change information in any Incident Dashboard. They can add events to the log, update the status of their position's objectives, send messages to other participants, and much more.</p>

Facility Administrator

Facility Administrators manage information about their facility, including the contacts, library, and plan. They can also create an incident and assign themselves and others to positions on an active incident.

Role	Description and Tasks
System	<p>All Facility Administrators can manage facility roles within their specific facility. In addition, they have access to the system's administrative features. They can:</p> <ul style="list-style-type: none">• Manage aspects of planning, including the plan itself, incident response guides, depth chart, objectives, and the labor pool.• Add and change accounts for users at their facility.• Manage their facility library by adding, editing, and deleting files and folders.• Work with the libraries for ended and closed incidents.• View and copy incident plans stored at the domain level.• Customize details for their facility.
Incident	<p>During an incident, an administrator assigned to a position defined in the associated incident response guide (IRG) takes on that position's role. These individuals can add to and change information in the Incident Dashboard, adding events to the log, updating the status of their position's objectives, sending messages to other participants, and much more.</p> <p>In addition, a Facility Administrator can:</p> <ul style="list-style-type: none">• End and close incidents for their facility.• Manage details and library files for ended and closed incidents.• Run reports on any incident, even those that are ended and closed.

Facility Staff

Facility Staff can work within eICS to update their profile information. They can also create an incident and assign themselves and others to positions on an active incident.

Role	Description and Tasks
System	<p>In general, Facility Staff members can access any non-administrative features in the system. They can:</p> <ul style="list-style-type: none">• Manage their profile, including their contact information.• Reset their own password.• View their facility's incident command plan, incident response guide (IRG) details, and facility library.• Start, escalate and end an incident when assigned to an incident position.• Open the dashboard of any active incidents for the facilities to which they have access.
Incident	<p>When an incident occurs, a staff member assigned to a position defined in the associated IRG takes on that position's role. These individuals can add to and change information in the Incident Dashboard by adding events to the log, adding to the incident's library, updating the status of their position's objectives, sending messages to other participants, and much more.</p>

Facility Staff Limited

Facility Staff Limited can work within eICS to update their profile information. They can also assign themselves to positions on an active incident.

Role	Description and Tasks
System	<p>In general, Facility Staff Limited members can access non-administrative features in the system. They can:</p> <ul style="list-style-type: none">• Manage their profile, including their contact information.• Reset their own password.• View their facility's incident command plan, incident response guide (IRG) details, and facility library.• Open the dashboard of any active incidents for the facilities to which they have access.

Incident	When an incident occurs, a staff member assigned to a position defined in the associated IRG takes on that position's role. These individuals can add to and change information in the Incident Dashboard by adding events to the log, adding to the incident's library, updating the status of their position's objectives, sending messages to other participants, and much more.
----------	---

External Contact

You can add partners, vendors, and other external individuals or entities to eICS. By doing so, you ensure these individuals and entities are notified as appropriate when an incident occurs. These individuals are known as External Contacts and have limited access to facilities. In most cases, these contacts do not need access to eICS. However, when necessary, you can provide these individuals with credentials so they can access eICS on a limited scale.

Role	Description and Tasks
System	<p>Some of your External Contacts may also be system users, enabling you to call on them to respond to incidents. Other External Contacts, however, may be included in your system simply to ensure that these individuals are notified of incidents.</p> <p>If an External Contact has a username, login email, and password, they can:</p> <ul style="list-style-type: none"> • Open the Incident Dashboard for an incident in a read-only format if they have also been assigned as a candidate to an ICS position. • Log in to eICS. • Access the eICS <i>Home</i> page, viewing brief, read-only details for an incident when assigned as a candidate to an ICS position. • Manage their profile, such as their contact information.
Incident	<p>When an incident occurs, an External Contact who is assigned to a position defined in the associated incident response guide (IRG) takes on that role. These individuals have access to the Incident Dashboard for the life of the incident. They can add to and change information in the Incident Dashboard by adding events to the log, adding to the incident's library, updating the status of their position's objectives, sending messages to other participants, and much more. Once the incident is ended, these users can no longer access the dashboard.</p> <p>External Contacts without user accounts do not have access to eICS. Generally, these are individuals in your Other Contacts to Notify group.</p>