Permissions

In eICS, contacts must be assigned a role for each facility to which they have access. Roles determine the permissions contacts have and permissions govern access to the system and, for those that have access, the level of tasks the contact can perform. Available roles include: Domain Administrator, Facility Administrator, Facility Staff, Facility Staff Limited, and External Contact.

When an incident occurs, another set of roles (positions) and permissions apply. In general, Facility Administrators and Staff take on ICS positions, acting as command staff, section chiefs, specialists, members of the labor pool, and so forth. As such, it is their incident position that governs their access and permissions during the incident.

The same is true for External Contacts. If an External Contact is assigned a position in an incident, this individual can access the incident dashboard during the incident and add to or make changes according to the permissions associated with their position.

Permissions by Feature

This table provides examples of common tasks or permissions and summarizes the ability of contact roles to perform the tasks.

Permission	Rights	External Contact	Facility Staff Limited	Facility Staff	Facility Admin	Domain Admin
Log In	Log in to eICS.	X*	X	X	X	X
Manage Personal Contact Information	Manage their own profile, including personal contact information, passwords, and security questions.	X*	X	X	X	X
View Facility Plan	View a facility's plan, contacts, and library.		X	X	X	X
Manage Incidents	Create, Escalate, End and Close Incidents			X	X	X
Administer Facility	Perform administrative tasks for a facility, such as managing contacts, the ICS plan, and library.				X	X
View Domain Plan	View a domain-level plan, library documents, and incident response guides, including performance objectives.			X	X	X
Copy Domain Plan	Copy a domain-level plan to start a new facility-level plan.				X	X
Administer Domain	Perform administrative tasks for the domain and its facilities, such as adding and editing facilities, assigning facilities to health system, managing domain-level users, and managing the facility plan template.					X

*Only applicable if the contact has access to eICS with an assigned login email and password.

> **Note**: An administrator has access to users in another facility or domain as long as the user for whom they are searching is in a health system associated with the administrator's facility.

Permissions by Incident

This table demonstrates user access and permissions during an active incident.

Permission	Rights	External Contact	Facility Staff Limited	Facility Staff	Facility Admin	Domain Admin
Start an incident	Start an incident at the facility.			X	X	X
View an incident	View all details of an incident for a facility.	X*	X	X	X	X
Update an incident	Add, edit, or delete details for an incident at their facility, change the operational period for an incident.	X+	X	X	X	X
Self assign to positions	Can assign themselves to incident positions.		X	X	X	X
End an incident	End an active incident.	X^	X^	X^	X	X
Close an incident	Close an incident that has ended and update details for a closed incident.				X	X
Report on *In Progress* and *Ended* incidents	Generate reports on an incident that is *In Progress* or *Ended*.		X	X	X	X
Report on *Closed* incidents	Generate reports on an incident that is *Closed*.				X	X

*External Contacts that are position candidates in the depth chart are automatically granted *View* rights for an active incident.

+Only applicable if the contact has access to eICS and has been assigned an ICS position for the incident.

^Only applicable if the contact has been assigned the Incident Commander position for the incident.

Library Access

When an administrator creates a facility, a library is automatically created for it based on the domain-level library. In addition, when an incident is created, a copy of the facility's library is created for the incident and is available from the incident's dashboard.

This table lists library-related access by role.

Role	Access
Domain Administrator	Domain library: Add, edit, delete items; view versions; open items; override checkouts Active and ended incident library: Full access to folders and files Closed incident library: View access to folders and files
Facility Administrator	Domain library: View Library for their facility: Add, edit, delete items; view versions; open items; override checkouts Active and inactive (ended and closed) incident library for their facility: Add, edit, delete items
Facility Staff	Library for their facility: View For any incident in which the staff member participated: • Active incident library: Add, edit, delete items • Ended incident library: Add, edit, delete items • Closed incident library: View
Facility Staff Limited	Library for their facility: View For any incident in which the staff member participated: • Active incident library: Add, edit, delete items • Ended incident library: Add, edit, delete items • Closed incident library: View
External Contact	If granted permission to use eICS, for any incident in which this contact is or was involved: • Active incident library: View • Inactive incident (ended and closed) library: No access