

## Groups, Roles, and Privileges

[supportcenter.nc4.com/hc/en-us/articles/218311867-Groups-Roles-and-Privileges](https://supportcenter.nc4.com/hc/en-us/articles/218311867-Groups-Roles-and-Privileges)

Users are individuals who are given an ID and password with which to access the E Team application. Each user must be assigned privileges within E Team using E Team Groups and Roles.

**Groups** establish which roles/privileges the user will have while using E Team. A Group in E Team is based on the logical grouping of users who need to perform similar tasks or functions. When you organize users into groups, you reduce the administrative requirements of maintaining E Team. The E Team application contains generic groups for administering E Team in a simple, straightforward manner. After you have created a user, you need only to add the user name to the appropriate group(s) or assign the group to the user, and that user then has all the access he/she requires. The E Team application is delivered with five predefined groups created specifically for each role. You can choose to use the groups that have been delivered with the application, or manually assign roles to individual users or groups.

E Team uses access levels referred to as roles. **Roles** relate to the ability of an individual user or a group to perform certain functions. Roles may apply to some but not all E Team reports and/or features.

**Privileges** define the access level(s) for each group or user. There are six (6) different types of privileges available within the E Team application. These privileges are identified on a report-by-report or feature-by-feature basis.

1. Reader – Grants the user access to read reports.
2. Author – NOT RECOMMENDED. Grants the user the right to create and update his/her OWN reports and read reports created by others. However, the user cannot edit reports created by others. This access level is not recommended since if User A creates a Resource Request and sends it to User B for processing, and User B has only Author access, User B will not be able to edit the document. Similarly, if User C creates an Incident Report, and User D needs to update this report with new information, if User D has only Author access, they won't be able to update the report. It is recommended that users be given Editor access instead. You can use the History and logging functions to catch inappropriate editing of documents and take appropriate action.
3. Editor – Grants the user access to create, read and edit reports.
4. Manager – Grants the user access to create, read, and edit reports.
5. Delete – Grants the user the right to delete reports.
6. Other – Grants user the rights to a specific feature or function of E Team and are clearly defined in the table provided. For example, this can be ability to see an option on the main toolbar, ability to approve document, ability to initiate transmission of document, ability to set access control or data sharing on a report.

*Download the attached E Team Privileges.docx to review all the privileges that are available for reports and features within the E Team application.*

### Roles

The E Team application is delivered with a number of predefined roles.

1. ETeam Admin – This role provides the user with majority of all privileges available within the E Team application.
2. ETeam Archive Restorer - This role provides the user with the ability to restore an archived document back to History.
3. ETeam ARE Access – This role provides the user with access to the ARE menu option on the E Team main screen when the ARE option has been enabled on your system.
4. ETeam Author – This role provides the user with all Author privileges for reports and features not related to the E Team Data Dictionary or E Team Administration functions.
5. ETeam CAP Transmit – This role provides users with the ability to see AND make changes to the Transmit field located on the CAP Alert document.
6. ETeam CustomFormViewConfig – This role provides the user with access to the Custom Form View Configuration document.
7. ETeam Dashboard Access – This role provides the user with access to the Dashboard option (when enabled) in the E Team Toolbar.
8. ETeam Data Archiver – This role provides the user with access to the Archive Configuration document and rights to initiate system wide data archive.
9. ETeam Editor – This role provides the user with all Editor privileges for reports and features not related to the E Team Data Dictionary or E Team Administration functions.
10. ETeam ERMS Admin – This role provides the user with access to the ERMS link visible on the Main Screen Toolbar when ERMS is enabled on the system and should be assigned to those users who manage their organization's ERMS account, including those who might be creating templates.
11. ETeam ERMS Enhanced Notification – This role provides the user with access to the Enhanced Notification option. When properly configured and enabled, this ERMS option will be visible under the Notification tab on E Team forms. ETERMSEnhancedNotification is contained in the new ETeam ERMS Enhanced Notification group only.
12. ETeam ERMS GeoNotification – This role provides the user with access to the Geo Notification option. When properly configured and enabled, this ERMS option will be visible under the Notification tab on E Team forms.
13. ETeam Everbridge Access – This role provides the user with access to the Everbridge notification option on the Notification tab of reports when the Everbridge option has been enabled on your system.
14. ETeam FormBuilderAccess – This role provides the user with all rights and access to the Form Builder (Custom Forms) option (when enabled). Option is located under the Administration menu.

15. Team Geoprocessing – This role provides the user with ability to see AND use the Intersect Layers tool in the Map Viewer when Geoprocessing has been enabled on your system.
16. ETeam Manager – This role provides the user with all privileges for reports and features not related to the E Team Administration functions.
17. ETeam Models – DO NOT USE
18. ETeam Overlay – This role provides users with the ability to view the overlay section of a report, and if given Editor privileges, create map overlays.
19. ETeam Override Lock – This role provides users with the ability to override document locks so that another user can take control of a document.
20. ETeam Profile Editor – This role provides user with the ability to edit all users Personal Profile documents.
21. ETeam Read All – This role provides users with the ability to view documents even though they are not a member of a Access Control Group (if Access Control was enabled on that report).
22. ETeam Reader-Only User – This role provides the user with all Reader privileges for reports and features not related to the E Team Data Dictionary or E Team Administration functions.
23. ETeam Registration Approver – This role provides users with the ability to see the Pending Registration and Registration History views, and the ability to approve/reject user registration. This role is contained in both ETeam System Admin and the new ETeam Registration Approver groups by default.
24. ETeam Release Locks – This role provides users with the ability to see the Document Locking view and release locks from within the view.
25. ETeam Resource Approver – This role provides users with the ability to see AND make changes to the Approved By field located on the Resource Request document.
26. ETeam Restore History – This role provides users with the ability to restore a deleted document in History to active use.
27. ETeam Task Approver – This role provides users with the ability to see AND make changes to the Approved By field located on the Task and Sub-Task reports.
28. ETeam TIP ISAC Editor – This role provides users with the ability to see AND make changes to the ISAC ONLY sections of the Tip Submission report.
29. ETeam TIP ISAC Reader – This role provides users with the ability to see the ISAC ONLY sections of the Tip Submission report.

*E Team roles ARE NOT editable and cannot be deleted. The majority of E Team customers continue to use these predefined roles, however, E Team provides the means by which to configure [new roles](#) that best meet the needs of each individual organization.*

## Groups

The E Team application is delivered with a number of predefined groups. These predefined groups work in conjunction with the predefined roles above.

1. ETeam ARE Access – This group contains the role ETeam ARE Access and is generally assigned to those users with Manager and Admin Roles.
2. ETeam Authors – This group contains the role ETeam Author. This Group is not recommended for most users and should be used only in special circumstances, such as, a special guest whose expertise is required but should have very limited access to the application.
3. ETeam CAP Transmit – This group contains the role ETeam CAP Transmit and should be assigned to those users who have authorization to initiate CAP transmissions.
4. ETeam CustomFormViewConfig – This role provides the user with access to the Custom Form View Configuration document and is generally assigned to those users with Manager and Admin Roles, as well as any user who will be expected to design custom forms.
5. ETeam Dashboard Access – This group contains the role ETeam Dashboard Access and is generally assigned to those users with Manager and Admin Roles.
6. ETeam Data Archiver – This group provides the user with access to the Archive Configuration document and rights to initiate system wide data archive.
7. ETeam Editors – This group contains the role ETeam Editor and is the most often assigned group to everyday E Team users.
8. ETeam ERMS Admin – This group contains the role ETeam ERMS Admin and should be assigned to those users who manage their organization's ERMS account, including those who might be creating templates.
9. ETeam ERMS Enhanced Notification – This role provides the user with access to the Enhanced Notification option. When properly configured and enabled, this ERMS option will be visible under the Notification tab on E Team forms. ETERMSEnhancedNotification is contained in the new ETeam ERMS Enhanced Notification group only.
10. ETeam ERMS GeoNotification – This group contains the role ETeam ERMS Geonotification and should be assigned to those users who have authorization to initiate ERMS geo notification broadcasts.
11. ETeam Everbridge Access – This group contains the role ETeam Everbridge Access and should be assigned to those users who have authorization to initiate Everbridge transmissions.
12. ETeam Formbuilder Access – This group contains the role ETeam Form Builder Access and is generally assigned to those users with Manager and Admin Roles, as well as any user who will be expected to design custom forms.
13. ETeam Geoprocessing – This group contains the role ETeam Geoprocessing and should be assigned to users who require the ability to use the Intersect Layers tool located on the Map Viewer when your system has been enabled for this feature
14. ETeam ISAC Editors – This group contains the role ETeam ISAC Editors and should be assigned to users who require the ability to enter data in fields designated as ISAC Only on the Tip Submission form.
15. ETeam ISAC Readers – This group contains the role ETeam ISAC Readers and should be assigned to users who require the ability to view data entered in fields designated as ISAC Only on the Tip Submission form.
16. ETeam Lock Override – This group contains the role ETeam Override Lock and is generally given to those users with Manager and Admin roles.

17. ETeam Managers – This group contains the role ETeam Manager and should be assigned to those individuals who need to have the ability to configure the E Team Data Dictionary keywords, color-coded status, and menus, and are authorized to delete documents within the system. E Team Managers DO NOT have access to the E Team administration functions.
18. ETeam Map Overlays – This group contains the role ETeam Overlay and should be assigned to those individuals who require the ability to view the overlay section of a report and, if given Editor privileges to that report, create map overlays.
19. ETeam Model – DO NOT USE
20. ETeam Profile Editor – This role provides user with the ability to edit all users Personal Profile documents.
21. ETeam Read All Docs – This group contains the role ETeam Read All and should be given with discretion as it allows a user to Read ALL documents within the application even if they have no Access Control rights to that document.
22. ETeam Read-Only Users – This group contains the role ETeam Reader. This group is most often assigned to visitors or observers who have no need to enter information into the application.
23. ETeam Registration Approver – This group contains the role ETeam Registration approver, providing users with the ability to see the Pending Registration and Registration History views, and the ability to approve/reject user registration.
24. ETeam Release Locks – This group contains the role ETeam Release Locks and is generally given only to those with System Admin privileges. A user in this group can release a lock from any document within the application.
25. ETeam Resource Approvers – This group contains the role ETeam Resource Approver. This is generally given only to those individuals whose responsibility it is to approve procurements.
26. ETeam Restore Archive – This role provides users with the ability to restore an archived document.
27. ETeam Restore History – This role provides users with the ability to restore a deleted document in History to active use.
28. ETeam System Admin – This group contains the role ETeam Admin and should be assigned only to those individuals who should have access to the E Team administration functions.
29. ETeam Task Approvers – This group contains the role ETeam Task Approver. This is generally given only to those individuals whose responsibility it is to approve tasks and sub-tasks.

*E Team groups ARE NOT editable and cannot be deleted. The majority of E Team customers continue to use these predefined groups, however, E Team provides the means by which to configure [new groups](#) that best meet the needs of each individual organization.*

### Creating a Groups and Roles and Assigning Access Levels

There are two steps required to create groups and assign roles/privileges within E Team.

- Create a group, and
- Create a role assigning privileges to the group

As an example, the steps below describe how to create a procurement group with the ability to edit resource requests and critical asset reports and read incident and event reports.

1. Select Group under Administration from the menu. The system displays the Groups by Name view in the View Frame.
2. Click on the *Create* button in the View Frame. The system displays a new Group Administration document in the update mode.
3. Enter *Group Name*. Example: Procurement Department, this name will display in the Groups selection window when assigning roles and privileges.
4. Enter a *Description* for this group. Example: Assign to all members of the Procurement Department. This description is for administration purposes only and will not display anywhere else in the system.
5. Click on *Submit*. The system saves the group and closes the document.
6. Select *Role* under Administration in the menu. The system displays the Role by name view in the View Frame.
7. Click on the *Create* button in the View Frame. The system displays a new Role Administration document in a new window.
8. Enter *Role Name*. Example: Procurement.
9. Enter a *Description* for this Role. Example: Full access to resources and assets, read only incidents/events. This description is for administration purposes only and will not display anywhere else in the system.
10. In the *Groups* field highlight the newly created Procurement Department group in the left window and click on *Add*. The system displays your selection in the window on the right.
11. In the *Privileges* field scroll through the list and highlight each of the following selections and click on Add. You can hold down the control key to make the multiple selections. This list is extensive and listed alphabetically.
  - *critical\_asset (EDITOR)*
  - *emergency\_event (READER)*
  - *incident (READER)*
  - *planned\_event (READER)*

*In addition to setting privileges to read and/or edit reports, you will need to provide the following functional privileges.*

- *attachments(EDITOR)*
- *notification(EDITOR)*
- *distributions(EDITOR)*
- *data\_sharing(EDITOR)*

*These privileges **MUST** be given if you want this group to have the ability to view and edit all sections of the documents to which they have been given EDITOR privileges AND to view these sections of the documents to which they have been given READER privileges.*

*Download the attached E Team Privileges.docx to review all the privileges that are available for reports and features within the E Team application.*

12. When all selections have been added to the Privilege window at the right, click on *Submit*. The system saves and closes newly created Role Administration document and displays it in the View Frame.

*Customer defined Roles and Groups can be deleted, however you **MUST** first remove the role/group from within any existing group or user document in order to ensure your users have proper access within E Team after the deletion(s) occur.*