

General System Configuration

 supportcenter.nc4.com/hc/en-us/articles/218144327-General-System-Configuration

Some of the information in the *General Configuration* document is obtained by the system during the installation process.

To begin, log into your E Team application:

1. Open your browser.
2. Enter the URL given to your application during the installation process. This URL will include the following: `http(s)://<server_ip>:<port>/<customer_name>`.
The system displays the E Team Welcome Screen.
3. Enter the User ID and Password created during installation and click on Login.
4. Click on Operations.
The system displays the E Team main window.
5. Complete the *Personal Profile* document presented and click on Submit.
The E Team main window displays.
6. Select the **Configuration** option under **Administration** from the menu.
The system displays the available General Configuration Document in the center View Frame.
7. Click on the hyperlink to the *General Configuration Document*.
8. Click on the **Update** button.
The system displays the General Configuration Document in update mode with the Basic Info tab in focus.
9. On each tab (shown following), enter the data necessary. When you are finished, click on **Submit** to save and close the document.

Basic Info Tab

1. System ID: No action required. Identifies the ID given to your application during the installation process. This must be provided to data sharing partner(s).
2. Customer Name: No action required. Identifies the Name given to your application during the installation process. This must be provided to data sharing partner(s).
3. Customer Display Name: Enter the "System" name that will appear to users at the top of the E Team main window.
4. Customer Time Zone: Make a selection from the drop down to set the Time Zone stamp that will be used throughout the application. The system default is PST. This value can be edited during installation.
5. Alternate Timezone Display: Used to display and alternate text value in place of the timezone acronym that normally displays with the selected timezone setting.
6. Enter text to display in your frame. Used to create a custom Welcome Page. Use this field to include text on your page. Please limit to 550 characters. Text will display in the top frame of the E Team Welcome screen. You must enter in standard html format as shown in the example below.

Example:

```
<html><body>

</body>

<center>

YOUR TEXT HERE

</center>

</html>
```

7. Customer Logo: Used to create a custom Welcome Page. Upload an image to display. Image used here must be .gif or .jpg 216w x 379h pixels.

Additional Info Tab

1. Report Refresh Interval: Make a selection from the drop down to set the frequency in which views are automatically refreshed. Valid choices are 1 thru 9. The default value is 1 minute.

Note: Auto-Refresh can be turned ON or OFF by users in E Team's View Frame. When ON, the E Team application refreshes the report views at the established intervals so that the most current information is displayed. A message displays at the top of the view screen to indicate how long it has been since the last refresh.
2. Records Per Listing Page: Enter the number of lines that will appear in a view. The default value is 99.
3. Lines of Situation Summary Displayed in View: Enter the number of lines that will appear in a view column for the situation summary field used on form instances.

4. SSL Only Enabled?: Make the proper selection to indicate whether your E Team system is SSL enabled.
 5. ARE Enabled?: Make the proper selection to enable or disable the ARE option. When disabled, the ARE icon on the toolbar of the E Team main window is hidden.
 6. ARE URL: To use the integrated viewer, enter url as shown: `http://<servername>:<portname>/nc4are`, or `http://<servername>:<portname>/nc4areTraining`.
 7. EIM Enabled?: Make the proper selection to enable or disable the EIM option. When disabled, the EIM icon on the toolbar of the E Team main window is hidden.
 8. EIM URL: Enter the full URL required to launch your EIM window.
 9. Dashboard Enabled?: Make the proper selection to enable or disable the Dashboard option. When disabled, the Dashboard icon on the toolbar of the E Team main window is hidden.
 10. Dashboard URL: Enter the full URL required to launch your Dashboard window.
 11. Configuration Parameter: Enter the full url to access Dashboard via SOAP. e.g., `http_protocol//server-ip:application- port/customer-name/`
 12. Password Format: Make the proper selection to set the password format required when creating User IDs and/or updating user passwords. The default is BASIC.
 - When BASIC is selected password MUST be a minimum of 6 and a maximum of 20 characters.
 - When STRONG is selected password MUST adhere to the following requirements.

Is at least seven characters long and contain characters from three of the following four character sets:

Uppercase Alphabet (A-Z), Lowercase Alphabet (a-z), Numeric digits (0-9), Punctuation !@#\$%^&+=/? but not: (- left parenthesis,) - right parenthesis, * - asterisk, \ - backslash, blank space.*
 13. User Action Logging Enabled?: Make the proper selection to enable or disable the User Action Logging option. The default is NO. When disabled user click actions will NOT be recorded. When enabled every click action taken by a logged in user will be recorded.
 14. No. of Invalid Login Attempts Before User is Locked Out: Make a selection from the drop down to set the number of consecutive, unsuccessful login attempts that can be made before a user is locked out of E Team. Valid choices are 0, 3, and 5. Default is 0, which disables this feature.
- When set to 3 or 5, a user will be prevented from logging into the E Team application after making the applicable number of consecutive invalid attempts or attempting password retrieval using the Forgot Password link from the login page.
- Login in error is based on entry of invalid username and/or password. Errors entering CAPTCHA string are excluded from this process.
15. Email Address for User Lockout Notification: Enter the email address to be used to notify a designated user with administrative privileges when a user has been locked out of E Team.
- The system will generate an email notification to the address provided in this field. It is intended to be the responsibility of this person to contact the user, authenticate using the security question contained in the associated Personal Profile document and unlock the login lock for the user id. Although only the designated admin user will receive an email notification regarding lock out, any E Team user with the proper rights will have the ability to complete the unlock process.
16. LTPA Configuration Encryption Key: Contact NC4 for additional information
 17. LTPA Encryption Passphrase: Contact NC4 for additional information
 18. Registration Process Enabled?: Make the proper selection to enable or disable the User Self Registration Process. The default is NO. When enabled, it will provide the capability for new users to self register.
 19. Default IPAWS Sender Name: Enter the name of the *Sender* on the CAP reports for NWEM. The NWEM HazCollect server expects Name, City, State. If this is left blank, the system will enter LastName, FirstName from the author's Personal Profile document.
 20. IPAWS Identifier Prefix: The value entered here is appended to the beginning of the Identifier on all CAP messages. This supports the ability to more easily identify the reports that have been sent by this system when viewing/retrieving alerts using the IPAWS - OPEN Alerts List. If this field is left blank the system will display your identifier with an NR then the alert number generated by the system. Ex: NR144926568031212

Notification Server Tab

1. SMTP Host: No action required. Outbound mail is established during the installation process.
2. SMTP User Name: No action required. Outbound (SMTP) mail User Name is entered during the installation process.
3. SMTP Password: No action required. Outbound (SMTP) mail Password is entered during the installation process.
4. POP Host: No action required. Mail-in host is established during the installation process.
5. POP User Name: No action required. Mail-in (POP) User Name is entered during the installation process.
6. POP Password: No action required. Mail-in (POP) Password is entered during the installation process.

7. Everbridge URL: Enter the URL supplied by Everbridge.
8. Everbridge Organization: Enter the Organization Name supplied by Everbridge.
9. Everbridge User Name: Enter the Member ID supplied by Everbridge.
10. Everbridge Password: Enter the Password supplied by Everbridge.

Prior to configuring E Team to use with Everbridge, your organization must already have an existing, or obtain a new, Everbridge account and have completed configuration within Everbridge. Configuration in E Team is NOT complete until Everbridge Notification is set to YES under the Agent tab. Go [here](#) for full information on using E Team with your Everbridge account.

11. ERMS URL: Enter the URL supplied by ERMS.
12. Organization ID: Enter the Organization Name supplied by ERMS.
13. API Password: Enter the Password supplied by ERMS
14. From User Id for Geo Notification: This must be the ID of a stakeholder within ERMS. The first and last name associated with this stakeholder will be used within the broadcast. You may create an ERMS ID with first name "City of" and last Name "Your City" for example. This value MUST match an existing stakeholder value in ERMS.
15. URL to be used for Single Sign On: Enter the URL supplied by ERMS.
16. Stakeholder/Site Daily Runtime: Enter the time of day (using 24 hour clock) to sync ERMS stakeholder and E Team user data. The E Team system is considered the master. E Team data will be used to update Stakeholder data in ERMS.
17. Email Address(es) to send daily report: Enter the email address(es) to be used by the system to generate notification report with results of Stakeholder/Site Daily Run.

Prior to configuring E Team to use with ERMS, your organization must already have an existing, or obtain a new, ERMS account and have completed configuration within ERMS. Configuration in E Team is NOT complete until ERMS Notification is set to YES under the Agent tab. Go [here](#) for full information on using E Team with your ERMS account.

Agent Tab

1. Notification Agent Enabled?: Make the proper selection to enable or disable Notification for each option.
 - Standard supports notification within E Team forms. Default is YES.
 - Everbridge supports notification using your Everbridge account. Default is NO. When set to YES, users with the proper rights will see the option to select *Enhanced Notification* on all E Team forms under the Notification tab.
 - ERMS supports notification using your ERMS account. Default is NO. When set to YES, users with the proper rights will see the option to select *Enhanced Notification* on all E Team forms under the Notification tab AND when used, the option to select *Geo Notification* to include transmission of a map overlay within the package transmitted to ERMS.

Both Standard and Everbridge or ERMS can be set to YES.

2. From Email Address for Notification: Enter the email address that should appear in the "from" field on notifications sent via the application.
3. From URL Address for Notification: No action required. Displays the application URL. This will be used when hyperlinks are contained within a notification sent via the application.
4. Automatic Profile Update Enabled?: Make the proper selection to enable or disable automatic profile update. The default is NO.

Download the attached file [AutoProfileUpdateEmail.docx](#) to view an example of the email generated to users.

5. Automatic Profile Update Age: Enter in days profile age to be used. The system is designed to allow for automatic update requests, via email, to E Team user's for which an email address has been established in their Profile Module. The email will state that their Profile has not been updated in "X" days, with "X" being the number set in this field Following is an example of what the automatic profile update looks like.

Every night at 4:00 am, the system will identify profiles that meet the criteria as defined in this field. If the system identifies Profiles requiring updates, it automatically sends out an email to those users.

When a user responds to the email sent by the system, incoming requests are processed automatically and the profiles are updated accordingly.

6. Automatic Profile Update Email: Enter email address where the return Profile Update emails go within your organization for processing.
7. Force Password Change on First Login?: Make the proper selection to enable or disable requirement for new users to change their password on first login.
8. Password Expiration: Make the proper selection to enable or disable the Password Expiration function. Default is NO.

If users have been restricted from updating their own passwords by setting the Data Dictionary keyword `UserChangePassword` to `DISABLE`, this field MUST be set to NO or users will be unable to reset their passwords at time of expiration.

9. Password Expiration Age: Enter the age to be used for password expiration. Valid choices are 30, 45, 60, and 90 days.

The field *Password Expiration* is used to enable/disable use of password expiration. If Password Expiration is set to “Yes” Password Expiration Age will be required.

A password expiration scheduler will run each day at midnight. When seven (7) or less days remain to password expiration or a password is expired, the system will generate an email notification to the associated user. Email address used will be from the “E-Mail” field on the associated Personal Profile document. If no email exists, no notification can be generated. Email notification will be generated each 24 hour period until such time as the user password is reset.

In addition to an email notification for password expiration, each time a user logs in during the 7 day expiration period they will be presented with a pop up dialog message warning them of impending password expiration.

Should a user NOT reset their password within the 7 day expiration period, on first login after expiration the user’s Personal Profile will be forced and on submit the user will be prompted to reset their password.

Submission of the profile will be prevented until such time as the password is reset.

10. Alert Bulletin Enabled?: Make the proper selection to enable or disable the Alert Bulletin Pop-up function available within E Team will be used. Default is YES.
11. Data Sharing Agent Enabled?: Make the proper selection to enable or disable the ETeam-to-ETeam Data Sharing feature. Default is NO.
12. Custom Forms Enabled?: Make the proper selection to enable or disable the Custom Forms feature based on your operational needs. Default is NO.
13. Auto Closure Enabled?: Make the proper selection to enable or disable the Auto-Closure feature.

When the top-level Event status is set to Blue-Report Closed, this feature enables the system to process all reports related to the Event, including related Incidents. The Auto Closure process is run on a timer, and the capability is featured on both Emergency and Planned Events.

When set to YES, the Auto Closure process is triggered on the Close of an Event and runs on a regular cycle, approximately every 17 minutes.

When set to NO, the Auto Closure process is disabled. All Events set to Auto Closure while the feature is disabled will remain in the Auto Closure queue. When next enabled, the Auto Closure process for all items in the queue will be triggered.

It is recommended that this be set to NO during activation or when running an Auto Closure that includes a significantly large number of reports, then reset to YES to allow for processing during low system usage to prevent potential performance hits.

Please download the attached E Team Auto-Closure Report Handling Detail.docx below to learn how each report will be handled by the system during the Auto Closure process.

14. Global Auto Refresh Enabled? Select the appropriate radio button. Establishes whether or not auto refresh of views has been enabled for all users. Default is NO. When set to YES the auto refresh option at the top of E Team view frame will be set to ON for all users. Once set to YES on the General Configuration document users will NOT have the option to turn it off.
15. Risk Center Incident Closure (Not Updated): Select the life cycle for NC4 Risk Center incidents within E Team. When properly configured the system will check for any Incident generated via the interface that has not been updated in the selected duration, and update the document changing the status to Blue-Closed, removing the Incident from the active E Team Incident views.
The available values are generated using the Data Dictionary keyword *IncidentRiskCenterDuration*. The delivered values are: Disable, 24, 48, 72, 96.
16. HeartBeat Interval: Enter the frequency through which the system controls document locking, user locking, targeted alert, and general alert pop-ups will display to users. Enter number of seconds between Alerts. Default value is 30 seconds.