

## NC4 Risk Center-to-E Team Configuration

[supportcenter.nc4.com/hc/en-us/articles/218015637-NC4-Risk-Center-to-E-Team-Configuration](https://supportcenter.nc4.com/hc/en-us/articles/218015637-NC4-Risk-Center-to-E-Team-Configuration)

### About the Interface

The NC4 Risk Center-to-E Team Interface allows users to configure an NC4 Risk Center alert profile to dynamically accept data feeds from NC4 Risk Center directly into their existing E Team database (profiles are established using the same filters currently available to E Team users). In addition, the interface includes the ability to capture and update ISA Incidents. In this way, incident data from both the NC4 Risk Center as well as from ISA is automatically integrated into the E Team system.

The NC4 Risk Center incident data is imported from the NC4 Risk Center database to an E Team incident report, and is shown as an incident with a status of gray. The text associated to the incident's status is the value as defined in the E Team Data Dictionary Color Code *StatusIncident* document.

The following fields are entered from NC4 Risk Center directly into an E Team Incident report:

- Incident Name
- Incident Number
- Incident Type
- Incident Date/Time and Location
- Incident Status
- Lead Agency (EOC) Situation Summary Date/Time and Updates (reflected as new Situation Summaries to existing incidents).

### Setting-Up the Connection

*An NC4 System Administrator or C&S member will provide assistance and guidance with setting-up NC4 Risk Center-to-E Team.*

Setting-up the connection requires:

- Outlining provisions to set up CAP
- Configuring the Alert Profiles
- Selecting the appropriate device type within the NC4 Risk Center application. CAP should be the choice.
- Entering the appropriate CAP address as your Notification Device.
- Developing an appropriate work flow.

### Deploying NC4 Risk Center for E Team

The information provided below details the steps required within ETeam. User must be an E Team System Administrator with access to the E Team server.

1. Obtain and unzip ESAISAImport.zip to \eTeamInc\TeamWebApp.  
*Please note there is no need to stop the eteam service.*
2. From a command prompt run ura. This does the following:
  - Moves all necessary files into place.
  - Asks for changes to the EteamImport.properties file.
  - Updates the war when necessary.

When opened and set up properly, the page should resemble the screen shot below.

The values at the bottom for status and prognosis will help determine the values for the \eTeamInc\TeamWebApp\ETeamImport.properties. Changes can be made to these values at any time following the instructions that are provided after running ura in the browser.



### Configuring NC4 Risk Center for use with E Team

The information provided below details the steps required within Risk Center.

NC4 Risk Center is configured by the user to their particular geo-graphic areas, the type of alerts they would like to see, and multiple device profiles for sending alerts. For the E Team interface, one of the device profiles must be set up to issue CAP alerts.

- Log into NC4 Risk Center and go to Device Profile3

#### Devices tab:

- Email:** Enter a value (this is not used for E Team but is required to complete the device setup)
- Service Provider:** Leave as Pick One
- Device Type:** Select CAP (if you do not see this option contact NC4 Support)
- Click **Save** when done.

#### Severity tab:

	Extreme	Severe	Moderate	Minor	Unknown
Device 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Under the Device number used for CAP, check the incident severity for which you wish to be notified. Check all that apply.
- Click **Save** when done.

#### Other Alert Types tab:

	Other Intel	Device Tracking	ActivWeather	Global Intelligence Relay	Location / Document	Error Messages
Device 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- No action needed.** All items are checked by default when CAP is selected as *Device Type*.

#### CAP tab:

- Under the Device number used for CAP

- **Destination URL:** This is the web address(must be a publicly accessible ) of the servlet installed on the host E Team system. For instance, given a standard E Team installation on server `http://nc4vm.nc4.us`, the value entered would be `http:// nc4vm.nc4.us /ESAISInterface/ETeamImport`.
  - **Handler:** Select SOAP handler
  - **Allow attachments:** Leave unchecked. The interface does not support attachments
  - **User ID:** This is a user name that matches a user name entered on the target E Team system with a minimum of editor rights.
  - **Password:** The corresponding E Team password of the user entered.
- Click **Save** when done.

The system can now begin issuing CAP alerts to the target E Team system.

#### Configuring E Team for NC4 Risk Center Maintenance

You may set a 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*. This will remove the Incident from the active E Team Incident views. The Incident will continue to be visible in the *Incident All (Includes Closed)* view.

To set the life cycle:

1. Log into E Team
2. Go to Data Administration > Configuration
3. Place the General Configuration document in update mode
4. Select the Agent tab
5. Using the drop down provided, set value for NC4 Risk Center Incident Closure (Not Updated)
6. Submit the document

Options provided in the *NC4 Risk Center Incident Closure (Not Updated)* field are generated using the Data Dictionary keyword *IncidentRiskCenterDuration*. The delivered values are: Disable, 24, 48, 72, 96.

#### NC4 Risk Center and E Team Field Mapping Guide

To see how Risk Center data appears on your E Team incidents, download the attached file *E Team NIMC Incident Interface Field Data Mapping.docx*.