

Version 25



Trapeze

Enterprise Asset Management

Risk, Incident, and Safety Compliance

Integration Guide

Trade Secret | July 2025

© 2025 Trapeze Software ULC, its subsidiaries and affiliates (collectively “TSU”). All rights reserved.

Trapeze Software ULC (“TSU”) Proprietary and Confidential: Information contained in this document is proprietary to TSU and its subsidiaries and may be used or disclosed only with written permission from TSU. This guide, or any part thereof, may not be reproduced without the prior written permission of TSU. The recipient acknowledges and agrees that disclosure of this document to recipient, and its use, are subject to the terms and conditions specified in their relevant software license agreement, software maintenance agreement, and/or non-disclosure agreement (“Governing Agreement”) under which this document was disclosed. This document is for internal use only in conjunction with TSU products. This document may not be modified in any way.

All other trademarks, registered trademarks, product names and company names or logos mentioned are the property of their respective owners.

Except as may be provided in the Governing Agreement, TSU and its affiliates, subsidiaries, officers, directors, employees, and agents provide the information contained in this manual on an “as-is” basis and do not make any express or implied warranties or representations with respect to such information including, without limitation, warranties as to non-infringement, reliability, fitness for a particular purpose, usefulness, completeness, accuracy or currentness. TSU shall not in any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including without limitation, damages resulting from use of or reliance on information presented herein, or loss of profits or revenues or costs of replacement goods, even if informed in advance of the possibility of such damages.

TSU reserves the right, to be exercised at its sole discretion and without notice, to change, modify or adapt the contents of this edition in order to accurately reflect any future upgrades to the TSU proprietary software and/or hardware. In the event of such changes, TSU expects, but does not represent or guarantee, that this current edition will continue to remain reasonably accurate insofar as it describes the basic functions of the TSU proprietary software and/or hardware. Furthermore, based on your system settings, certain functionality, such as application screens, may not function exactly as shown or described in this guide.

Technical Support

Trapeze provides several ways to connect with the Customer Care team. Please provide detailed information to the representative. If you are reporting an issue by e-mail, include any error messages, screen shots of your problem, and steps to replicate the issue.

Customer Care is available Monday through Friday, 8:00 a.m. to 8:00 p.m., Eastern Standard Time.

Toll-Free Telephone: 1-877-411-8727

E-mail: cc@trapezegroup.com

FTP Site: <https://ftps.trapezegroup.com/>

Web Site: <https://collaborate.trapezegroup.com>

The website provides access to Trapeze Collaborate which offers resources to implement and operate the software, search knowledge, participate in communities, log/track service requests, sign-up for release alerts, view product health recommendations, and download updates or documentation. For secure access to Collaborate, contact Customer Care through the website or by calling the number above.

Product Compatibility

Refer to the latest [Product Compatibility](#) information on Trapeze Collaborate for requirements including operating system information, databases, Crystal reports, network protocol, HTTP servers and browsers that are supported.

RISC – Integration Guide

Version 25.x

July 2025

Contents

1. Overview	2
Requirements	2
2. EAM Application Configuration.....	2
Safety Event Management Portal Configuration in EAM.....	3
Safety Event Management Portal in EAM	3
Data Requirements.....	5
3. MAXQueue Configuration.....	6
Trapeze - RISC - Incidents - Inbound.....	6
Trapeze - RISC - Service Requests - Inbound.....	7
Trapeze - RISC - Service Requests - Outbound	8
Trapeze - RISC - Delays - Outbound	9
Trapeze - RISC - Roles - Outbound	9
Trapeze - RISC - Users Outbound	10

1. Overview

EAM Incident Management can now be integrated with RISC (Risk, Incident, and Safety Compliance). This allows clients to interact directly with RISC to manage incidents while integrating with EAM which provides feedback for reporting or performance evaluation to schedule service requests and maintenance on assets.

EAM and RISC Integrations sync data between systems using 2-way integrations and Data Services API to keep information up-to-date.

Requirements

- EAM Version 24.1.0 or higher
- EAM API must be installed and accessible
 - EAM Data Services API Enterprise License is required for RISC to access API endpoints
- EAM MAXQueue Package including RISC Integrations – RISC Integration Services must be installed and enabled

2. EAM Application Configuration

Safety Event Management Portal Configuration in EAM

1. Launch the **Setup - Options** screen.
2. Check the **Use RISC for Incident Management** check box. This feature will not allow EAM users to make any changes to incidents in the EAM application.
3. Enter the RISC login URL: <https://risc.trapezeapps.com>.

The screenshot shows the 'Setup - Options' screen in EAM. The top header is 'Setup - Options' with a red circle labeled '1'. Below the header is a table with columns: 'Row #', 'Maximum days before today for valid date entry', 'Maximum days after today for valid date entry', and 'Account ID'. The 'Options' section is expanded, showing 'Edit Criteria - General'. In this section, the 'Maximum days from today for valid date entry' is set to 'Before' and 'After'. The 'Account ID' dropdown is set to 'REQUIRED'. The 'Require account group ID for account ID' checkbox is unchecked. The 'Restrict account ID choicelist based on department supported accounts' dropdown is set to 'NEVER'. The 'Current year' and 'Fiscal year end month' are set to '1' and '1' respectively. The 'Reset historical cost fiscal settings' button is visible. The 'Use RISC for Incident Management' checkbox is highlighted with a red box and a red circle labeled '2'. The 'RISC URL' text box is highlighted with a red box and a red circle labeled '3'.

Safety Event Management Portal in EAM

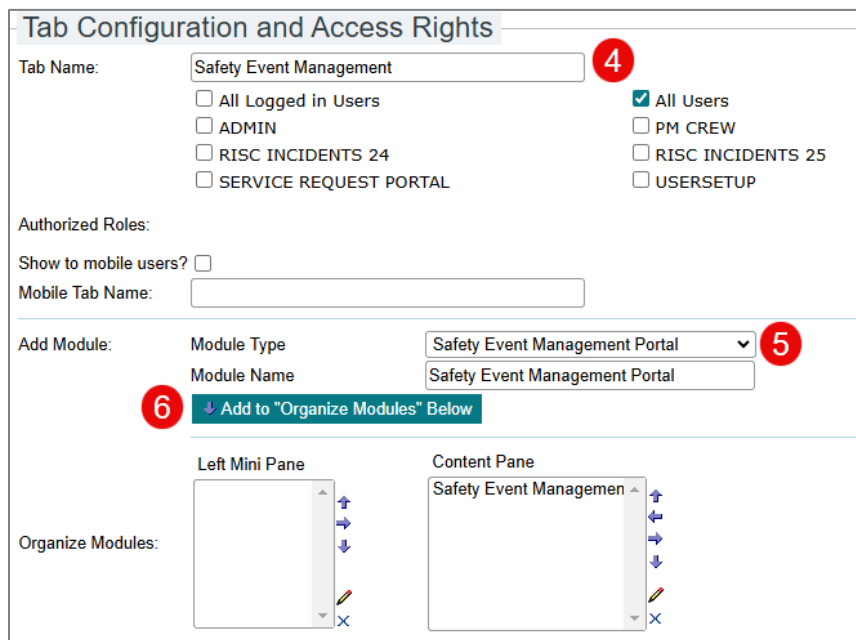
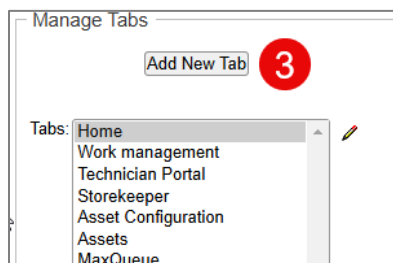
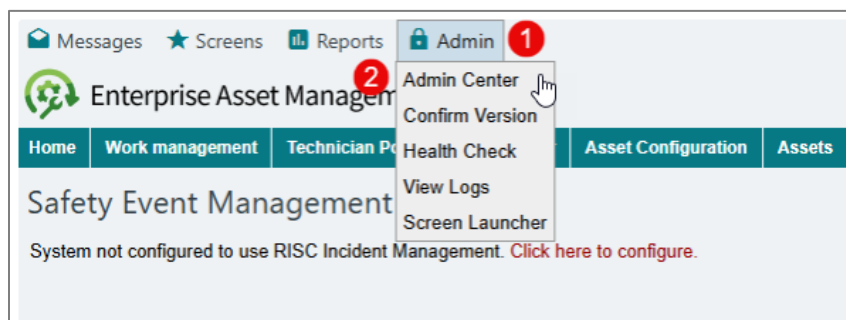
1. Click the **Admin** button at the top center of the screen.
2. Click the **Admin Center** button.
3. Click **Add New Tab** button.
4. Name the RISC tab **Safety Event Management**.
5. Select the Safety Event Management Portal as the module type.

6. Click the **Add to Organize Modules Below** button.

7. Click **Save**.

After that, the EAM user can navigate to the **Safety Event Management** tab and click the **Open RISC Safety Event Management** button. This button will redirect the EAM user to the RISC portal.

 Note: If the portal displays the following message: “System not configured to use RISC Incident Management. Click here to configure”, the EAM user needs to configure the RISC settings in the **Setup - Options** screen.



Data Requirements

Users

A user is required for RISC to connect to the Trapeze API. Create a new RISC user for the API to connect.

User ID	RISC-API-USER	RISC API USER
Basic Info		
Name	RISC API USER	

3. MAXQueue Configuration

Trapeze - RISC - Incidents - Inbound

The MAXQueue User must enable Timer adapter and commit changes.

MAXQueue User must open the Instance Configuration settings to input configuration values for the MAXQueue integration.

MAXQueue User must enter the following EAM application credentials:

1. vars.ApplicationUser - Enter username
2. vars.ApplicationPassword - Enter user password

MAXQueue user must enter RISC API credentials:

1. vars.RISCAuthorizationApiUrl - Enter RISC authorization API URL
2. vars.RISCApiClientId - Enter RISC API client Id
3. vars.RISCApiClientSecret - Enter RISC API client secret
4. vars.RISCApiScope - Enter RISC API scope
5. vars.RISCIncidentApiUrl - Enter RISC Incidents API URL

Create RISC Incident Attribute:

MAXQueue service creates RISC type incidents and adds an attribute name to it. This attribute name helps distinguish between RISC type incidents and non-RISC type incidents. The value can be configured in the Incident Attribute Name field in the Instance Configuration settings. The default value is RISCSAFETYEVENTID.

The EAM user needs to launch the Incident Attributes screen then enter the Incident Attribute ID field RISCSAFETYEVENTID or any other field name configured in the Incident Attribute Name field. This will cause any RISC incident in EAM to have the RISCSAFETYEVENTID value. This value distinguishes between RISC incident types and non-RISC incident types. When a new RISC type incident is created in EAM via the MaxQueue service, the EAM user should be able to find it on the Attributes tab of the Incident Management screen. The Attribute ID and Name should be RISCSAFETYEVENTID. The Text value field should have the RISC GUID ID.



Note: The MAXQueue user should NOT change the Incident Attribute ID field after initial configuration. This is because the service will ignore any EAM incidents that do not have an attribute name that matches vars.IncidentAttributeName which means the service will not delete or update them unless they have the matching attribute names.

Delete RISC Incident:

EAM does not delete incidents. If a RISC incident is deleted, the MaxQueue service will *soft delete* it. It will change the status to the value configured in vars.DeletedIncidentStatus. The default value is VOID.

The MaxQueue user can change it by opening the Instance Configuration settings. Under Service Variables, the vars.DeletedIncidentStatus value can be changed.

Change Staging Table Event Type for RISC:

RISC sends data to EAM 's staging table. MaxQueue service parses the data and transforms it into EAM data. MaxQueue service searches for the Event Key column for the value stored in vars.RISCIncidentsStagingEventType. The default value is RISCINCIDENTS. If the MaxQueue user wants to change the event key value, it needs to be done in the RISC environment and in the Instance Configuration, vars.RISCIncidentsStagingEventType value.

Trapeze - RISC - Service Requests - Inbound

MaxQueue user must enable Timer adapter and commit changes.

MaxQueue user must open the Instance Configuration settings to input configuration values for the MaxQueue integration.

MaxQueue user must enter EAM application credentials:

1. vars.ApplicationUser - Enter username
2. vars.ApplicationPassword - Enter user password

MaxQueue user must enter the following RISC API credentials:

1. vars.RISCAuthorizationApiUrl - Enter RISC authorization API URL
2. vars.RISCApiClientId - Enter RISC API client Id
3. vars.RISCApiClientSecret - Enter RISC API client secret
4. vars.RISCApiScope - Enter RISC API scope
5. vars.RISCServiceRequestsApiUrl - Enter RISC Service Requests API URL

MaxQueue user must enter Service Variables for Service Request defaults

1. vars.DeletedSRStatus - EAM Status to apply to Service Requests marked as Deleted from RISC (ie: *Closed*)

2. vars.DefaultShopLocation - EAM Location to apply as the fallback Default Shop Location if it cannot be retrieved by the Asset or Symptom

Create RISC Service Request:

When RISC sends data to EAM, it is saved in the MaxQueue staging table. MaxQueue service tries to match the vars.RISCsRsStagingEventType value with the Event Key column in the table. The default value is "RISCservicerequest".

Change Staging Table Event Type for RISC Service Requests:

If MaxQueue wants to change the Event Key value for RISC service requests, it needs to do it in RISC environment and change the value vars.RISCsRsStagingEventType to match.

Trapeze - RISC - Service Requests - Outbound

MaxQueue user must enable Timer adapter and commit changes.

MaxQueue user must open the Instance Configuration settings to input configuration values for the MaxQueue integration.

MaxQueue user must enter the following EAM application credentials:

1. vars.ApplicationUser - Enter username
2. vars.ApplicationPassword - Enter user password

MaxQueue user must enter the following RISC API credentials:

1. vars.RISCauthorizationApiUrl - Enter RISC authorization API URL
2. vars.RISCapiClientId - Enter RISC API client Id
3. vars.RISCapiClientSecret - Enter RISC API client secret
4. vars.RISCapiScope - Enter RISC API scope
5. vars.RISCsRapiUrl - Enter RISC Service Requests API URL

Create RISC Service Request in EAM:

EAM user must add a RISC type Incident ID to any RISC type service request because that is how MAXQueue service checks if a service request is of RISC type. It checks the parent incident's attribute.

Any changes that happen to the service request will be synced with RISC database as long as the service request has RISC type incident Id.

Trapeze - RISC - Delays - Outbound

MaxQueue user must enable Timer adapter and commit changes.

MaxQueue user must open the Instance Configuration settings to input configuration values for the MAXQueue integration.

MaxQueue user must enter the following EAM application credentials:

1. vars.ApplicationUser - Enter username
2. vars.ApplicationPassword - Enter user password

MaxQueue user must enter the following RISC API credentials:

1. vars.RISCAuthorizationApiUrl - Enter RISC authorization API URL
2. vars.RISCApiClientId - Enter RISC API client Id
3. vars.RISCApiClientSecret - Enter RISC API client secret
4. vars.RISCApiScope - Enter RISC API scope
5. vars.RISCIncidentApiUrl - Enter RISC Incidents API URL

Create RISC Delay:

All RISC delays must be connected to RISC type incidents. MAXQueue user needs to configure Trapeze - Incidents - Inbound service before configuring this one.

EAM user needs to launch Incidents - Delays screen. EAM user needs to connect the delay to the incident by inputting the RISC Incident ID in the Parent Incident ID field. MAXQueue service will track any changes to the delay.

Trapeze - RISC - Roles - Outbound

MaxQueue user must enable Timer adapter and commit changes.

MaxQueue user must open the Instance Configuration settings to input configuration values for the MQ integration.

MaxQueue user must enter the following EAM application credentials:

1. vars.ApplicationUser - Enter username
2. vars.ApplicationPassword - Enter user password

MaxQueue user must enter the following RISC API credentials:

1. vars.RISCAuthorizationApiUrl - Enter RISC authorization API URL
2. vars.RISCApiClientId - Enter RISC API client Id
3. vars.RISCApiClientSecret - Enter RISC API client secret
4. vars.RISCApiScope - Enter RISC API scope
5. vars.RiscRoleApiUrl - Enter RISC Roles API URL
6. vars.GroupExternalCategory - Enter RISC group category

Create RISC Role:

MaxQueue service distinguishes between RISC type groups and non-RISC type groups by the value on the external category field in the User Groups screen. If the value in the field matches vars.GroupExternalCategory value, any users under that group will be tracked by this MaxQueue service and Trapeze - RISC - Users.

After launching the User Groups screen, the EAM user must enter the MaxQueue user input for vars.GroupExternalCategory in the External Category field. The EAM user needs to enter the External Identifier field into the RISC Role Id as it appears in RISC Roles API.



Note: The MaxQueue user should NOT change the External Category field after initial configuration. This is because the service will ignore any EAM roles that do not have an external category value that matches vars.GroupExternalCategory which means that the service will not delete or update users unless they have a user group with external category matching the vars.GroupExternalCategory value.

Trapeze - RISC - Users Outbound

MaxQueue user must enable Timer adapter and commit changes.

MaxQueue user must open the Instance Configuration settings to input configuration values for the MaxQueue integration.

MaxQueue user must enter the following EAM application credentials:

1. vars.ApplicationUser - Enter username
2. vars.ApplicationPassword - Enter user password

MaxQueue user must enter the following RISC API credentials:

1. vars.RISCAuthorizationApiUrl - Enter RISC authorization API URL
2. vars.RISCApiClientId - Enter RISC API client Id

3. vars.RISCApiClientSecret - Enter RISC API client secret
4. vars.RISCApiScope - Enter RISC API scope
5. vars.RiscUserApiUrl - Enter RISC Users API URL

Create RISC Users:

MAXQueue service processes changes to user records (create, update, delete) that belong to a RISC type role. Before using this service, the MAXQueue user needs to configure RISC roles in MAXQueue Trapeze - RISC – Roles service.

To add a user to RISC, the EAM user needs to add RISC role type to the user by launching the Users screen and adding a new RISC type group to the Groups Currently Assigned tab. If the service is running and the User has RISC role listed, any updates to the details in the Users screen will be synced with RISC Users API.

To remove a user from a RISC group, the EAM user must remove the RISC role from the Groups Currently Assigned list.