

Version 25



Trapeze

Enterprise Asset Management

Reporting Location Access Rights

Administrator and User Guide

Trade Secret | February 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://ftp.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.

Reporting Location Access Rights – Administrator and User Guide

Version 25.x
February 2025

Contents

1. Introduction	2
Purpose	2
Define EAM Crystal Reporting	2
Prerequisites	2
2. Enabling Location Access Rights Support	3
Overview	3
Crystal	3
Configure the Crystal Report	3
Configure the Screen ID in the report's xml file	4
Configure the choicelist SQL for each supported filter	5
EAM	6
Enable Location Access Rights for Users	6
Setup Location Access Rights for the Report's ScreenID	7
Extra: Setup the Location Access Rights template for Asset Chooser	7

1. Introduction

Purpose

The purpose of this document is to convey the necessary knowledge about the new support for Location Access Rights added to Trapeze EAM's Crystal Reporting module.

Define EAM Crystal Reporting

EAM supports a few different platforms for running reports against its database. One of these is Crystal Reporting. It allows for the execution of pre-created reports that can have real-time filters applied.

Prerequisites

1. Working EAM environment, including Crystal reporting being fully operational.
2. Access to the folder where EAM reports are stored. Modifications will need to be made to the .rpt and .xml files. Note: Modifying the .rpt file will require the Crystal Designer program is installed.
3. Working knowledge of how to use the Crystal Designer to design a report.
4. Working knowledge of SQL if you wish to apply Location Access Rights to report filter choice-lists.
5. Access to User Groups and Location Rights Template screens to configure them.

2. Enabling Location Access Rights Support

Overview

The ability to apply Location Access Rights security to Crystal reports has been added.

Each user in EAM will have a list of supported LocationIDs defined for a designated ScreenID that represents a specific report. This list of LocationIDs will be passed through to the report and the report will filter its data using them.

In the sections below, the necessary setup steps to enable and apply this new functionality are covered. It will require work to be done in the following areas:

1. Crystal
 - i. Configure the Crystal report in a report design.
 - ii. Configure the ScreenID in the report's .xml file.
 - iii. Configure the choice-list SQL to use for each supported filter in the .xml file.
2. EAM
 - i. Enable Location Access Rights for the users.
 - ii. Setup the Location Access Rights template for the report.
 - iii. Setup the Location Access Rights template for Asset Chooser

Crystal

Configure the Crystal Report

First, the Crystal report needs to support receiving a list of Location IDs from EAM. This will be done by editing the report in the Crystal Designer. There are two Formula Fields to add:

1. ReportLocationAccessRightsFlag
 - i. This is a field to indicate if EAM has determined that location access rights should be applied for this report. It will always exist and have the value of 'TRUE' or 'FALSE', with true meaning Location Access Rights should be applied.
2. ReportLocationAccessRights

- i. This is a '|' delineated list of EAM Location IDs that can be used to filter the data sources in the report.
- ii. If no EAM Location IDs were found, this will have a single value of 'EAMNOLOCATIONFOUNDEAM', which will not map to any location in your database and should return no records. Do not define this LocationID on the "Locations – Primary Information" screen as it is expected to not exist.

See the example below for an example of how to consume these fields. You will want to apply this to any data source to which you want to apply Location Access Rights security. In the example below, "RPT_EQUIPMENT.Access Rights Location" is the Access Rights Location defined on the asset and each record will be tested to verify this location is in the list provided from EAM. If it is not, the record will not be shown in the report.

```
(  
if {@ReportLocationAccessRightsFlag} = 'TRUE'  
then {RPT_EQUIPMENT.Access Rights Location} IN  
Split({@ReportLocationAccessRights}, "|")  
else  
1 = 1  
)
```

Configure the Screen ID in the report's xml file

To hook into the existing Location Access Rights infrastructure, each report that supports this will be assigned a unique ScreenID that does not exist in the system (e.x. ScreenID 9950). This Screen ID will be defined in the *.xml file associated to the report. Please do the following steps:

1. Determine a unique ScreenID that is not already in use in the system. As a starting value, you may use 9500 and increment by 1 for each report to which you wish to add support. Make note of the ScreenID you choose as you will need it later.
2. In File Explorer, navigate to the folder where EAM's report files are stored. Go to the report for which you want to add Location Access Rights.
3. Edit the xml file that has the same name as the *.rpt file.
4. At the bottom of the XML, after all the <FilterItem> tags but before the closing </ReportSettings> tag, enter the following XML, replacing the ScreenID value with the ScreenID that you chose.

- i. <ScreenID><Value>9500</Value></ScreenID>

5. Save and close the file.

This report has now been assigned the ScreenID that you chose. We will use this value later to configure what Locations a user/group has access to for this report.

See below for an example of what the .xml file would look like:

```
<ReportSettings>
  <FilterItem>
    <Name>Asset</Name>
    <DefaultValue>[ALL]</DefaultValue>
    <ChoiceList>RPTLV_EQ_ID</ChoiceList>
    <IsAsset>Y</IsAsset>
  </FilterItem>
  <ScreenID>
    <Value>9501</Value>
  </ScreenID>
</ReportSettings>
```

Configure the choicelist SQL for each supported filter

Crystal reports allows users running them in EAM to provide filter values to restrict data in the report (for example, choose a Priority ID). These filters have choice-lists associated with them that allow the user to see data defined in the system and pick what they want. To apply Location Access Rights to these choice-lists, you may define custom SQL to filter them based on the locations to which the user has access rights.

This SQL will support a keyword {ReportLocationAccessRights} that will swap the user's supported locations into the SQL query. This keyword will be a list of locations, so you will want to use the SQL IN operator to support it.

We will be adding an XML node into the report's XML file:

1. In File Explorer, navigate to the folder where EAM's report files are stored. Go to the report for which you would like to add Location Access Rights.
2. Edit the xml file that has the same name as the rpt file.
3. For each <FilterItem> tag that contains a <ChoiceList> tag, add a <SQL> tag to define the custom SQL that will consume the keyword.

- i. Example: <SQL>SELECT EQ_EQUIP_NO, DESCRIPTION FROM EQ_MAIN WHERE LOC_ACCESS_RTS_LOC IN ({ReportLocationAccessRights})</SQL>
 - ii. Note that the keyword ReportLocationAccessRights is surrounded by curly braces { }.
 - iii. Note that the curly braces are surrounded by parentheses ().
4. This SQL statement will be the data you see in the choice-list. The first column returned will be the value the user is wanting to select.
5. Save and close the file.

Those choice-lists will now have Location Access Rights security applied to them. See below for an example of what the XML file would look like:

```
<ReportSettings>
  <FilterItem>
    <Name>Asset</Name>
    <DefaultValue>[ALL]</DefaultValue>
    <ChoiceList>RPTLV_EQ_ID</ChoiceList>
    <SQL>SELECT EQ_EQUIP_NO, DESCRIPTION FROM EQ_MAIN WHERE
LOC_ACCESS_RTS_LOC IN ({ReportLocationAccessRights})</SQL>
  </FilterItem>
  <ScreenID>
    <Value>9501</Value>
  </ScreenID>
</ReportSettings>
```

EAM

Now that the reports will support Location Access Rights, we need to define the data in EAM to support this.

Enable Location Access Rights for Users

We now have to add support to Location Access Rights templates for the ScreenID assigned to the report. For each ScreenID you specified in the previous steps, we will define what locations are allowed for it.

Note: If you already have location access rights enabled, you may already have this configured and can advance to the next step.

Do the following steps:

1. Sign into EAM's Web Modules application.
2. Launch the User Groups screen.
3. For each User Group you want Location Access Rights applied for, do the following:
 - i. Edit the group.
 - ii. Check "Grant access to data only for authorized location IDs" on the Special Rights window.
 - iii. Create and assign a Location access template on the Rights Templates window.
 - iv. Save the screen.

Setup Location Access Rights for the Report's ScreenID

Now that we have a Location Rights template for that User Group, we will add rights for the Report's assigned ScreenID. Please do the following:

1. Open the Location Rights Template screen, filter to the template to which you would like to add permissions.
2. Edit the record.
3. Manually type in the ScreenID that you chose for the report in the previous steps.
4. Specify the Location ID to support (this supports wildcards).
5. Check "View".
6. If you have other locations to support, repeat steps 3-5 for each new LocationID.
7. Save the screen.

Any users that belong to a user group with this Location Rights Template will now have the data in that report filtered by the Locations defined on it.

Extra: Setup the Location Access Rights template for Asset Chooser

If you have Location Access Rights already setup, you may have already taken care of this. However, since this is a part of reporting, we are calling it out here.

If a report has a filter/choice-list for an Asset, the report's XML file may define the `<IsAsset>Y</IsAsset>` tag for that filter to have it open the Asset Chooser when the user clicks the ellipses button in Web Modules.

This Asset Chooser feature inherently has Location Access Rights support built into it. When Location Access Rights security is enabled for a user, it will restrict the assets available to them based on the following ScreenIDs (to be defined on their Location Rights Template record):

1. 2424 – Assets defined on the “Asset – Primary Information” screen.
2. 2024 – Assets defined on the “Fleet Equipment” screen.
3. 2231 – Assets defined on the “Rail Equipment” screen.
4. 2232 – Assets defined on the “Stationary Equipment” screen.
5. 2217 – Assets defined on the “Linear Assets – Primary Information” screen.
6. 2180 – Components defined on the “Components – Primary Information” screen.