



Data Permissions



Contents

Chapter 1: Overview	1
About Data Permissions	2
About the Cumulative Effect of Data Permissions	2
About the Inheritance of Data Permissions	3
Access the Data Permissions Page	4
Chapter 2: Manage Data Permissions	5
View Existing Data Permissions	6
Grant Data Permissions	6
Remove Data Permissions	8

Copyright GE Digital

© 2020 General Electric Company.

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of All other trademarks are the property of their respective owners.

This document may contain Confidential/Proprietary information of and/or its suppliers or vendors. Distribution or reproduction is prohibited without permission.

THIS DOCUMENT AND ITS CONTENTS ARE PROVIDED "AS IS," WITH NO REPRESENTATION OR WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF DESIGN, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. ALL OTHER LIABILITY ARISING FROM RELIANCE UPON ANY INFORMATION CONTAINED HEREIN IS EXPRESSLY DISCLAIMED.

Access to and use of the software described in this document is conditioned on acceptance of the End User License Agreement and compliance with its terms.

Chapter 1

Overview

Topics:

- [About Data Permissions](#)
- [About the Cumulative Effect of Data Permissions](#)
- [About the Inheritance of Data Permissions](#)
- [Access the Data Permissions Page](#)

About Data Permissions

You can use data permissions to define which Security Users and Security Groups can access records associated with a given family. By setting up data permissions, you can determine whether users will be able to view, modify, create, and delete records belonging to particular families.

For example, a Security User with Create permissions on the Equipment family will be able to create new Equipment records, while users with View permissions on the Equipment family will only be able to search for and view existing Equipment records.

Data permissions can be defined for both entity families and relationship families. For each family, you can define View, Update, Insert, and Delete permissions, but the functionality associated with each level of permissions is slightly different for entity families and relationship families.

More Details

When assigning data permissions, you can assign permissions for individual Security Users or for entire Security Groups.

- When you assign data permissions at the Security Group level, all members of that Security Group will have those permissions.
- When you assign data permissions at the Security User level, only that specific Security User will have those permissions.

Assigning permissions at the Security Group level can be more efficient because the permissions assigned to a Security Group will be inherited by every member of that group. Assigning permissions at the Security User level, however, gives you more flexibility in customizing permissions for individual Security Users.

Some data permissions are configured for the baseline Security Groups to provide access to the baseline GE Digital APM families. Others permissions will need to be configured manually before users will be able to access certain features in GE Digital APM. In addition, you will need to configure permissions manually for families that you create.

About the Cumulative Effect of Data Permissions

You can define data permissions for both Security Users and Security Groups. Because each type of permission offers different advantages, you will probably want to use a combination of both Security User and Security Group permissions to achieve the specific permissions that are needed for your system.

Note: Data permissions are cumulative. A given Security User will be granted the sum of all permissions assigned to him and to all the Security Groups of which he is a member. In addition, permissions that are granted to Security Groups spread down automatically to all of their security subgroups.

Cumulative Permissions

Consider an example where:

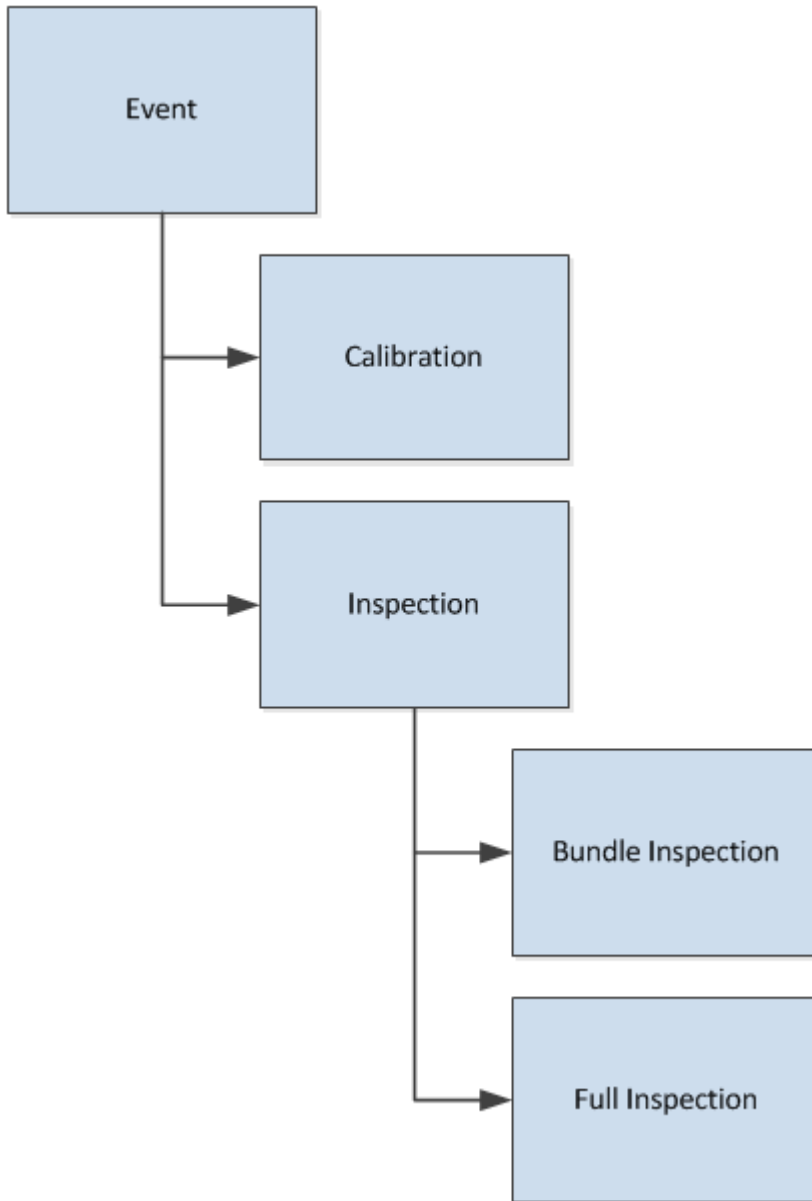
- John Smith has View permissions on the Inspection Recommendation family.
- The MI Inspection Security Group has View, Update, Insert, and Delete permissions on the Recommendation family.

If John Smith is a member of the MI Inspection Security Group, he will have all permissions on the Recommendation family. The permissions assigned to the MI Inspection group are added to the permissions assigned to John Smith at the Security User level, therefore giving him full permissions to the Recommendation family.

Due to the cumulative effect of data permissions, you will want to assign to a given Security Group the lowest level of permissions that you want to grant to any member of that Security Group. Then, you should grant additional permissions to individual Security Users who need to have more permissions.

About the Inheritance of Data Permissions

The permissions that are assigned for a family are automatically inherited by its subfamilies. For instance, consider the following hierarchy.



In this example, any permissions that are defined for the Event family will also apply to the Calibration and Inspection families. Similarly, any permissions that are defined for the Inspection family will also apply to the Bundle Inspection and Full Inspection families.

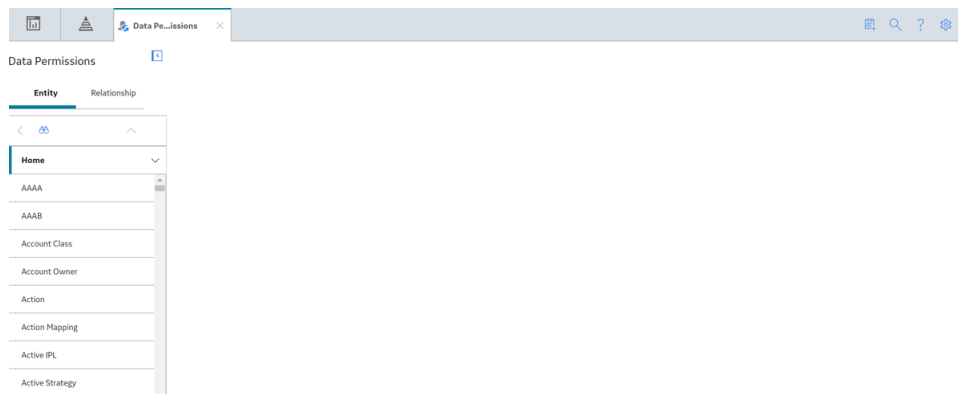
In various places throughout GE Digital APM, families are displayed using a hierarchical view. In these cases, users must have at least View permissions at the highest level in the hierarchy in order to access any subfamily within that branch of the tree.

For instance, users would need View permissions to the Event family in order to see the Calibration subfamily in a hierarchical view.

Access the Data Permissions Page

Procedure

In the module navigation menu, select **Admin > Configuration Manager > Data Permissions**. The **Data Permissions** page appears, displaying a list of **Entity** and **Relationship** families in the left pane.



Next Steps

- [Grant Data Permissions](#)

Chapter 2

Manage Data Permissions

Topics:

- [View Existing Data Permissions](#)
- [Grant Data Permissions](#)
- [Remove Data Permissions](#)

View Existing Data Permissions

Procedure




1. Access the [Data Permissions](#) page.
2. In the left pane, select the family whose permissions you want to view.
The list of Security Groups and Security Users who currently have access to the family appear in the workspace.

Next Steps

- [Grant Data Permissions](#)

Grant Data Permissions

Procedure

1. Access the [Data Permissions](#) page.
2. Select the family whose permissions you want to manage.
The workspace for the selected family appears, displaying a list of assigned Security Users and Groups for the Family.
3. To assign a Security User, select .
-or-
To assign a Security Group, select .
Depending on the selection, the **Assign Users** or **Assign Groups** window appears.
4. In the list, select the Security User or Security Group to which you want to assign permissions.
5. Select **Save**.
The selected Security Users or Security Groups are assigned to the Family.
6. Select the check box next to the Security Users or Security Groups to which you want to assign permissions.
7. Next to each type of permission that you want to assign, select the check box. You can select from the following options:
 - **View:** The Security Group or User will be able to view records that belong to the family.
 - **Insert:** The Security Group or User will be able to create records in the family.
 - **Update:** The Security Group or User will be able to update records that belong to the family.
 - **Delete:** The Security Group or User will be able to delete records that belong to the family.
8. Select .
The permissions are granted.

About Entity Family Data Permissions

For each entity family, you can grant users View, Update, Insert, and Delete permissions. The following table provides details about each permission.

Permission	Description	Notes
View	Users can view records that belong to the family. Users with only View permissions on a family will be able to open existing records belonging to that family but would not be able to create, modify, or delete them.	<p>For typical users, View permissions are a prerequisite to Update, Insert, and Delete permissions because they provide users with the initial access required for modify, create, and delete operations.</p> <p>For example, users with View permissions on a family can:</p> <ul style="list-style-type: none"> • Search for records in that family and open them in the Record Manager. • Create a Select query on that family. • Open reports that include that family.
Update	Users can modify records that belong to the family. Users with only Update permissions on a family would be able to modify existing records belonging to that family but would not be able to view, delete, or create records in that family.	Typically, you would not grant Update-only permissions to a user because, while that user would be able to modify records in that family, without View permissions, they would not be able to search for them or open them. Update-only permissions, however, may be used to support processes and operations that occur outside of the user interface (i.e., interfaces or scheduled jobs).
Insert	Users can create records in the family. Users with only Insert permissions on a family would be able to create records in that family, but would not be able to view, modify, or delete them.	Typically, you would not grant Insert-only permissions to a user because, while that user would be able to create records in that family, without View permissions, they would not be able to initiate the record-creation process in GE Digital APM. Insert-only permissions, however, may be used to support processes and operations that occur outside of the user interface (i.e., interfaces or scheduled jobs).
Delete	Users can delete records that belong to the family. Users with only Delete permissions on a family would be able to delete records belonging to a family, but would not be able to view, modify or create them.	Typically, you would not grant Delete-only permissions to a user because, while that user would be able to delete records in that family, without View permissions, they would not be able to perform a search to find the records that they wanted to delete. Delete-only permissions, however, may be used to support processes and operations that occur outside of the user interface (i.e., interfaces or scheduled jobs).

About Relationship Family Data Permissions

Relationship family permissions are similar to [entity family permissions](#) in that the same permission levels are available: View, Update, Insert, and Delete. Each permission level, however, provides access that is slightly different from the access provided through entity family permissions.

Remember that relationship families are used to create links between records in entity families. Consider an example where the Equipment family is related to the Failure family through the Has Failure relationship. In this case, to provide a user with full access to an Equipment record and its associated Failure record, that user would need permissions to three families: Equipment, Failure, and Has Failure.

Note: Permissions to a relationship family do not automatically provide access to the predecessor and successor families; for that, explicit entity family permissions are required.

The following table provides details about each relationship family data permission.

Permission	Description	Notes
View	Users have basic access to the links that relate predecessor and successor records. Users with View-only access to a relationship family can open existing linked records, but cannot link and unlink records using that relationship.	None
Update	Users can modify existing links in a relationship family.	This applies only in cases where fields are defined for the relationship family. Users with Update permissions will also need View permissions.
Insert	Users can link records together using that relationship family. Using the previous example, a user would need Insert permissions on the Has Failure family to link Equipment records to Failure records.	Users with Insert permissions will also need View permissions.
Delete	Users can unlink records associated with the relationship family. Using the previous example, a user would need Delete permissions on the Has Failure family to unlink Failure records from Equipment records.	Users with Delete permissions will also need View permissions.

Remove Data Permissions

Procedure

1. Access the [Data Permissions](#) page.
2. Select the family whose permissions you want to manage.
The workspace for the selected Family appears, displaying a list of assigned Security Users and Groups for the Family.
3. Next to each Security User or Group from which you want to remove permissions, select the check box.

4. To remove all permissions that the Security Groups and Users have to the family, select .

-or-

Next to each family permission that you want to remove from the Security Groups and Users, clear the check box.

5. Select .
- The permissions are removed.