



Aras Innovator 33

User Visibility Policy Admin Guide

Document #: D-008133

Last Modified: 8/22/2024

Copyright Information

Copyright © 2024 Aras Corporation. All Rights Reserved.

Aras Corporation
100 Brickstone Square
Suite 100
Andover, MA 01810
Phone: 978-691-8900

E-mail: support@aras.com

Website: <https://www.aras.com/>

Notice of Rights

Copyright © 2024 by Aras Corporation and/or its affiliates. All rights reserved.

This document is protected by U.S. and international copyright laws and conventions. No copyright may be obscured or removed from this document. This document may not be modified or altered, or reproduced or transmitted in any form, without the explicit permission of the copyright holder.

Aras Innovator, Aras, and the Aras Corp "A" logo are registered trademarks of Aras Corporation in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

Notice of Liability

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY, AND THE CONTENTS HEREOF ARE SUBJECT TO CHANGE WITHOUT NOTICE. THE INFORMATION CONTAINED IN THIS DOCUMENT IS DISTRIBUTED ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR A WARRANTY OF NON-INFRINGEMENT. ARAS SHALL HAVE NO LIABILITY TO ANY PERSON OR ENTITY WITH RESPECT TO ANY LOSS OR DAMAGE CAUSED OR ALLEGED TO BE CAUSED DIRECTLY OR INDIRECTLY BY THE INFORMATION CONTAINED IN THIS DOCUMENT OR BY THE SOFTWARE OR HARDWARE PRODUCTS DESCRIBED HEREIN.

Table of Contents

Send Us Your Comments	4
1 Overview	5
2 Users and Identities in Aras Innovator	6
3 Creating a User Visibility Policy	7
3.1 Creating User Visibility Rules.....	7
3.1.1 <i>Exempt Identities</i>	8
3.2 Activating the User Visibility Policy	8
3.2.1 <i>Activating the User Visibility Policy MAC Policy</i>	8
3.2.2 <i>Activating the User Identity Derived Relationship Family</i>	10
3.3 Deactivating the User Visibility Policy	11

Send Us Your Comments

Aras Corporation welcomes your comments and suggestions on the quality and usefulness of this document. Your input is an important part of the information used for future revisions.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where and what level of detail?
- Are the examples correct? Do you need more examples?
- What features did you like most?

If you find any errors or have any other suggestions for improvement, indicate the document title, and the chapter, section, and page number (if available).

You can send comments to us in the following ways:

Email:

TechDocs@aras.com

Subject: Aras Product Documentation

Or,

Postal service:

Aras Corporation
100 Brickstone Square
Suite 100
Andover, MA 01810
Attention: Aras Technical Documentation

If you would like a reply, provide your name, email address, address, and telephone number.

If you have usage issues with the software, visit <https://www.aras.com/support/>

1 Overview

Aras Innovator provides administrators the tools necessary to create a set of rules that form a policy controlling access to User Information. You can use The User Visibility Policy to help ensure compliance with provisions of the General Data Protection Regulation (GDPR) regarding the protection of User Data access. GDPR, which came into effect in May 2018, aims to protect data and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). Because an organization's GDPR compliance is assessed holistically in the context of its processes and procedures to manage personal data, simply implementing a User Visibility Policy does not make your usage of Aras Innovator fully GDPR compliant. Many of the provisions in GDPR are specific to data storage and data transfer which are specific to company infrastructure and protocols, of which Aras Innovator is likely only one aspect of your data storage and processing infrastructure. This document guides you through the process of creating a User Visibility Policy and provides details regarding rules and limitations to assist your organization in establishing a GDPR-compliant information and data processing environment with respect to Aras Innovator.

2 Users and Identities in Aras Innovator

In Aras Innovator, user information is stored in the **User** ItemType. A User Item stores a unique login name as well as additional user information such as Name, Email, and Telephone Number. Each user belongs to a unique User **Identity** defined by an alias assignment. User Identities are then assigned access rights, and can be grouped into Group Identities. A Group Identity may be composed of Individual Identities or other Group Identities. Each identity may have its own set of access rights.

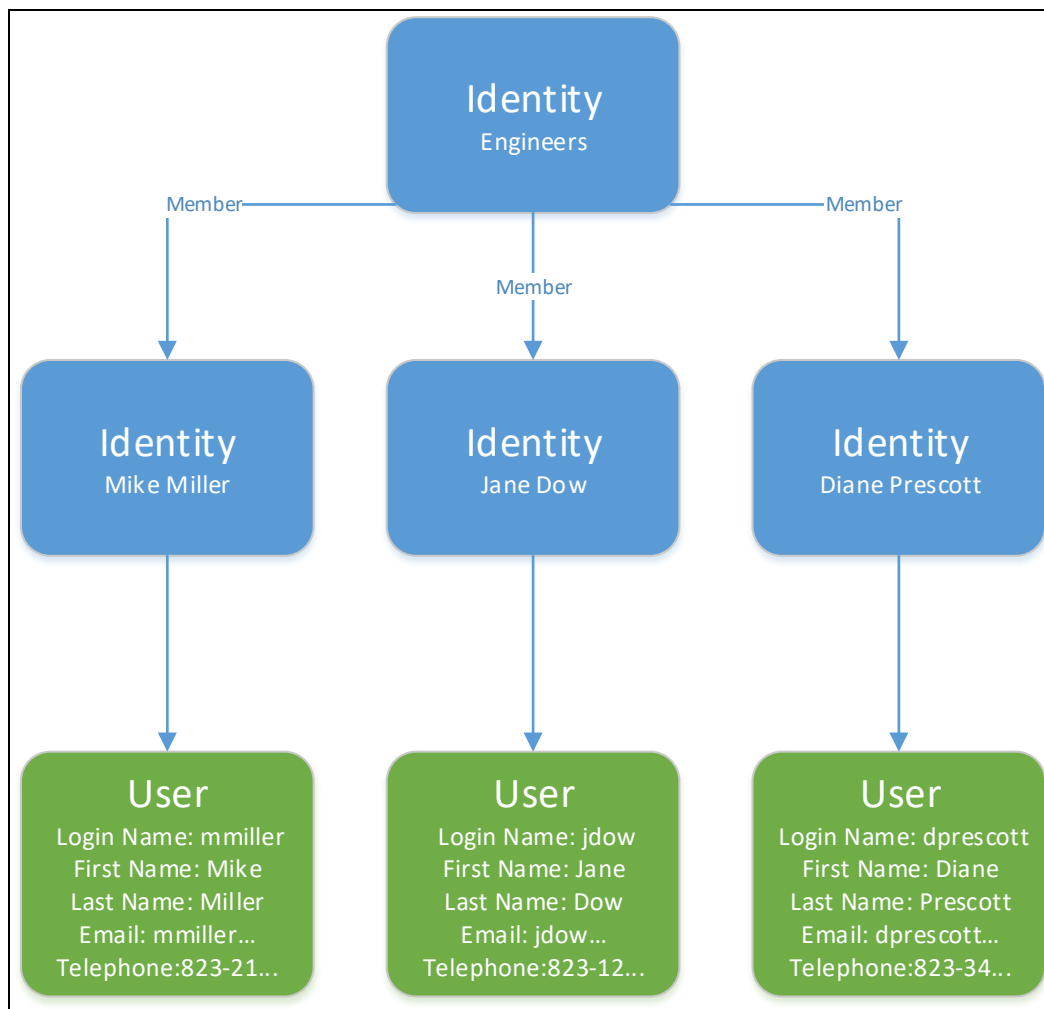


Figure 1.

The User Visibility Policy determines which identities can see the user information associated with users belonging to particular identities. Out of the box, Aras Innovator does not have any restrictions regarding which Identities can see user information.

3 Creating a User Visibility Policy

The Administrator creates a User Visibility Policy. The policy is composed of User Visibility Rules that restrict which Identities can see user information belonging to other Identities. In order for the User Visibility Rules to become active in the system, the Administrator must use the procedure described in the following section.

3.1 Creating User Visibility Rules

The **User Visibility Rule** ItemType is used to create a list of Identity rules that determine the overall User Visibility Policy for the system. Each **User Visibility Rule** Item is composed of the following properties:

- **Source Identity:** a group or user Identity accessing a user's information.
- **Access Identity:** a group or user Identity being accessed.
- **Is Active:** an indicator whether a given Rule is active in the system when the **User Identities** Derived Relationship Family and **User Visibility Policy** MAC Policy are in the **Active** state.

Use the following procedure to create a **User Visibility Rule**:

1. Go to **Contents --> Administration --> Access Control --> User Visibility Rules** to create or search for existing rules. The menu shown in Figure 2 appears.

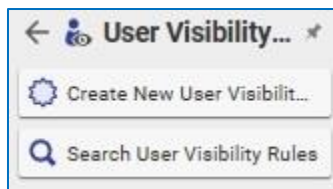



Figure 2.

2. Click **Create New User Visibility Rule**. A blank **User Visibility Rule** dialog appears.



Figure 3.

3. Click the **ellipses** in the **Source Identity** field to select the appropriate identity from the **Identity Search** dialog.
4. Click the **ellipses** in the **Access Identity** field to select the appropriate identity from the **Identity Search** dialog.
5. Enter the appropriate information in the **Description** field and click  to save and unlock the Rule.

3.1.1 Exempt Identities

User Administrators: a group Identity exempt from the User Visibility Rules. User Identities that are members of the **User Administrators** group have full permissions (Get, Update, Delete, Can Discover) to all User and Identity Items.

User Readers: a group Identity exempt from the User Visibility Rules. User Identities that are members of the **User Readers** have Get and Discover permissions to all User and Identity Items.

Note: Aras Innovator Administrators should exercise caution when adding members to the **User Administrators** and **User Readers** groups.

3.2 Activating the User Visibility Policy

Once you specify the User Visibility Rules you need to activate the **User Identities** Derived Relationship Family and the **User Visibility Policy** MAC Policy. You can modify or add User Visibility Rules to an active User Visibility Policy.

Note: After the activation process, if there are no User Visibility Rules defined or if none of the User Visibility Rules have the **Is Active** option selected, only Administrators will be able to see all Users. Users will still have access to their own information.

3.2.1 Activating the User Visibility Policy MAC Policy

The **User Visibility Policy** MAC Policy is responsible for tracking all Identities related to a User. In order for the User Visibility Policy to take effect, this MAC Policy must be in the active state.

Use the following procedure to activate the Derived Relationship Family:

1. Go to **Contents --> Administration --> Access Control --> MAC Policies**. The menu shown in Figure 4 appears.



Figure 4.

2. Click **Search MAC Policies** to access the search grid.
3. Open the **User Visibility Policy** MAC Policy in the search grid.
4. Click **Activate** in the **Actions** menu to promote the **MAC Policy** Item to the **Active** state.

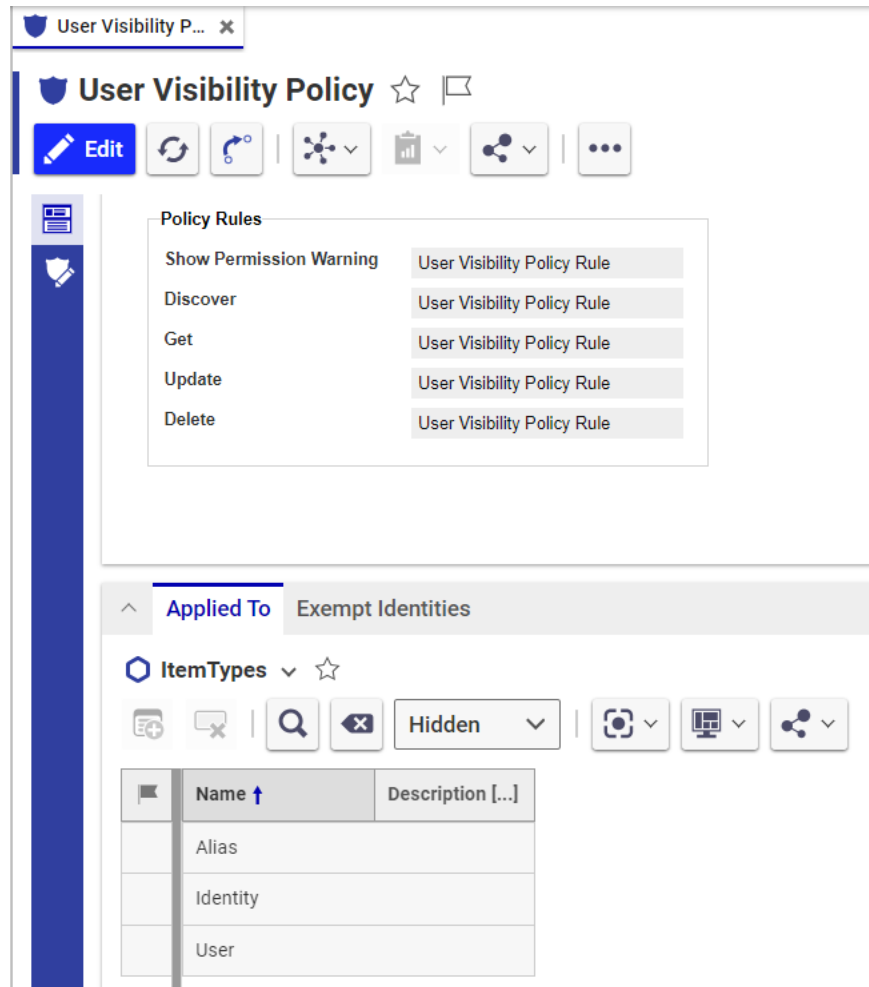


Figure 5.

Warning Do not edit the User Visibility Policy MAC Policy.

3.2.2 Activating the User Identity Derived Relationship Family

The **User Identity** Derived Relationship Family is responsible for tracking all Identities related to a User. In order for the User Visibility Policy to take effect, this Derived Relationship must be in the active state.

Use the following procedure to activate the Derived Relationship Family:

1. Go to **Contents --> Administration --> Configuration --> Derived Relationship Family**. The menu shown in Figure 6 appears.

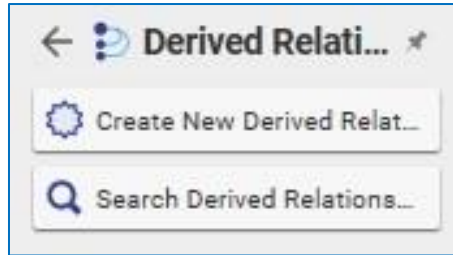



Figure 6.

2. Click **Search Derived Relationships**. The search grid appears.
3. Open the **User Identities** Derived Relationship Family from the search grid.
4. Click the **Promote**  button. The **Promote User Identities** dialog box appears.

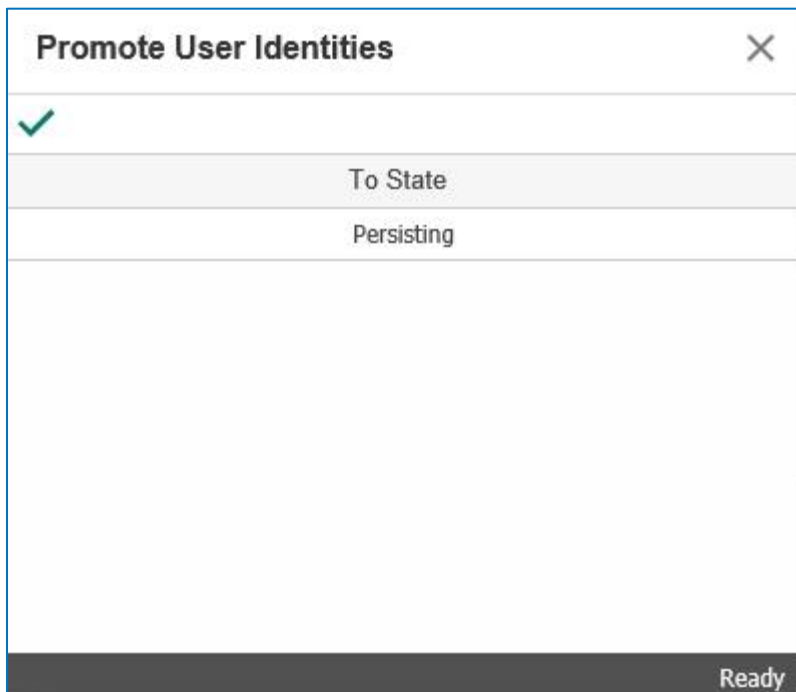


Figure 7.

5. Select **Persisting** and click the **green arrow** to promote the **Derived Relationship** Family. The system then performs all the necessary calculations and the **Derived Relationship** Family is automatically promoted to the **Active** State once the Persistence operation is complete. You can monitor the progress of the persistence Process by observing the Persistence section of the **Derived Relationship** Family form.

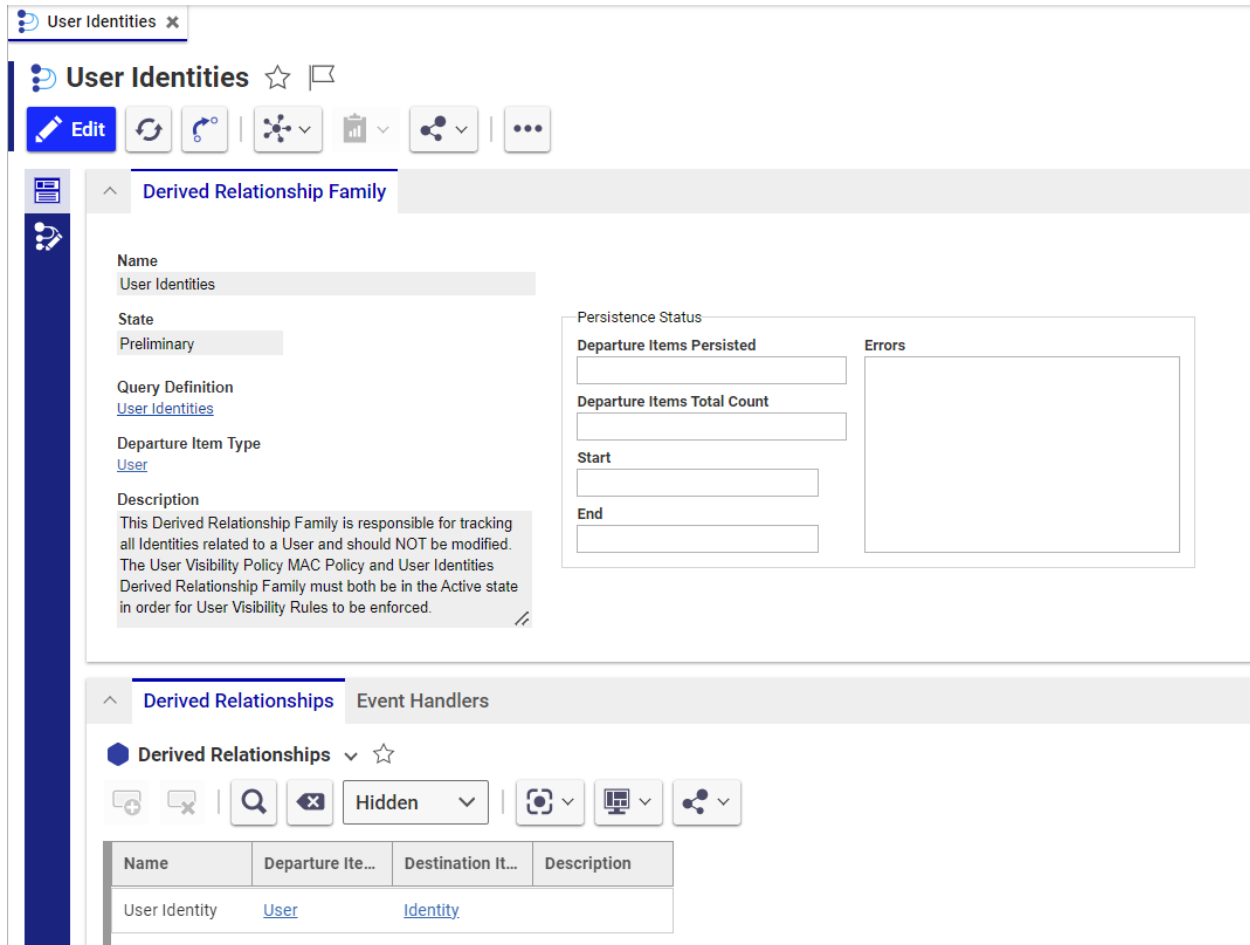


Figure 8.

Warning Do not edit the User Identity Derived Relationship Family.

3.3 Deactivating the User Visibility Policy

Use the following procedure to deactivate a User Visibility Policy if necessary:

1. Deactivate the **User Visibility Policy** MAC Policy by opening the MAC Policy and running the **Deactivate** Action. Once the MAC Policy is no longer in the **Active** state, none of the User Visibility Rules will be applied.
2. Promote the **User Identity** Derived Relationship Family from the **Active** to **Preliminary** State as this Derived Relationship Family is no longer needed.