

# 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.

## 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.



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

User Visibility Rule 1

Save Done Delete

User Visibility Rule

Source Identity Access Identity Is Active

Description

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 null to save and unlock the Rule.

### 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.

### Important



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

## 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**.

### Important

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.

## 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.



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.





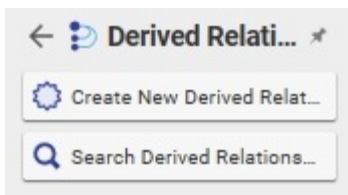
Do not edit the User Visibility Policy MAC Policy.

## Activating the User Identity Derived Relationship Family

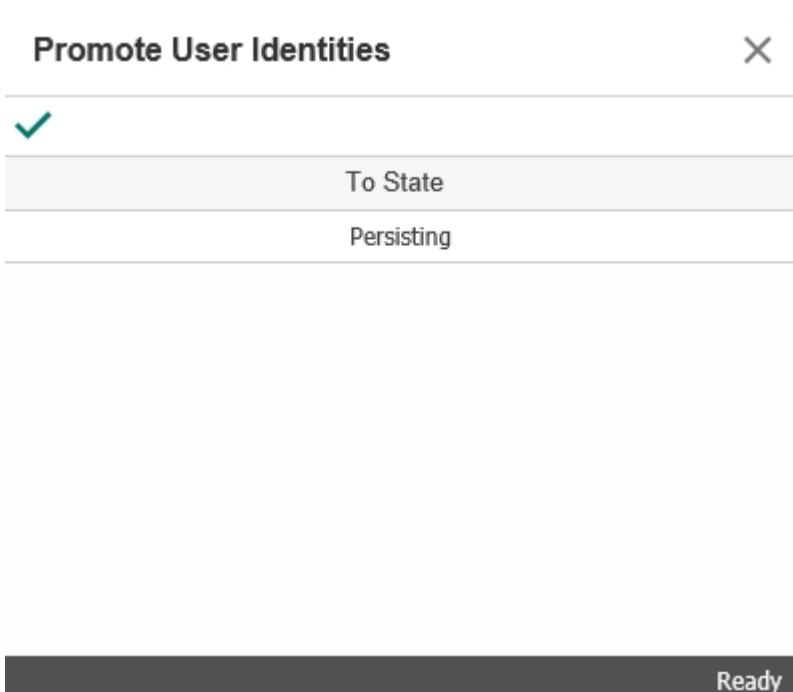
The **User Identity** Derived Relationship Family is responsible for tracking all Identities related to a User. In order for the User Visibility Policy to take effect, this Derived Relationship must be in the active state.

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.



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 null button. The Promote User Identities dialog box appears.



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.

User Identities x

User Identities

Edit

Refresh

Link

Star

Share

More

Derived Relationship Family

Name

User Identities

State

Preliminary

Query Definition

User Identities

Departure Item Type

User

Description

This Derived Relationship Family is responsible for tracking all Identities related to a User and should NOT be modified. The User Visibility Policy MAC Policy and User Identities Derived Relationship Family must both be in the Active state in order for User Visibility Rules to be enforced.

Persistence Status

Departure Items Persisted

Departure Items Total Count

Start

End

Errors

Derived Relationships Event Handlers

Derived Relationships

Search

Filter

Hidden

Share

| Name          | Departure It... | Destination It... | Description |
|---------------|-----------------|-------------------|-------------|
| User Identity | User            | Identity          |             |

## Important

**Do not edit the User Identity Derived Relationship Family.**

## 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.

