ACE 2019
INNOVATE
TRANSCEND
REALIZE

Technical: Access Control Mechanisms

Mike Gavlak

4/16/2019

Innovator Access Control Mechanisms

- Role Based -
  - Identities and Permissions
  - Special Identities
  - Teams and Roles
- Attribute Based – Mandatory Access Control (Innovator 11 SP11) *
  - Supports Security/Clearance Level scenarios
  - Can support location based restrictions
- Relationship Based – Domain Access Control (Innovator 11 SP15) *
  - Supports project-based scenarios
- User Visibility Rules (Innovator 12)
  - Restricts access to user attributes for privacy scenarios like GDPR

* Note – MAC and DAC are not currently enforced by Enterprise Search

© 2018 Aras

Role Based Access Controls

ACE 2019
INNOVATE
TRANSCEND
REALIZE

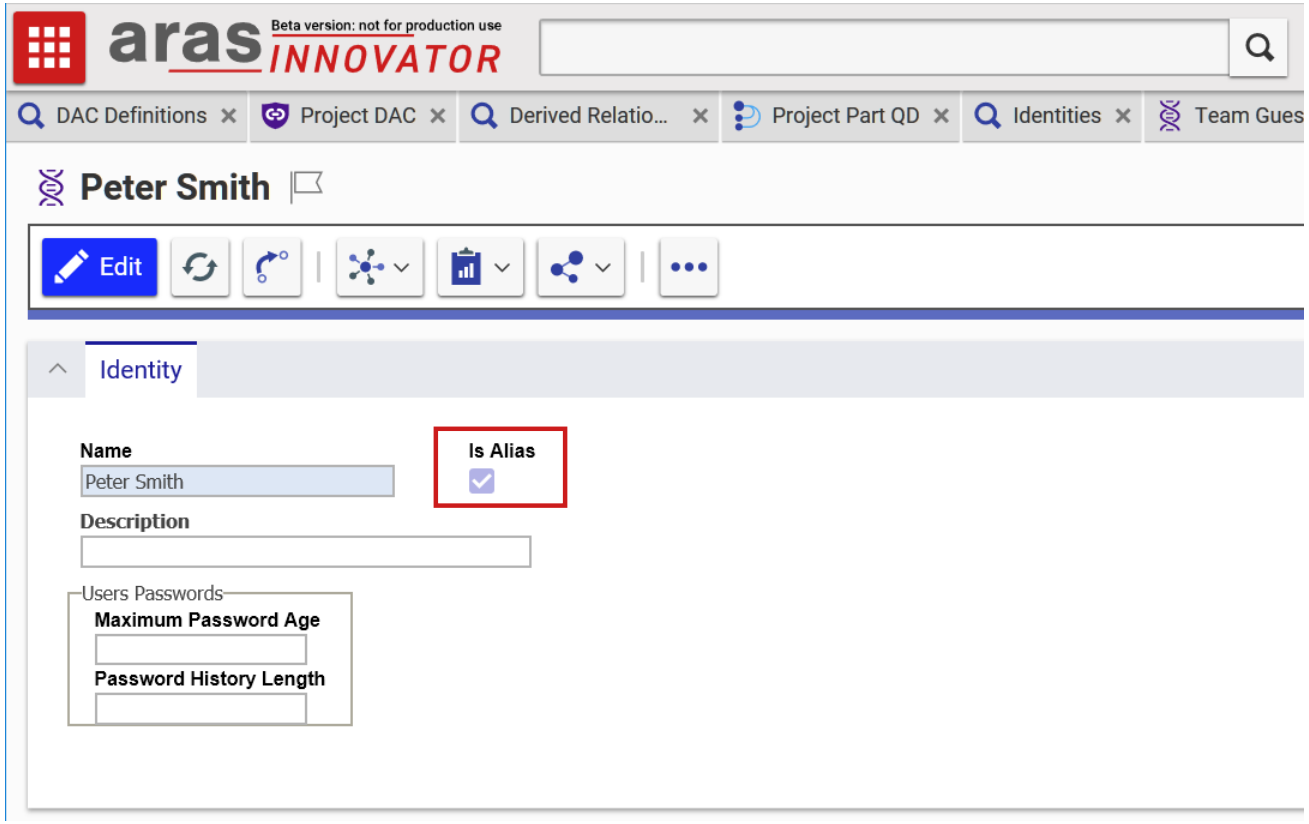
Defining Identities

- Identities may represent:
  - An individual (Alias Identity)
  - A group of individuals (Group Identity)
  - A group of groups (Group Identity)
  - Roles like Creator, Owner, Manager (Built-In Identity)
- Identities are used when defining:
  - ItemType Permissions
  - TOC Access and Can Add
  - ItemType Views
  - Workflow Assignments, Notifications, etc.
  - Lifecycle transitions

© 2018 Aras

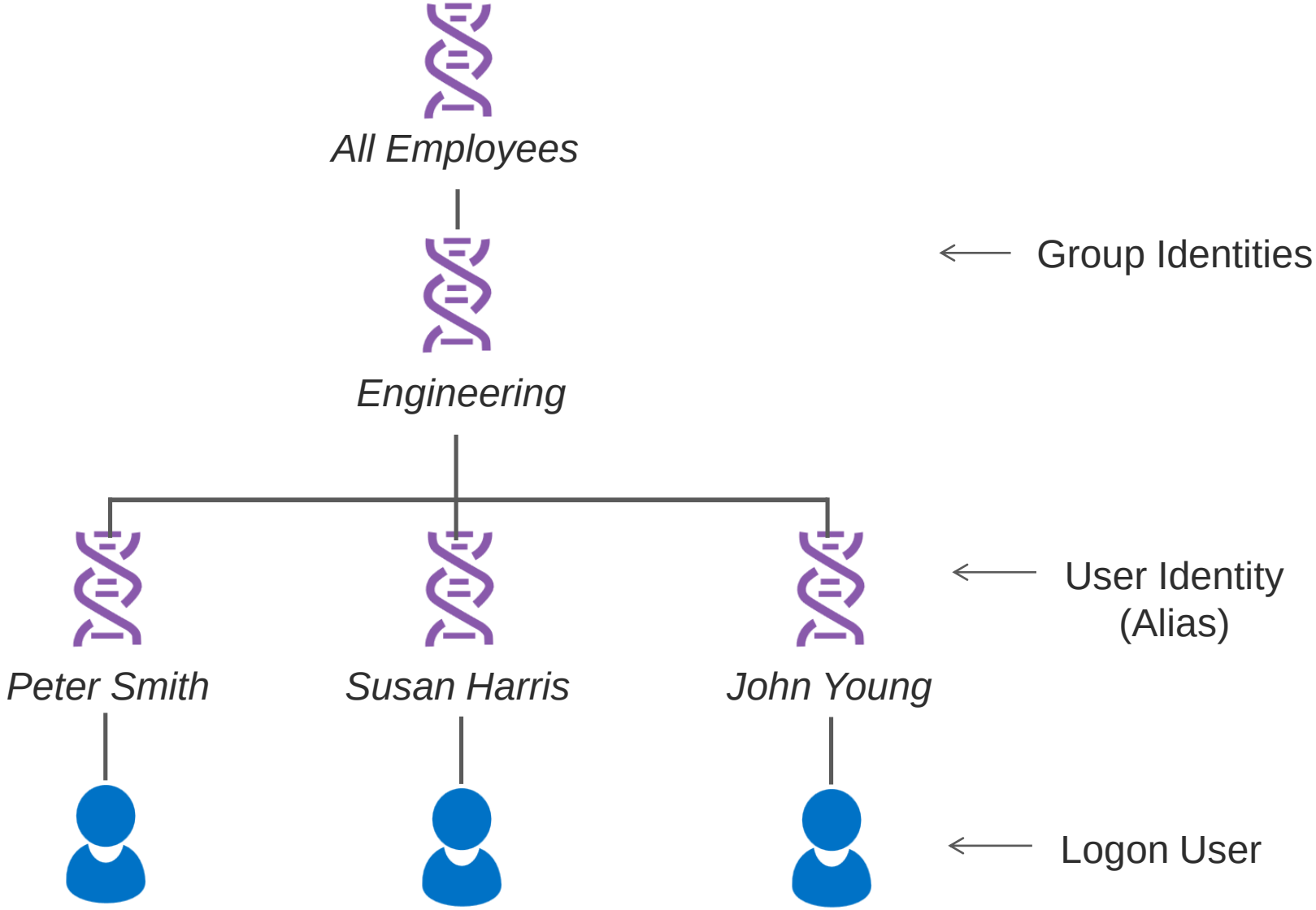
Alias Identity

- Automatically created for each User
- Normally do not have any members



© 2018 Aras

Hierarchy Example



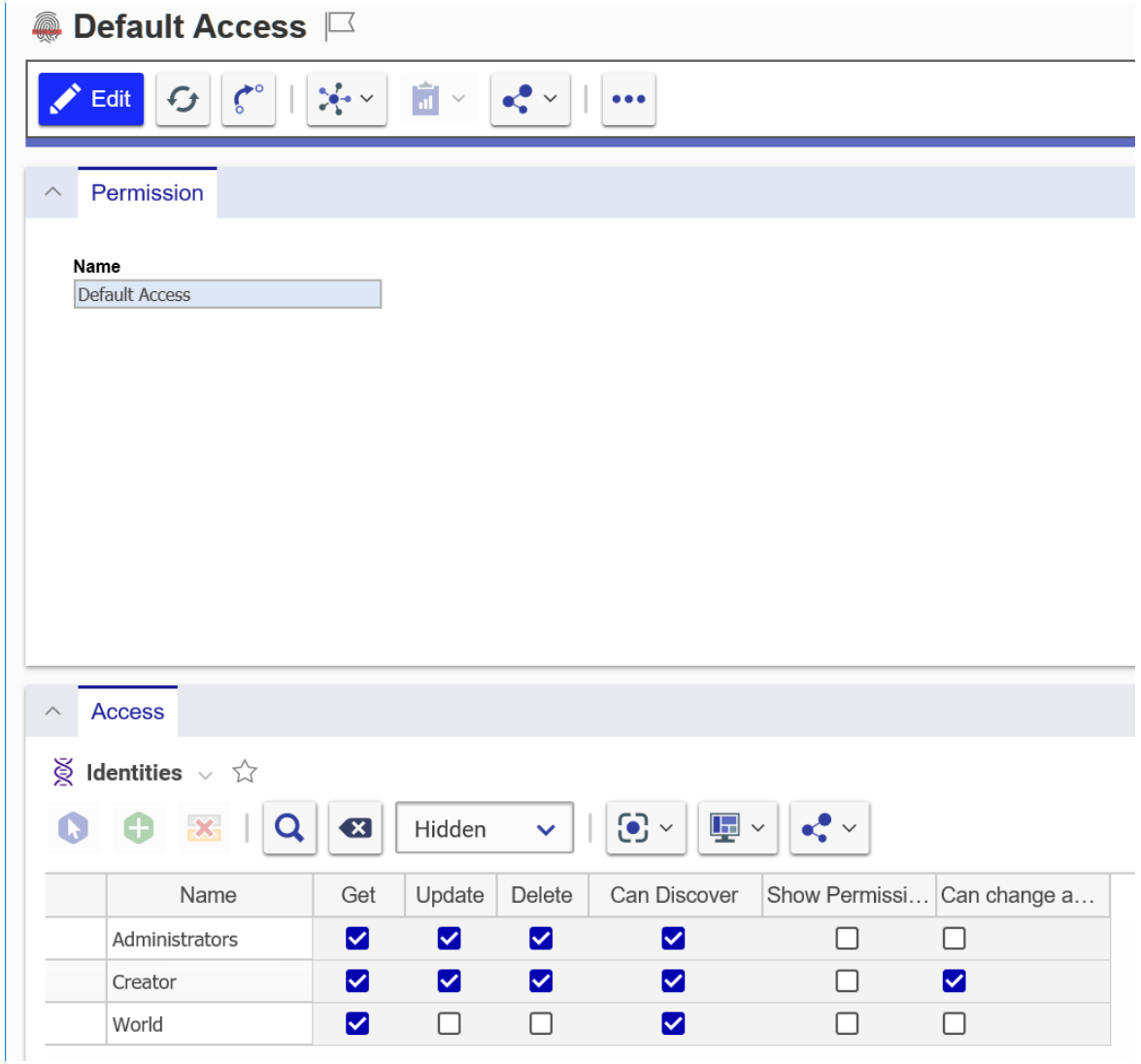
© 2018 Aras

Defining Permissions

- Define which Identities may:
  - Get (Retrieve) an Item
  - Update an Item
  - Delete an Item
  - Discover an Item (Search) (if Enforce Discovery enabled for the ItemType)
  - Show Permission Warnings on an Item (if Enforce Discovery enabled for the ItemType)
  - Change Access on an Item
- Each Item must have a Permission (most are shared)
- A single Item can have an individually assigned permission (Private, if enabled for the ItemType)

© 2018 Aras

Creating a Permission



© 2018 Aras

Discovery and Get Access Behavior

- Get Access
  - Users will be allowed to view all information and open forms
- Discover Only Access
  - Items will be returned in main grid and relationship grids when they match the search criteria
  - Users will be restricted to viewing only the information returned in the grid and will not have the ability to open the form
  - A warning will be displayed in the lock status column of the grids
- No Access – No get or discover
  - Items will not be returned in main grid or relationship grid even if they match the search criteria
  - Warning will be displayed in the status bar indicating “Permissions Limited” if “Show Permissions Warning” access is set and there are any items missing from the search result due to no permission to get or discover
- Similar behavior in relationship grid and main search grid
  - If the user has permission to get/discover the relationship, but not the related item, hidden2 properties will show “Restricted”
  - Properties of datatype Item which a user does not have get/discover permission will show “Restricted” instead of the keyed name value in a grid or on a form

© 2018 Aras

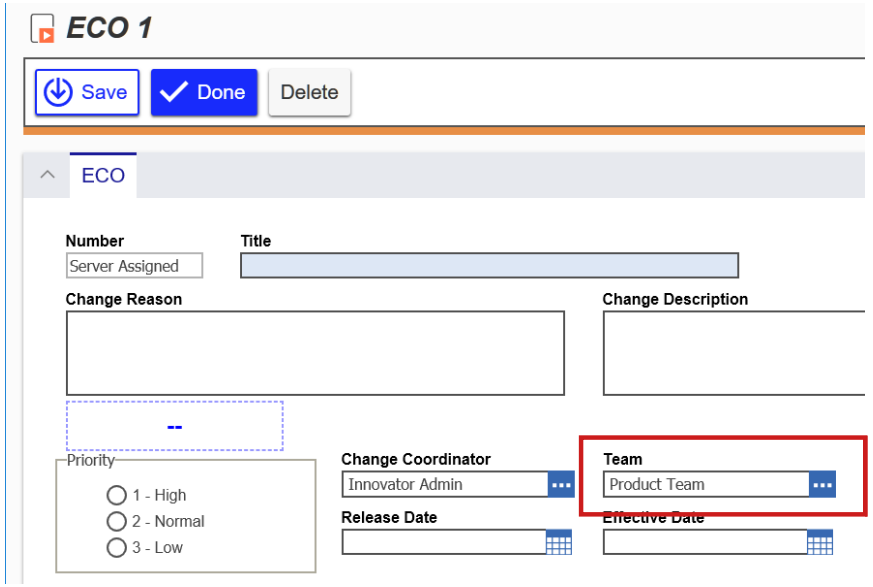
Using System Identities

- Creator (created_by_id)
  - User that created (first saved) an item
  - This value is stored in the created_by_id item property (User)
- Owner (owned_by_id)
  - Identity that "owns" the item, may be labeled for a different meaning
  - This value is stored in the owned_by_id item property (Identity)
- Manager (managed_by_id)
  - Identity that "manages" the item, may be labeled for a different meaning
  - This value is stored in the managed_by_id item property (Identity)
- Team (team_id)
  - Team is a separate ItemType that assigns identities into roles
  - A Team can be assigned to any item in Innovator to enable an unlimited number of special identities
  - Teams are also used in DAC Definition permissions

© 2018 Aras

Working with Teams

- The Team item is a group of one or more Identities (group or alias) that are each assigned to Role(s)
- Every Item in Innovator has a system team_id property, which may or may not be visible on the grids and forms
- A Team can be assigned to an individual Item to define permissions for team members
- Permissions can call out team roles just like alias and group identities for access rights



Mobile Products

Susan Harris, Team Manager
Peter Smith, Team Member

Computing Products

John Young, Team Manager
Susan Harris, Team Member

© 2018 Aras

Assigning Team Roles

- Member Identities can be assigned a Team Role that indicates their level of responsibility on a Team
- Standard Team Roles include:
  - Team Manager
  - Team Member
  - Team Guest

Team Manager

- If a role is not assigned to a member of a Team they assume the role of “Team”
- “Team” (which means any role) or any defined team role may be used in a Permission
- Custom Team Roles may be created
  - Edit the Identity form to add a field for the classification property
  - Create a new Identity and set its classification to “Team” to make it a Team Role
  - All teams may now use the new Team Role

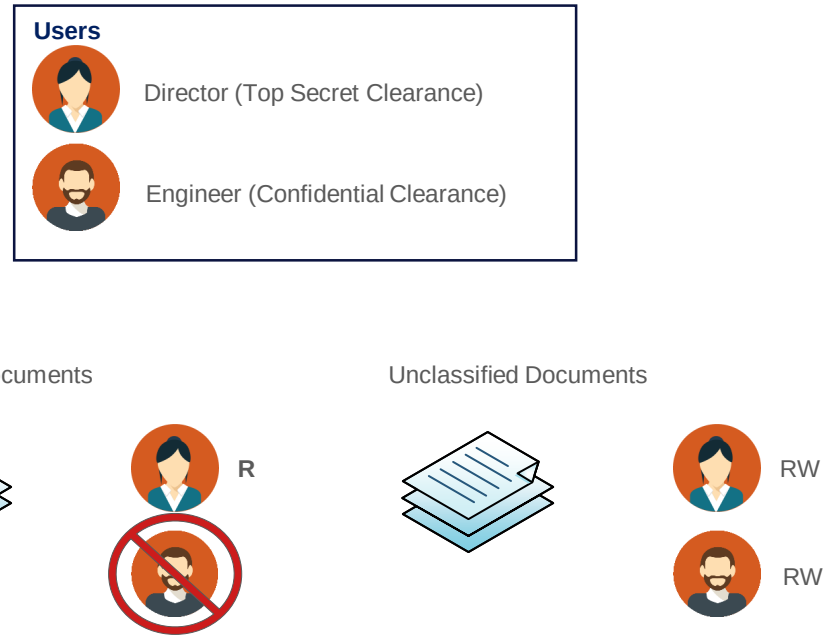
© 2018 Aras

Attribute Based Access Controls – Mandatory Access Contol (MAC)

ACE 2019
INNOVATE
TRANSCEND
REALIZE

MAC Use Case: Clearance Levels

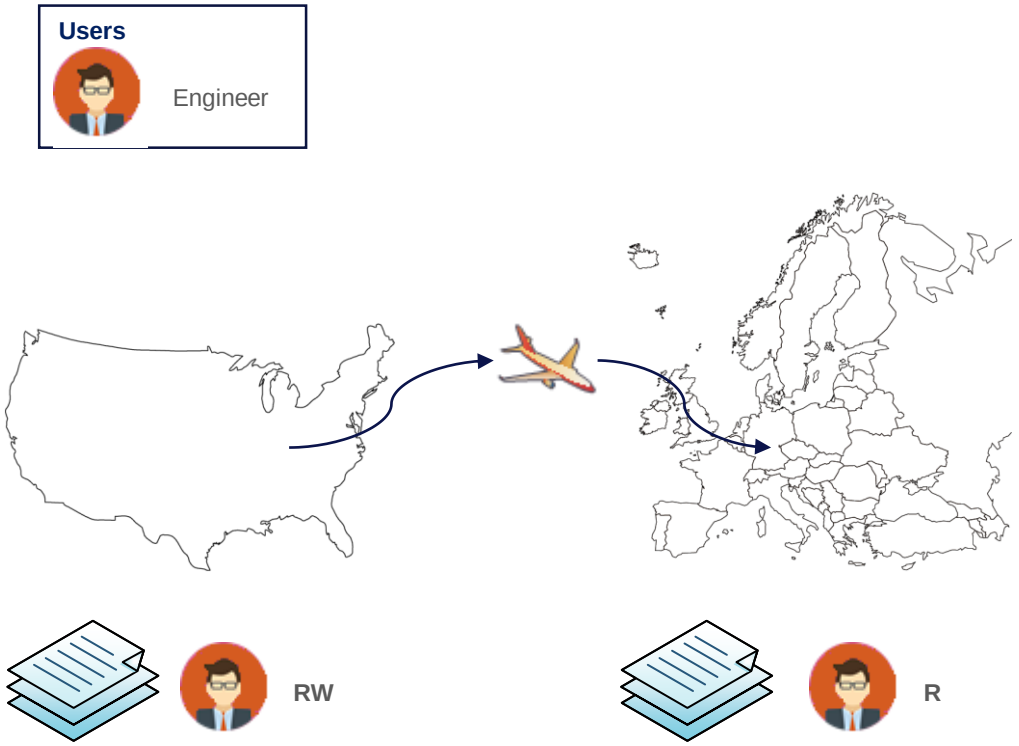
- Military style security model
  - If User Clearance Level >= Item Security Classification, grant Permissions
- Example:
  - U.S. Military Classifications: Top Secret > Secret > Confidential >Restricted > Unclassified
  - A Director has Top Secret Security Clearance and thus has Read Permissions to Top Secret Documents
  - Both the Director and Engineer have Read and Write Permissions to Unclassified Documents



© 2018 Aras

MAC Use Case: Location Access Restrictions

- Environment-based Restrictions
  - Location or time sensitive access rights
- Example:
  - An Engineer has Read and Write Permissions to Documents when Inside the US.
  - When the Engineer travels outside of the US, they only have Read Permissions to Documents.
  - An Engineer has Read and Write Permissions between the hours of 7 AM and 6 PM



© 2018 Aras

MAC Policies

- Restrict/block access a user has (by alias, group and team role permissions, or by DAC) if a user does not meet additional MAC criteria calculated based on –
  - Properties of the user
  - Properties of the item being accessed
  - External environment
- MAC Policies can not grant access to a user if they don’t have access by permissions to the item
- A MAC Policy can be applied to one or more ItemTypes
- MAC Policies must be Active to be enforced, and may be Activated, Deactivated, or versioned using actions

© 2018 Aras

MAC – For More Information -

- See “Aras Innovator 11.0 - MAC Policies” in the Innovator CD Image Documentation folder
- Review the slides from “Training: MAC Policies Bob Ellis – Aras” from the ACE training session held earlier today

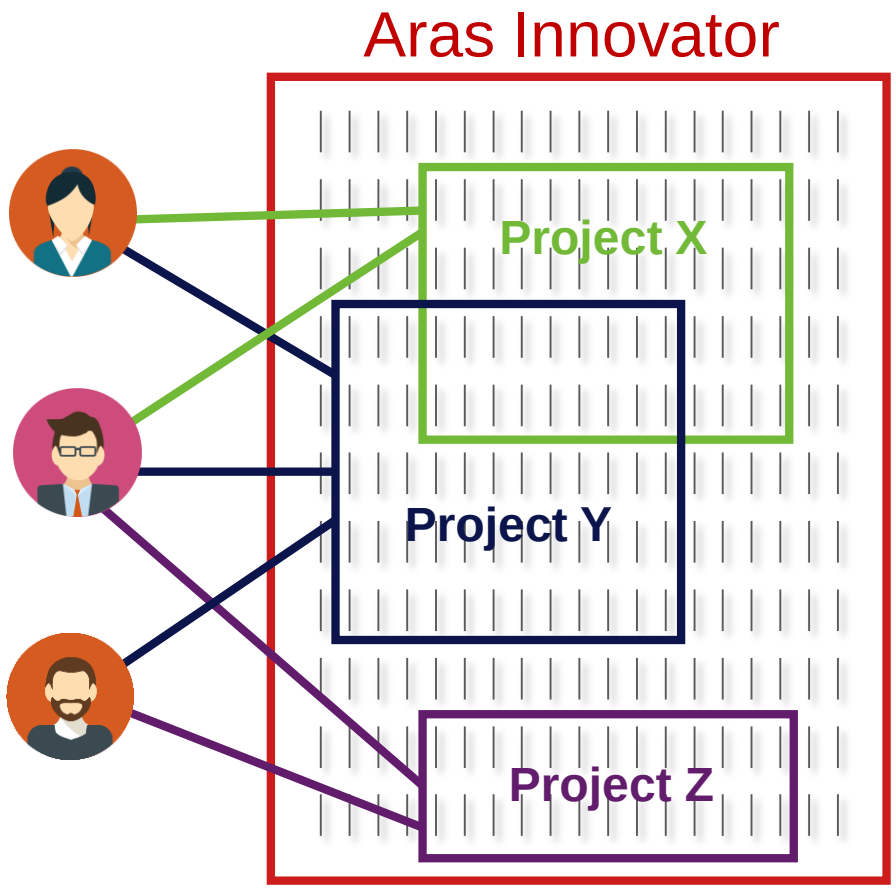
© 2018 Aras

Relationship Based Access Controls – Domain Access Control (DAC)

ACE 2019
INNOVATE
TRANSCEND
REALIZE

Domain Access Control

- DAC can be used to grant access to “project” or “workspace” specific data.
- Items within the project may be grouped and categorized with different levels of access assigned to each group i.e. “Project Reference Parts”, “Project Released Parts”, “Project Design Parts”, etc.
- Each project will have project-specific roles and users assigned to it. Users can belong to more than one project, in different roles.



© 2018 Aras

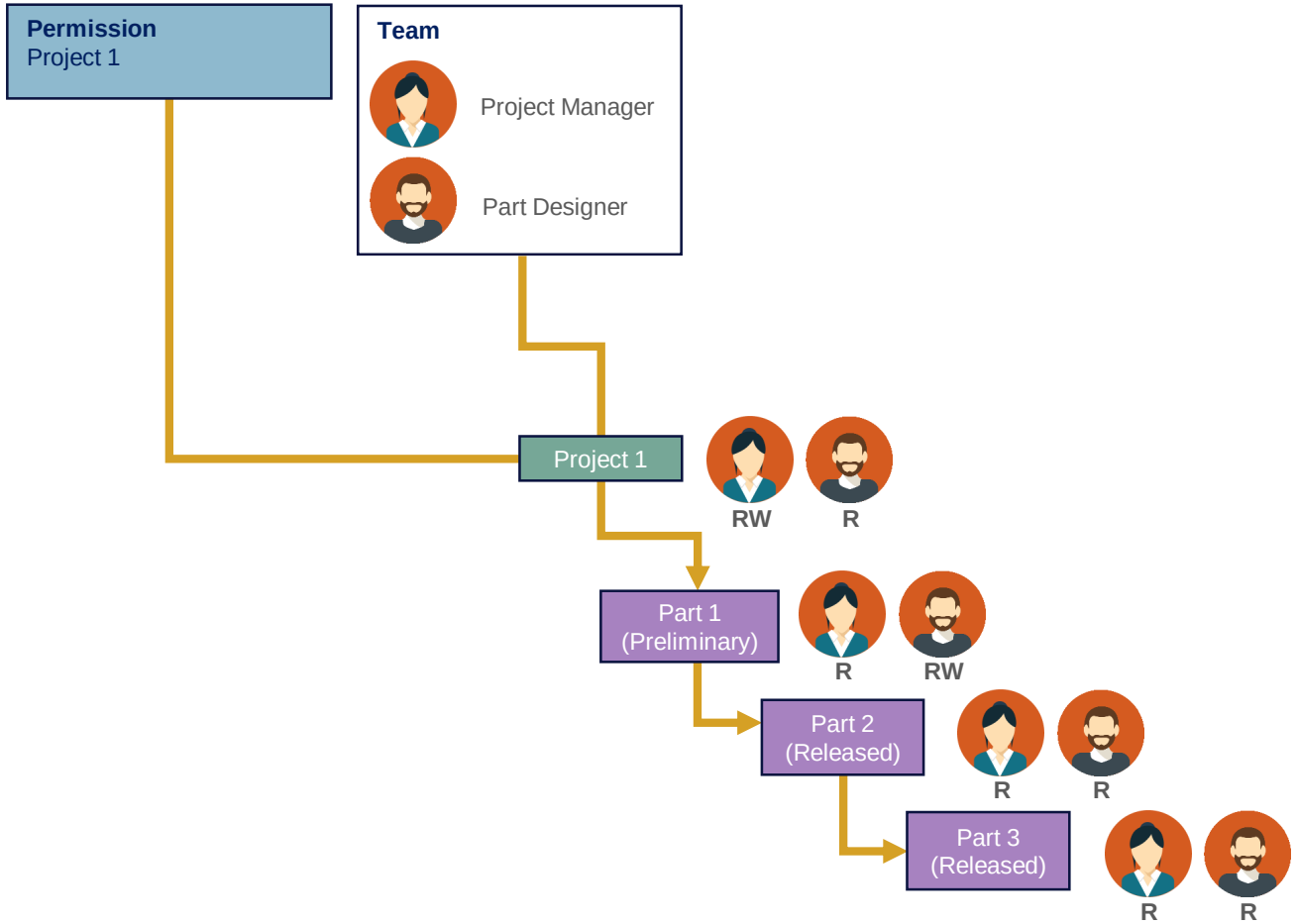
DAC Use Cases

- High-level Business Cases:
  - Project Workspace (Root – Project)
    - An organization has many concurrent projects each with related items and assigned users with project specific roles.
  - Partner/Supplier/Customer Data Release (Root – Manufacturer, Supplier, or Customer)
    - An organization has suppliers providing parts related to a product and would like to set specific project related permissions for supplier access.
    - An organization has an obligation to release certain product related information to a customer and would like to set specific permissions for customers accessing this data.
  - Development Collaboration across Multiple Companies (Roots – multiple)
    - An organization is collaborating simultaneously with multiple companies in the same project and would like to set specific project related permissions for each company.

© 2018 Aras

DAC Use Case: Parts in Different States within a Project

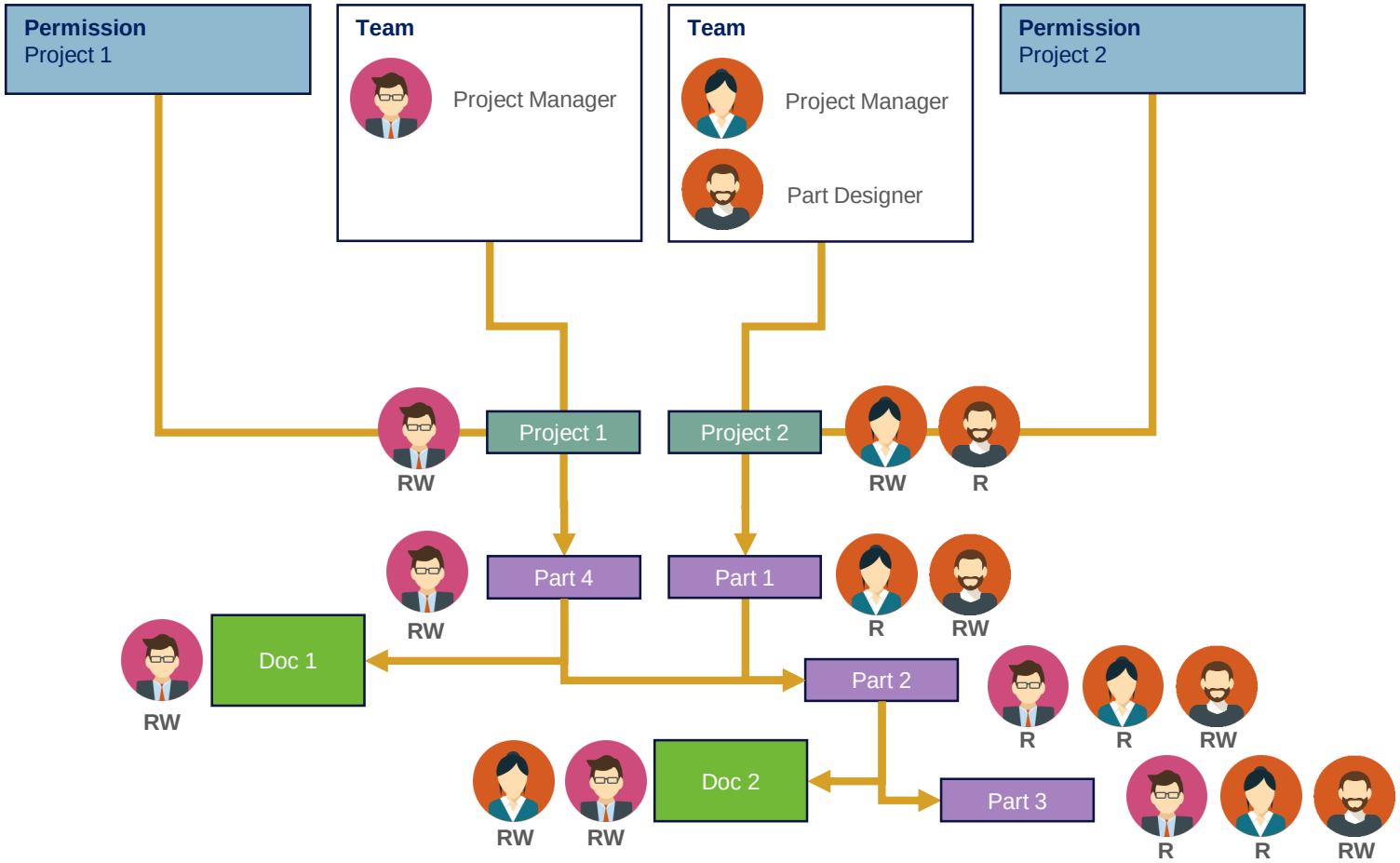
- Permissions for Items in different life cycle states which are part of a project
- Example:
  - Part Designer has Read and Write permissions to Parts in the “project” that are in the *Preliminary* State.
  - The Part Designer only has Read permissions to Parts in the “project” that are in the *Released* State.
  - The Project Manager has Read and Write permissions to the “project” but only Read permissions to all related parts.



© 2018 Aras

DAC Use Case: Multiple Overlapping Projects

- Permissions for Items which are part of a project with users having specific project roles.
- Example:
  - Part Designer has Read and Write permissions to Parts in the “Project”, Project Managers only have Read permissions.
  - The Project Manager has Read and Write permissions to the “Project” but only Read permissions to all related parts.



© 2018 Aras

DAC Mechanism

- DAC is defined by creating a Query Definition from the root itemtype which will have a Team assigned
- A Derived Relationship Family (which references the Query Definition) must be created to generate the derived relationships from the root item to the related items into a “domain”, promoted to “Active”
- A DAC Definition (which references the Derived Relationship Family) must be created to assign (project team member) Permissions based on root item permission and destination domain item state.
  - Permissions used in the DAC Definition should only include team roles, not system, group or alias identities

© 2018 Aras

Combining Access Controls

ACE 2019
INNOVATE
TRANSCEND
REALIZE

Combining Access Controls

- Permissions using all of the mechanisms may be combined to provide the desired access controls
- A specific user will be granted access to an item if –

  (The active permission on an item grants them access as a group or alias identity

  - OR -

  They have a role on the team identified for the item which grants them access

  - OR -

  They have a defined team role for a team defined for a root item, and an active DAC Domain Definition grants them access)

  - AND

  They meet the criteria for all MAC Policies in effect

© 2018 Aras

Important Considerations

- Performance –
  - MAC Policies have been shown not to have a significant impact on performance
  - DAC definitions may affect performance in two main ways, so they should be used with caution
    - When items change, recalculation of domain relationship family impacts may be triggered
    - Access calculations must take into account all of the domains an item belongs to
- Enterprise Search does not currently enforce MAC and DAC

© 2018 Aras

User Visibility Rules

ACE 2019
INNOVATE
TRANSCEND
REALIZE

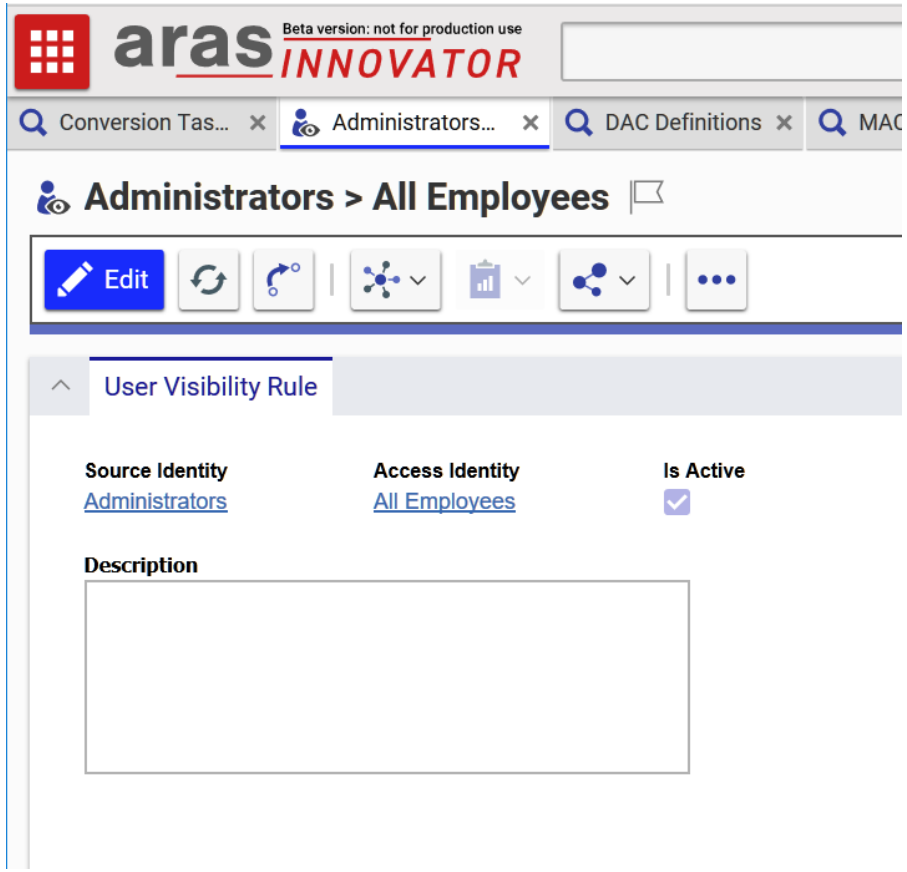
User Visibility Rules

- Scenarios like GDPR require companies and systems to meet user privacy rules
- User Visibility Rules are a form of MAC specially constructed to restrict permissions for certain groups to view identity and user information
- A new “User Visibility Rule” ItemType specifies a group identity with rights to access identity and user information from another specified group identity

© 2018 Aras

User Visibility Filter ItemType

- Allows Admin's to configure which Source (Requestor) Identity can access information of an Access (Subject) Identity.
- The system will support as many User Visibility Filters as needed.
- In the backend, a few MAC Policies are used to enforce the system User Visibility Filters for User and Identity ItemTypes.



© 2018 Aras

ACE 2019
INNOVATE
TRANSCEND
REALIZE

Thank You

Mike Gavlak

mgavlak@aras.com