Securing IP using Advanced Agile PLM Capabilities

Sharad Udyawar
IT Analyst
Coherent

Problems to be Solved

1. Many Items and Changes in Agile contain very sensitive IP – should be secured
2. Some IP is subject to multiple legal restrictions (ITAR, EAR, etc.)
3. IP must be controlled, yet allow “appropriate” collaboration
4. Enable users (not IT) to manage their own IP security
5. Business wants granular security but minimal data entry.
6. Security model must be scalable across classes of objects
7. Security model must be maintainable with minimum effort

Advanced Features Used

1. Dynamic Lists
2. $USERGROUP variable
3. Event Framework
4. Groovy Scripting

Dynamic Lists

1. Contains a list of values that are updated at run time.
2. Based on a criteria

$USERGROUP variable

1. $ variables are system variables that can be used in building Privilege Mask Criteria

2. $USERGROUP maps to the name(s) of PLM user groups. So, if a field is tied to the Admin list for User Groups, criteria can match a user to a user group; this criteria can then be used with Read and Discover privileges to grant object access and control to a group of users.

Event Framework

1. Events act as trigger points for generating an automation action within the PLM application.

2. Event is generated from a source within Agile PLM applications. The source can be a business action triggered by a user, a UI action, or system initiated source such as a timer.

Event Types

Name
Approve for Workflow
Audit for Workflow
Cancel Check Out Files
Change Approvers or Observers for Workflow
Change Status for Sourcing Object
Change Status for Workflow
Check In Files
Check Out Files
Comment for Workflow
Compliance Rollup on Object
Create Object
Create Variant Instance
Delete Object
Derive Variant Model Option BOM
Escalation for Workflow
Export Object
Extend Actions Menu
Extend Tools Menu
Get File
Incorporate Item
Promotion Failure for Workflow
Purge Version Files
Reject for Workflow
Reminder for Workflow
Save As Object
Scheduled Event
Transfer Authority
Unincorporate Item
Update Relationship
Update Table
Update Title Block
Update Variant Configuration
Validate Variant Configuration
Validate Variant Instance Selections
Validate Variant Model Option BOM

Groovy Scripting

1. Groovy is an object-oriented programming language that can be used as a scripting language for the Java Platform.

2. Can be used in Script PX which can be called from Events

3. Scripts can be used to Automate functions with simple business logic such as data validation, notification, or defaulting field values

Solution Architecture

1. Create Page 2 attributes for Security on Agile classes
2. Create User Groups to represent Orgs, Legal Classification and Suppliers
3. Tag each User group as Org/ Legal Classification/Supplier
4. Create 3 Dynamic Lists for Orgs/Legal Classification/Supplier
5. Attach dynamic lists to the corresponding security attributes on all classes
6. Assign appropriate User Groups to users
7. Use Event Framework with Groovy Script for Defaulting
8. Use Event Framework with Groovy Script for Validation
9. Control access with Criteria based on $USERGROUP

High-Level Approach

- Specify ownership (Design Org) for every object (Part or Change)
- New object security defaults to the "Design Org" of the creator rather than "Public".
- Every object carries security attributes that define its access
- To gain access, a user must belong to the proper User Group
- Access is at the Discovery level. If you do not have access, the object is not visible.

High Level Flow

1. Upon creation of a new Item or Change, default security attributes to:
   - Security Level = "Org"
   - Access Orgs = the "Home Org" of the creator
   - Supplier Access = blank
   - File Access Orgs = blank
2. Creator can modify these values at first.
3. Once the Item is released or the Change is Submitted, only a Security Officer can modify security.
4. Multiple Orgs can be added if the Item or Change must be actively used by another Org.
5. One or more Suppliers can be added if they either make or buy the item, or need to review or approve the Change.

Security Attributes

Security

Security Class*: Restricted
Access Orgs: ORG001; ORG002
Legal:
Supplier Access:
File Access Orgs: ORG002

Security Attribute	Determines What?
Security Class	Which kinds of groups get access (controls the other values) Public – every user has access Restricted – only specified access orgs/suppliers allowed
Access Orgs	Which Org(s) get access
Legal	Which legal restrictions apply (EAR, ITAR, etc.)
Supplier Access	Which Suppliers get access
File Access Orgs	Which Org(s) get access to attachments If blank, then uses list from “Access Orgs” attribute

User Group – Access Org

ORG001
User Group

Actions

General Info | Users | Escalations | Assignments | Share | Attachments | History

Page Two

Name: ORG001
Type: User Group
Description:
Status: Active
Global/Personal: Global

Page Two

Access Org: Yes
ITAR: No
Supplier: No

User Group – Legal

ITAR
User Group

Actions

General Info | Users | Escalations | Assignments | Share | Attachments | History

Page Two

Name: ITAR
Type: User Group
Description:
Status: Active
Global/Personal: Global

Page Two

Access Org: No
ITAR: Yes
Supplier: No

User Group – Supplier

SUPPLIER001
User Group

Actions

General Info | Users | Escalations | Assignments | Share | Attachments | History

Page Two

Name: SUPPLIER001
Type: User Group
Description:
Status: Active
Global/Personal: Global

Page Two

Access Org: No
ITAR: No
Supplier: Yes

Dynamic List

Criteria:Access_Orgs_Criteria

General Information | Criteria | Where Used | History

Criteria:

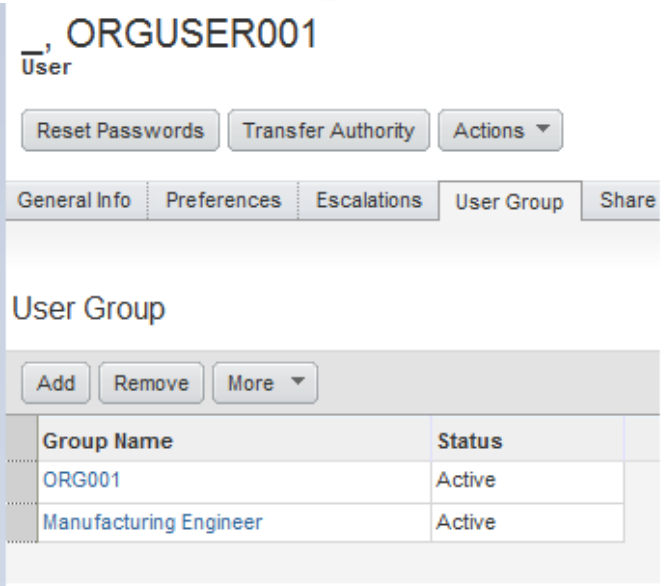
```
User groups  Page Two.Access Org In Yes  And
 General Info.Status In Active  And
 General Info.Global/Personal In Global
```

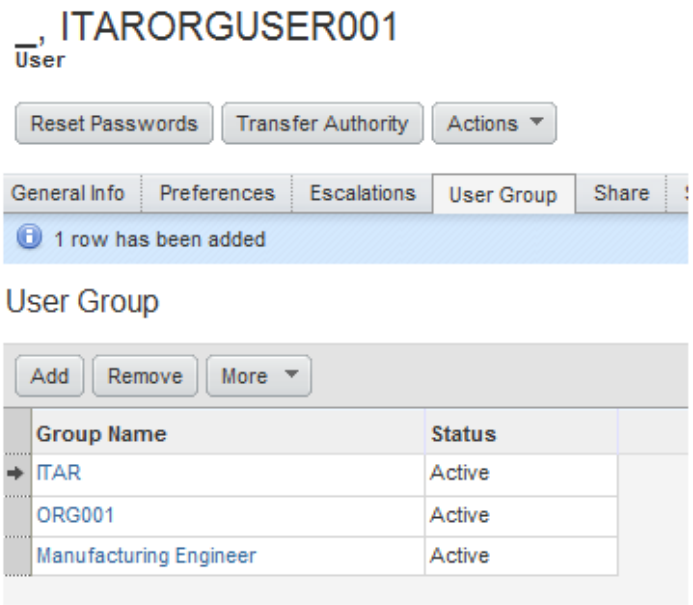
List:Access_Org_List

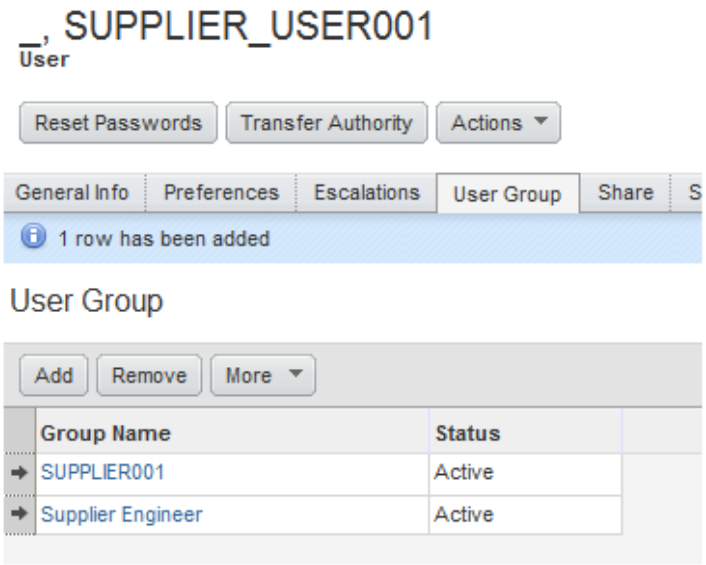
General Information | List | Where Used | History

Name	Access_Org_List
API Name	Access_Org_List
Description	Access_Org_List
Enabled	Yes
List Type	Dynamic
Display Type	List
Criteria	Access_Orgs_Criteria

User Provisioning







Groovy Script - Defaulting

Event:Security Defaulting - Items

General Information | Where Used | History

Event Type	Create Object
Name	Security Defaulting - Items
API Name	SecurityDefaultingItems
Description	
Enabled	Yes
Object Type	Items

Event Subscriber:Security Default_Items Subscriber

General Information | Monitor | History

Name	Security Default_Items Subscriber
API Name	SecurityDefault_ItemsSubscriber
Description	
Enabled	Yes
Event	Security Defaulting - Items
Event Type	Create Object
Object Type	Items
Event Handler	Security Defaulting
Handler Type	Script PX
Trigger Type	Post
Execution Mode	Synchronous
Order	0
Error Handling Rule	Continue

Event Handler:Security Defaulting

General Information | Where Used | History

Handler Type	Script PX
Name	Security Defaulting
API Name	SecurityDefaulting
Description	
Role	
Enabled	Yes

Script

```
import com.agile.*

void invokeScript(IBaseScriptObj obj) {

        user = session.getCurrentUser()
        userHomeOrg = user.getValue(UserConstants.ATT_PAGE_TWO_LIST11);
        Object[] userGroups = [userHomeOrg];

        Map map = new HashMap();

        cell = dObj.getCell(CommonConstants.ATT_PAGE_TWO_LIST17);
        values = cell.getAvailableValues();
        values.setSelection(userGroups);
        map.put(CommonConstants.ATT_PAGE_TWO_LIST17, values);

        cell = dObj.getCell(CommonConstants.ATT_PAGE_TWO_MULTILIST05);
        values = cell.getAvailableValues();
        values.setSelection(userGroups);
        map.put(CommonConstants.ATT_PAGE_TWO_MULTILIST05, values);

        map.put(CommonConstants.ATT_PAGE_TWO_LIST16, "Restricted");

        obj.setValues(map);
}
```

Groovy Script - Validation

Event:Security Attributes Validation Event

General Information | Where Used | History

Event Type	Update Title Block
Name	Security Attributes Validation Event
API Name	SecurityAttributesValidationEvent
Description	
Enabled	Yes
Object Type	Items

Event Subscriber:Security Attributes Validation Subscriber

General Information | Monitor | History

Name	Security Attributes Validation Subscriber
API Name	Security_Attributes_Validation_Subscriber
Description	
Enabled	Yes
Event	Security Attributes Validation Event
Event Type	Update Title Block
Object Type	Items
Event Handler	Security Attributes Validation
Handler Type	Script PX
Trigger Type	Pre
Execution Mode	Synchronous
Order	0
Error Handling Rule	Stop

Event Handler:Security Attributes Validation

General Information | Where Used | History

Handler Type	Script PX
Name	Security Attributes Validation
API Name	SecurityAttributesValidation
Description	
Role	
Enabled	Yes

Script

```
import com.agile.api.*
void invokeScript(IBaseScriptObj obj)
{
        accessOrg = dataObj.getValue(CommonConstants.ATT_PAGE_TWO_MULTILIST05);
        legal = dataObj.getValue(CommonConstants.ATT_PAGE_TWO_MULTILIST04);
        securityClass = dataObj.getValue(CommonConstants.ATT_PAGE_TWO_LIST16);
        supplierAccess = dataObj.getValue(CommonConstants.ATT_PAGE_TWO_MULTILIST03);

        if (!securityClass){
                throw new AgileDSLException( "Security Class is mandatory");
        }
        if ( (securityClass == "Restricted") && (!accessOrg)){
                throw new AgileDSLException( "Access Org is needed when Security Class = Restricted");
        }
        if ((securityClass == "Public") && ((accessOrg)  || (legal)  )){
                throw new AgileDSLException( "You cannot assign a Access Org/Legal when Security Class = Public");
        }
        if ( (legal) && (supplierAccess)){
                throw new AgileDSLException( "You cannot assign Supplier Access for ITAR or EAR items");
        }
        if ( (securityClass == "Public") && (supplierAccess)){
                throw new AgileDSLException( "You cannot assign Supplier Access for Public items");
        }
}
```

Discovery Criteria

Criteria:Item Discovery Criteria

General Information | Criteria | Where Used | History

Criteria:

```
Parts  Page 2.Security Class* In Public  Or
( Page 2.Access Orgs Contains Any $USERGROUP  And
 Page 2.Legal Is Null  And
 Page 2.Security Class* In Restricted ) Or
( Page 2.Access Orgs Contains Any $USERGROUP  And
 Page 2.Legal Contains Any $USERGROUP  And
 Page 2.Security Class* In Restricted ) Or
```

Attachment Security Criteria

Criteria:Attachments Access Criteria

General Information | Criteria | Where Used | History

Criteria:

```
Parts  Page 2.Security Class* In Public  Or
(( Page 2.File Access Orgs Contains Any $USERGROUP  Or
( Page 2.Access Orgs Contains Any $USERGROUP  And
 Page 2.File Access Orgs Is Null )) And
 Page 2.Legal Is Null  And
 Page 2.Security Class* In Restricted ) Or
(( Page 2.File Access Orgs Contains Any $USERGROUP  Or
( Page 2.Access Orgs Contains Any $USERGROUP  And
 Page 2.File Access Orgs Is Null )) And
 Page 2.Legal Contains Any $USERGROUP  And
 Page 2.Security Class* In Restricted ) Or
```

Problems Solved

1. Many Items and Changes in Agile contain very sensitive IP – should be secured

   Access control now available at Org level – default is to secure by Org

2. Some IP is subject to multiple legal restrictions (ITAR, EAR, etc.)

   Item/Change can be tagged as ITAR,EAR and immediately secured

3. IP must be controlled, yet allow “appropriate” collaboration

   Other orgs can be easily added for access

4. Enable users (not IT) to manage their own IP security

   Access security fully controllable by users without IT intervention

5. Business wants granular security but minimal data entry

   Security defaults to creator’s org – this is all that is needed 98% of the time

Problems Solved

6. Security model must be scalable across classes of objects

   Same Page 2 attributes and same Security Mechanism is used on Item, Documents, Change Orders, Change Requests, Manufacturer Orders and Deviations

7. Security model must be maintainable with minimum effort

   When a new business org is set up all that is needed is to create a user group with the org name and assign that user group to the users

   When security needs to be extended to a new Agile class(even in a new module like NCR in the PQM module), all we need to do is

   - Enable the same Page 2 security attributes on that new class
   - Enable the equivalent events for the new class