SAP Integrated Business Planning - User Management

Unmesh Gandhi & Evelyina Holban, SAP
October, 2019
Agenda

- Overall Concept

- IBP User Provisioning
  - Mass Employee and Business User Creation
  - SOAP Service

- IBP Delivered Content

- User Groups

- Data Filters
  - Permission Filters
  - Attribute Permissions
Concept
IAM: User Management Concept

- All functionality exposed to the customer is provided as web-enabled user interfaces (Fiori Applications)

- User management in IBP is based on already existing standard structures and persistencies, such as SU01 (Transaction for User Maintenance) or PFCG (Transaction for Role Maintenance).

- Types of users:
  - **Business users** for consuming the IBP functionality
  - **Technical users** e.g. SAP Support users, Communication users

- An initial key user, the SAP admin user and technical users are pre-delivered by SAP with the initial IBP system.

- Business users will be created by the SAP admin user, along with a minimum set of employee data.
IAM: Main Entities

Business User
Business Role
Business Catalog
Fiori App
System Landscape: IBP & IAS (as identity provider)

**Simplified Overview**

**User**

Browser

SSO (Logon w/o entry of user/password)

MS Excel

**IAS***

User Authentication

**IBP System**

**User** (identified via ID, E-Mail, etc.)

**Business User Employee**

*IAS: SAP Cloud Identity Authentication Service
*SAML2: Security Assertion Markup Language 2.0 is a version of the SAML standard for exchanging authentication and authorization data between security domains.
**System Landscape: IBP & IAS & Customer IDP**

**Simplified Overview**

- **Customer IDP**
  - Browser
  - MS Excel
  - User Authentication
  - SSO (Logon w/o entry of user/password)
  - SAML2*

- **IBP System**
  - User Authentication
  - User (identified via ID, E-Mail, etc.)
  - Business User Employee
  - IAS* Proxy Mode

* **SAML2**: Security Assertion Markup Language 2.0 is a version of the SAML standard for exchanging authentication and authorization data between security domains.
* **IAS**: SAP Cloud Identity Authentication Service
* **IDP**: Identity Provider
IBP User Provisioning
Identity and Access Management Fiori Apps (IAM)

Identity and Access Management

Maintain Business Users

Locked users

Maintain Business Roles

Business Role Templates

Display Technical Users

IAM Information System

Business Catalogs

Display Restriction Types

Display Authorization Trace

Employee Master Data

Maintain Employees
IAM: Fiori Launchpad

Initial User:
- Customer gets administrator user (and password)
- This user has the authority to logon to Fiori Launchpad
- On the Fiori Launchpad two groups are displayed:
  - Employee Master Data
  - Identity and Access Management

Admin user is able to:
1. Maintain Employee:
   - To store employee information like E-Mail, phone number, etc.
   - Business partner is created in IBP system
2. Maintain Business User:
   - To store regional settings like date/time formatting, decimals, etc.
   - SU01 user is created in backend and linked to business partner (= employee)
3. Upload users to IAS tenant (to enable SSO for users)
4. Maintain Business Roles:
   - Assign one or multiple business catalogs to a business role
   - Assign restriction-values to business role
   - Assign business users to business role
1 Maintain Employee

- List of all employees
- Additional information (first name, last name)
- Mass creation
1 Maintain Employee

Add new employee:
- Personal Data
- Employee Data
1 Maintain Employee

Create Business User
2 Maintain Business Users

- List all existing business users
- Create New business user from the list of employees
2 Maintain Business Users

- Personal Data
- User Data
- Regional Settings
- Assigned Business Roles
- Application Jobs
2 Maintain Business Users

- Download for IDP
- Download Users
- Download User Role Assignments
2 Maintain Business Users

- Upload User Role Assignment
- Display Changes
Lock User:

- Multiple or single users can be locked / unlocked
- If the checkbox ‘Locked’ is set, then this user will not be able to logon
- User / Password are still valid. Only the logon is not possible.
- Password policy is configured on IAS
- To unlock the user, just clear the checkbox
Maintain Business User App:

- Download Business Users to CSV File
3 Upload of business user into IAS

IAS Tenant*:

- Open the IAS Administration Console and log on with your e-mail address and password
- Choose the Fiori app "Import Users"
- Upload CSV File in order to enable SSO for each customer user
- Afterwards choose "Send E-Mails" and then click on "Send" to send activation e-mails to all users that are not active yet.

*: SAP Cloud Identity
4 Maintain Business User Roles

List:
- Business roles
- Assigned users
- Assigned business catalogs
4 Maintain Business User Roles

Detail:
- General Information
4 Maintain Business User Roles

**Detail:**

- Assign Business Catalogs to Business Role
- Maintain Restrictions
Maintain General Restrictions

“Restriction”:
- In the backend SAP defined a mapping of authority objects to the so-called restrictions
- Among others this includes the fields of the authority object and the activity
- The different activities are simplified to
  - WRITE
  - READ
  All deviations of activities are mapped these two
- Customer can maintain:
  - Type of the WRITE/READ access:
    - Restricted
    - Unrestricted
    - No access
  - In case the access is restricted, then the customer can enter restriction values
4 Maintain Business User Roles

- Assign Business User to Business Role
4 Maintain Business User Roles

- Copy
- Download
- Delete
- Create From Template
User Provisioning via Services

IBP System

Customer Owned Identity Management System (SOAP)

SAP CP – IPS
(Identity Provisioning Service)

SAP COM_0093

SAP COM_0193
User Provisioning from External Identity Management Systems

- The communication scenario Identity Management Integration (SAP_COM_0093) allows to provision business users and assign roles to users from an identity management system via SOAP services:
  - `MANAGEBUSINESSUSERIN` lets you create business users and assign roles in your system
  - `QUERYBUSINESSUSERIN` lets you read existing business user
User Provisioning via SAP Cloud Platform Identity Provisioning Service

- The communication scenario SAP Cloud Platform Identity Provisioning Integration (SAP_COM_0193) allows you to connect to SAP Cloud Platform Identity Provisioning Service with SAP Integrated Business Planning.

- You can provision business users and assign business roles to business users from an identity management system, for example, SAP Cloud Platform Identity Authentication Service in SAP Integrated Business.
IBP Delivered Content
Business Role Template
Business Catalogs

1

Deprecated in use

Business Catalogs (87)

<table>
<thead>
<tr>
<th>Business Catalog</th>
<th>Business Catalog ID</th>
<th>Read Only</th>
<th>Status</th>
<th>Release</th>
<th>Used In Business Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC - XYZ Segments</td>
<td>SAP_BIP_BC_ABCXYZ_SEGMENT_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alert Definition and Subscription</td>
<td>SAP_BIP_BC_ALERTDEF_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alert Monitor</td>
<td>SAP_BIP_BC_ALERTMON_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics</td>
<td>SAP_BIP_BC_ANALYTICS_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Jobs Test</td>
<td>SAP_BIP_BC_APPJ_TEST_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Job Template</td>
<td>SAP_BIP_BC_APPJETEMPLATE_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Jobs</td>
<td>SAP_BIP_BC_APPLICATIONJOB_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Available-to-Deploy Profiles</td>
<td>SAP_BIP_BC_ATDPROFILE_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Attribute Permissions</td>
<td>SAP_BIP_BC ATTPERM_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic Functions</td>
<td>SAP_BIP_BC_BASIC_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cases</td>
<td>SAP_BIP_BC CASES_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Categories</td>
<td>SAP_BIP_BC_CATEGORIES_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings For Change History</td>
<td>SAP_BIP_BCCHANGEHISTORYSET_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change History</td>
<td>SAP_BIP_BC_CHANGEHISTORY_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collaboration</td>
<td>SAP_BIP_BC_COLLABORATION_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared Content Administration</td>
<td>SAP_BIP_BC CONTENTADM_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customers</td>
<td>SAP_BIP_BC CUSTOMER_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Sharing Plan Execution</td>
<td>SAP_BIP_BC_DASHEXE_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Sharing Plan Management</td>
<td>SAP_BIP_BC_DASHPLM_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Integration</td>
<td>SAP_BIP_BC_DATANTEGRATION_PC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Important Business Catalogs

Identity and Access Management
- User Management SAP_CORE_BC_IAM_UM
- Role Management SAP_CORE_BC_IAM_RM
- Role Assignment SAP_CORE_BC_IAM_RA

IBP
- Manage Permission Filters SAP_IBP_BC_VISFILTER_PC
- Manage Attribute Permissions SAP_IBP_BC_ATTPERM_PC
- User Groups SAP_IBP_BC_USERGROUP_PC
- Basic Planning Tasks SAP_IBP_BC_EXCEL_ADDIN_PC
- Contains only Business Authorizations! No FIORI Apps!
- Application Jobs - SAP_IBP_BC_APPLICATIONJOB_PC
IAM Information System

Displays the usage and relations between
- Applications
- Business Catalogs
- Business roles
- Users
Display Authorization Trace

- Helps analyze authorizations which are missing
- Activate/deactivate a trace
- Display authorization check results
User Groups
User Groups

- **User Groups** allow administrators to associate sets of users in a common set (Group). Groups can in turn be used when sharing and assigning IBP objects (such as IBP Cases, Alerts, Permission Filters, Attribute Permissions).
Permission Filters
Permission Filters

- Permission filters allows an administrator to restrict user access to specific master data types and key figure values

- A permission filter is defined as one or more set of conditions (Attribute/Value pairs) along with a selection of key figures, which are associated to specific planning area
  - The first set of conditions (Attribute/Value pairs), defines a user’s READ scope
  - The key figure selection, allows us to restrict the write access of a user to the selected key figures
  - The second set of conditions (Attribute/Value pairs), defines a user’s WRITE scope atop of the selected key figures
  - The write scope only applies to key figure values and is currently only limits WRITE access within an Excel planning view
  - It is possible to set the ACCESS levels to UNRESTRICTED for READ and WRITE
  - WRITE access can be revoked explicitly by selecting a “NO ACCESS” flag
## Define Permission Filters

### Filter Criteria for Read Access
- **Product Group**: Equal to Consumer Electronics

### Write Access for Key Figures
- **Write Key Figure**: DEMANDPLANNING.QTY

### Filter Criteria for Write Access
- **Product ID**: Equal to \( \_\_\_\_\_\_\_\_ \)
## Permission Filter (Read & Write)

<table>
<thead>
<tr>
<th>Planning Area</th>
<th>PRDGROUP</th>
<th>Demand Planning Qty</th>
<th>Key Figure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer Electronics</td>
<td>HT_001</td>
<td>12570</td>
<td>CONSENSUSDEMAND</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7133785</td>
<td>5989544</td>
</tr>
<tr>
<td></td>
<td>HT_002</td>
<td>10480</td>
<td>7022301</td>
</tr>
<tr>
<td></td>
<td>HT_003</td>
<td>3809031</td>
<td>1342069</td>
</tr>
<tr>
<td></td>
<td>HT_004</td>
<td>3809031</td>
<td>1342069</td>
</tr>
</tbody>
</table>

### READ
- **PRDGROUP = 'Consumer Electronics'**

### WRITE
- **PRDID = 'HT_001'**

**Permission Filter Conditions:**
- Attribute/Value pairs are associated to specific Planning Areas.
- When assigned to a user, the condition is transformed into the intersection of two "where-clauses".

**Example:**
- `PRDGROUP = 'Consumer Electronics'` and `PRDID = 'HT_001'` are applied to queries run on behalf of the user at the data set level.
Assigning Users to Permission Filters

Assign User – direct \ indirect

Search and Manage Assignment
Auto-Complete Filter Criteria Values

- When turn-on, the Auto-Complete Filter Criteria Values feature triggers an automatic generation of values for the dependent attributes of a given key figure.

- On top of the attributes user select for filter, the base planning level may contain other attributes that need to be nullified. When the switch is active, the app analyzes the data model of all key figures with member attributes that user have included in the filter criteria and generates values for the dependent attributes. This way user don’t have to worry about specifying the dependent attribute values.
Change History

- User can review all changes that were made to a permission filter on the Change History tab.
- The change history shows what was changed where and by whom.
Attribute Permissions
Attribute Permissions

Goal: The user should only access those master data attributes to which he/she has read permissions.

Benefits:

- **Security** – end users only see the attributes they are allowed to.
- **Performance** – Limiting the number of attributes. This leads to improved performance in areas like excel and analytics.
- **Usability** – End User has a better user experience with working on the attributes that are more relevant for them instead of browsing and filtering through several attributes in the model.

Remarks:

- Attribute Permissions complements the existing concept of IBP Permission Filters.
- IBP Permission Filters restricts the values of the attributes whereas Attribute Permissions restricts the set of master data attributes that are visible to end users.
- External OData service
Read Attribute Permissions (IBP 1905)

As an example, FINANCEGROUP attribute of Product Master Data Type should only be allowed to be viewed by Finance Planners and should be hidden for all other users.

<table>
<thead>
<tr>
<th>Product ID</th>
<th>Description</th>
<th>FinanceGroup</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>P001</td>
<td>Product 001</td>
<td>AOP</td>
<td>Consumer Electronics</td>
</tr>
<tr>
<td>P002</td>
<td>Product 002</td>
<td>AOP</td>
<td>Consumer Electronics</td>
</tr>
<tr>
<td>P003</td>
<td>Product 003</td>
<td>FIN</td>
<td>Kitchen Appliance</td>
</tr>
</tbody>
</table>

Define following Attribute Permissions:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Attribute Permission</th>
<th>Read Attribute Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter 1</td>
<td>AP_FINANCEGROUP</td>
<td>Unrestricted</td>
</tr>
<tr>
<td>Filter 2</td>
<td>AP_OTHERS</td>
<td>Exclude = FINANCEGROUP</td>
</tr>
</tbody>
</table>

For Master Data Maintenance - Planners need to have following restriction in their role:
- Master Data – Read Restriction
- Master Data Type = PRODUCT
- Planning Area = ‘XYZ’
- Version (IBP_VRSIO) = * (unrestricted)
- Scope (MD_EDIT_SCOPE) = * (unrestricted)
Edit Attribute Permissions

For an example, User has visibility to all attributes of the Master Data Type Product, but can only edit the Description attribute.

<table>
<thead>
<tr>
<th>Product ID</th>
<th>Description</th>
<th>FinanceGroup</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>P001</td>
<td>Product 001</td>
<td>AOP</td>
<td>Consumer Electronics</td>
</tr>
<tr>
<td>P002</td>
<td>Product 002</td>
<td>AOP</td>
<td>Consumer Electronics</td>
</tr>
<tr>
<td>P003</td>
<td>Product 003</td>
<td>FIN</td>
<td>Kitchen Appliance</td>
</tr>
</tbody>
</table>

Define following Attribute Permission

<table>
<thead>
<tr>
<th>Attribute Permission</th>
<th>Read Attributes</th>
<th>Write Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP_WRITE_ONLY_DESCR</td>
<td>Unrestricted</td>
<td>= DESCRIPTION</td>
</tr>
</tbody>
</table>

For Master Data Maintenance - Planners need to have following restriction in their role:

- Master Data – WRITE Restriction
- Master Data Type = PRODUCT
- Planning Area = ‘XYZ’
- Version (IBP_VRSIO) = * (unrestricted)
- Scope (MD_EDIT_SCOPE) = * (unrestricted)
# Rules of applying Attribute Permissions

| AP1: READ | PRDID, BRAND, PRDGROUP | WRITE: | Exclude PRDID |
| AP2: READ | LOCID, BRAND, REGION | WRITE: | REGION |

User A has AP1 assigned
- Can **READ**: PRDID, BRAND, PRDGROUP
- Can **Write**: BRAND, PRDGROUP

User B has AP1 and AP2 assigned
- Can **READ**: PRDID, BRAND, PRDGROUP, LOCID, REGION
- Can **Write**: BRAND, PRDGROUP, REGION
Manage Attribute Permissions App
### Manage Attribute Permissions App

#### Attribute Permissions Table

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Description</th>
<th>Has Read Access</th>
<th>Has Write Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>A0</td>
<td>A0</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>A00</td>
<td>A00</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>A000</td>
<td>A000</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>AG0TIMEZONE</td>
<td>44324234</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>A6LOC</td>
<td>location2</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>AG6ODESCR</td>
<td>Location Description</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>AG6PROD</td>
<td>agl product</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>AG6PRODDESCR</td>
<td>product description</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>A1</td>
<td>attribute1</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Change History**

<table>
<thead>
<tr>
<th>Changed On</th>
<th>Changed By</th>
<th>Section</th>
<th>Key</th>
<th>Type of Change</th>
<th>Field</th>
<th>Previous Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/30/2019, 12:24:28</td>
<td>Umesh Gandhi</td>
<td>Read Criteria</td>
<td>2</td>
<td>Add</td>
<td>OPERATOR</td>
<td>Excludes</td>
<td>Includes</td>
</tr>
<tr>
<td>09/30/2019, 12:24:28</td>
<td>Umesh Gandhi</td>
<td>Read Criteria</td>
<td>2</td>
<td>Add</td>
<td>SIGN</td>
<td>Excludes</td>
<td>Includes</td>
</tr>
<tr>
<td>09/30/2019, 12:24:28</td>
<td>Umesh Gandhi</td>
<td>Read Criteria</td>
<td>2</td>
<td>Add</td>
<td>VAL_LOW</td>
<td>Excludes</td>
<td>Includes</td>
</tr>
<tr>
<td>09/30/2019, 12:24:28</td>
<td>Umesh Gandhi</td>
<td>Information</td>
<td>IBP1908_DEMO</td>
<td>Modify</td>
<td>ACCESS_READ</td>
<td>Unrestricted</td>
<td>Restricted</td>
</tr>
</tbody>
</table>
Usage of Attribute Permissions

- Analytics – Advanced app
- Define and Subscribe to Custom Alerts app
- Dashboard - Advanced app
- Manage Cases app
- IBP Excel Add-in app
- Data Integration Jobs app
- Planning Filters app
- Application Logs
- External OData services
Backward Compatibility

- Attribute Permission filter (SAP_ALLATTRIBUTES) with unrestricted read and write attributes will be delivered by SAP.

- All existing business users will have the SAP_ALLATTRIBUTES permission filter assigned.

- For new business users the SAP_ALLATTRIBUTES filter will be assigned by default if global parameter ATTPERM_ASSIGN_NEW_USER is set to ‘X’.
Integrating External Systems with Permission Filters and Attribute Permissions

- The communication scenario Planning - Permissions Integration (SAP_COM_0069) allows users to maintain permission filters and attribute permissions from external systems.
  - The OData service /IBP/VISIBILITY_FILTER_SRV offers operations to read, create and maintain permission filters and assign them to users and user groups.
  - The OData service /IBP/ATTPERM_API_SRV offers operations to read, create and maintain attribute permissions and assign them to users and user groups.

- For more information about the related Web service and setting up the communication arrangement, see [2604799](https://example.com/2604799) and [2810444](https://example.com/2810444).
Resources

- IBP Security Aspects
- Identity and Access Management
- User Authentication
- Integrating Business Users from an External Identity Management System
- Permission Filters
- Attribute Permissions
- Integrating External Systems with Permission Filters and AttributePermissions
Thank you.

Contact information:

Unmesh Gandhi
u.gandhi@sap.com

Evelyna Holban
evelyna.holban@sap.com