



Identity Application



Agenda

- Organizational Chart
- SOD Enhancement
- Role Approval [Role to Role / Role to Group / Role to Container]
- Resource Weightage
- RRSD Performance improvements
- Workflow and Form Service

General

- Show/hide photo as user preference
- User/Group search based on cn
- SOD check when requesting IG permission
- RIS API support
- UI performance improvement
- Sorting Column based on full name configuration

Organizational Chart

- Enhanced UI layout
- Support to display multiple relationships in one Organization chart as long as the relationships share the source entity
- Support displaying of Multi-valued Manager Attributes in Manager-Employee relationship
- Show/hide user photo in case of relationships involving user as either source and/or target entity
- Configure default relationship to display on navigating to Org chart from People menu
- Configure default relationship for each of the entities
- Configure attributes to show in Organization chart for an entity
- Pagination and customizable search feature

Organizational Chart

Organization Chart

Search in users by First Name, Last Name

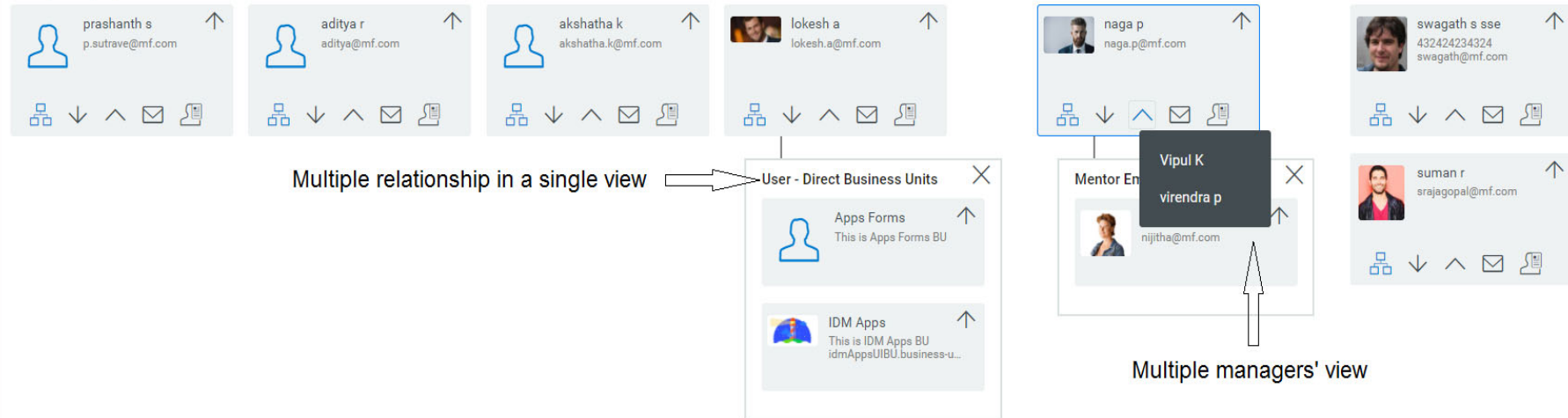
Show/hide photo



virendra p
virendra@mf.com

↓ ↑ ✉ 📄

Manager-Employee



prashanth s
p.sutrave@mf.com

aditya r
aditya@mf.com

akshatha k
akshatha.k@mf.com

lokesh a
lokesh.a@mf.com

naga p
naga.p@mf.com

swagath s sse
432424234324
swagath@mf.com

Multiple relationship in a single view

User - Direct Business Units

- Apps Forms
This is Apps Forms BU
- IDM Apps
This is IDM Apps BU
idmAppsUIBU.business-u...

Multiple managers' view

Vipul K
virendra p

Mentor En
nijitha@mf.com

suman r
sraajagopal@mf.com

Organizational Chart Configuration

- General
- Access
- Customization
- Branding
- Helpdesk
- Dashboard Widgets

CN

Search Attribute

Description

This setting will be used in the custom item listing page. Boolean attributes will only be a part of advanced search.

Base Container

data

Select Container

Default Orgchart Relationship

This setting will be used when one navigates to Organization Chart from entities listing page [Clear selection](#)

Organization Chart View

Any changes here are applicable in the orgchart page

Primary attributes

Business ID

Secondary attributes

Description Subordinate Business Units

Attributes

Manager Direct Members Parent Business Unit CN

Favourite Icecream

Orgchart Photo

Profile Picture

The value of this attribute will be used as a photo in Orgchart oard view.



SOD Enhancements

Detection of SOD conflicts in case of:

- Role to Groups or Containers assignments
- Inherited role SOD conflicts on requesting a parent role for User/group/container

SoD handling for groups and containers

User Application

- Members of group/container having conflicting roles will be detected when requesting a role
- Affected users and conflicting roles will be displayed in UI.
- Role admin can decide to assign the role to group/container by providing justification (or) remove the group/container containing conflicting user(s) from request.

Role and Resource Driver

- SOD check on re-sync when a Group (Static/Dynamic) membership is changed
- User is moved from one container to another
- Traces are captured in RRSD driver logs
- SoD Exception auto approval CEF audit event is triggered on such cases

SoD handling for groups and containers (Role and Resource Driver)

Sample Driver trace:

SOD conflicts detected on Resync - *Identity dn*: O=data\OU=container1\CN=user1, *SOD Conflict*: {"SOD CN":"hr-soft", "SOD DN":"O=system\\CN=driverset1\\CN=User Application Driver\\CN=AppConfig\\CN=RoleConfig\\CN=SoDDefs\\CN=Hr_softwareEng ", "*Conflicting Roles*":["O=system\\CN=driverset1\\CN=User Application Driver\\CN=AppConfig\\CN=RoleConfig\\CN=RoleDefs\\CN=Level30\\CN=Hr-assistant", "O=system\\CN=driverset1\\CN=User Application Driver\\CN=AppConfig\\CN=RoleConfig\\CN=RoleDefs\\CN=Level30\\CN=software-engineer"]}

SOD handling for Inherited role conflict

User Application

- When Role with conflicting child roles is requested for a user/group/container, SOD will be identified, and conflicts will be shown in feedback.
- When a user in a group or container requested a role with conflicting child roles, those conflicts will also be detected and shown in UI. (SOD handling for Group/containers use case)

Role and Resource Driver

- On Resync in RRSD when a Group membership is changed
- user is moved from one container to another
- when a child role is added to an already assigned role
- SOD exception auto approval audit event
 - When user is added to a group/container that contains conflicting roles assigned
 - When a new role is added as a child role to an already assigned role

Sample CEF event

CEF:0|NetIQ|Identity Manager|4.8.1.0|31613|SOD Exception Auto Approval|1|cs1=Implicit Container Role Add msg=SOD exception with Auto Approval was processed. Requested by Role Resource Driver; Target DN: O\=data,OU\=containersodCheck,CN\=aasoduser; Source DN:O\=system,CN\=driverset1,CN\=User Application

Driver,CN\=AppConfig,CN\=RoleConfig,CN\=RoleDefs,CN\=Level30,CN\=aasodrole2; Request DN:Request initiated by Role and Resource Service driver on Resync of O\=data\OU\=containersodCheck-CONTAINER; Request Category: Implicit Container Role Add; Request Status: PROVISIONED; Original Request Status: PROVISIONED; SOD DN: O\=system\CN\=driverset1\CN\=User Application
Driver\CN\=AppConfig\CN\=RoleConfig\CN\=SoDDefs\CN\=aaasodconflict;
fname=O\=system\CN\=driverset1\CN\=User Application
Driver\CN\=AppConfig\CN\=RoleConfig\CN\=RoleDefs\CN\=Level30\CN\=aasodrole2 rt=1588669115729 cs3=Set by the Role and resource driver.. cs2=O\=system\CN\=driverset1\CN\=User Application
Driver\CN\=AppConfig\CN\=RoleConfig\CN\=SoDDefs\CN\=aaasodconflict cs4=NEW_REQUEST dpriv=Request initiated by Role and Resource Service driver on Resync of O\=data\OU\=containersodCheck-container cs1Label=Request Category cs4Label=Original Request Status dtz=Asia/Kolkata spriv=O\=system\CN\=driverset1\CN\=User Application
Driver\CN\=AppConfig\CN\=RoleConfig\CN\=RoleDefs\CN\=Level30\CN\=aasodrole2 cs6Label=Request Object dvc=164.99.90.132 act= PROVISIONED suser=Role Resource Driver cs3Label=Request status Description dvchost=SLES12SP2-NIJITHA-90132 cat=DirXML\Driver\RoleAssignmentRequest\SOD_Exception_Auto_Approval\Add

duser=O\=data\OU\=containersodCheck\CN\=aasoduser cs2Label=SOD DN fileType=Role cs6={"gid":"","Data":"<sod><sod-dn>O\=system\CN\=driverset1\CN\=User Application
Driver\CN\=AppConfig\CN\=RoleConfig\CN\=SoDDefs\CN\=aaasodconflict<\sod-dn><sod-name>aaasodconflict<\sod-name><conflicting-roles><conflicting-role-0>O\=system\CN\=driverset1

\CN\=User Application

Driver\CN\=AppConfig\CN\=RoleConfig\CN\=RoleDefs\CN\=Level30\CN\=aasodrole1<\conflicting-role-0><conflicting-role-1>O\=system\CN\=driverset1\CN\=User Application

Driver\CN\=AppConfig\CN\=RoleConfig\CN\=RoleDefs\CN\=Level30\CN\=aasodrole2<\conflicting-role-1><\conflicting-roles><\sod>"}

Role Approval

(For Role-group, Role-Container and Role-Role assignments)

1. Enable approval when assigning a Role to Group or Container. (if configured)
2. Enable child roles approval process when we map a Role – Role. (if configured)
3. Approval information of role assignments to user/Role will be displayed in UI in permissions page and also in Role assignment page (in case of role-role mapping)
4. Audit information will contain the approval details.

Example: when a role is assigned to a group, RRSD will trigger audit event as “Implicit role to group Add”. This event will contain the approval information on how the group has got the role.

Role Approval

(For Role-group, Role-Container and Role-Role assignments)

- To configure Role approval setting: (In 4821, this setting was under settings -> Customization section)
 - Navigate to Configuration page -> Roles and Resources -> Expand Role Settings

Enable Role Approval

Role to Role

Role to Group

Role to Container

- Approval Info in UI:

The screenshot displays the NetIQ Identity Manager interface. On the left, the 'Permissions of other' section is visible, showing a search for 'brooks' and a result for 'Brooks kelly'. The main content area shows details for the role 'PWCCUSTOM'. The role description is 'PWCCustom', with an effective date of 'May 27, 2013 1:45 PM' and no expiration date. The reason for assignment is 'This role assigned to the user because of the role assignment to the group pwcGroup2'. The role is assigned via 'pwcgroup1'. Below this, a section titled 'View Role to Group Assignment information' shows the role was assigned via '-pwcGroup2'. The request was made by 'UserApplication Administrator' with the description 'Assign role to group'. The 'Approver details' section lists four approvers:

Approved by	
1	UserApplication Administrator approved, May 29, 2013 3:03 AM
2	Adams Mitchell approved, May 29, 2013 3:08 AM
3	Clark Robinson approved, May 29, 2013 3:13 AM
4	Davis Cooper approved, May 29, 2013 3:16 AM

Role Approval

(For Role-group, Role-Container and Role-Role assignments)

Sample CEF Audit event:

```
Jun 06 10:47:30 IdentityManager CEF:0|NetIQ|Identity Manager|4.8.2.0|31600|Role
Provisioning|1|cs1=Implicit Group Role Add msg=Requested by cn\=Role and Resource
driver,cn\=driverset1,o\=system; Target DN: cn\=cevans,o\=data; Source
DN:cn\=pwcrole1,cn\=Level30,cn\=RoleDefs,cn\=RoleConfig,cn\=AppConfig,cn\=User Application
Driver,cn\=driverset1,o\=system; Request DN:; Provisioning Category: Implicit Group Role Add; Correlation ID:
fname=cn\=pwcrole1,cn\=Level30,cn\=RoleDefs,cn\=RoleConfig,cn\=AppConfig,cn\=User Application
Driver,cn\=driverset1,o\=system rt=1370495850083 cs3=Set by the User Application on a newly created
nrfRequest object. cs4=NEW_REQUEST cs1Label=Request Category cs4Label=Original Request Status
dtz=Asia/Kolkata spriv=cn\=pwcrole1,cn\=Level30,cn\=RoleDefs,cn\=RoleConfig,cn\=AppConfig,cn\=User
Application Driver,cn\=driverset1,o\=system cs6Label=Request Object dvc=164.99.163.249
act=NEW_REQUEST suser=cn\=Role and Resource driver,cn\=driverset1,o\=system cs3Label=Request status
Description dvchost=sles12sp2-nijitha-163249
cat=DirXML\\\\Driver\\\\RoleProvisioning\\\\Role_Provisioning\\\\Add duser=cn\=cevans,o\=data
fileType=Role
cs6={"gid":"","Data": "<assignment><start_tm>20130606051730Z<\\start_tm><cause><group>cn\=finalchec
k,ou\=groups,o\=data<approval><start_tm>20130603205507Z<\\start_tm><process_id>281a55d2d6c34408
9a51223716dba3dd<\\process_id><activity>\\n<user>cn\=uaadmin,ou\=sa,o\=data<\\user>\\n<action>ap
proved<\\action>\\n<action_tm>20130603205543Z<\\action_tm>\\n<\\activity>\\n<end_tm>201306032
05544Z<\\end_tm><\\approval><req>cn\=uaadmin,ou\=sa,o\=data<\\req><req_desc>Assin<\\req_desc>
<\\group><\\cause><\\assignment>"}

```

Resource Weightage

Problem statement:

Assignment/Revocation of Role with entitlements mapped in User Application, results in error in the connected system.

Reason for error: Order of revocation of entitlements

Ex:- if user account is revoked first before group membership then revocation of group membership later will result in an error

Solution: Assign weightage to resources in User Application (Administration -> Resources page) and RRSD will take care of the order of Assignment/Revocation based on the weightage.

Weightage order: Values 100,200,300,400 & 500

- Assignment : 100 – Assigned first, 500 – Assigned last
- Revocation : 500 – revoked first ,100 – revoked last

By default, Resource weightage value will be set to empty implies that there is no weightage associated.

Scenario: Applicable when the entitlements are mapped to a single role with/without child roles.

Pre Requisites:

- eDirectory Schema update
- User application base package upgrade from 4.8 to 4.8.1
- Role and Resource driver update

RRSD Performance improvements

Problem statement:

When a child role is removed from a parent, the RRSD processes the event with a single thread and blocks all other events in the queue. When the parent has a lot of user assignments this will take a considerable time to complete as the recalculations for each user are done in series.

Solution:

Parallel processing of role recalculations on adding/removing a child role from parent role based on configuration.

RRSD Configuration:

“Enable Parallelization of role recalculation for users on add/remove of inherited role from parent role” – Boolean property is added as part of RRSD 483 package.

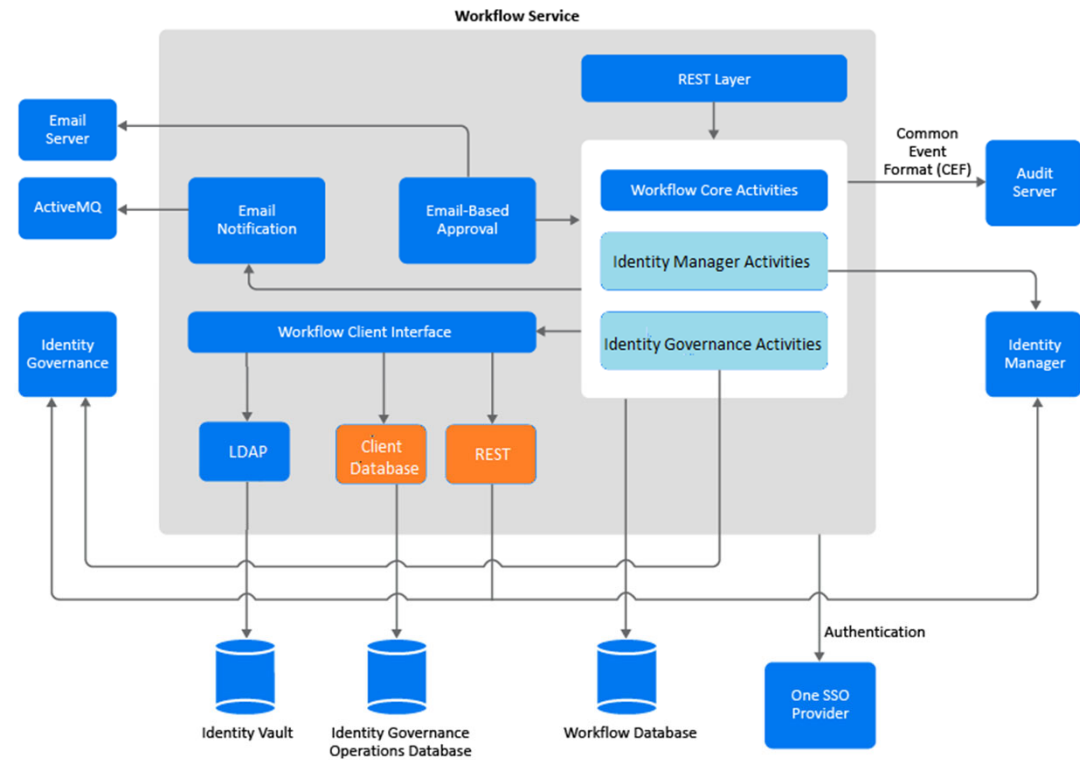
Setting the property to true, will ask for another configuration to specify the Number of threads to be used for Parallel processing ranging from 2 to 5. Based on this configuration, role recalculation process will be processed parallelly and decrease the time taken to process the role recalculations on removing or adding a child role to a parent role.

Note: Thread count can be considered based on the setup hardware specifications.



Demo

Workflow Service

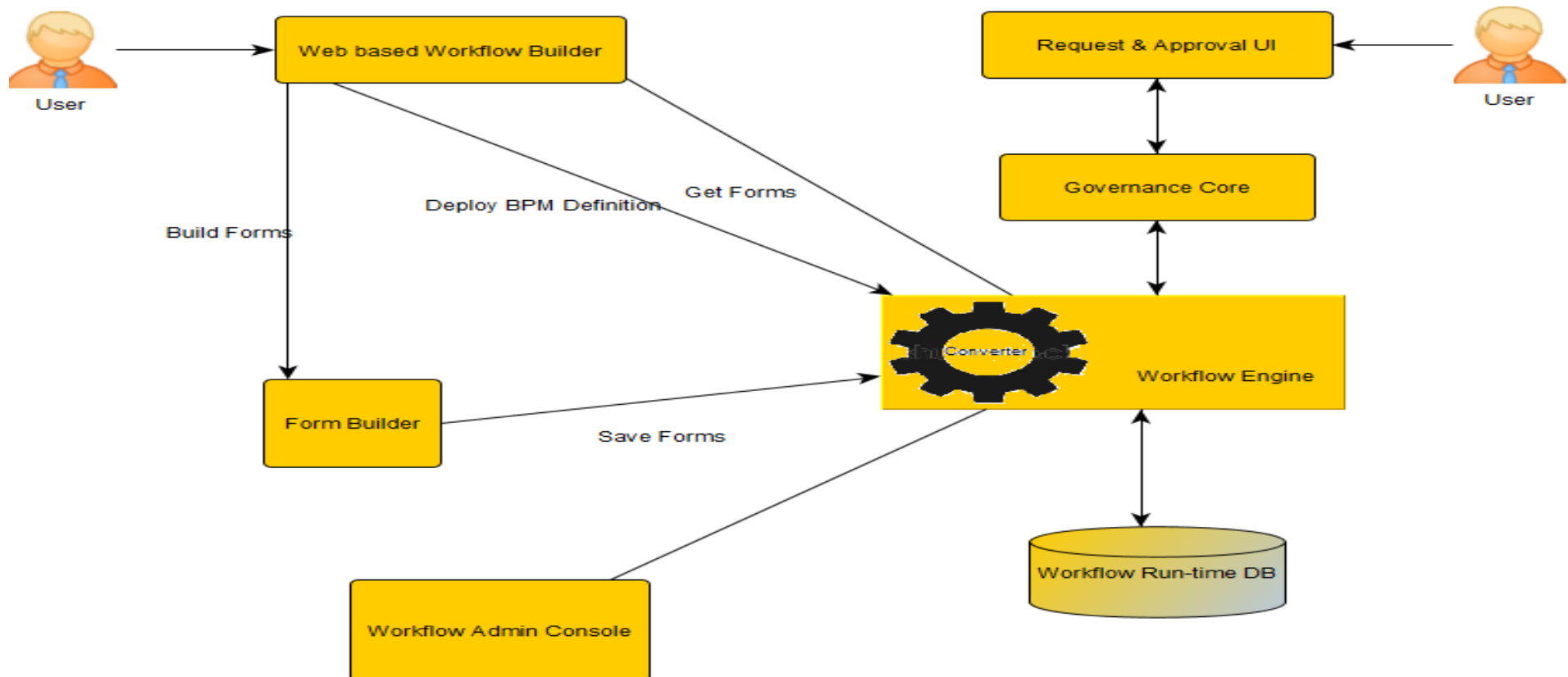


- Implements IGA vision
- Can be used by any products including IDI
- Improved IG – IDM Integration

Highlights

- Decoupled from Identity applications
- Own database
- RESTful Services
- OAuth based access
- Configuration
- Audit – CEF
- Workflow Definitions – IDV or Database
- Email Based Approval
- Identity Information – IDV or REST(IGA)
- Workflow Admin Console
- Web based workflow builder

Web based Workflow Builder





Form Service

- Form Renderer
- Form Builder



Questions?