



# ForgeRock

I<sup>3</sup> Open Platform  
“Securing your business”

Matthias Tristl

# Business Model

## ✓ Subscription

- Service Level Agreement
- Sustaining
- Research & Development

## ✓ Training

## ✓ Products

- OpenAM
- OpenDJ
- OpenIDM



# World Wide Coverage

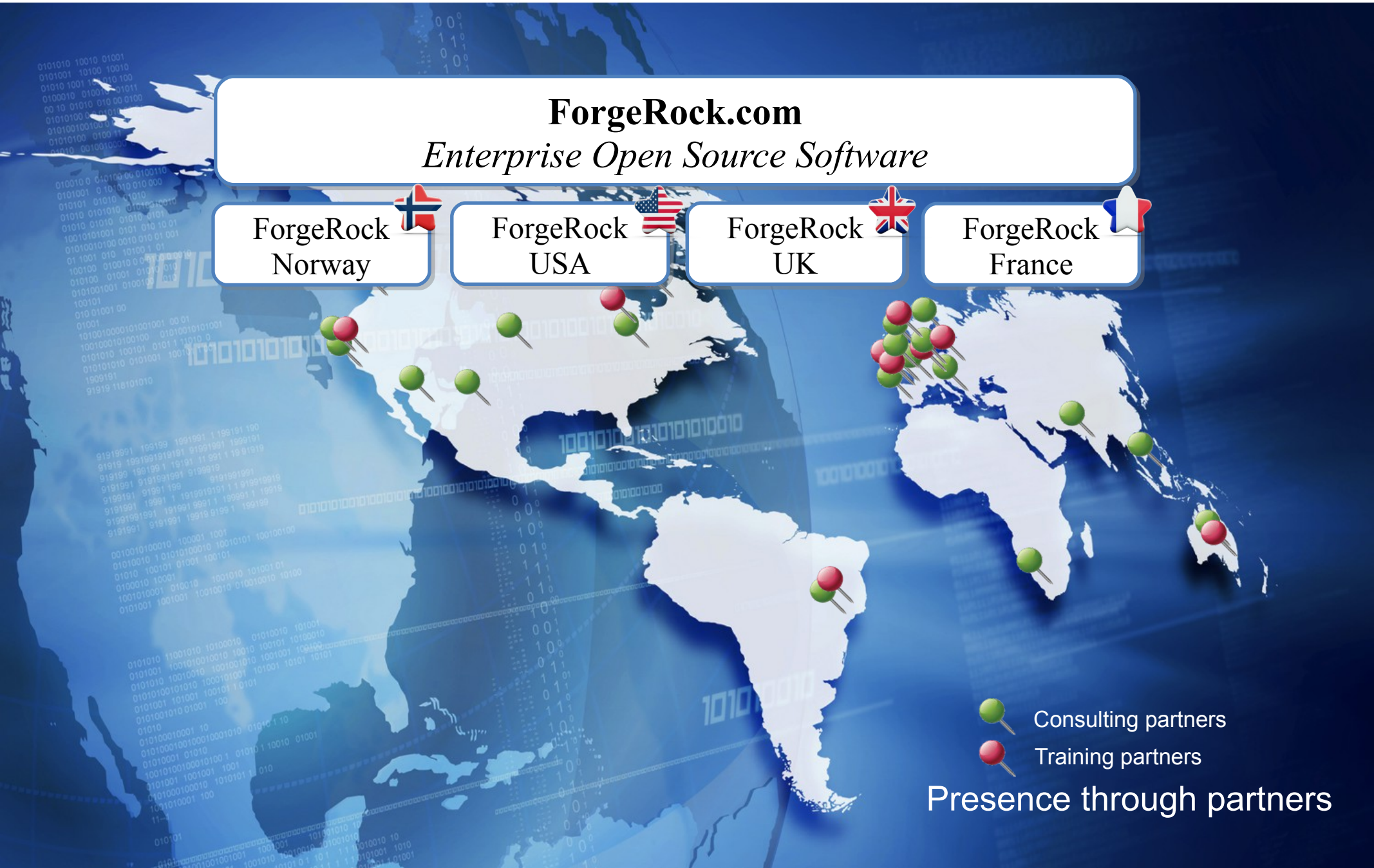
**ForgeRock.com**  
*Enterprise Open Source Software*



ForgeRock   
Norway

ForgeRock   
USA

ForgeRock   
UK

ForgeRock   
France



-  Consulting partners
-  Training partners

Presence through partners

---

**OpenIDM**   
Initiate - Validate - Perpetuate

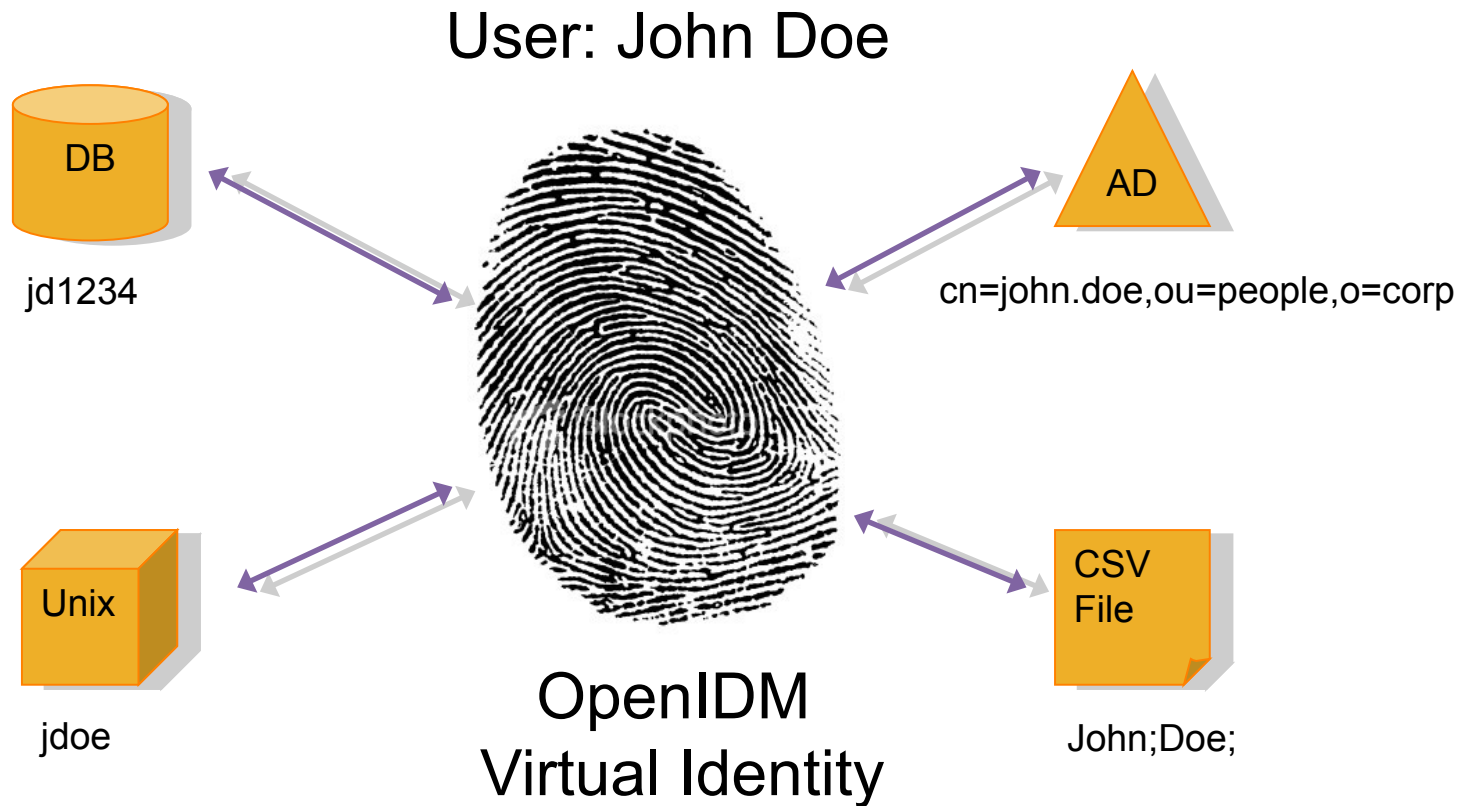
# The classics of IdM

---

- ✓ **Life cycle management of Identities...**
  - Joiners/Movers/Leavers –  
Onboarding/Offboarding
- ✓ **... and dealing with their physical and digital access and entitlements**
  - Provisioning and de-provisioning to systems
- ✓ **Keeping track of who did what, why and when?**
  - Reporting and Auditing



# Virtual Identity



# Typical Use-Cases

---

- ✓ HR (or authoritative source) driven provisioning
- ✓ Orphan accounts report (using external reporting engine) and cleansing
- ✓ Password Synchronization
- ✓ Synchronize identity data between resources.
- ✓ Basic CRUD via RESTful API for custom UIs.

# Basic Requirements

---

- ✓ **Lightweight**
  - JSON, small foot print, few dependencies
- ✓ **Developer friendly**
  - Consistent APIs, Favored components
- ✓ **Modular**
  - OSGi – Use and run only services needed.
- ✓ **Flexible**
  - Plenty of extension points and integration capabilities.



# Components

---

- OpenIDM
  - OSGi
  - JSON
- OpenICF
  - Framework
- Repository
  - Flexible
- Password Sync Plugins
  - Optional
- Activiti

# Advantages of OSGi

---

- ✓ **Dynamic Updates** - Bundles can be installed, started, stopped, updated, and uninstalled without bringing down the whole system.
- ✓ **Reduced Complexity**
  - The internal components are bundles, they hide their internals from other bundles and communicate through well defined *services*.
  - Hiding internals means more freedom to change later.
- ✓ **Simple, Small, Easy, Lazy, Versioning and Fast**
  - <http://www.osgi.org/About/WhyOSGi>

# OpenICF

---

- Based on Sun's connector project
- An independent project
- Can be seen as a unified interface to multiple (IDM-based) Resources
- Can be run built in into OpenIDM or as a separate process
- Expose capabilities to
  - Create, Update, Read, Delete
  - Search
  - Execute scripts

# Current Connectors

Active Directory (.net)	CA Unidesk (groupware)
Database Table (db)	XML File (file)
Scripted SQL (db)	CSV File (file)
DB2 (db)	Tivoli Access Manager (sso)
MySQL (db)	Solaris (os)
Oracle (db)	VMS (os)
MS SQL (db)	Oracle ERP (erp)
LDAP (ldap)	SalesForce.COM (cloud)
Exchange (.net)	
SPMLv2 (Webservices)	
RACF (mainframe)	
Web TimeSheet (cloud)	
Google Apps (cloud)	

# The Repository I

---

- Default (but currently not supported in production)
  - Orient DB
- JDBC (recommended)
  - MySql
  - DB2
  - Oracle
- LDAP (planned)

# The Repository II

---

- ✓ Identity Management related data is stored as Managed Objects.
- ✓ Managed objects are stored by OpenIDM in its data store.
- ✓ All managed objects are JSON-based data structures.
- ✓ System Accounts are stored as System Objects

# Password Management

---

- ✓ Capability to synchronize passwords to integrated resources
- ✓ Intercept password changes natively on OpenDJ and ActiveDirectory via plug-ins.
- ✓ Supports password changes and resets according to password policy.



# Outbound Services

---

- ✓ Outbound Integration
  - Email Notifications
  - REST calls
- ✓ Information can be routed to any type of store (CSV, RDBMS, web services etc)
- ✓ Reporting Engines and Business Intelligence solutions can provide reports – OpenIDM provides the data.
- ✓ Fully configurable format on what to publish and when



# Inbound Service: REST

---

- Authentication
- Authorization
- Repository Objects
- Resource Objects
- Commands

# REST Examples

## GET

```
curl -u user:password -X GET "http://localhost:8080/openidm/managed/user/jdoe"
```

## GET

```
curl -u user:password -X GET "http://localhost:8080/openidm/system/myDB/accounts/joey"
```

## PUT

```
-X PUT -d '{"lastname":"Berg", "firstname":"James", "password":"asdfkj23"}' "http://.../user/ddoe"
```

## POST

```
-X POST "http://localhost:8080/openidm/sync?_action=recon&mapping=SystemAdAcc_MU"
```

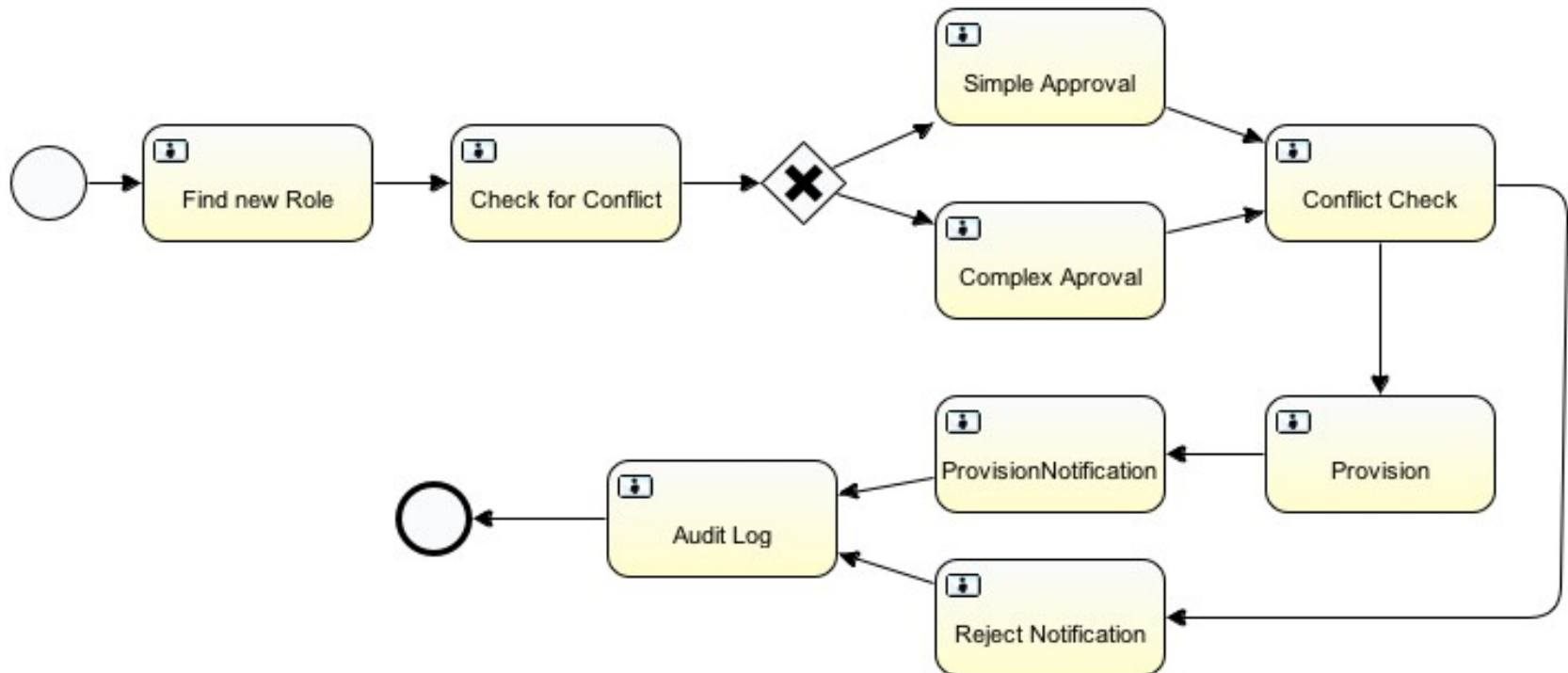
# Business Logic and Rules

---

- ✓ By design pluggable to enable various languages such as Groovy, Ruby, JavaScript, Python etc
- ✓ Call outs to Java methods or REST web services.
- ✓ Built in Workflow Engine: Activiti
- ✓ Object Router

# Activiti

- Full Java and Scripting integration
- Full BPMN integration
- XML based

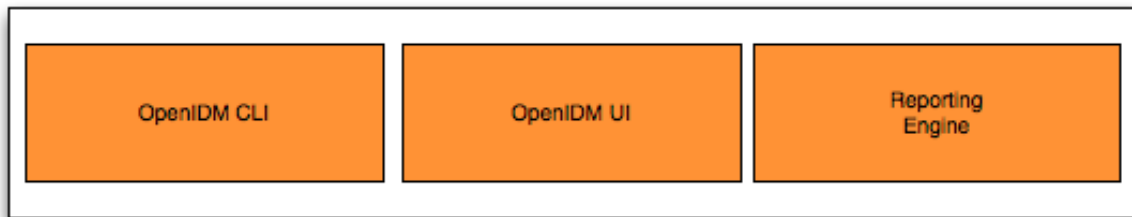


# Scheduler

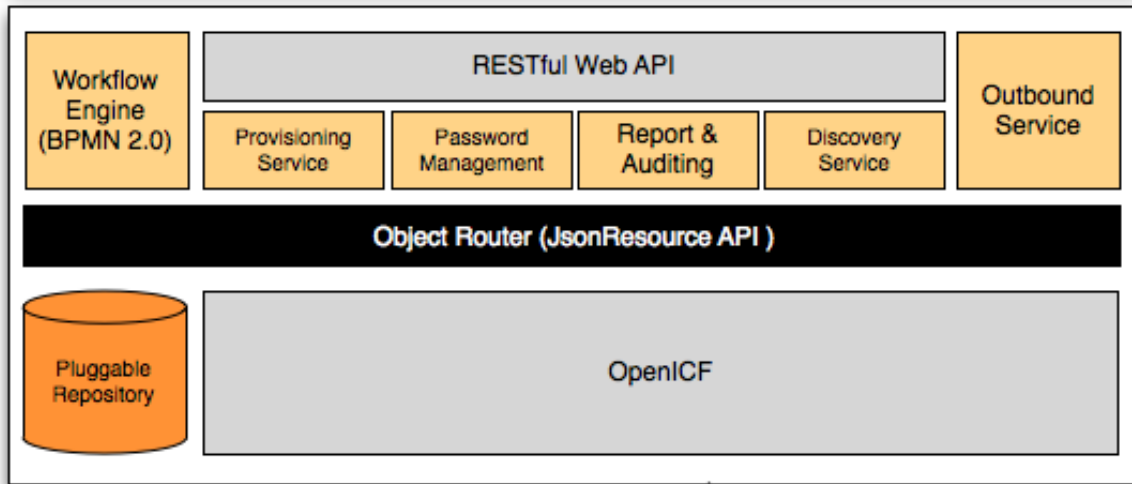
```
{ "enabled"      : true,  
  "type"        : "cron",  
  "startTime"   : "(optional) time",  
  "endTime"     : "(optional) time",  
  "schedule"    : "cron expression",  
  "timeZone"    : "(optional) time zone",  
  "invokeService" : "service identifier",  
  "invokeContext" : "service specific context info" }
```

```
{ "enabled": false,  
  "type": "cron",  
  "schedule": "0 0/30 * * * ?",  
  "invokeService": "sync",  
  "invokeContext": {  
    "action": "reconcile",  
    "mapping": "systemLdapAccounts_managedUser" }} }
```

# Architecture Summary



External Services



OSGi Core Services





# Configurations: sync.json

```
"mappings" : [{  
  "name" : "systemHrAccounts_managedUser",  
    "source" : "system/HR/account",  
    "target" : "managed/user",  
  "properties" : [ {  
    "source" : "employeeNumber",  
    "target" : "employeeNumber"},...  
  "correlationQuery" : {  
    "type" : "text/javascript",  
    "file" : "script/ldapBackCorrelationQuery.js"},...  
  "policies" : [{  
    "situation" : "ABSENT",  
    "action" : "CREATE"...  
  "onCreate" : {  
    "type" : "text/javascript",  
    "source" : "target.dn = 'uid=' + source.userName + ',ou=People,dc=example,dc=com';"},...  
}
```

# Configurations: Provisioner

## Connector Server

```
"connectorHostRef" : "dotnet",
```

## External Connection

```
"configurationProperties" :  
"DirectoryAdminName" : "EXAMPLE\Administrator",  
"LDAPHostName" : "127.0.0.1",
```

## Objectclass Attribute Mapping

```
"account" :  
  "nativeType" : "__ACCOUNT__",  
  "mail" : { "type" : "string",  
            "nativeName" : "mail",  
            "nativeType" : "string"
```

# Configurations: Router Service

- Interface to all objects in OpenIDM:
  - managed objects, system objects, configuration objects...

```
{ "filters": [  
    filter object,  
    ... ]}
```

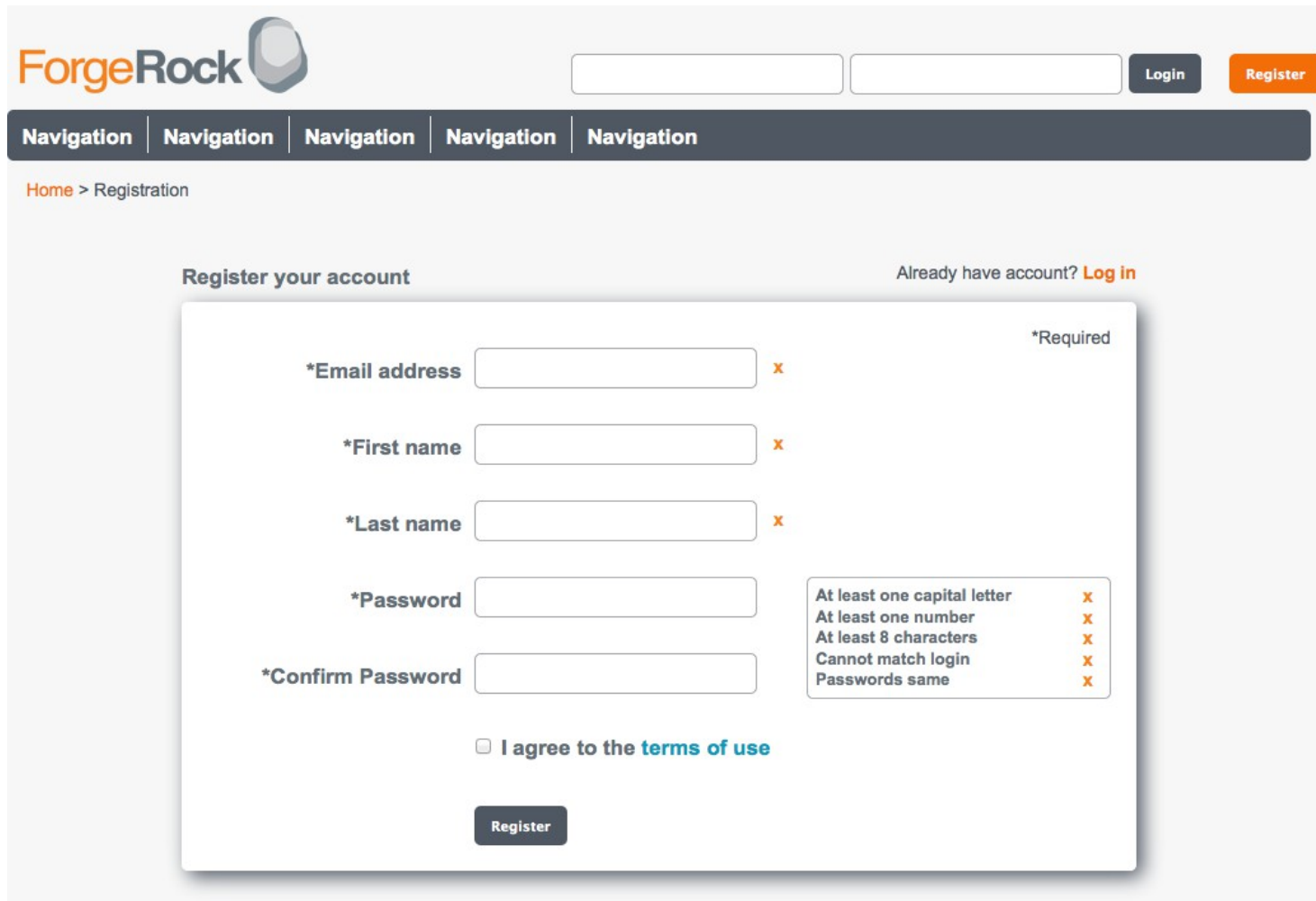
```
{  
  "pattern": string,           "^managed/user/.*"  
  "methods": [ string, ... ], "create", "update"  
  "condition": script object, true  
  "onRequest": script object, "java.lang.System.out.println('Hallo!');"  
  "onResponse": script object, "java.lang.System.out.println('Hallo back!');"  
  "onFailure": script object  "java.lang.System.out.println('Hallo back!');"  
}
```


# Functional Overview

---

- ✓ Workflow and Business Process support
- ✓ Audit & Event publisher
  - Provides logging capabilities that external reporting engine can leverage.
- ✓ Provisioner Service
  - Exposes CRUD capabilities via REST.
- ✓ Discovery Service
  - Provides Reconciliation and Synchronization
- ✓ Outbound Service
  - Email notifications
  - Outbound REST

# Self-Service Registration





[Navigation](#) | [Navigation](#) | [Navigation](#) | [Navigation](#) | [Navigation](#)

[Home](#) > Registration

**Register your account**
Already have account? [Log in](#)

\*Required

\*Email address  x

\*First name  x

\*Last name  x

\*Password 

At least one capital letter x  
 At least one number x  
 At least 8 characters x  
 Cannot match login x  
 Passwords same x

\*Confirm Password

I agree to the [terms of use](#)

Besten Dank!

[matthias.tristl@forgerock.com](mailto:matthias.tristl@forgerock.com)