



**2nd Annual
MidPoint Community Meetup
Application Onboarding**

Evolveum



Funded by the
European Union
NextGenerationEU

**[RECOVERY
AND RESILIENCE]
PLAN**

Pavol Mederly, May 2026
Interim Chief Product Officer

80%

80%

of cyberattacks are identity-related

The Bottlenecks in IGA



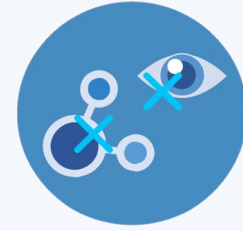
**100s to 1000s
applications**

shadow IT



**Manual and slow
app onboarding**

coverage often
only 10-30%



**Unconnected
applications**

no visibility,
no automation,
no compliance

Application Onboarding Challenges

1

Discovery

find the app

2

**Technical
connection**

make the app talk to
the IGA engine

3

**Data
connection**

make sense of the
data

4

**Roles and
policies**

fully govern the
application

Application Onboarding Challenges

1

Discovery

- reviewing documents
- interviewing stakeholders
- querying CMDB
- tracking IT expenses
- examining SSO and SSE platforms
- OAuth registrations and API token usage
- network traffic
- cloud control plane
- browser telemetry

Application Onboarding Challenges

2

Technical connection

- SCIM
- REST
- database
- CSV files
- LDAP
- SDKs
- cloud APIs
- messaging
- connector catalogs
- integration templates
- low-code approach
- wizards
- SCIM-first
- OpenAPI introspection
- generative AI

Application Onboarding Challenges

3

Data connection

- object classification
- identities correlation
- attribute mapping
- different kinds of objects
- integration templates
- questionnaires, guidelines
- wizards
- rules/patterns
- machine learning
- heuristics
- AI

Application Onboarding Challenges

4

Roles and policies

- roles
- classification
- approvals
- SoD
- owner
- manager
- templates
- guidelines
- methodologies

Application Onboarding Challenges

1

Discovery

find the app

2

Technical connection

make the app talk to the IGA engine

3

Data connection

make sense of the data

4

Roles and policies

fully govern the application

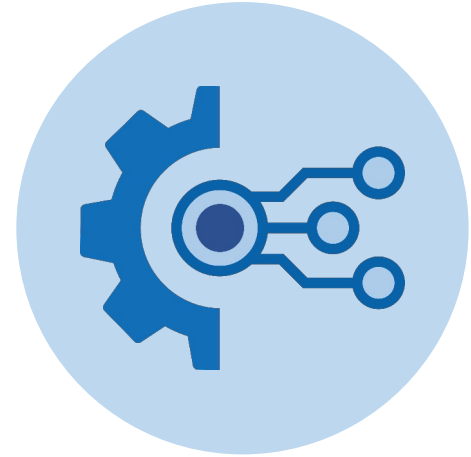
midPilot

Main Components

- Technical connection: **Smart connector wizard**
 - today 13:00 – 14:40
- Data connection: **Smart resource wizard**
 - today 11:00 – 11:15
- **Integration catalog**
 - today 10:05 – 10:30

Smart Connector Wizard

- Supporting **REST**, **SCIM** and **database** connector creation
- **Configuration** instead of writing code (no code / low code)
- Supported by **AI** in a **safe** way
 - small amount of code, always human-reviewed before execution
 - not a vibe coding!
- Easy **development, review, maintenance**
 - even for **less technically experienced** people
- Uses the **documentation** for the system being connected
 - we can extend it to using data later



[☰ Summary](#)[⋮ Basic settings](#)

Application identification

In progress

Identify the Target Application

Tell us which application you want to connect to. Based on this information, midPoint will identify the target system and locate the appropriate documentation to prepare everything needed for connector generation.

Application name * [i](#)

OpenProject

A Z

**Description** [i](#)**Version of application** [i](#)**Integration type *** [i](#)

Rest

**Deployment type** [i](#)

Undefined



Entering basic information about the application being connected

[Next →](#)

☰ Summary

⚙ Basic settings

Application identification

Complete

Documentation

In progress

Provide Integration Documentation

Documentation helps the AI understand how your system communicates, which endpoints it exposes, and what data structures it uses. By analyzing this information, the AI can generate a more accurate and tailored connector for your integration.

🔗 Documentation found AI has found matching documentation or configurations. Please review them to ensure they fit your needs.

▾

+ Add URL 📁 Upload file + Create new

API documentation 🔗 AI

Please note that we intend to keep this specification as accurate and stable as possible, however work on the API is still ongoing and not all resources and actions in OpenProject are yet accessible through the API. This document will be subject to changes as we add more endpoints and functionality ... 👁 🗑

<https://www.openproject.org/docs/api/>

OpenProject OpenAPI specification 🔗 AI

OpenAPI specification 👁 🗑

<https://www.openproject.org/docs/api/v3/spec.yml>

Approving or augmenting the documentation found by the wizard

Next →

☰ Summary

Basic settings

Complete

Connection

Complete

Object class

Complete

Object class

Object classes

In progress

Select Object Class to Be Configured

The midPilot analyzed your documentation and found object classes that might be available for integration. Select one to begin its configuration.

Not seeing what you expected?

Try checking the list of other object classes using the 'More classes' button.

Recommended Object Classes

More classes

User

- Represents an individual who can interact with the system...

Group

- Represents a group of users that can be used for...

Role

- Role represents a set of permissions that can be...

Membership

- Represents the association between a principal (user o...

Principal

- Generic representation of an identity that can be a user,...

Workspace

- Workspace is a container for resources and users with...

Project

- A workspace that contains work packages, wikis, and...

Program

- Represents a program, a container grouping projects...

Portfolio

- A workspace that groups projects, work packages, an...

Selecting what objects should the connector support

Next →

☰ Summary

Basic settings
Complete

Connection
Complete

Object class: User
Complete

🔄 Object class: User
Object classes
Complete
Schema scripts validation
Complete
Schema validation
In progress

Review Schema Attributes

View the object schema attributes which were extracted from the schema script. Check if everything matches your expectations.

Search

☰ Items 15

☰ Definition settings

Display name ⓘ × Name ⓘ × More... ▾ 🔍 Basic ▾

Name * ⓘ	Type * ⓘ	Display name ⓘ	Order ⓘ	Required ⓘ	Multivalue ⓘ	Indexed
language	String		120	False	False	
updatedAt	Date time		130	False	False	
firstName	String		140	False	False	
email	String		150	False	False	
identity_url	String		160	False	False	
name	String		170	False	False	
	String		180	False	False	
	String		190	True	False	

Validating that the wizard correctly understood the schema from the documentation

☰ Summary

Basic settings

Complete

Connection

Complete

Object class: User

Complete

🔄 Object class: User

Object classes

Complete

Schema scripts validation

Complete

Schema validation

Complete

Search endpoints

Search All Script Validation

This step validates the Search All script to ensure it correctly retrieves and processes all available objects from the target system.

```
1 objectClass("User") {
2     search {
3         endpoint("/users") { // List endpoint as defined in extracted_endpoints
4             objectExtractor {
5                 // Extract the list of User objects from the HAL+JSON response
6                 return response.body().get("_embedded")?.get("elements")
7             }
8         }
9         pagingSupport {
10            // Pagination parameters as defined by the API
11            request.queryParameter("size", paging.pageSize)
12            .queryParameter("offset", paging.pageOffset)
13        }
14    }
15 }
```

🔄 Regenerate

✓ Yes, this script is correct

The code that will retrieve all users generated by the wizard

Search all script validation

Summary

Basic settings

Complete

Connection

Complete

Object classes

Complete

Object class: User

Object classes

Complete

Schema scripts validation

Complete

Schema validation

Complete

Search endpoints

Connector summary

Connector readiness

Essential requirements for a functional connector

1 step to Read-only

Basic information Configure

OpenProject

Version	1.1
Integration type	Rest
Deployment type	Unknown

Connection Configure

Connected

BaseUrl	http://localhost:8888/ap...
Test endpoint	my_preferences
Auth method	Basic auth

Documentation Configure

Good coverage

Files	Links
0	6

Object classes

1

View all object classes

Relationships

0

View all relationships

Connector actions

Create resource

Upload connector

Uploading the prepared connector, adding its JAR file...

Add new object class

Start configuration for a different object class which...

Add relationship

Set up relation between object classes which is useful for...

Displaying current state of the connector, suggesting next actions

Smart Resource Wizard

- Supporting creation of resource definition for **any** connector
 - object **classification** ~ definition of object types
 - object **correlation** ~ matching object identity
 - object **mapping** ~ matching & mapping object attributes
 - **synchronization** rules
- Supported by **AI + heuristics** in a **safe** way
 - safe expression language, so the human review is optional
 - small amount of code
- Uses the **schema** and the **data** of the system (and midPoint)
 - documentation is used indirectly (via the schema); may be changed later



Administrator Accounts

Administrative accounts residing under the administrators OU.

Show filter  

Kind: account

Intent: admin

Object class: inetOrgPerson

Focus type: UserType

Service Accounts

Service accounts residing under the service-accounts OU.

Show filter  

Kind: account

Intent: service

Object class: inetOrgPerson

Focus type: UserType

Employee Accounts

Employee accounts within the users OU that have an employee number.

Hide filter  

Kind: account

Intent: employee

Object class: inetOrgPerson

Focus type: UserType

Filter:

c:attributes/ri:employeeNumber exists

 AI

Base context filter:

c:attributes/ri:dn = "ou=users,dc=example,dc=com"


 AI

Base context object class:

organizationalUnit

Suggested classification of LDAP objects



 Suggestion



Name correlator

Suggested based on matching of attributes/empnum to name

 name (Exact)

Stats


1.0
Weight

1
Tier

93.0
Efficiency


Actions

 Discard

 Accept

 View rule




 Suggestion



PersonalNumber correlator

Suggested based on matching of attributes/empnum to personalNumber

 personalNumber (Exact)

Stats


1.0
Weight

1
Tier

93.0
Efficiency

Actions

 Discard

 Accept

 View rule

Suggested correlation rules

✂ Suggestions generated

7 suggestions have been generated. Review and apply them.

↻ Re-generate

Last run: May 6, 2026, 7:11:43 PM • Elapsed time: 2m 0s

→ Inbound mappings (to MidPoint)

↔ Outbound mappings (to Resource)

ON ✂ Suggestions Enabled

Legend: ● Purple = AI-powered suggestions ● Blue = System suggestions

+ Add inbound

All mappings ▾

🔍 Search

<input type="checkbox"/>	Name ⓘ	Resource attribute * ⓘ	Expression ⓘ	MidPoint property ⓘ	Lifecycle state ⓘ	...
<input type="checkbox"/>	↻ ● initials-into-additionalName	initials	As is	additionalName		✓ Accept ✗ Discard ...
<input type="checkbox"/>	↻ ● sn-into-familyName	sn	As is	familyName		✓ Accept ✗ Discard ...
<input type="checkbox"/>	^ Mapping suggestions 2 for: fullName			fullName		✓ Accept selected ...
<input checked="" type="radio"/>	↻ ● cn-into-fullName	cn	As is	fullName		...
<input type="radio"/>	↻ ● displayName-into-fullName	displayName	As is	fullName		...
ⓘ Only one suggestion per fullName can be applied. Others will be discarded upon accepting.						
<input type="checkbox"/>	↻ ● givenName-into-givenName	givenName	As is	givenName		✓ Accept ✗ Discard ...
<input type="checkbox"/>	↻ ● l-into-locality	l	As is	locality		
<input type="checkbox"/>	↻ ● title-into-title	title	Script	title		

Suggested attribute mappings

Deployment Options

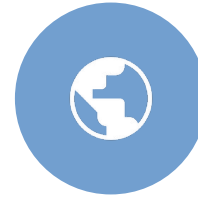
All components are **open source**, therefore you can utilize:



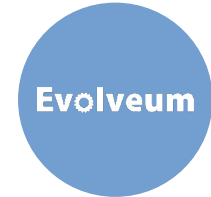
self-hosted
solution



existing
cloud services



public
AI services



Evolveum
AI services

Balancing **privacy, cost, and performance.**

More information: **MidPilot – A Look Behind the Curtain**
tomorrow, 01:00 – 02:40

Beyond 4.11 – Guided Top-Down Approach

- MidPoint is extremely powerful since day one
 - **make common things easy** – and all things possible
- In the 2010s
 - **easy** meant **XML** with **simple Groovy scripting**
 - **possible** meant **heavy Groovy scripting** (to up clockwork hooks)
- Now
 - **easy** means **GUI**
 - **possible** means **XML** with some **Groovy/MEL scripting**
 - the user is guided by the methodology (out-of-band)
- In the future
 - **easy** will mean **GUI navigating the user** according to the **methodology**



Top-Down: Applications, Resources, Connectors

- Originally there were **connectors** and **resources**
- Now we have **connectors**, **resources**, and **applications**
 - “First steps” methodology starts with resources
 - “IGA” methodology (being prepared) will deal with applications
- We contemplate **integrated top-down** approach
 - starting with the **concept of application** (not necessarily connected!), optionally defining owner, manager, initial role structure, basic policies, ...
 - then we can **connect the application** using either existing resource (like LDAP) or a dedicated one, using standard or custom connector
 - the solution can be **gradually improved**, like
 - accounts → entitlements and/or organizational structure
 - read-only with ITSM → full automation
 - optionally changing the resource/connector as needed
 - guided by the **methodology**





Google Workspace

Google Workspace integration for provisioning and managing users

Status	✓ Active
Version	1.0.0.1.93
Owner	JD John Doe
Manager	JS Jason Smith

Lifecycle state

Active

Overview

Basic

Objects

Application roles

Approvals

Certification

Segregation of duties

Configuration

Setup assistant



Recommended setup complete (100%)

All recommended configuration steps have been completed

[Review checklist](#)

Connected resource

1 resource



Google Workspace

Version 3.8.1

Operational

Connector

Google Workspace Admin SDK

Version

1.0.0

Configured capabilities

ACTIVATION ACTIVATION STATUS CREATE READ UPDATE DELETE TEST CONNECTION
SCRIPT LIVE SYNC

Governance definitions



Approvals

2 approval policies active



Certification

1 review scheduled



Segregation of Duties

No SoD constraints defined



Users with access

342

[View all](#)

Application roles

12

[View all](#)

Privileged roles

3

[View all](#)

Compliance violations

2 violations

[View all](#)



Google Workspace

Google Admin SDK resource

Status Up

Ability Read-Write

Connector Google Admin SDK

Object types 3

Lifecycle state

Active

Overview

- Basic
- Objects <
- Schema handling <
- Configuration <

Setup assistant

Recommended setup complete (100%)
All recommended configuration steps have been completed

[Review checklist](#)

Accounts

1342

[View all](#)

Groups

52

[View all](#)

Roles

34

[View all](#)

Connector



Google Workspace Admin SDK

Version 1.0.0

Operational

Author

Evolveum

Configured capabilities

ACTIVATION ACTIVATION STATUS CREATE READ UPDATE DELETE TEST CONNECTION
SCRIPT LIVE SYNC

Mappings

Configured

12

Inbound

8

Outbound

4

Overrides

[View all](#)

Schema

Configured

3

Object types

47

Attributes

1

Association types

[View all](#)

Correlation

Configured

3

Rules

94.2%
Match rate

18

Unmatched accounts

[View all](#)

Synchronization

Live sync

Sync reactions

6

Last run

24-02-2025 07:00:00

Processed objects

1,247

Errors

0

[View all](#)

Account Breakdown

1,342 total

Linked

1280

Unmatched

44

Disputed

8

Unlinked

10

Protected

12

[View all](#)



2nd Annual
MidPoint Community Meetup

What about the discovery?

- We think about **connectors** for
 - **CMDB** systems like ServiceNow, Device42, etc.
 - **SSO** (Single Sign On) platforms like Keycloak, CAS, etc.
 - **SSE** (Security Service Edge) platforms like Netskope, Zscaler, etc.
 - **Cloud inventories** like AWS Config, Azure Resource Graph, etc.
- Connectors can be
 - **ConnId**, where applicable
 - **custom ones**, like for event gathering
 - or implementing **SSF** (Shared Signal Framework) receiver



Summary

- Effective application onboarding is key to IGA success
- MidPoint has a lot of offer here
- **Tell us what you need**



Evolveum

Thank you for your attention

Feel free to ask your questions now!



Funded by the
European Union
NextGenerationEU

**RECOVERY
AND RESILIENCE
PLAN**



2nd Annual
MidPoint Community Meetup