



2nd Annual MidPoint Community Meetup

Updated MidPoint Deployment Methodology

Evolveum



Funded by the
European Union
NextGenerationEU

**[RECOVERY
AND RESILIENCE]
PLAN**

Ivan Noris, May 2026
Expert Identity Engineer

Agenda

- Identity security challenges
- MidPoint deployment methodology
 - For newcomers: Introduction and purpose
 - For veterans: Updates and changes since last year
- Conclusion



When In Doubt... Just Listen

- Some slides are “text-heavy” (for your post-MCM reference)
- No need to read ahead. I’ll read everything... except the images :-)
- Just sit and enjoy the show

This is not “déjà vu”!
If you attended *Workshop: AI Assisted Integration of First Systems with MidPoint*,
you *will* recognize some parts.



Identity Security Challenges Without A Complete IGA Solution

“

True wisdom is knowing
what you don't know.

”

Confucius

Identity Security Challenges Without A Complete IGA Solution

- “Everyone has *some* identity management or IGA solution” (the devil is in the details)
- Usually, IDM/IGA is *partially* automated for *some* target systems
 - No overall visibility of accesses
 - Identity data quality is low; mistakes in data and accesses
 - Orphaned accounts may exist
 - Manual provisioning takes long time
- Home-grown or unsupported solution
 - Usually more IDM than IGA
 - Relying on specific experts' knowledge

“

**True wisdom is knowing
what you don't know.**

”

Confucius

MidPoint Deployment Challenges Without A Proper Plan

“

By failing to prepare,
you are preparing to fail.

”

B. Franklin

MidPoint Deployment Challenges Without A Proper Plan

- “How do we replace our current solution with midPoint?
Can we replace it in a single day? Can we just ‘turn it *on*’?
Business must continue!”
 - Very important consideration, stay tuned!
- Proceeding without a plan *now* may cause significant problems *later*
 - Are you brave enough to make mistakes?

“

**By failing to prepare,
you are preparing to fail.**

”

B. Franklin

Motivation: Why Methodology?

- **Full disclosure:** *this is not the only way of deploying midPoint, but it is the best to start with*
- **Guided approach:** explanation of goals and steps to achieve them
- **Iterative approach:** small steps that deliver the value early on and further refine the solution towards your goal
- We call this methodology “First Steps”
- **Please note:** midPoint 4.11 is a work in progress



First Steps Methodology

“

The journey of a thousand miles
begins with one step.

”

Lao Tzu

First Steps Methodology

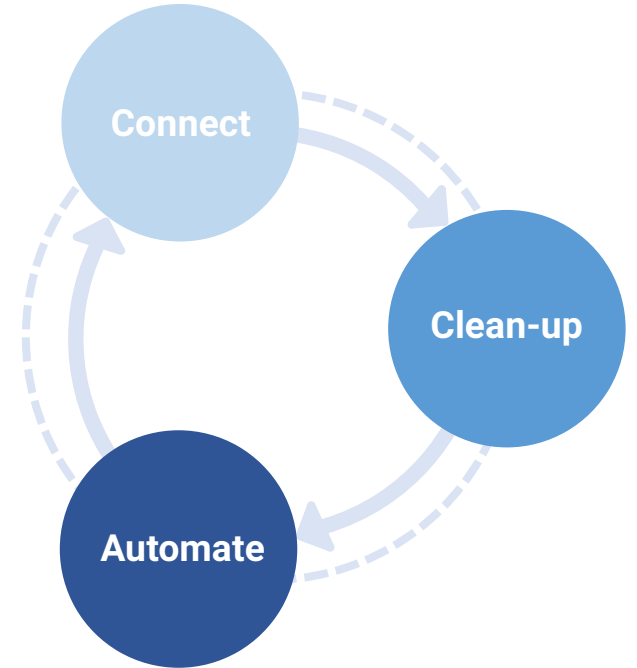
- *Iterative* identity management program (Est. 2023)
- Guides you through the quick midPoint deployment in three steps
- **Connect, Clean-up, Automate**
- Docs: [First Steps Methodology](#) (expect updates for midPoint 4.11)

“ **The journey of a thousand miles
begins with one step.** ”

Lao Tzu

First Steps Methodology (2)

- **Connect:** Connect new system(s) to the solution. Read/analyze data
- **Clean-up:** Improve data quality. Correlate, resolve orphaned accounts, identify data errors
- **Automate:** Speed up the processes, improve the efficiency. On-boarding, data updates, off-boarding (JML – Joiners, Movers, Leavers)



How First Steps Methodology Works

- **Goal: start using midPoint** in your organization by connecting your first source and target systems
- **Simple** – GUI wizards, no XML
- **Safe** – prevents unexpected changes or deletions of existing data by using simulations and marks (exceptions)
- Increases **confidence** even with low-quality data
- **Configuration assistants (AI/heuristics)** – enable administrators to focus on data and business requirements rather than midPoint internals
- **MidPilot**: AI-powered assistant designed to accelerate application onboarding into midPoint (generate connector code, recommend attribute mappings and correlations, and more)

NEW | MIDPILOT



How First Steps Methodology Works (2)

- **Complete** – applies to accounts and entitlements alike
- **Flexible** – enables variability in the time and scope of the integration, e.g. multiple account/group/membership types; migrated gradually or at once
 - We will not cover groups/memberships in this presentation
- **Connector-agnostic** – connect systems using built-in or non-built-in connectors
- All the time, it is still: **Connect, clean-up, automate**



First Steps Methodology Overview

1 Plan Your Deployment

Identify data sources, targets, plan resources, timing and money

2 Connect The First Source System (HR)

Connect HR system and preview data

3 Import Source Data

Import data from HR system, create users in midPoint

4 Connect the First Target System

Connect the most important target system and preview data

5 Target System Integration

Correlate existing accounts to midPoint users

6 (Opt.) Import Usernames from Target System

Import usernames from the first target system to midPoint

7 Enable Provisioning to Target System

Configure Target for provisioning from midPoint, first with simulation

8 Automate Integration

Automate Source→Target account provisioning (JML)

9 Override Incorrect Data

Make sure we can override incorrect data from HR if needed

First Steps Methodology Overview

“

Motivational quotes
wear out without screenshots.

”

Ivan Noris

1. Plan Your Deployment (Kick-off)

- Gather people in your organization interested in IGA (Senior IT engineer/architect, administrators of critical IT systems, HR, security professional)
- Think in iterations
- Identify data sources and the most important targets
- Discuss security (requirements & wishes, do not overdo it)
- Discuss resources, timing, and rough plan
- Get a green light from your management



1. Plan Your Deployment (Kick-off) – Identify Source and Target Systems

Source system: HRIS export (CSV); employees + contractors (emptype)
ID: empnum (employee number)

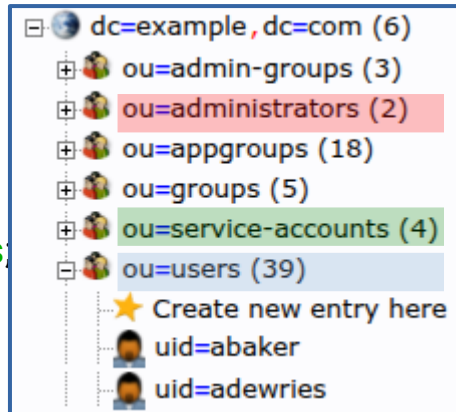
| empnum | firstname | surname | emptype | job | status | locality |
|--------|-----------|-----------|------------|---------------------------------------|-----------------|---------------------|
| 1001 | Geena | Green | FTE | 124#CEO | Active | Hot Lava City |
| 1002 | Ana | Lopez | FTE | 125#CFO | Active | Hot Lava City |
| 1003 | Jimmy | Taylor | FTE | 107#Junior Consultant | Former employee | Small Red Rock City |
| 1004 | Peter | Hunter | FTE | 910#HR Consultant | Active | White Stone City |
| 1016 | Jane | Anderson | FTE | 107#Junior Consultant | Long-term leave | Hot Lava City |
| 8000 | Janet | Garner | CONTRACTOR | 899#Cleaning & Maintenance Specialist | Active | Hot Lava City |
| 8001 | Ben | Goosehead | CONTRACTOR | 899#Cleaning & Maintenance Specialist | Active | Hot Lava City |
| 8002 | María | Alvarez | CONTRACTOR | 899#Cleaning & Maintenance Specialist | Active | Small Red Rock City |

Fixed set

Prefix

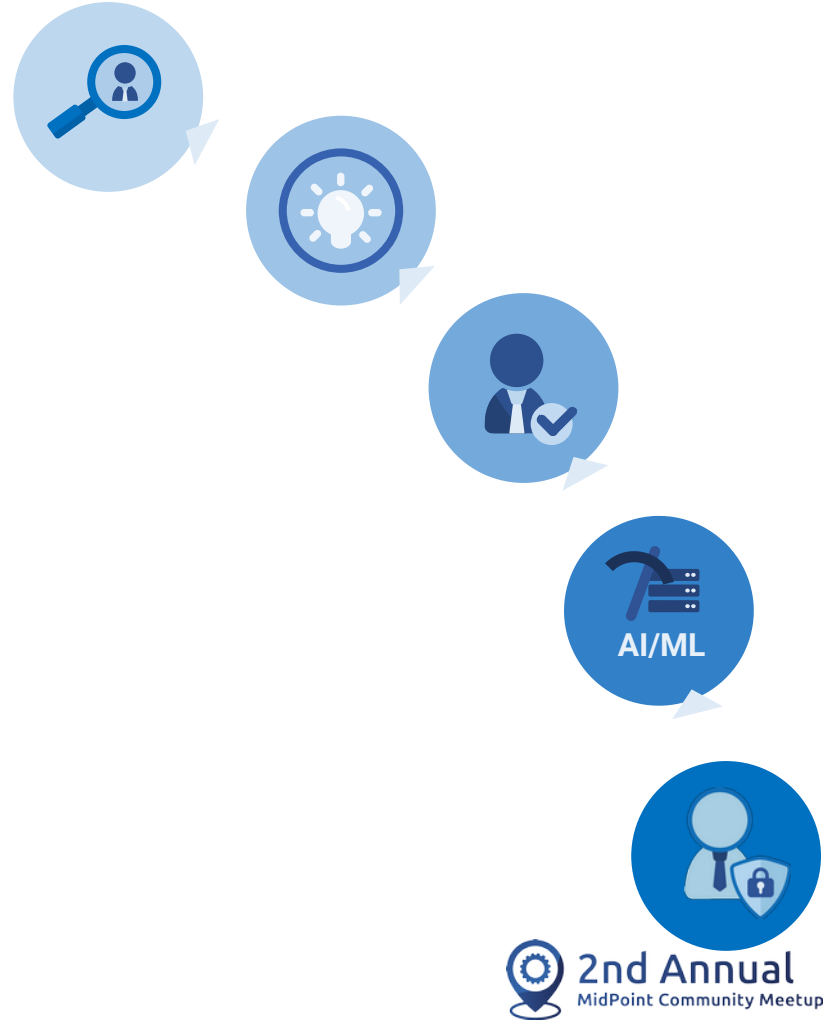
Fixed set

Target system: corporate directory server (LDAP);
standard accounts + admin accounts + service accounts;
internal groups + application groups + admin groups
Account ID: uid



2. Connect the First Source System (HR)

- Connect Source system using a CSV file and preview resource data
- Classify data from resource object classes into object types
- Configure object types
- **Use a series of wizards and configuration assistants**



2. Connect the First Source System (HR) – Create Resource

New resource

Home > All resources > New resource

Create new resource

A resource represents an external source or target system which midPoint manages, e.g., an LDAP directory, database, or application. Through resources, midPoint can read, create, modify, and disable accounts and other objects. [More details](#)

From Scratch **Inherit Template** **Copy From Template** **NEW | MIDPILOT**

Help ×

To speed up configuration and ensure consistency, you can base your resource on an existing resource template.

With "Inherit Template", the resource stays linked to the template. Future template changes will also apply to this resource.

With "Copy From Template", the template is used only as a starting point. After creation, the resource is independent.

For more information, see [midPoint documentation](#).

2. Connect the First Source System (HR) – Create Resource

1 Basic information — 2 Configuration — 3 Discovery — 4 Resource Schema

Establish a connection

Configure midPoint connection to the remote system. [More details](#)

NEW | MIDPILOT

Configuration ⓘ

File path * ⓘ

`\${midpoint.home}/resources` export.csv

Hide empty fields

← Back Next : Discovery →

2. Connect the First Source System (HR) – Create Resource

1 Basic Information 2 Configuration 3 Discovery 4 Resource Schema

MidPoint discovery

Your resource has gone through the discovery process and midPoint found the following configuration parameters. [More details](#)

☰ Discovered options ⓘ

Field delimiter ⓘ
.

Quote ⓘ
"

Multivalue delimiter ⓘ

"Unique ID" column (required) ⓘ
empnum

"Name" column ⓘ
empnum

"Password" column ⓘ

ⓘ Show empty fields

← Back Exit wizard Next : Resource Schema →

NEW | MIDPILOT

"Unique ID" column (required)

empnum

"Name" column ⓘ

empnum

"Password" column ⓘ

2. Connect the First Source System (HR) – Create Resource

Resource HR has been created

Your resource HR has been successfully created and configured, now select what you want to do next



Preview Resource
Data

Recommended



Configure Object
Types



Configure
Association Types

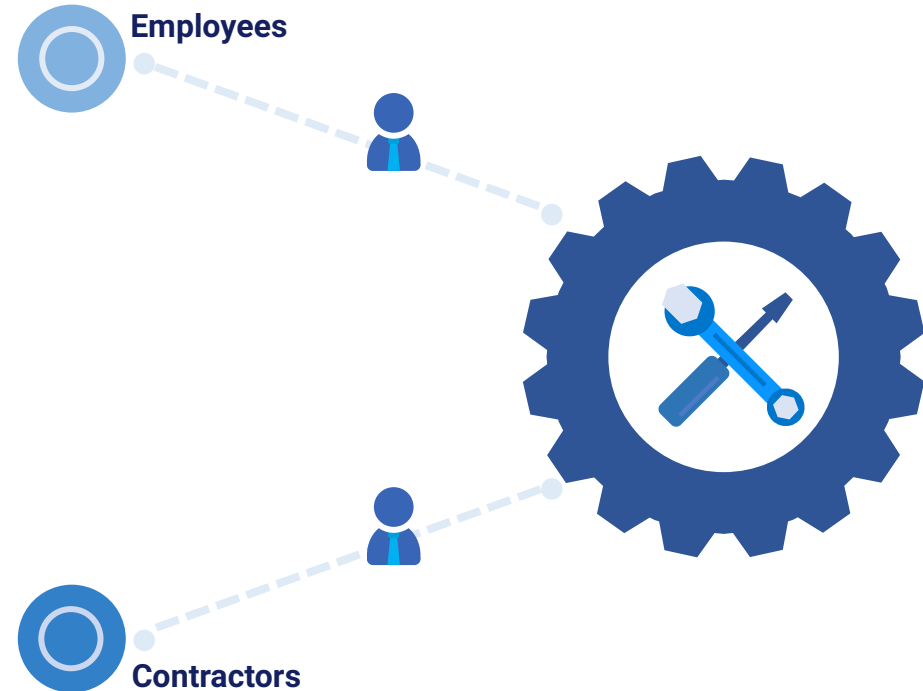


Go To Resource

Exit wizard

2. Connect the First Source System (HR) – Classify Data Into Object Types

- Object types specify the appearance of resource objects and how midPoint handles them
- Classify data into object types using configuration assistants (AI/heuristics) or manually **NEW | MIDPILOT**
- Examples:
 - Employees, Contractors



2. Connect the First Source System (HR) – Classify Data Into Object Types


HR / Object types


Object type manager

Here is a table with all the objects available in the selected resource, manage existing or create a new one


No object type to show

There are no object types yet. Create one, or ask for a suggestion.

 Add object type

 Generate suggestions

 Exit wizard

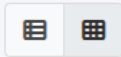
 Save settings

2. Connect the First Source System (HR) – Classify Data Into Object Types

HR / Object types /  Suggest object type

Select object class


Choose the object class that best represents the type of objects you want to manage. This will determine the available attributes and suggested configurations and suggest the proper object type.




AccountObjectClass ...

Description for this object class is not ready yet, but it will be available soon.

Object count **50** View schema

 Exit suggestions

 Suggest for selected

2. Connect the First Source System (HR) – Classify Data Into Object Types

 Allow AI to analyze your resource data?

To generate accurate suggestions, selected resource data may be sent to an external AI service for processing.

No authentication credentials or user passwords will be shared.

Without the selected data, suggestions may be limited to built-in heuristics or be unavailable.

Select which data can be used:

- Schema
Use the resource and midPoint schema.
- Statistical data
Use aggregated statistical data from the resource.

[Learn more](#)

Cancel

Allow and continue

2. Connect the First Source System (HR) – Classify Data Into Object Types

HR / Object types / [Review suggestions](#)

Select object type to review

Review the suggested object types generated based on your resource data. Select the one that best matches the kind of objects you want to manage. You can discard and refresh to possibly find new suggestions to review.

Full-time employee accounts



Accounts where c:attributes/ri:emptype indicates a full-time employee (FTE). This attribute is stable and uniquely identifies the employment type of the account holder, making it suitable for partitioning.

Hide filter ^ ...

Kind: account

Intent: employee

Object class: AccountObjectClass

Focus type: UserType

Filter:

c:attributes/ri:emptype = "FTE"

[AI](#)

Contractor accounts



Accounts where c:attributes/ri:emptype indicates a contractor (CONTRACTOR). This stable attribute separates contractor accounts from full-time employees.

Show filter v ...

Kind: account

Intent: contractor

Object class: AccountObjectClass

Focus type: UserType

[Exit suggestions](#)

[Refresh suggestions](#)

[Review selected](#)

2. Connect the First Source System (HR) – Review Classifications

Basic information about the object type

Basic information

Display name

Employees

Description

Accounts with employee type FTE.

Kind *

Account

Intent

employee

Security policy

Default

True

Lifecycle state

Active (production)

Hide empty fields

Specify the midPoint data

Define the Type (and optionally Archetype) that will represent the resource objects classified under this object type in midPoint. [More details](#)

MidPoint data

Type *

User

Archetype

- No archetype
- Use existing archetype
- Create new archetype

Person

Select archetype

Hide empty fields

← Back

Exit wizard

✓ Save settings

Specify the

Define resource objects that belong to (are classified under) this object type, either by the object class alone or using additional resource filters.

Resource data

Object class *

AccountObjectClass

Auxiliary object class

+ Add value - Clear all

Filter

+ Add value - Clear all

:c:attributes/ri:emptype = "FTE"

Show empty fields

← Back

Exit wizard

Next: MidPoint data →

2. Connect the First Source System (HR) – Review Classifications

HR / Object types










Object type manager



Here is a table with all the objects available in the selected resource, manage existing or create a new one





Suggestions available

Let analyze your resource and propose relevant object types. This helps you start faster without manual setup.


 Generate Suggestions

| <input type="checkbox"/> | Display name | objectClass  | Kind  | Intent  | Default  | Lifecycle state  | ... |
|--------------------------|---|---|--|--|---|---|--|
| <input type="checkbox"/> | Employees | AccountObjectClass | ACCOUNT | employee | true | Active (production)  |  Edit ... |
| <input type="checkbox"/> | Contractor accounts  | AccountObjectClass | ACCOUNT | contractor | | Ready to review |  Review ... |

 Add object type ON  Suggestions Enabled

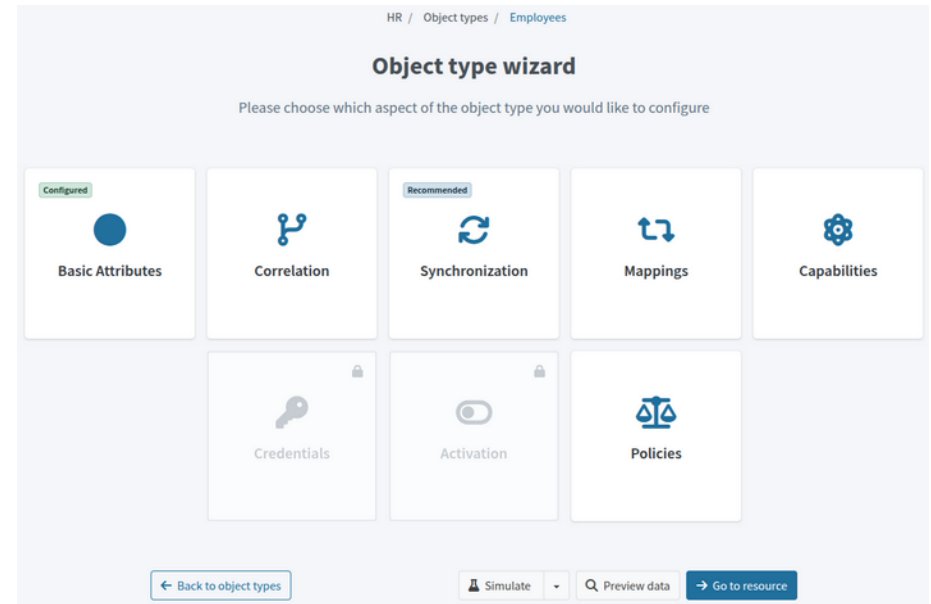
Rows per page 1 to 2 of 2    

 Exit wizard

 Save settings

2. Connect the First Source System (HR) – Configure Object Types

- Start with a single object type
- Configure object type using configuration assistants (AI/heuristics) or manually **NEW | MIDPILOT**
- Basic, Correlation, Synchronization, Mappings, Capabilities, etc.
- MidPoint suggests the order of configuration **NEW | MIDPILOT**



2. Connect the First Source System (HR) – Configure Object Types

We can skip correlation as there is no midPoint data yet.

The screenshot shows the 'Object type wizard' interface for configuring an object type. The breadcrumb path is 'HR / Object types / Employees'. The title is 'Object type wizard' and the instruction is 'Please choose which aspect of the object type you would like to configure'. There are eight configuration options arranged in two rows:

- Basic Attributes**: Labeled 'Configured' (green tag), represented by a blue circle icon.
- Correlation**: Represented by a blue branching icon.
- Synchronization**: Labeled 'Recommended' (blue tag), represented by a blue circular refresh icon.
- Mappings**: Represented by a blue double-headed arrow icon.
- Capabilities**: Represented by a blue gear icon.
- Credentials**: Represented by a grey key icon and a grey lock icon.
- Activation**: Represented by a grey toggle switch icon and a grey lock icon.
- Policies**: Represented by a blue scales of justice icon.

At the bottom, there are three buttons: '← Back to object types', 'Simulate' (with a dropdown arrow), and 'Preview data' (with a search icon). A dark blue button '→ Go to resource' is also present.

2. Connect the First Source System (HR) – Configure Object Types – Synchronization

List of reactions

Suggest default synchronization reactions

MidPoint will suggest one or more synchronization reactions based on your answers to the following questions. You can review and edit the result after confirmation.

SELECT THE SYNCHRONIZATION DIRECTION:

Source
The resource provides data to midPoint.

Target
MidPoint sends data to the resource.

Linked resource objects will be automatically synchronized between midPoint and the resource.
Unlinked resource objects will be automatically linked to an existing midPoint focus.

ANSWER THOSE QUESTIONS

What should happen if a **new resource object** is detected?

Import the resource object to midPoint

Do nothing

What should happen if a **resource object is deleted**?

Delete the midPoint object owning the resource object

Disable the midPoint object owning the resource object

Remove the broken link and synchronize

Just remove the broken link

Close Confirm and generate

| Action | Lifecycle state | |
|-------------|---------------------|--|
| Add focus | Active (production) | |
| Synchronize | Active (production) | |
| Link | Active (production) | |
| Synchronize | Active (production) | |

Rows per page: 20 | 1 to 4 of 4 | Page 1

Generate reactions Save synchronization settings

2. Connect the First Source System (HR) – Configure Object Types – Inbound Mappings

Mappings

Map data from your source to midPoint (Inbound mappings) and from midPoint to your target (Outbound mappings).

Suggestions generated
10 suggestions have been generated. Review and apply them.

[Re-generate](#)
Last run: May 4, 2026, 1:30:01 PM • Elapsed time: 0m 19s

→ Inbound mappings (to MidPoint)↔ Outbound mappings (to Resource)

Suggestions Enabled | Legend: ● Purple = AI-powered suggestions ● Blue = System suggestions

| <input type="checkbox"/> | Name | Resource attribute | Expression | MidPoint property | Lifecycle state | |
|--------------------------|---|--------------------|------------|---------------------------------|-----------------|--|
| <input type="checkbox"/> | status-into-activation/administrativeStatus | status | Script | activation/administrativeStatus | | <input checked="" type="button" value="Accept"/> <input checked="" type="button" value="Discard"/> ... |
| <input type="checkbox"/> | surname-into-familyName | surname | As is | familyName | | <input checked="" type="button" value="Accept"/> <input checked="" type="button" value="Discard"/> ... |
| <input type="checkbox"/> | Mapping suggestions 2 for: fullName | | | fullName | | <input type="button" value="Show suggestion"/> |
| <input type="checkbox"/> | firstname-into-givenName | firstname | As is | givenName | | <input checked="" type="button" value="Accept"/> <input checked="" type="button" value="Discard"/> ... |
| <input type="checkbox"/> | status-into-lifecycleState | status | Script | lifecycleState | | <input checked="" type="button" value="Accept"/> <input checked="" type="button" value="Discard"/> ... |
| <input type="checkbox"/> | locality-into-locality | locality | As is | locality | | <input checked="" type="button" value="Accept"/> <input checked="" type="button" value="Discard"/> ... |
| <input type="checkbox"/> | empnum-into-name | empnum | As is | name | | <input checked="" type="button" value="Accept"/> <input checked="" type="button" value="Discard"/> ... |

2. Connect the First Source System (HR) – Configure Object Types – Inbound Mappings

Attribute statistics may help you to create/validate script expressions if needed. “Status” has just three possible values (“Active” / “Long-term leave” / “Former employee”).

NEW | MIDPILOT







status-into-lifecycleState status Script All set Show script lifecycleState Active (production)

Total values
40

Unique values
3

Empty values
0

| Value Counts | | Value Patterns | |
|-----------------|-------|----------------|--|
| Value | Count | Percentage | |
| Active | 33 | 82.50% | |
| Long-term leave | 5 | 12.50% | |
| Former employee | 2 | 5.00% | |

-  Edit
-  Duplicate
-  Simulate mapping
-  Resource statistics
-  MidPoint statistics
-  Delete

2. Connect the First Source System (HR) – Configure Object Types – Inbound Mappings







Attribute statistics may help you to create/validate script expressions if needed.
“Job” contains a numeric code followed by “#” and text (e.g.: “113#Sales Representative”)

NEW | MIDPILOT

job-into-title job As is title Active (production)

| Total values | Unique values | Empty values |
|--------------|---------------|--------------|
| 40 | 24 | 0 |

| Value Counts | | Value Patterns | |
|-------------------------------------|-------|----------------|--|
| Value | Count | Percentage | |
| 107#Junior Consultant | 6 | 15.00% | |
| 113#Sales Representative | 4 | 10.00% | |
| 106#Agent Recruitment Specialist | 3 | 7.50% | |
| 222#Careers Advisor | 2 | 5.00% | |
| 331#Contract Termination Specialist | 2 | 5.00% | |

-  Edit
-  Duplicate
-  Simulate mapping
-  Resource statistics
-  MidPoint statistics
-  Delete

2. Connect the First Source System (HR) – Configure Object Types – Inbound Mappings

Final accepted mappings (scripts generated or added manually based on attribute data statistics)

| Name | Resource attribute | Expression | MidPoint property | Lifecycle state |
|----------------------------|--------------------|----------------|-------------------|---------------------|
| surname-into-familyName | surname | As is | familyName | Active (production) |
| firstname-into-givenName | firstname | As is | givenName | Active (production) |
| status-into-lifecycleState | status | Script All set | lifecycleState | Active (production) |
| locality-into-locality | locality | As is | locality | Active (production) |
| empnum-into-name | empnum | As is | name | Active (production) |
| empnum-into-personalNumber | empnum | As is | personalNumber | Active (production) |
| job-into-title | job | Script All set | title | Active (production) |

Code 113#Sales Representative

```
1 basic.substringAfter(input, '#')
```

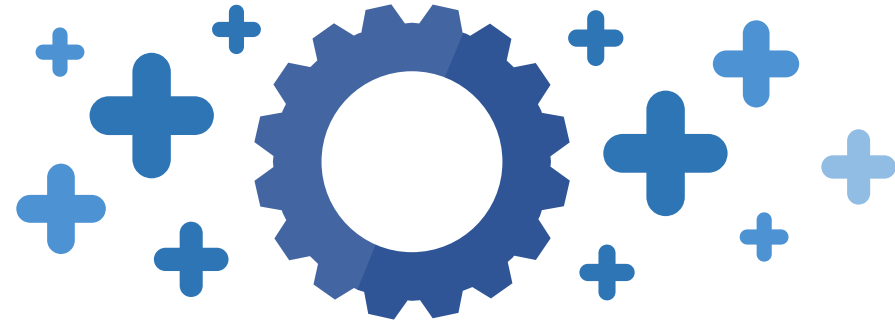
Active → active
Long-term leave → suspended
Former employee → archived

Code

```
1 // Map application status values to c:lifecycleState
2 switch (input) {
3   case 'Active':
4     return 'active'
5   case 'Long-term leave':
6     return 'suspended'
7   case 'Former employee':
8     return 'archived'
9   default:
10    return null
11 }
```

3. Import Source Data (HR)


- Simulate source data import to validate the configuration (especially mappings)
- Import data from Source system and create users in midPoint





3. Import Source Data (HR) – Development Simulation


Object type wizard


Please choose which aspect of the object type you would like to configure


Configured

Basic Attributes



Correlation


Configured

Synchronization

Configured

Mappings


Capabilities


Credentials



Activation



Policies

[← Back to object types](#) [🧪 Simulate](#) [🔍 Preview data](#) [→ Go to resource](#)

Configuration of simulation

Use the simulation configuration type context. This affects how the rule is evaluated and what data is used.


Production
Active configuration used in regular midPoint operations...


Development
Configuration under development. Safe for testing,...

3. Import Source Data (HR) – Development Simulation

HR / Object types / Employees / Simulation result

Simulation result

[← Back to object type wizard](#) [View processed objects](#)

| Simulation task details | |
|-------------------------|---|
| Start timestamp | May 4, 2026, 1:57:25 PM UTC |
| End timestamp | May 4, 2026, 1:57:28 PM UTC |
| Finished in | 3 seconds |
| Task | Preview of Reconciliation: HR: Employees |
| Status | Finished |
| Configuration | Development |
| Added objects | 40 |
| Deleted objects | 0 |
| Modified objects | 40 |
| Unmodified objects | 0 |
| All processed objects | 80 |

Event marks

| | | | |
|---|--|------------------------------------|-------------------------------------|
| Focus activated 33 More info | Focus deactivated 0 | Focus renamed 0 | Focus assignments changed 0 |
| Focus archetype changed 0 | Focus parent organization reference 0 | Focus role membership changed 0 | Projection activated 0 |
| Projection deactivated 0 | Projection renamed 0 | Projection identifier changed 0 | Projection entitlement changed 0 |
| Projection password changed 0 | Resource object affected 0 | | |

3. Import Source Data (HR) – Development Simulation

Event mark ? Undefined ▼ State ? Undefined ▼ × More... ▼ 🔍 Basic ▼

| <input type="checkbox"/> | ^ Name | Type | State | Changes | 👁 |
|--------------------------|---|--------|-----------------------|---|-------------------------------|
| <input type="checkbox"/> | 👤 1001 (Geena Green) 🔔 Focus activated | User | Added | <div style="width: 100%;"><div style="width: 100%;"></div></div> 11 Additions of total 11 | 👁 ▼ |
| <input type="checkbox"/> | 👤 1001 (Account 1001 (employee) on HR) | Shadow | Modified | <div style="width: 100%;"><div style="width: 0%;"></div></div> No changes | 👁 ▼ |
| <input type="checkbox"/> | 👤 1002 (Account 1002 (employee) on HR) | Shadow | Modified | <div style="width: 100%;"><div style="width: 0%;"></div></div> No changes | 👁 ▼ |
| <input type="checkbox"/> | 👤 1002 (Ana Lopez) 🔔 Focus activated | User | Added | <div style="width: 100%;"><div style="width: 100%;"></div></div> 11 Additions of total 11 | 👁 ▼ |

🔍 Changes 🔍 Simple 🔍 Advanced

👤 Add User Geena Green (1001) ▼

| Item ↕ | Value |
|---------------------|-------------------------------|
| Name | + 1001 |
| Lifecycle state | + active |
| Full name | + Geena Green |
| Given name | + Geena |
| Family name | + Green |
| Title | + CEO |
| Personal Number | + 1001 |
| Locality | + Hot Lava City |
| Projections | + 1001 [Default] |

Archetype **Person** assigned. ◀

User was **enabled**.

3. Import Source Data (HR) & Create Users in MidPoint

Persons

Full name × Name × Users with a

Users without account ResourceType

| <input type="checkbox"/> | ^ Name | Personal Number | Full name |
|--------------------------|--------|-----------------|---------------|
| <input type="checkbox"/> | 1001 | 1001 | Geena Green |
| <input type="checkbox"/> | 1002 | 1002 | Ana Lopez |
| <input type="checkbox"/> | 1003 | 1003 | Jimmy Taylor |
| <input type="checkbox"/> | 1004 | 1004 | Peter Hunter |
| <input type="checkbox"/> | 1005 | 1005 | Emanuel Young |

Geena Green (1001)
CEO

✓ Enabled
✗ No organizations
Person

Operations
← Back Save Preview changes Change archetype Delete object Edit raw

Options
Options

Basic

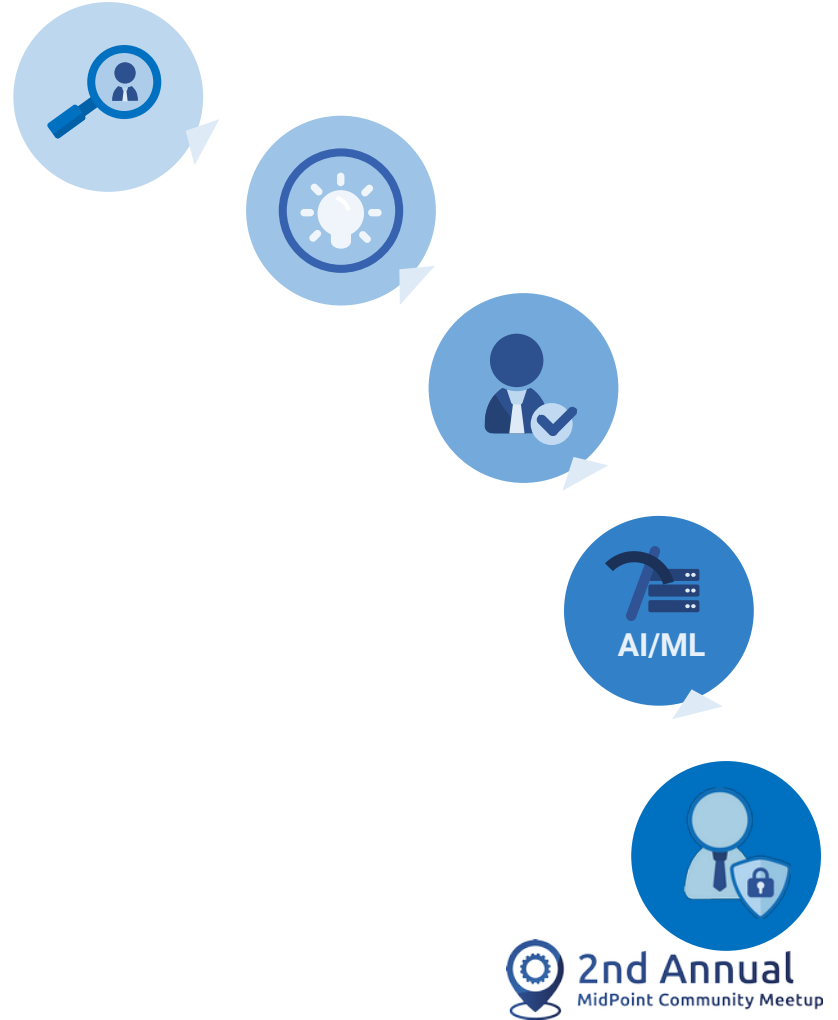
- Projections 1
- All accesses
- Assignments 0 <
- Activation
- Password
- OTP 0
- History
- Cases 0
- Personas 0
- Delegations 0

Properties

- Name 1001
- Lifecycle state Active (production)
- Full name Geena Green
- Given name Geena
- Family name Green
- Title CEO
- Personal Number 1001
- Locality Hot Lava City

4. Connect the First Target System (LDAP)

- Typically Microsoft Active Directory or corporate LDAP server
- Connect the Target system and preview resource data
- Configure object types
- **Use a series of wizards and configuration assistants**



4. Connect the First Target System (LDAP) – Create Resource

1 Basic information 2 Configuration 3 Discovery 4 Resource Schema

Establish a connection

Configure midPoint connection to the remote system. [More details](#)

⚙️ Configuration

Host ⓘ
ldap

Port number ⓘ
389

Connection security ⓘ

Bind DN ⓘ
cn=idm,ou=service-accounts,dc=example,dc=com

Bind password ⓘ
 Use clear value
 Use secret provider

Docker secrets ▾ ldap_password
Select provider and insert key value where password is stored

👁️ Hide empty fields

← Back ↺ Exit wizard Next: Discovery →

4. Connect the First Target System (LDAP) – Create Resource

1 Basic information 2 Configuration 3 Discovery 4 Resource Schema

MidPoint discovery

Your resource has gone through the discovery process and midPoint found the following configuration parameters. [More details](#)

☰ Discovered options ⓘ

Base context ⓘ

dc=example,dc=com

VLV sort attribute ⓘ

uid,cn,ou

☰ Discovered options ⓘ

Base context ⓘ

dc=example,dc=com

VLV sort attribute ⓘ

uid,cn,ou

VLV ordering rule ⓘ

2.5.13.3

Operational attributes ⓘ + Add value - Clear all

Use permissive modify ⓘ

always

Managed association pairs ⓘ + Add value - Clear all

Lockout strategy ⓘ

Undefined

ⓘ Show empty fields

← Back ↺ Exit wizard Next : Resource Schema →

4. Connect the First Target System (LDAP) – Create Resource

Most-commonly used object classes are selected by default

NEW | MIDPILOT

1 Basic information 2 Configuration 3 Discovery 4 Resource Schema

Resource Schema

Select object classes that midPoint should be restricted to, otherwise all object classes will be available. Keep default if unsure. [More details](#)

Resource Schema

Selected item

organizationalUnit X groupOfUniqueNames X inetOrgPerson X groupOfNames X

| <input type="checkbox"/> | Name | Native name | Type |
|--------------------------|-------------------|-------------------|------------|
| <input type="checkbox"/> | account | account | Structured |
| <input type="checkbox"/> | alias | alias | Structured |
| <input type="checkbox"/> | applicationEntity | applicationEntity | Structured |

4. Connect the First Target System (LDAP) – Create Resource

Resource LDAP has been created

Your resource LDAP has been successfully created and configured, now select what you want to do next



Preview Resource
Data

Recommended



Configure Object
Types



Configure
Association Types

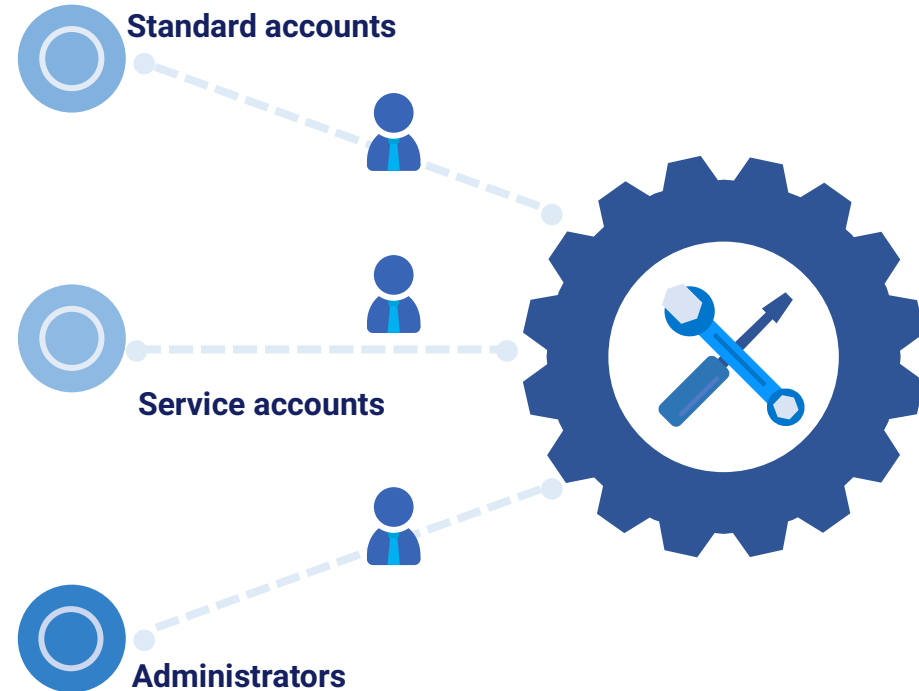


Go To Resource

← Exit wizard

4. Connect the First Target System (LDAP) – Classify Data Into Object Types

- Object types specify the appearance of resource objects and how midPoint handles them
- Classify data into object types using configuration assistants (AI/heuristics) or manually **NEW | MIDPILOT**
- Examples:
 - Standard accounts, Service accounts, Administration accounts
 - Internal groups, Application groups, Administration groups



4. Connect the First Target System (LDAP) – Classify Data Into Object Types

LDAP / Object types / [Suggest object type](#)

Select object class

Choose the object class that best represents the type of objects you want to manage. This will determine the available attributes and suggested configurations and suggest the proper object type.

GroupOfNames ...
Description for this object class is not ready yet, but it will be available soon.
Object count **26** [View schema](#)

InetOrgPerson ...
Description for this object class is not ready yet, but it will be available soon.
Object count **44** [View schema](#)

GroupOfUniqueNames ...
Description for this object class is not ready yet, but it will be available soon.
Object count **0** [View schema](#)

OrganizationalUnit ...
Description for this object class is not ready yet, but it will be available soon.
Object count **6** [View schema](#)

[Exit suggestions](#) [Suggest for selected](#)

4. Connect the First Target System (LDAP) – Classify Data Into Object Types

User accounts

Regular user accounts located under ou=users,dc=example,dc=com. Show filter ▾ ⋮

Kind: account Intent: user Object class: inetOrgPerson Focus type: UserType

Service accounts

Service accounts located under ou=service-accounts,dc=example,dc=com, typically identified by UID ending with -svc. Show filter ▾ ⋮

Kind: account Intent: service Object class: inetOrgPerson Focus type: UserType

Administrator accounts

Administrator accounts located under ou=administrators,dc=example,dc=com, typically identified by UID ending with -admin. Show filter ▾ ⋮

Kind: account Intent: admin Object class: inetOrgPerson Focus type: UserType

[↩ Exit suggestions](#) [🔄 Refresh suggestions ▾](#) [🔍 Review selected](#)

4. Connect the First Target System (LDAP) – Review Classifications

Basic information about the object type

Describe the intended purpose of the object type. An object type specifies how a particular kind of resource object (e.g., account or entitlement) is handled.

● Basic information

Display name
User accounts

Description
Regular user accounts located under ou=users,dc=example,dc=com

Kind * ⓘ
Account

Intent ⓘ
user

Security policy ⓘ

Default ⓘ
True

Lifecycle state ⓘ
Active (production)

⊞ Hide empty fields

↩ Exit wizard

Specify the resource

● Resource data

Object class * ⓘ
inetOrgPerson

Auxiliary object class ⓘ ⊕ Add value 🔴 Clear all

Filter ⓘ ⊕ Add value 🔴 Clear all

Object class (base context) ⓘ
organizationalUnit

Filter (base context) ⓘ
c:attributes/ri:dn = "ou=users,dc=example,dc=com"

⊞ Show empty fields

← Back

↩ Exit wizard

Next : MidPoint data →

Specify the midPoint data

Define the Type (and optionally Archetype) that will represent the resource objects classified under this object type in midPoint. More details

● MidPoint data ▾

Type * ⓘ
User

Archetype ⓘ
 No archetype
 Use existing archetype
 Create new archetype

⊞ Hide empty fields

← Back

↩ Exit wizard

✓ Save settings

4. Connect the First Target System (LDAP) – Review Classifications


LDAP / Object types












Object type manager



Here is a table with all the objects available in the selected resource, manage existing or create a new one





Suggestions available

Let analyze your resource and propose relevant object types. This helps you start faster without manual setup.


 Generate Suggestions

| <input type="checkbox"/> Display name | objectClass  | Kind  | Intent  | Default  | Lifecycle state  | ... |
|---|---|--|--|---|---|--|
| <input type="checkbox"/> User accounts | inetOrgPerson | ACCOUNT | user | true | Active (production)  |  Edit ... |
| <input type="checkbox"/> Service accounts  | inetOrgPerson | ACCOUNT | service | | Ready to review |  Review ... |
| <input type="checkbox"/> Administrator accounts  | inetOrgPerson | ACCOUNT | admin | | Ready to review |  Review ... |

 Add object type ON  Suggestions Enabled

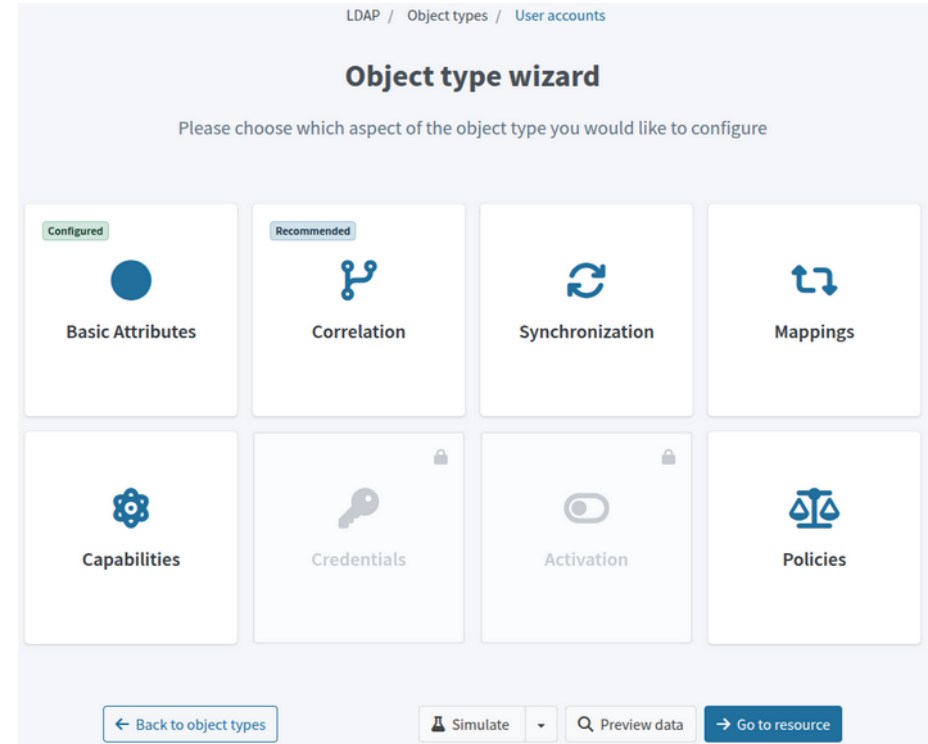
Rows per page 1 to 3 of 3    

 Exit wizard

 Save settings

4. Connect the First Target System (LDAP) – Configure Object Types

- Start with a single object type
- Configure object type using configuration assistants (AI/heuristics) or manually **NEW | MIDPILOT**
- Basic, Correlation, Synchronization, Mappings, Capabilities, etc.
- Correlation simulation **NEW | MIDPILOT**
- MidPoint suggests the order of configuration **NEW | MIDPILOT**











4. Connect the First Target System (LDAP) – Configure Object Types

LDAP / Object types / User accounts

Object type wizard

Please choose which aspect of the object type you would like to configure

| | | | |
|--|--|--|---|
| Configured  Basic Attributes | Recommended  Correlation |  Synchronization |  Mappings |
|  Capabilities |  Credentials |  Activation |  Policies |

[← Back to object types](#) [Simulate](#) [Preview data](#) [→ Go to resource](#)

4. Connect the First Target System (LDAP) – Configure Object Types – Correlation

LDAP / Object types / User accounts / Correlation

Correlation rules

Correlation is a mechanism used for correlating resource objects with existing midPoint objects. You can define one or more correlation rules using different items and weights to support automatic matching, while allowing ambiguous cases to be reviewed and resolved manually. [More details](#)

No correlation rule to show

There are no correlation rules yet. Create one, or ask for a suggestion.

+ Create new

🔮 Generate suggestions

4. Connect the First Target System (LDAP) – Configure Object Types – Correlation

Correlation rules

Correlation is a mechanism used for correlating resource objects with existing midPoint objects. You can define one or more correlation rules using different items and weights to support automatic matching, while allowing ambiguous cases to be reviewed and resolved manually. [More details](#)

Suggestions generated
2 suggestions have been generated. Review and apply them. Re-generate

Last run: May 4, 2026, 2:43:30 PM • Elapsed time: 1m 0s

ON Suggestions Enabled + Create new

Suggestion More options

Name correlator
Suggested based on matching of attributes/employeeNumber to name

name (Exact)

Stats

| | | |
|------------|--------|-----------------|
| 1.0 Weight | 1 Tier | 97.0 Efficiency |
|------------|--------|-----------------|

Actions

[View rule](#)

Suggestion More options

PersonalNumber correlator
Suggested based on matching of attributes/employeeNumber to personalNumber

personalNumber (Exact)

Stats

| | | |
|------------|--------|-----------------|
| 1.0 Weight | 1 Tier | 97.0 Efficiency |
|------------|--------|-----------------|

Actions

[View rule](#)

Suggestion More options

PersonalNumber correlator
Suggested based on matching of attributes/employeeNumber to personalNumber

personalNumber (Exact) **NEW | MIDPILOT**

Stats

| | | |
|------------|--------|-----------------|
| 1.0 Weight | 1 Tier | 97.0 Efficiency |
|------------|--------|-----------------|

Actions

[View rule](#)

More options


- Delete
- Simulate
- View rule


4. Connect the First Target System – Configure Object Types – Correlation Simulation


LDAP / Object types / User accounts / Correlation / Simulation result


Simulation result

[← Back to correlation rules](#) [Export](#)





Correlated i 
38
[View objects](#)

Uncertain correlations i 
0
[View objects](#)

Not correlated i 
1
[View objects](#)

Total processed i 
39
[View objects](#)

Event mark i Shadow owner found State i Undefined More... Basic

| <input type="checkbox"/> | Status | Name | Correlation candidate | <input type="text"/> |
|--------------------------|--------|----------------|---|---|
| <input type="checkbox"/> | > | Correlated | uid=abaker,ou=users,dc=example,dc=com |  1021 <input type="text"/> |
| <input type="checkbox"/> | > | Correlated | uid=adewries,ou=users,dc=example,dc=com |  1030 <input type="text"/> |
| <input type="checkbox"/> | > | Correlated | uid=afreeman,ou=users,dc=example,dc=com |  1010 <input type="text"/> |
| <input type="checkbox"/> | > | Not correlated | uid=test123,ou=users,dc=example,dc=com |  No match found <input type="text"/> |

4. Connect the First Target System – Configure Object Types – Correlation Simulation

You can mark objects right in the correlation simulation to define exceptions (these objects will be ignored)

LDAP / Object types / User accounts / Correlation / Simulation result

Simulation result

← Back to correlation rules Export

Correlated ⓘ

38

View objects

Uncertain correlations ⓘ

0

View objects

Not correlated ⓘ

1

View objects

Total processed ⓘ

39

View objects

Event mark ⓘ Shadow owner not found ▾ State ⓘ Undefined ▾ × More... ▾ Basic ▾

| | Status | Name | Correlation candidate | |
|--------------------------|--------|---|---|--|
| <input type="checkbox"/> | > | <code>uid=test123.ou=users,dc=example,dc=com</code> Do not touch | ⚠ No match found | 🛡️ ▾ |

4. Connect the First Target System (LDAP) – Configure Object Types – Correlation

Accepting correlation configuration prompts to create inbound correlation mappings

NEW | MIDPILOT

i This rule requires additional mappings

Before accepting this correlation rule suggestion, please note that it relies on attribute mappings that do not yet exist in your configuration. These mappings will be automatically created as part of the acceptance process.

| Name | Resource attribute | Expression | Target |
|----------------------------------|--------------------|------------|----------------|
| employeeNumber-to-personalNumber | employeeNumber | As is | personalNumber |

1 to 1 of 1


Cancel ✓ Accept and add


4. Connect the First Target System (LDAP) – Configure Object Types – Synchronization


LDAP / Object types / User accounts


Object type wizard


Please choose which aspect of the object type you would like to configure


Configured

Basic Attributes


Configured

Correlation


Recommended

Synchronization


Mappings


Capabilities


Credentials


Activation


Policies

[← Back to object types](#) [Simulate](#) [Preview data](#) [→ Go to resource](#)

4. Connect the First Target System (LDAP) – Configure Object Types – Synchronization

NEW | MIDPILOT

Suggest default synchronization reactions

MidPoint will suggest one or more synchronization reactions based on your answers to the following questions. You can review and edit the result after confirmation.

SELECT THE SYNCHRONIZATION DIRECTION:

Source
The resource provides data to midPoint.

Target
MidPoint sends data to the resource.

Linked resource objects **will be automatically synchronized** between midPoint and the resource. Unlinked resource objects **will be automatically linked** to an existing midPoint focus.

ANSWER THOSE QUESTIONS

What should happen if a **new resource object** is detected?

- Disable the resource object
- Delete the resource object
- Do nothing

What should happen if a **resource object is deleted**?

- Remove the broken link and synchronize
- Just remove the broken link

What should happen if **correlation finds multiple candidate owners or if the correlation confidence is low**?

- Create a correlation case for the human operator to decide
- Do nothing

Close

| | Situation | Action | Lifecycle state | |
|--|-----------|-------------------------|---------------------|--|
| | Unmatched | Delete resource object | Active (production) | |
| | Deleted | Synchronize | Active (production) | |
| | Disputed | Create correlation case | Active (production) | |
| | Unlinked | Link | Active (production) | |
| | Linked | Synchronize | Active (production) | |

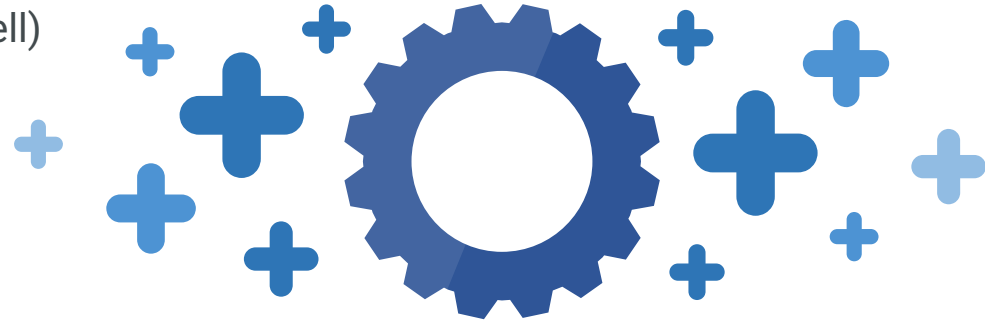
20 1 to 5 of 5 << < 1 > >>

What should happen if a **new resource object** is detected?

- Disable the resource object
- Delete the resource object
- Do nothing

5. Target System Integration (LDAP)

- Simulate reconciliation
- Mark uncorrelatable data as exceptions and plan to handle them later (we can do it in correlation simulation as well)
 - Orphaned accounts
 - System (service) accounts
 - Unmatched accounts with invalid correlation data
- Correlate & link existing accounts to midPoint users
- Majority of the target system accounts are now linked to their midPoint owners



5. Target System Integration (LDAP) – Reconciliation – Development Simulation

LDAP / Object types / Employee accounts / Simulated objects

Simula

[← Back to simulation tasks](#)





Event mark ⓘ U

Changes

Simple Advanced

Modify User Geena Green (1001)

| Item ↓ | Old value | New value |
|-------------|----------------|---|
| Projections | 1001 [Default] | <div style="border: 2px solid red; padding: 5px;">uid=geena,ou=users, + dc=example,dc=com [Default]</div> |

| <input type="checkbox"/> | Name | Type | State | Changes | |
|--------------------------|--|------|----------|--|--|
| <input type="checkbox"/> |  1001 (Geena Green) | User | Modified | <div style="width: 100%; height: 10px; background-color: green;"></div> 1 Additions of total 1 |  ▾ |
| <input type="checkbox"/> |  1004 (Peter Hunter) | User | Modified | <div style="width: 100%; height: 10px; background-color: green;"></div> 1 Additions of total 1 |  ▾ |

Intermezzo: Simulations & Marks

“

Look before you leap

”

Aesop

Why Simulations?

- Data can be unexpectedly deleted or modified by incorrect configuration and/or if target system data is inconsistent during midPoint deployment
- **“What would happen if...”** → You have time to react before you damage anything
- Clever usage of “lifecycle state” and “execution mode” to perform “Development” and “Production” simulation
 - Development: process “Active” and “Proposed” configuration
 - Production: process “Active” and “Deprecated” configuration
- Docs: [Simulations](#)

“

Look before you leap.

”

Aesop

Real Life Scenario: Forgotten Correlation Rule (Suggested, Not Saved)

Simulation result

← Back to object type wizard View processed objects

Simulation task details

| | |
|-----------------------|--|
| Start timestamp | May 4, 2026, 3:16:44 PM UTC |
| End timestamp | May 4, 2026, 3:16:45 PM UTC |
| Finished in | 1 second |
| Task | Preview of Reconciliation: LDAP: User accounts |
| Status | Finished |
| Configuration | Development |
| Added objects | 0 |
| Deleted objects | 38 |
| Modified objects | 0 |
| Unmodified objects | 0 |
| All processed objects | 38 |

Event marks

| | | | |
|-------------------------------------|---|---|------------------------------------|
| Projection activated 0 | Projection deactivated 38 More info | Projection renamed 0 | Projection identifier changed 0 |
| Projection entitlement changed 0 | Projection password changed 0 | Resource object affected 38 More info | |



What should happen if a **new resource object** is detected?

- Disable the resource object
- Delete the resource object**
- Do nothing

Real Life Scenario: Simulation Saved The Day

Simulation result

[← Back to object type wizard](#) [View processed objects](#)

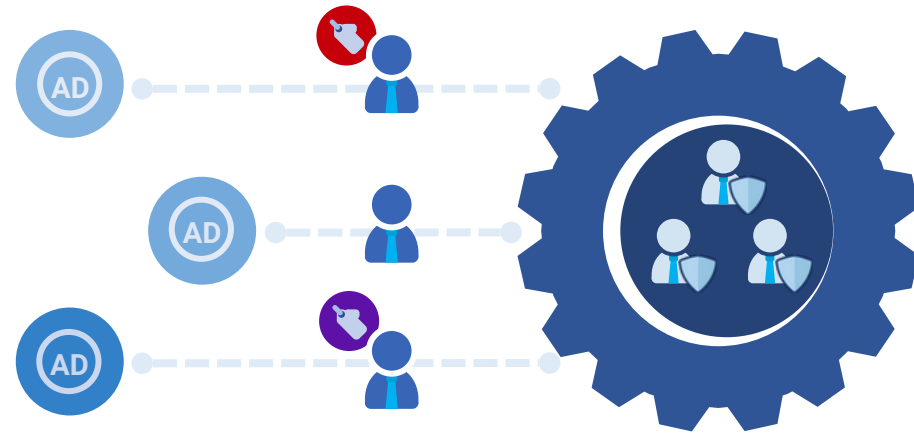
| | |
|-------------------------|--|
| Simulation task details | |
| Start timestamp | May 4, 2026, 3:16:44 PM UTC |
| End timestamp | May 4, 2026, 3:16:45 PM UTC |
| Finished in | 1 second |
| Task | Preview of Reconciliation: LDAP: User accounts |
| Status | Finished |
| Configuration | Development |
| Added objects | 0 |
| Deleted objects | 38 |
| Modified objects | 0 |
| Unmodified objects | 0 |
| All processed objects | 38 |

Event marks

| | | | | | |
|-------------------------|---|------------------------|----|-------------------------------|---|
| Projection activated | 0 | Projection deactivated | 38 | Projection identifier changed | 0 |
| Projection entitlements | 0 | Projection affected | 0 | Projection info | 0 |

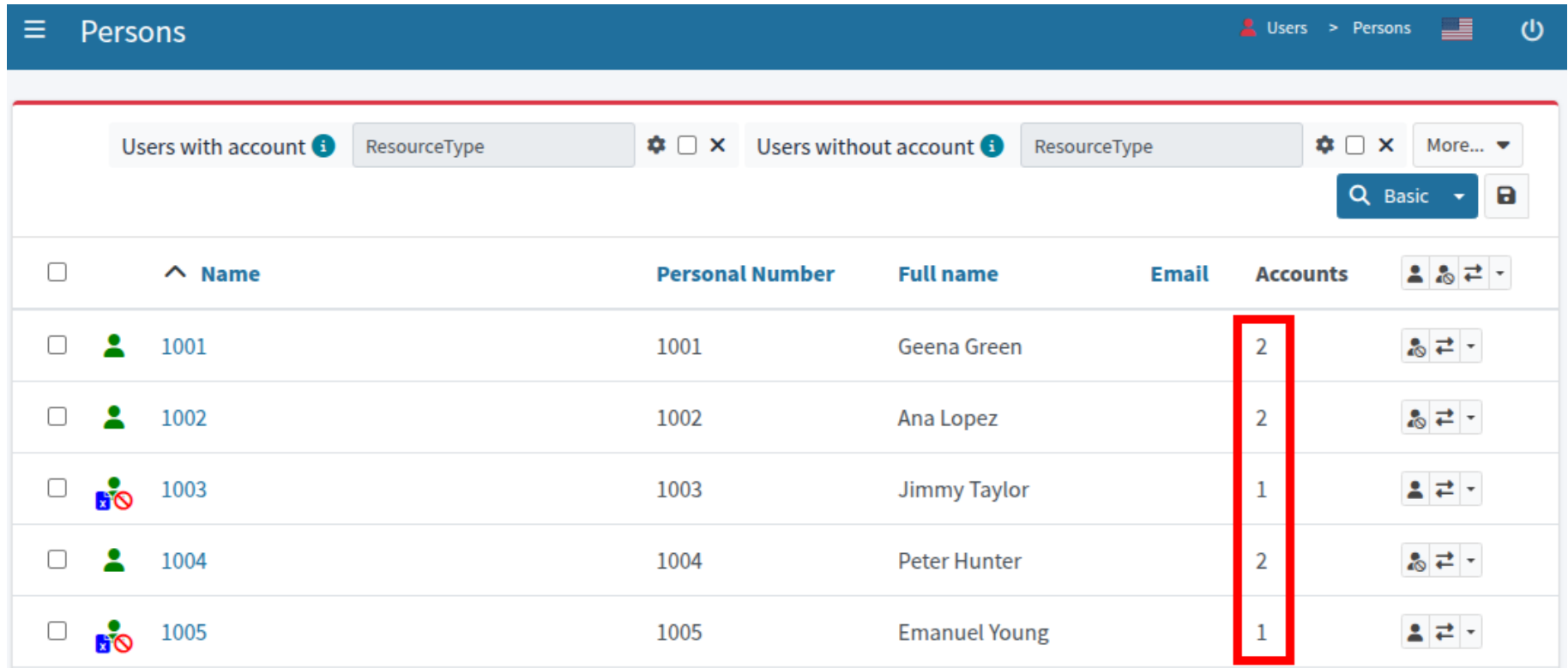
Why (Account) Marks?

- **Marks** allow **exceptions** from policies
 - Protected, Do not touch, Correlate later and more
- Example: protect certain accounts from being processed or deleted
 - Permanently, e.g. system accounts that won't be managed by midPoint
 - Temporarily/postpone decision, e.g. uncorrelated, undecided accounts
- Allow the deployment process to continue (e.g., accounts that seem to be system accounts)
- Also useful in reporting and analytics













5. Target System Integration (LDAP) – Reconciliation & Linking Accounts

All *correlatable* Target system accounts are linked to their owners in midPoint












The screenshot shows the 'Persons' management interface in midPoint. At the top, there are filters for 'Users with account' and 'Users without account', both set to 'ResourceType'. A search bar is set to 'Basic'. The main table lists users with columns for Name, Personal Number, Full name, Email, and Accounts. The 'Accounts' column values are 2, 2, 1, 2, and 1 for the five users shown. A red box highlights the 'Accounts' column.

| <input type="checkbox"/> | Name | Personal Number | Full name | Email | Accounts | |
|--------------------------|--|-----------------|---------------|-------|----------|---|
| <input type="checkbox"/> |  1001 | 1001 | Geena Green | | 2 |  |
| <input type="checkbox"/> |  1002 | 1002 | Ana Lopez | | 2 |  |
| <input type="checkbox"/> |  1003 | 1003 | Jimmy Taylor | | 1 |  |
| <input type="checkbox"/> |  1004 | 1004 | Peter Hunter | | 2 |  |
| <input type="checkbox"/> |  1005 | 1005 | Emanuel Young | | 1 |  |

6. (Optional) Import Usernames from Target System (LDAP)

- You can import usernames to midPoint (if HR system does not have them)
- Reconfigure the original mapping in Source resource to be “weak” (E.g.: empnum → name)
- Prepare a new inbound mapping from Target system
- Simulate username import from Target system to midPoint
- Import usernames from Target system to midPoint

| | | | | |
|--------------------------|--|------------|------|-------------------|
| <input type="checkbox"/> |  | abaker | 1021 | Alice Baker |
| <input type="checkbox"/> |  | adewries | 1030 | Amanda de Wries |
| <input type="checkbox"/> |  | afreeman | 1010 | Alexander Freeman |
| <input type="checkbox"/> |  | ajackson | 1029 | Ashley Jackson |
| <input type="checkbox"/> |  | alopez | 1002 | Ana Lopez |
| <input type="checkbox"/> |  | bcarpenter | 1024 | Brad Carpenter |
| <input type="checkbox"/> |  | cwhitehe | 1039 | Charles Whitehead |
| <input type="checkbox"/> |  | ddavis | 1007 | Diane Davis |
| <input type="checkbox"/> |  | diverson | 1022 | David Iverson |

6. (Optional) Import Usernames from Target System – Set HR Mapping to “Weak”

→ 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 <i>i</i> | Resource attribute * <i>i</i> | Expression <i>i</i> | MidPoint property <i>i</i> | Lifecycle state <i>i</i> | ... |
|--------------------------|----------------------------|-------------------------------|---|----------------------------|--------------------------|-----|
| <input type="checkbox"/> | surname-into-familyName | surname | As is | familyName | Active (production) | ... |
| <input type="checkbox"/> | firstname-into-givenName | firstname | As is | givenName | Active (production) | ... |
| <input type="checkbox"/> | status-into-lifecycleState | status | ScriptAll set Show script | lifecycleState | Active (production) | ... |
| <input type="checkbox"/> | locality-into-locality | locality | As is | locality | Active (production) | ... |
| <input type="checkbox"/> | empnum-into-name | empnum | As is | name | Active (production) | ... |
| <input type="checkbox"/> | empnum-into-personalNumber | empnum | As is | personalNumber | Active (production) | ... |
| <input type="checkbox"/> | job-into-title | job | ScriptAll set Show script | title | Active (production) | ... |

6. (Optional) Import Usernames from Target System – Add Inbound Mapping

This mapping overrides username mapping from HR

User accounts / Mappings

Mappings

Map data from your source to midPoint (Inbound mappings) and from midPoint to your target (Outbound mappings).

Suggestions available
Let analyze your resource and propose relevant object types. This helps you start faster without manual setup. [Generate Suggestions](#)

→ Inbound mappings (to MidPoint) **↔ Outbound mappings (to Resource)**

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"/> | uid-into-name | uid | As is | name | Active (production) | ... |
| <input type="checkbox"/> | employeeNumber-to-personalNumber | employeeNumber | As is | personalNumber | Active (production) | ... |

6. (Optional) Import Usernames from Target System (LDAP) – Reconciliation – Simulation

Simulation result

[← Back to object type wizard](#) [View processed objects](#)

Simulation task details

| | |
|--------------------|--|
| Start timestamp | May 4, 2026, 3:38:11 PM UTC |
| End timestamp | May 4, 2026, 3:38:13 PM UTC |
| Finished in | 2 seconds |
| Task | Preview of Reconciliation: LDAP: User accounts |
| Status | Finished |
| Configuration | Development |
| Added objects | 0 |
| Deleted objects | 0 |
| Modified objects | 38 |
| Unmodified objects | 76 |

Event marks

| | | | | | | | |
|-------------------------|---|--------------------------------|---|------------------------------|----|---------------------------|---|
| Focus activated | 0 | Focus deactivated | 0 | Focus renamed | 38 | Focus assignments changed | 0 |
| Focus archetype changed | 0 | Focus parent organization refe | 0 | Focus role membership change | 0 | Projection activated | 0 |
| Projection deactiv | 0 | Projection passw | 0 | | | | |

Changes [Simple](#) [Advanced](#)

Modify User Geena Green (geena)

| Item ↓ | Old value | New value |
|--------|-----------|-----------|
| Name | 1001 | geena |

6. (Optional) Import Usernames from Target System (LDAP) – Reconciliation

Owners of all *linked* Target system accounts are renamed

| <input type="checkbox"/> | Name | Personal Number | Full name | Email | Accounts | |
|--------------------------|-------------|------------------------|-------------------|--------------|-----------------|--|
| <input type="checkbox"/> | 1003 | 1003 | Jimmy Taylor | | 1 | |
| <input type="checkbox"/> | 1005 | 1005 | Emanuel Young | | 1 | |
| <input type="checkbox"/> | abaker | 1021 | Alice Baker | | 2 | |
| <input type="checkbox"/> | adewries | 1030 | Amanda de Wries | | 2 | |
| <input type="checkbox"/> | afreeman | 1010 | Alexander Freeman | | 2 | |

7. Enable Provisioning to Target System (LDAP)

- Configure Target resource for provisioning from midPoint (Outbound Mappings + Activation, Credentials) using AI/heuristics configuration assistants or manually **NEW | MIDPILOT**
- Set all outbound mappings' lifecycle state to: Proposed
- Simulate reconciliation, review data inconsistencies
 - Update mappings, use marks or allow midPoint to update target system data
- Set all outbound mappings' lifecycle state to: Active
- Run reconciliation with Target System



7. Enable Provisioning to Target System (LDAP): Outbound Mappings

→ Inbound mappings (to MidPoint) ↔ Outbound mappings (to Resource)

ON Suggestions Enabled Legend: ● Purple = AI-powered suggestions ● Blue = System suggestions

| <input type="checkbox"/> | Name ⓘ | MidPoint property | Expression ⓘ | Resource attribute* ⓘ | Lifecycle state ⓘ | ... |
|----------------------------------|---|-------------------|--------------|-----------------------|-------------------|--|
| <input type="checkbox"/> | ● fullName-to-cn | fullName | As is | cn | | <input type="button" value="✓ Accept"/> <input type="button" value="✗ Discard"/> ... |
| <input type="checkbox"/> | ● fullName-to-displayName | fullName | As is | displayName | | <input type="button" value="✓ Accept"/> <input type="button" value="✗ Discard"/> ... |
| <input type="checkbox"/> | ^ Mapping suggestions 2 for: dn | | | dn | | <input type="button" value="✓ Accept selected"/> ... |
| <input checked="" type="radio"/> | ● name-to-dn | name | Script | dn | | ... |
| <input type="radio"/> | ● name-to-dn | name | Script | dn | | ... |
| <input type="info"/> | Only one suggestion per dn can be applied. Others will be discarded upon accepting. | | | | | |
| <input type="checkbox"/> | ● personalNumber-to-employeeNumber | personalNumber | As is | employeeNumber | | <input type="button" value="✓ Accept"/> <input type="button" value="✗ Discard"/> ... |
| <input type="checkbox"/> | ● givenName-to-givenName | givenName | As is | givenName | | <input type="button" value="✓ Accept"/> <input type="button" value="✗ Discard"/> ... |
| <input type="checkbox"/> | ● locality-to-homePostalAddress | locality | As is | homePostalAddress | | <input type="button" value="✓ Accept"/> <input type="button" value="✗ Discard"/> ... |

7. Enable Provisioning to Target System (LDAP): Outbound Mappings

Outbound mappings generated, accepted and ready for simulation (Proposed).

| <input type="checkbox"/> Name ⓘ | MidPoint property | Expression ⓘ | Resource attribute * ⓘ | Lifecycle state ⓘ | ... |
|---|---|--|---|-----------------------|-----|
| <input type="checkbox"/> ● fullName-to-cn | <input type="text" value="fullName x"/> | As is | <input type="text" value="cn"/> | Proposed (simulation) | ... |
| <input type="checkbox"/> ● fullName-to-displayName | <input type="text" value="fullName x"/> | As is | <input type="text" value="displayName"/> | Proposed (simulation) | ... |
| <input type="checkbox"/> ● name-to-dn | <input type="text" value="name x"/> | ScriptAll set ✓ <input type="button" value="Show script"/> | <input type="text" value="dn"/> | Proposed (simulation) | ... |
| <input type="checkbox"/> ● personalNumber-to-employeeNumber | <input type="text" value="personalNumber x"/> | As is | <input type="text" value="employeeNumber"/> | Proposed (simulation) | ... |
| <input type="checkbox"/> ● givenName-to-givenName | <input type="text" value="givenName x"/> | As is | <input type="text" value="givenName"/> | Proposed (simulation) | ... |
| <input type="checkbox"/> ● locality-to-l | <input type="text" value="locality x"/> | As is | <input type="text" value="l"/> | Proposed (simulation) | ... |
| <input type="checkbox"/> ● familyName-to-sn | <input type="text" value="familyName x"/> | As is | <input type="text" value="sn"/> | Proposed (simulation) | ... |
| <input type="checkbox"/> ● title-to-title | <input type="text" value="title x"/> | ScriptAll set ✓ <input type="button" value="Show script"/> | <input type="text" value="title"/> | Proposed (simulation) | ... |
| <input type="checkbox"/> ○ name-to-uid | <input type="text" value="name x"/> | As is | <input type="text" value="uid"/> | Proposed (simulation) | ... |

7. Enable Provisioning to Target System (LDAP): Outbound Mappings

Attribute statistics may help you to create script expressions if needed.

NEW | MIDPILOT

| Value | Count | Percentage |
|------------------------------|-------|------------|
| Junior Consultant | 5 | 13.16% |
| Sales Representative | 4 | 10.53% |
| Agent Recruitment Specialist | 3 | 7.89% |
| Negotiation Specialist | 2 | 5.26% |
| Senior Consultant | 2 | 5.26% |

| Value | Count | Percentage |
|--|-------|------------|
| Junior Consultant (Example, Inc.) | 5 | 13.16% |
| Agent Recruitment Specialist (Example, Inc.) | 3 | 7.89% |
| Sales Representative (Example, Inc.) | 3 | 7.89% |
| Service Development Specialist (Example, Inc.) | 2 | 5.26% |
| Senior Consultant (Example, Inc.) | 2 | 5.26% |

title-to-title title × Script All set ✓ Show script title Proposed (simulation) Edit Duplicate Change mapping name Resource statistics MidPoint statistics Delete

7. Enable Provisioning to Target System (LDAP): Outbound Mappings

Outbound mapping scripts generated by AI (including descriptions)

| <input type="checkbox"/> | Name ⓘ | MidPoint property | Expression ⓘ | Resource attribute * ⓘ | Lifecycle state ⓘ | ... |
|--------------------------|----------------|------------------------------------|------------------------------|------------------------|-----------------------|-----|
| <input type="checkbox"/> | name-to-dn | <input type="text" value="name"/> | Script All set ✓ Show script | dn | Proposed (simulation) | ... |
| <input type="checkbox"/> | title-to-title | <input type="text" value="title"/> | Script All set ✓ Show script | title | Proposed (simulation) | ... |

Description

Compose DN: uid=<name>,ou=users,dc=example,dc=com

Language

Groovy (default)

Code

```
1 basic.composeDnWithSuffix('uid', name, 'ou=users,dc=example,dc=com')
```

Description

Append company suffix to title

Language

Groovy (default)

Code

```
1 // Append company suffix to title
2 title ? title + " (Example, Inc.)" : title
```

7. Enable Provisioning to Target System (LDAP): Outbound Credentials + Activation Mappings

Employee accounts / Credentials

Credentials configuration

Map credentials from your source to midPoint (Inbound mappings) and from midPoint to your target (Outbound mappings). This allows you to synchronize passwords between midPoint and resources.

→ Inbound 0

↔ Outbound 2

Proposed (simulation) ▾



initial-password-generate
Mapping is weak and use
Generate evaluator

Settings

Remove

Proposed (simulation) ▾



password-change
Mapping is normal and use As
is evaluator

Settings

Remove

Add outbound

Employee accounts / Activation

Activation configuration

Map activation data from your source to midPoint (Inbound mappings) and from midPoint to your target (Outbound mappings). This allows you to synchronize object status details between midPoint and resources and manage object lifecycle situations.

→ Inbound 0

↔ Outbound 3

Proposed (simulation) ▾



Administrative status
Mapping is normal and use As
is evaluator

Settings

Remove

Proposed (simulation) ▾



Disable instead of delete
Instead of deleting the user
changes its state to
"Disabled"

Settings

Remove

Proposed (simulation) ▾



Delayed delete
Definitively deletes the user
within the specified
timeframe

Settings

Remove

Add outbound

7. Enable Provisioning to Target System (LDAP): Reconciliation – Simulation

Simulation result

[← Back to object type wizard](#) [View processed objects](#)

Simulation task details

| | |
|--------------------|--|
| Start timestamp | May 4, 2026, 3:59:19 PM UTC |
| End timestamp | May 4, 2026, 3:59:22 PM UTC |
| Finished in | 2 seconds |
| Task | Preview of Reconciliation: LDAP: User accounts |
| Status | Finished |
| Configuration | Development |
| Added objects | 0 |
| Deleted objects | 0 |
| Modified objects | 10 |
| Unmodified objects | 104 |

Event marks

| | | | | | | | |
|-----------------------------|---|-----------------------------------|---|-------------------------------|---|--------------------------------|---|
| Focus activated | 0 | Focus deactivated | 0 | Focus renamed | 0 | Focus assignments changed | 0 |
| Focus archetype changed | 0 | Focus parent organization referer | 0 | Focus role membership changed | 0 | Projection activated | 0 |
| Projection deactivated | 0 | Projection renamed | 0 | Projection identifier changed | 0 | Projection entitlement changed | 0 |
| Projection password changed | 0 | Resource object affected | 5 | | | | |

[More info](#)

7. Enable Provisioning to Target System (LDAP): Reconciliation – Simulation

Review changes; some are actually corrections of low quality data.

Modify Shadow uid=ejones27,ou=users,dc=example,dc=com

Modify Employee accounts **attributes**

| Item ↓ | Old value | New value |
|--------|-------------|--------------|
| cn | ✖ Ema Jones | ✔ Emma Jones |

Modify Shadow uid=afreeman,ou=users,dc=example,dc=com

Modify User accounts **attributes**

| Item ↓ | Old value | New value |
|-------------|----------------|--|
| title | ✖ Sales Rep. | ✔ Sales Representative (Example, Inc.) |
| cn | ✖ Alex Freeman | ✔ Alexander Freeman |
| givenName | ✖ Alex | ✔ Alexander |
| displayName | ✖ Alex Freeman | ✔ Alexander Freeman |

Real Life Scenario: Simulation Saved the Day Again

Review changes; some could be **very dangerous!** Here, all account passwords would be changed.

| | | | |
|--|--|------------------------------------|-------------------------------------|
| Focus activated 0 | Focus deactivated 0 | Focus renamed 0 | Focus assignments changed 0 |
| Focus archetype changed 0 | Focus parent organization referenc 0 | Focus role membership changed 0 | Projection activated 0 |
| Projection deactivated 0 | Projection renamed 0 | Projection identifier changed 0 | Projection entitlement changed 0 |
| Projection password changed 38 More info | Resource object affected 38 More info | | |





Real Life Scenario: Simulation Saved the Day Again






Review changes; some could be **very dangerous!** Here, all account passwords would be changed.







7. Enable Provisioning to Target System (LDAP): Reconciliation

- Review data inconsistencies detected by simulations and decide:
 - Update mappings (e.g. mapping expressions depending on specific users, etc.)
 - Use marks to make exceptions for specific data (to temporarily ignore certain accounts)
 - Let midPoint update target system data

Audit Log Viewer Audit Log Viewer  

Time  3/27/26, 12:00 AM   More...  Basic 

| Time | Initiator | Event Stage | Event Type | Target | Target owner | Channel | Outcome |
|--------------------------|---------------|-------------|---|---|--------------|----------------|---------|
| 2026-03-27T11:34:29.662Z | administrator | Request |  Synchronization | alopez | | Reconciliation | |
| 2026-03-27T11:34:29.064Z | administrator | Execution |  Synchronization | afreeman | | Reconciliation | Success |
| 2026-03-27T11:34:28.939Z | administrator | Resource |  Modify object | uid=afreeman,ou=users,dc=example,dc=com | | Reconciliation | Success |
| 2026-03-27T11:34:28.541Z | administrator | Request |  Synchronization | afreeman | | Reconciliation | |

8. Automate Integration

- Automate Source (HR) → Target (LDAP) provisioning (Joiners – Movers - Leavers)
- Deactivate username inbound mappings in both resources
- Turn on (or customize) the username generator in midPoint for all Person users
- **Suspend the legacy on-boarding/provisioning processes for Target system**
- Schedule reconciliation with Source system
- **Person archetype aggregates all birthright accesses for new users**



8. Automate Integration – Add Birthrights Inducements to Person Archetype

Use case: “Every Person should have access to LDAP (account only)”.

Select application resource

Select resource in which your role will manage access to the application.

Application resource

Name More... Basic

| Name | Description |
|------|-------------|
| HR | |
| LDAP | |

Rows per page 20 1 to 2 of 2 << < 1 > >>

Select resource object type

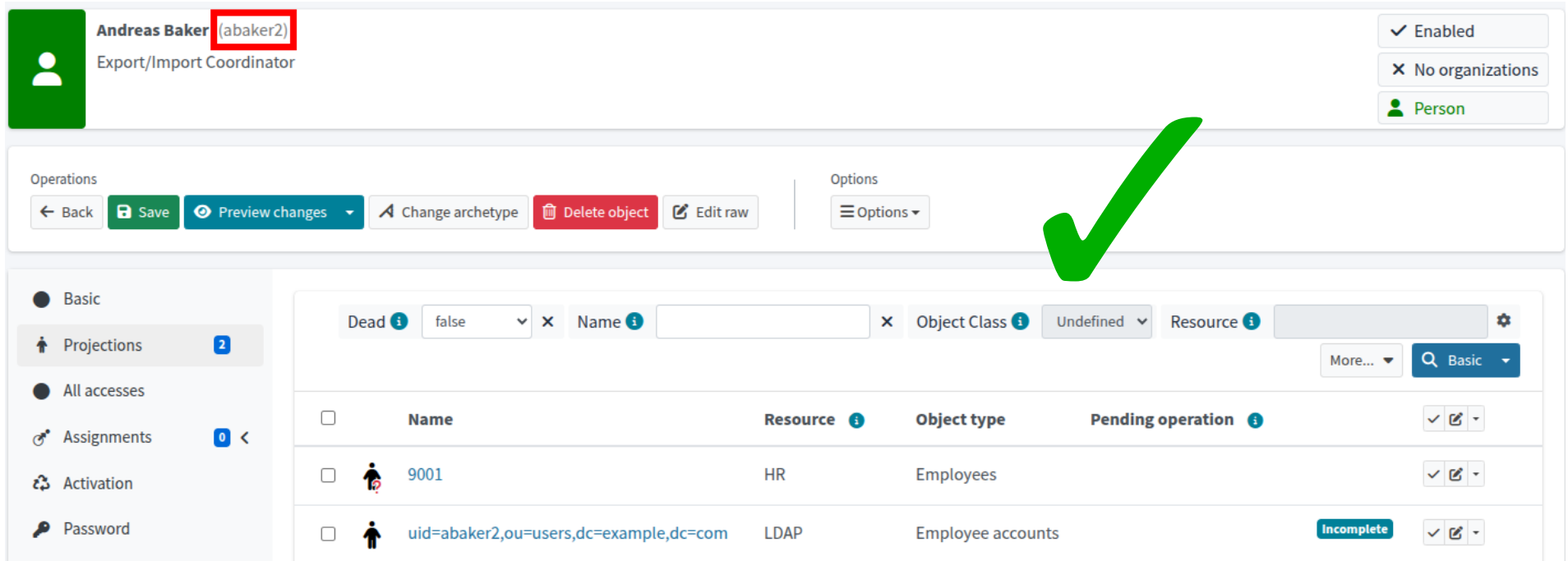
Select type of object your role will create or modify on the resource.



User accounts
Regular user accounts located under
ou=users,dc=example,dc=com

8. Automate Integration – Person Birthrights In Action

Result: Every Person has an account in LDAP (and unique usernames in midPoint and LDAP, too).



Andreas Baker (abaker2)
Export/Import Coordinator

Operations: Back, Save, Preview changes, Change archetype, Delete object, Edit raw

Options: Options

Dead: false, Name: [], Object Class: Undefined, Resource: []

More... Basic


| Name | Resource | Object type | Pending operation |
|--|----------|-------------------|-------------------|
| 9001 | HR | Employees | |
| uid=abaker2,ou=users,dc=example,dc=com | LDAP | Employee accounts | Incomplete |

9. Override Incorrect Data

- MidPoint trusts data in Source system and behaves accordingly
- If source data is incorrect, midPoint can temporarily override it
- Examples:
 - Forcing deactivation of incorrectly enabled users
 - Forcing incorrect data override using “Invalid Data” mark
 - Username change

Accounts Employees Active (production) Configure Tasks

Name Situation

| <input type="checkbox"/> | Name | Identifiers | Situation | Owner |
|--------------------------|--|--------------|-----------|-------|
| <input type="checkbox"/> | 9006  | empnum: 9006 | LINKED | jdoe |

9. Override Incorrect Data – HR Data Overridden by MidPoint (“Invalid Data” Mark)

Result: The user can be corrected in midPoint until HR fixes their data

Employee Number

First Name

Surname

Employee Type

Job Title

Status

Locality

John Doe (jdoe)
CXO

✓ Enabled
✗ No organizations
Person

Operations

← Back Change archetype

Options

Options ▾

Basic

- Projections 2
- All accesses
- Assignments 0 <
- Activation
- Password
- OTP 0
- History
- Cases 0
- Personas 0
- Delegations 0
- Delegated to me 0

Properties

Name jdoe

Lifecycle state **Active (production)**

Full name John Doe

Given name John

Family name Doe

Title CXO

Personal Number 9006

Locality **Fast River City**

Run Another Iteration

- Evaluate the results of the iteration vs expectations
- Improve the solution
 - Add handling for additional source/target attributes
 - Add more object types
- Add more resources
- Extend the solution using methodology extensions
- Remember: **Connect, clean-up, automate**



Methodology Extension for Entitlement Management

- The First Steps Methodology was originally designed with a focus on users and their accounts
- However, it is not limited to them and has since been extended for entitlement (group) management: Group Synchronization methodology
- The methodology outlines the systematic approach for addressing other follow-up challenges beyond user/account management
- Docs: [Group synchronization methodology](#) (expect updates for midPoint 4.11)
- Set your course to IGA



Work In Progress (Planned Improvements & Extensions in 2026)

- More secure scripting language
[MidPoint Expression Language](#)
- Rapid application onboarding using no-code/low-code connectors for read operations combined with manual ITSM connectors for write operations **NEW | MIDPILOT**
 - Create connectors using [AI connector generator service](#)
- Corrections and improvements based on testing and (your) feedback
 - Do not hesitate to provide opinions



Work In Progress: (Single) Mapping Simulation

Simulation of a specific *single* mapping (works even with *unsaved* mappings!) Useful for testing before saving.

There are *limitations* though (currently only inbounds; normal mappings simulated as strong, no other mappings are evaluated, ...)

The screenshot shows a web interface for managing mappings. At the top, there are two tabs: "Inbound mappings (to MidPoint)" and "Outbound mappings (to Resource)". Below the tabs, there is a legend indicating that purple dots represent AI-powered suggestions and blue dots represent system suggestions. A search bar and a "Search" button are also present. The main area displays a table of mappings with columns for Name, Resource attribute, Expression, MidPoint property, and Lifecycle state. Two mappings are visible: "uid-into-name" and "employeeNumber-to-personalNumber". A context menu is open over the second mapping, with the "Simulate mapping" option highlighted in red. Other options in the menu include Edit, Duplicate, Resource statistics, MidPoint statistics, and Delete. At the bottom left, there is an "Exit wizard" button, and at the bottom right, there is an "Attribute over" button.

| Name | Resource attribute | Expression | MidPoint property | Lifecycle state |
|----------------------------------|--------------------|------------|-------------------|---------------------|
| uid-into-name | uid | As is | name | Active (production) |
| employeeNumber-to-personalNumber | employeeNumber | As is | personalNumber | Active (production) |

Work In Progress: (Single) Mapping Simulation


User accounts / Mappings / Simulation result

Simulation result

[← Back to mapping](#)


[View processed objects](#)

Simulated mapping: **uid-into-name** Source: uid → Target: name Strength: ● **strong**

Added attribute items ⓘ 

1

[View values](#)


Deleted attribute items ⓘ 

0

Modified ⓘ 

38

[View values](#)

Unchanged attribute items ⓘ 

0

Total processed ⓘ 

39

[View values](#)

Event mark ⓘ Undefined ▾ State ⓘ Undefined ▾ × More... ▾ [Basic](#) ▾

Situation

^ Object

Changes

Details

Modified

panderson (Patrick Anderson)

1032 → panderson

Modified

rnelson (Robert Nelson)

1012 → rnelson

Added

test123

(empty) → test123

AI Service Configuration Alternatives

- Self-hosted (GPU)
- External service (OpenRouter, Google, OpenAI, AWS, ...)
- We are preparing Evolveum services



Conclusion

- We recommend our methodical approach to succeed with your midPoint deployments
- First Steps methodology: integrate the first source and target systems (**Connect, clean-up, automate**)
- Iterative, safe approach using simulations and marks
- Gradual migration to support business continuity
- **New configuration assistants** (AI/heuristics) to speed up the configuration
- The current **MidPoint Deployment: First Steps self-paced training** is [available free of charge for everyone](#)
- Trainings will be updated for midPoint 4.11
- See how you can [access our learning portal](#)



(Hopefully Not)

“

Before I came here
I was confused about this subject.
Having listened to your lecture
I am still confused. But on a higher level.

”

Enrico Fermi

Evolveum

Thank you for your attention

Feel free to ask your questions now!



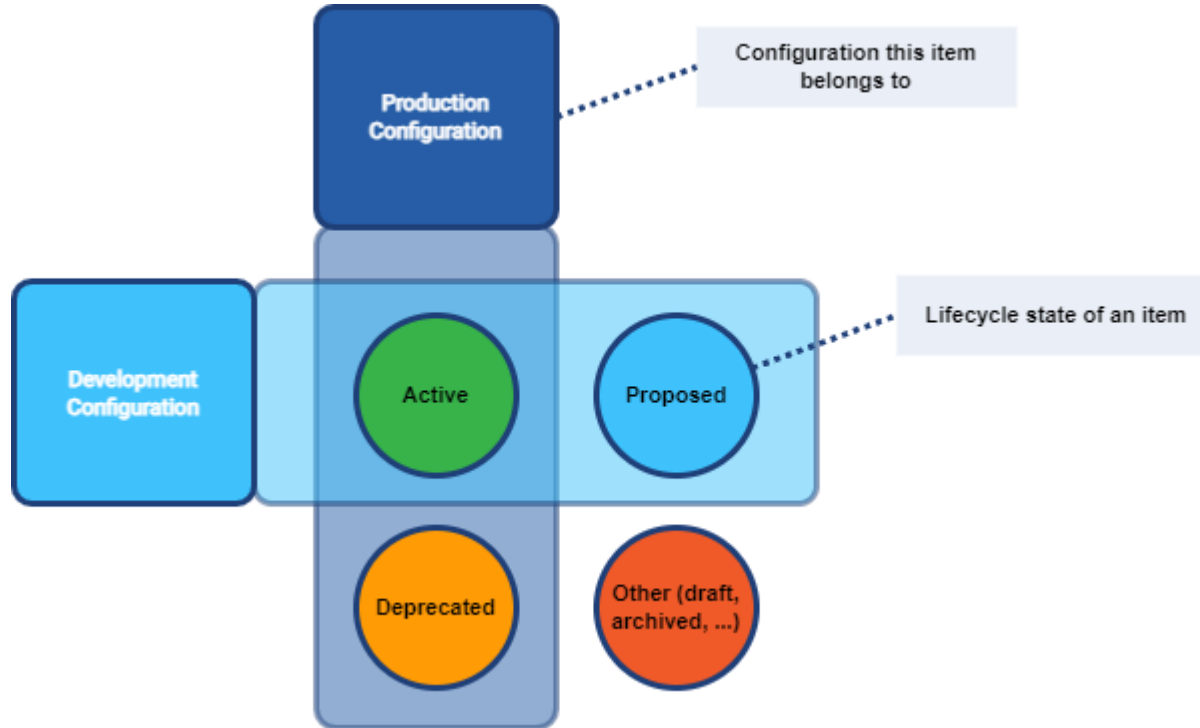
Funded by the
European Union
NextGenerationEU

[RECOVERY
AND RESILIENCE]
PLAN



2nd Annual
MidPoint Community Meetup

BONUS: Configuration Item Lifecycle and System Configurations



Docs: [Configuration Item Lifecycle and system Configurations](#)