



## **Teaser: MidPoint Deployment Intermediate Training**

Ivan Noris, 6/2024  
Expert Identity Engineer

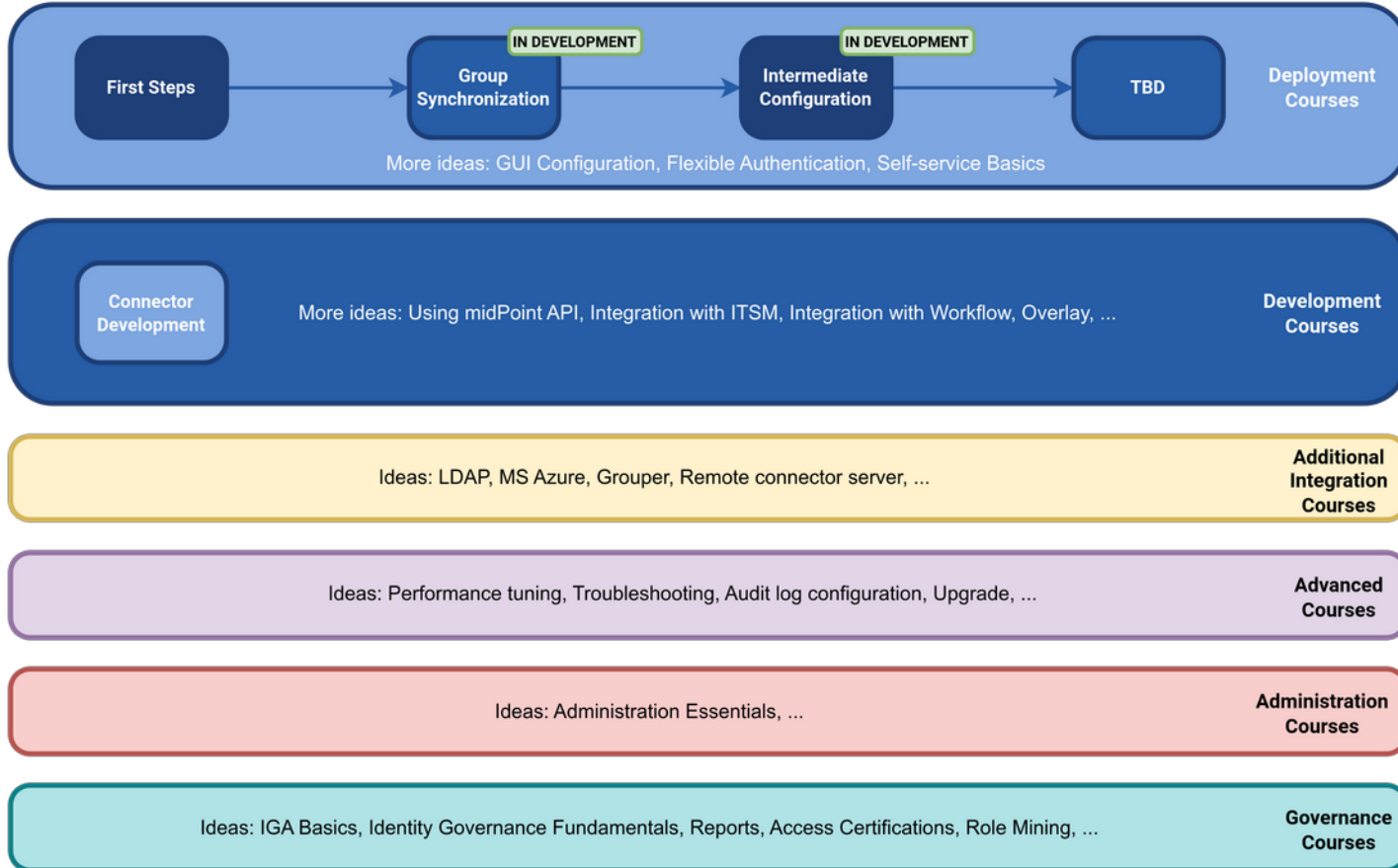
# Agenda

- Introducing Evolveum Training Curriculum (WIP)
- Introducing “Intermediate training”
- Training Preview (Live demo)
- Conclusion & Discussion



# Evolveum Training Curriculum (WIP)

Subject to change



## MidPoint Deployment: Intermediate Configuration Training Course Goals

- Extend the usage of “First Steps Methodology”
- Extend midPoint schema using schema extension and use it in mappings
- Configure midPoint to use multiple account types for provisioning of privileged accounts
- Learn MidPoint Query Language
- Learn MidPoint Object Language to describe midPoint objects (XML) and understand configuration from previous training(s)



## MidPoint Deployment: Intermediate Configuration Training Course Goals (2)

- Use MidPoint Studio to download, review and upload midPoint configuration
- Use MidPoint Studio to clean up configuration before storing it in Git
- Using midPoint Studio to compare and synchronize configuration objects between midPoint repository and midPoint project
- **Introduce streamlined support for midPoint deployment using GitOps**



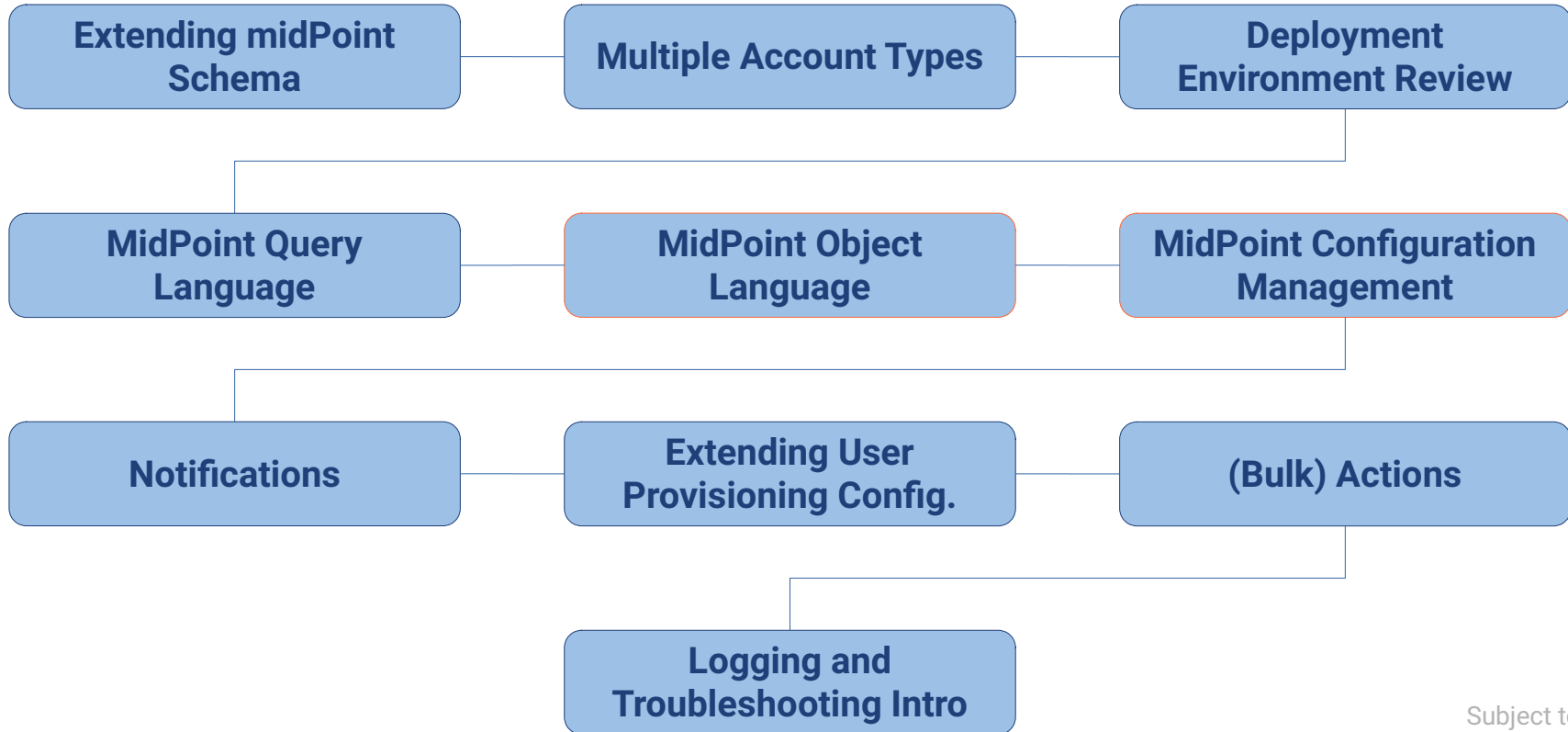
## MidPoint Deployment: Intermediate Configuration Training Course Goals (3)

- Configure and use e-mail notifications (including HTML and attachments)
- Introduce Live Synchronization
- Use (Bulk) Actions for bulk operations on midPoint data
- Use logging & tracing to troubleshoot midPoint configuration
- **MidPoint 4.9\***



\*) Screenshots in this presentation are based on midPoint 4.9-SNAPSHOT and MidPoint Studio 4.9.0-SNAPSHOT

# MidPoint Deployment: Intermediate Configuration Training Course Topics



Subject to change

# Would You Like Some Tea(ser)?

**TrainingSchemaExtension** (TrainingSchemaExtension)

Operations: [← Back](#) [Save](#) [Edit raw](#)

Schema extension in GUI!

Basic

Definitions 1

+ New definition

UserExtensionType

Name *	Type *	Display name	Order	Required	Indexed	
countryCode	String	Country Code	130	false	True	
country	String	Country	140	false	True	

+ New item

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

Definition settings

country-remove-prefix country - Script Show script → extension/country Active (production)

Evaluator value is set



# Would You Like Some Tea(ser)?

Display name	Kind <i>i</i>	Intent <i>i</i>	Default <i>i</i>	Description	Lifecycle state	
Normal Account	ACCOUNT		true		Active (production) <i>v</i>	<i>-</i> <i>+</i> <i>↕</i>
AD Group	ENTITLEMENT	adGroup	true		Active (production) <i>v</i>	<i>-</i> <i>+</i> <i>↕</i>

+ Add object type

Rows per page 20

- Delete
- Edit
- Duplicate**

Duplicating object type in GUI!

Testing assignment of role referring to a *proposed* object type using simulation

Alice Baker (abaker)

Operations

← Back Save Preview changes *v* Change archetype Delete object Edit raw Options

**Preview with development configuration**

- Basic
- Projections 2
- All accesses
- Assignments 0 *v*
- All
- Role
- Organization

	Name	Activation <i>i</i>	Relation	Identifier
<input type="checkbox"/>	Role which creates admin account in AD	enabled	Default	AD - admin account

# Would You Like Some Tea(ser)?










Advanced, yet readable search queries







extension/country = "Rocky State" and (givenName startsWith "D" or givenName startsWith "E")



Advanced



<input type="checkbox"/>	Name	Personal Number	Full name	Email	Accounts	
<input type="checkbox"/>	 diverson	1022	David Iverson		2	 
<input type="checkbox"/>	 ejones	1023	Ellen Jones		2	 
<input type="checkbox"/>	 emason	1008	Elisabeth Mason		2	 

Rows per page  1 to 3 of 3 << < 1 > >>

# Would You Like Some Tea(ser)?

Query item and filter completion (currently partial support in Studio)

```
<adminGuiConfiguration>  
  <objectCollectionViews>  
    <objectCollectionView>  
      <type>RoleType</type>  
      <collection>  
        <filter>  
          <q:text>  
name starts  
startsWith  
Press Enter to insert, Tab to replace Next Tip  
        </objectCollectionView>  
  </objectCollectionViews>  
</adminGuiConfiguration>
```

MidPoint Browse Objects Console Encrypted Properties

User MidPoint Query Raw

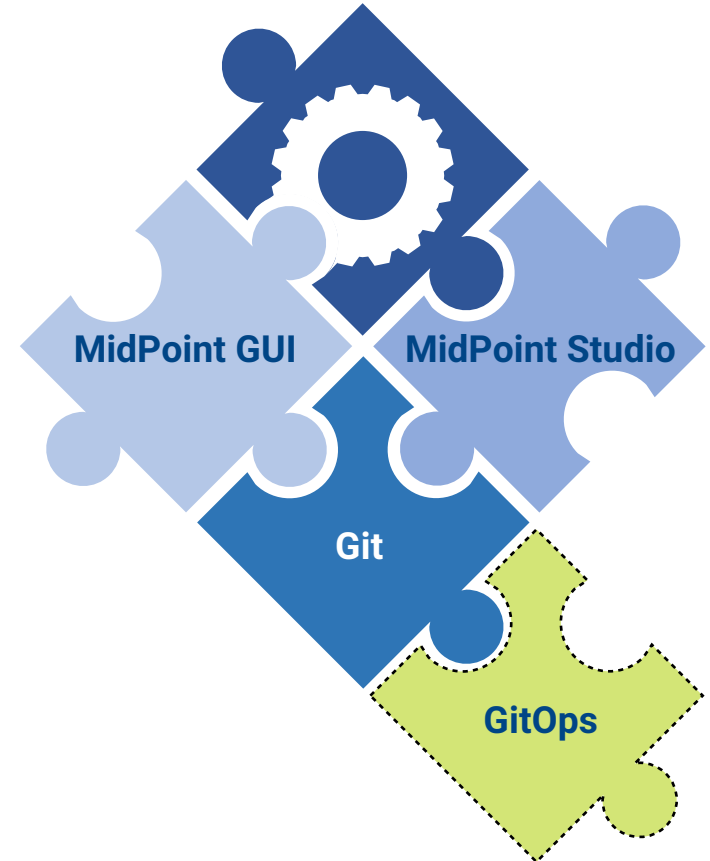
name = "Alice" and giv

givenName givenName

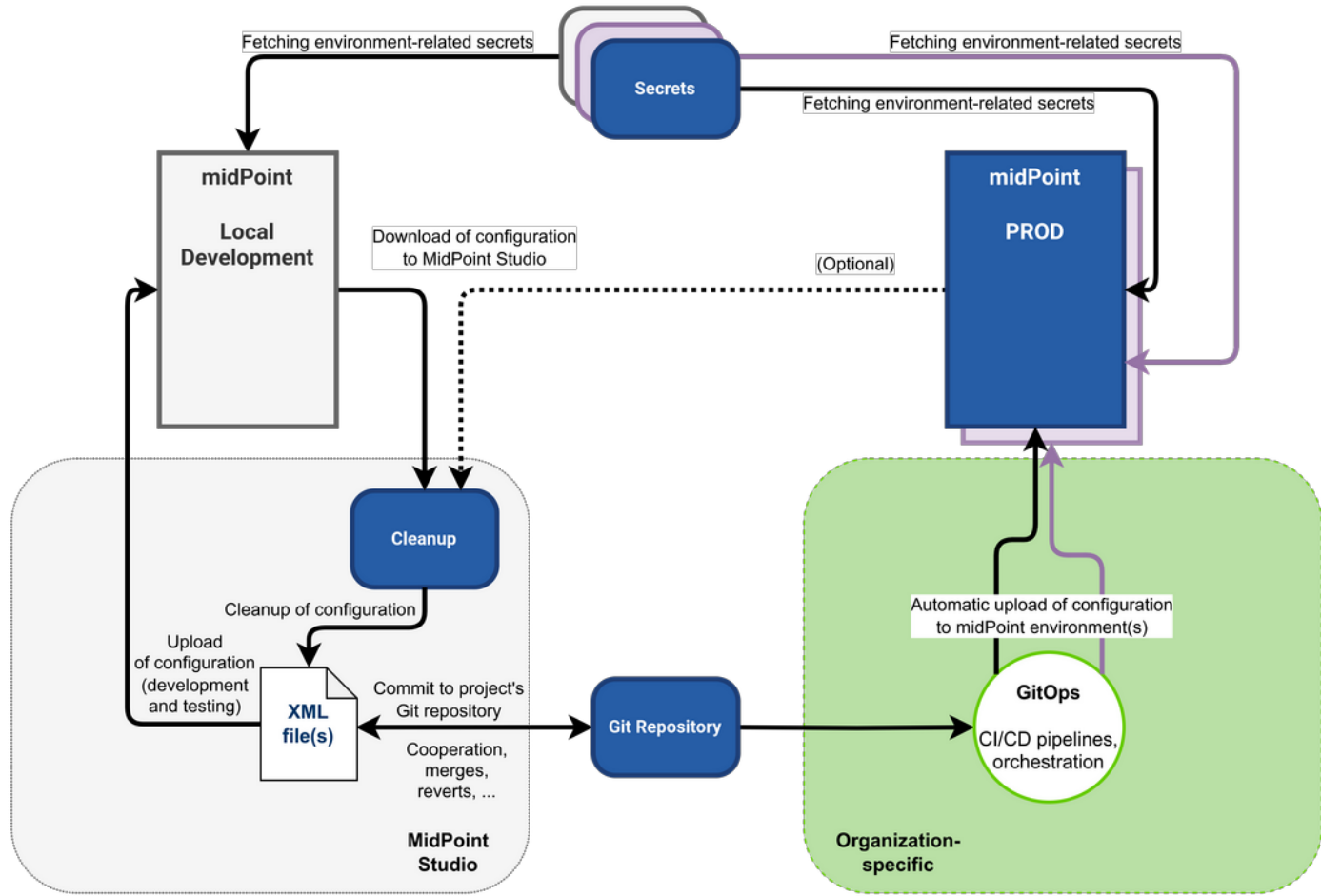
Press Ctrl+. to choose the selected (or first) suggestion and insert a dot afterwards Next Tip

## Streamlined Support for MidPoint Deployment Using GitOps

- MidPoint can be configured using XML (Studio) or GUI
- Configuration can be stored in Git repository
- Once cleaned, configuration can be uploaded to other environments using GitOps



# MidPoint Deployment Using GitOps



# Configuration Cleanup: Why & What

- Metadata & operational properties *usually* don't need to be stored in Git
  - Elements are marked as operational in midPoint schema
- Connector references based on connector oids are not portable
- Resource schema definition can be automatically fetched during “Test connection”, we don't need to store it in git
- Encrypted passwords are not portable
- Associations based on Shadow oids are not portable

Some examples for resource

```
1 <resource xmlns="http://midpoint.evolveum.com/xml/ns/public/common/common-3" xmlns:c="http://midpoint.evolveum.c
2 <name>AD</name>
3 <description>EXAMPLE, Inc. AD resource</description>
4 <metadata...>
9 <lifecycleState>active</lifecycleState>
10 <operationExecution id="74"...>
29 <iteration>0</iteration>
30 <iterationToken/>
31 <operationalState...>
37 <operationalStateHistory id="78"...>
43 <connectorRef oid="69c8dff3-72c3-4e88-a115-f9ce51c203f3" relation="org:default" type="c:ConnectorType">
44 <description>Reference to the ConnId LDAP connector. This is dynamic reference, it will be translated to
45   OID during import.
46   Only connector which is available is used (connector objects without existing JAR are ignored).
47 </description>
48 <filter>
49 <q:text>connectorType = "com.evolveum.polygon.connector.ldap.LdapConnector" and available = "true"</
50 </filter>
51 </connectorRef>
52 <connectorConfiguration xmlns:icfc="http://midpoint.evolveum.com/xml/ns/public/connector/icf-1/connector-sch
53 <schema>
54 < cachingMetadata>
55 < retrievalTimestamp>2024-05-28T12:33:32.622Z</retrievalTimestamp>
56 < serialNumber>1ce3f4d7406f3d34-bcbfd02f7ad2076d</serialNumber>
57 </ cachingMetadata>
58 < generationConstraints>
59 < generateObjectClass>ri:inetOrgPerson</generateObjectClass>
60 < generateObjectClass>ri:groupOfUniqueNames</generateObjectClass>
61 < generateObjectClass>ri:groupOfNames</generateObjectClass>
62 < generateObjectClass>ri:organizationalUnit</generateObjectClass>
63 </generationConstraints>
64 < definition>
65 < xsd:schema xmlns:a="http://prism.evolveum.com/xml/ns/public/annotation-3" xmlns:ra="http://midpoint
66 < xsd:import namespace="http://prism.evolveum.com/xml/ns/public/annotation-3"/>
67 < xsd:import namespace="http://midpoint.evolveum.com/xml/ns/public/resource/annotation-3"/>
68 < xsd:complexType name="groupOfNames">
69 < xsd:annotation>
70 < xsd:appinfo>
71 < a:container>true</a:container>
72 < ra:resourceObject>true</ra:resourceObject>
73 < ra:nativeObjectClass>groupOfNames</ra:nativeObjectClass>
74 < ra:default>false</ra:default>
75 < ra:auxiliary>false</ra:auxiliary>
76 < ra:namingAttribute>ri:dn</ra:namingAttribute>
77 < ra:displayNameAttribute>ri:dn</ra:displayNameAttribute>
```

## Configuration Cleanup: How

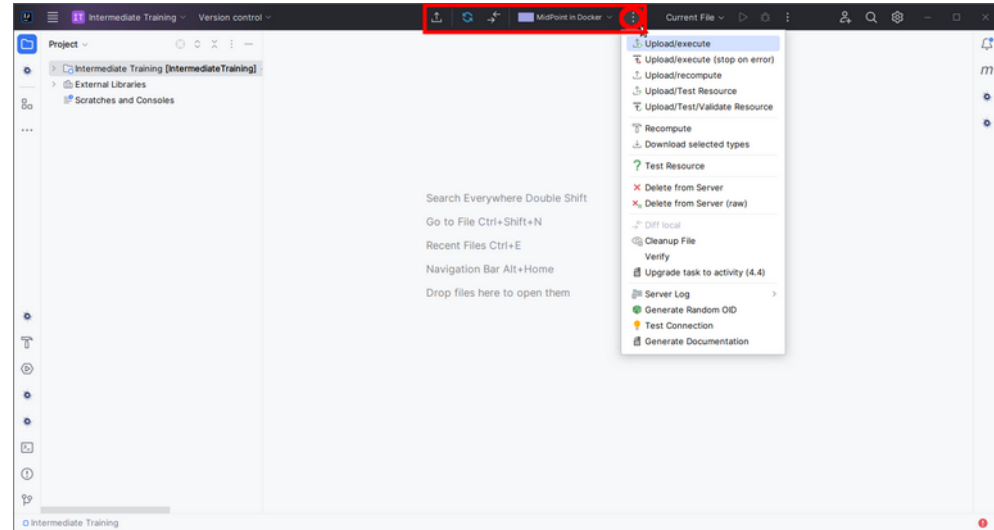
- MidPoint Studio allows to manage your configuration (upload, download, cleanup)
- Git will be used to store cleaned midPoint configuration
- GitOps can use Git contents to manage midPoint configuration in other environments



# MidPoint Studio Introduction in 60 Seconds

- IntelliJ IDEA plugin
- Uses midPoint REST API
- Multiple projects; multiple project environments
- Browse/search midPoint objects
- Download/upload midPoint objects
- Cleanup, Object Synchronization actions
- Bulk task creation “wizard”
- (IntelliJ IDEA: Git integration)

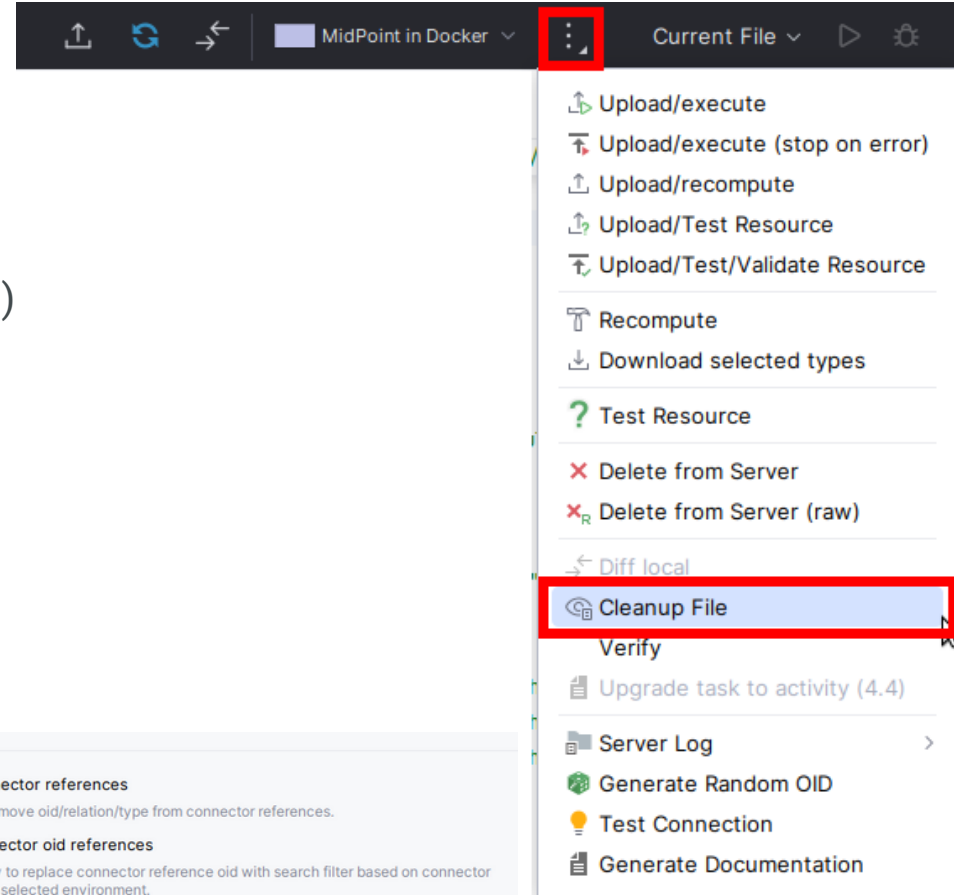
Docs: [MidPoint Studio](#)





# MidPoint Studio Cleanup

- One or multiple files at once
- Automatic actions (selectable; some with confirmation)
  - Metadata & operational properties
  - Resource schema definition
  - Connector references
  - Warnings for missing referenced objects + handling
- Additional cleanup actions (passwords, associations)



# Cleanup: Missing Referenced Objects

- Cleanup action can detect missing referenced objects (not downloaded in project)
- You can **download** all missing objects, or (more likely) you can **decide** which of them you want to download to project (**Configure missing...**)
- Typically you don't want to download unchanged midPoint built-in objects

The screenshot displays two panels from a software application. The top panel, titled 'Cleanup File' (15:19), shows the results of a cleanup operation: 'Cleanup File finished.', 'Processed: 1 objects', 'Skipped: 0 objects', 'Failed to process: 0 objects', 'Processed files: 1', and 'Skipped files: 0'. Below this text are two buttons: 'Configure missing...' (highlighted with a red box) and 'Download missing'. The bottom panel, titled 'Cleanup warning' (15:19), lists 'Cleanup warnings for object 'SystemConfiguration':' followed by several 'Unresolved reference (locally):' entries with long alphanumeric IDs and '(ArchetypeType)'. Overlaid on the bottom right is a 'Missing references configuration' dialog box. This dialog has a table with two columns: 'Reference' and 'Action'. The 'Reference' column lists various system configuration items, and the 'Action' column shows 'Ignore' or 'Download' for each. The 'Default Security Policy (restricted special characters) (Security policy)' is highlighted with a blue selection bar and has 'Download' selected in the 'Action' column. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Reference	Action
All	Ignore
System configuration	Ignore
SystemConfiguration (System configuration)	Ignore
Default Security Policy (restricted special characters) (Security policy)	Download
My cases (Object collection)	Ignore
Manual provisioning case (Archetype)	Ignore
Operation request (Archetype)	Ignore
Approval case (Archetype)	Ignore
Correlation case (Archetype)	Ignore
Reconciliation task (Archetype)	Ignore
Recomputation task (Archetype)	Ignore
Import task (Archetype)	Ignore
Live synchronization task (Archetype)	Ignore
Asynchronous update task (Archetype)	Ignore
Cleanup task (Archetype)	Ignore
Report tasks (Object collection)	Ignore
Single bulk action task (Archetype)	Ignore
Iterative bulk action task (Archetype)	Ignore
Report import task (Archetype)	Ignore

## Cleanup: Association

```
<association id="6">
  <ref>ri:adGroup</ref>
  <outbound>
    <strength>strong</strength>
    <expression>
      <value xsi:type="c:ShadowAssociationValueType">
        <shadowRef oid="8fd4e525-b6f8-49e9-8b9e-9e140def7d6b" type="c:ShadowType"/>
      </value>
    </expression>
  </outbound>
</association>
```

Role-like object

```
<association id="6">
  <ref>ri:adGroup</ref>
  <outbound>
    <strength>strong</strength>
    <expression>
      <associationTargetSearch>
        <filter>
          <q:text>
            attributes/dn = "cn=all-users,ou=groups,dc=example,dc=com"
          </q:text>
        </filter>
        <searchStrategy>onResourceIfNeeded</searchStrategy>
      </associationTargetSearch>
    </expression>
  </outbound>
</association>
```

Resource

## Cleanup: Passwords (From Encrypted Passwords...)

```
<cfg:bindPassword>
  <t:encryptedData>
    <t:encryptionMethod>
      <t:algorithm xmlns="http://prism.evolveum.com/xml/ns/public/types-3">http://www.w3.org/2001/04/xmlenc#aes256-cbc</t:algorithm>
    </t:encryptionMethod>
    <t:keyInfo>
      <t:keyName>aY7PzKsf66rq10PMYA20p7bVebg=</t:keyName>
    </t:keyInfo>
    <t:cipherData>
      <t:cipherValue>6RmRqz7/fCtzqfEhHn8NyQNVGiSLccPFthM1h9jT2w=</t:cipherValue>
    </t:cipherData>
  </t:encryptedData>
</cfg:bindPassword>
```

Resource

## Cleanup: Passwords (... To Docker Secrets)

```
<cfg:bindPassword>  
  <t:externalData>  
    <t:provider>my-docker-secrets</t:provider>  
    <t:key>ad_password</t:key>  
  </t:externalData>  
</cfg:bindPassword>
```

Resource

```
<secretsProviders>  
  <docker>  
    <identifier>my-docker-secrets</identifier>  
    <description>Allow accessing docker secrets. Debug:  
      com.evolveum.midpoint.common.secrets TRACE/DEBUG</description>  
    <cache>PT30M</cache>  
    <display>  
      <label>Docker secrets</label>  
      <icon>  
        <cssClass>fa fa-play</cssClass>  
      </icon>  
    </display>  
  </docker>  
</secretsProviders>
```

SystemConfiguration

Bind password ⓘ

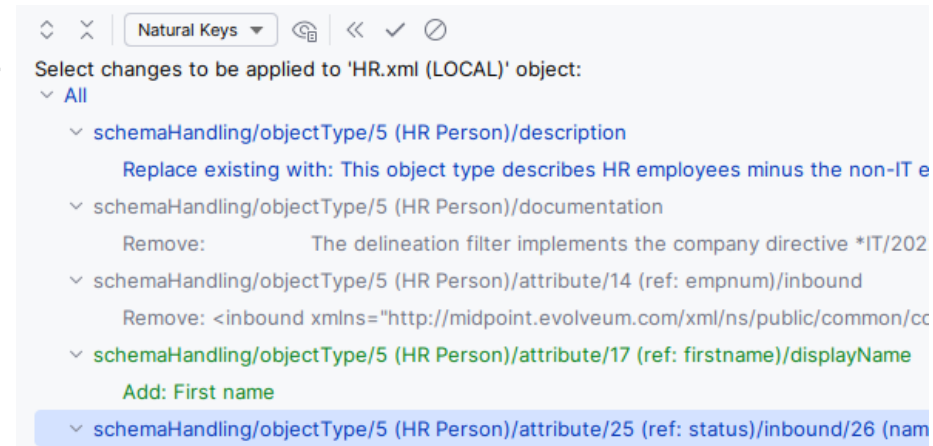
- Use clear value
- Use secret provider

Docker secrets ▼ ad\_password

Select provider and insert key value where password is stored

# Object Synchronization

- *A long time ago in a galaxy far, far away...* we used to manage configuration in Studio and always uploaded it to midPoint
- Then **First Steps methodology** came: use GUI for whatever you can to make midPoint your best friend
- Sooner or later, configuration will need to be managed in both midPoint GUI and Studio (XML)
- Upload-only or download-only decision may not be always possible
- Synchronize Objects action in MidPoint Studio has been developed to help engineers
  - Replaces the original “Remote Diff” action



# Object Synchronization

The screenshot displays the Evolveum Object Synchronization interface. At the top left, a red box highlights the file selection area, showing a checkbox and the file name "HR.xml (HR) (Pending: remote)".

The main area is titled "Select changes to be applied to 'HR.xml (LOCAL)' object:". It lists several changes under the "All" category:

- schemaHandling/objectType/5 (HR Person)/description: Replace existing with: This object type describes HR employees minus the non-IT employees which are excluded from midPoint processing using the classification query based on...
- schemaHandling/objectType/5 (HR Person)/documentation: Remove: The delineation filter implements the company directive \*IT/2022-119\*.
- schemaHandling/objectType/5 (HR Person)/attribute/14 (ref: empnum)/inbound: Remove: <inbound xmlns="http://midpoint.evolveum.com/xml/ns/public/common/common-3" xmlns:c="http://midpoint.evolveum.com/xml/ns/public/common/common-3" xmlns:...
- schemaHandling/objectType/5 (HR Person)/attribute/17 (ref: firstname)/displayName: Add: First name
- schemaHandling/objectType/5 (HR Person)/attribute/25 (ref: status)/inbound/26 (name: status-to-lifecycle-state)/expression: Expression: ScriptExpressionEvaluatorType
- schemaHandling/objectType/5 (HR Person)/attribute/32 (ref: job)/inbound/36 (name: job-to-title-nice)/expression: ...

At the bottom, a side-by-side diff viewer is shown, comparing the "Before" and "After" states of the XML. The "After" state shows a change in the script expression, where the 'Former employee' case is now 'archived' instead of 'archived' (the text is identical in the image, but the context suggests a change in the script logic). The diff viewer includes a "Differences ignored" button and a "Highlight words" dropdown.

At the bottom left, there are "Save local" and "Update remote" buttons. At the bottom center, there are "Object Delta" and "Text" tabs.

# Intermediate Training Preview – Live Demo

midPoint 4.9-SNAPSHOT  
MidPoint Studio 4.9.0-SNAPSHOT

The demo is based on “Intermediate Training” (in development).  
Some configuration has been prepared in advance.



## Conclusion

- Intermediate training will extend your midPoint knowledge and allows to streamline support for midPoint deployment using GitOps
- Training will use midPoint / MidPoint Studio 4.9
- “Group Synchronization” training is being developed as well (midPoint 4.9)



# Thank you for your attention

Do you have any **questions**? Feel free to contact us at [info@evolveum.com](mailto:info@evolveum.com)

**Follow us** on social media or **join us** at GitHub or Gitter!



/Evolveum



@Evolveum



/Evolveum



/Evolveum



/Evolveum

**Evolveum**

© 2024 Evolveum s.r.o. All rights reserved.

# Zoom Poll