



MidPoint Deployment: First Steps [MID301]

Student Lab Guide - Module 8

Evolveum, s.r.o.

Revision 4.8-LTS-A.01, 2023-11-06

This lab guide is not a standalone document and should be used only for the purpose of this training. If there are any questions during the course related to the content of the training or this lab guide itself, do not hesitate to ask the instructor.

If there are any errors, typos or typographic convention mistakes, please report them to the instructor as well. Thank you.

All labs were tested with the midPoint version used during the training.

We assume you have already installed the prerequisites before this training (if there were any).

Disclaimer

The names, organizations and places portrayed in this training course are fictitious. No identification with actual persons (living or deceased), organizations, places or events is intended or should be inferred.

Table of Contents

Module 8: Automating Integration **3**

LAB 8-1: Generate Usernames in midPoint 3

LAB 8-2: Automate Active Directory Account Creation For All Persons 9

LAB 8-3: Automate Active Directory Group Membership For All Persons 12

LAB 8-4: Enforcing AD Account Data 16

LAB 8-5: Handling HR Data Updates 20

LAB 8-6: Handling Long-term Leave 21

LAB 8-7: Handling Leavers 23

LAB 8-8: Adding A New Outbound Mapping 26

LAB 8-9: Adding New Attribute Provisioning From HR to AD 29

LAB 8-10: Exchanging Inbound Mapping 32

Module 8: Automating Integration

LAB 8-1: Generate Usernames in midPoint

Estimated Time: 15 min.

In this lab, we will turn on midPoint username generator and start using it instead of using user's employee number from HR or existing AD username.

We will switch off the existing configuration first.

In your browser with midPoint:

1. go to **Resources** › **All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. click **Configure**, then **Mappings** tile
 - a. edit inbound mapping **empnum-to-name** using **Edit** and set:
 - i. change **Lifecycle state** to: **Archived** to disable it
5. click **Save mappings**
6. click **Back** to get to the list of resources
7. edit **AD** resource
8. click **Accounts** menu item
9. click **Configure**, then **Mappings** tile
 - a. for the inbound mapping **mapping-inbound-username-to-name-for-import**:
 - i. change **Lifecycle state** to: **Archived** to disable it
10. click **Save mappings**



We use **Archived** lifecycle state to indicate that the mapping is unlikely to be active again. For temporary mapping deactivation you may use **Suspended** lifecycle state. Both states (and also **Draft**) represent deactivated mappings, but we have those three states to express different reasons for mapping deactivation.

Now we will use object template to generate the username instead.

1. go to **Object templates** › **All object templates**
2. click **Person Object Template**

3. click **Mappings** menu item
 - a. for the mapping **generate-name-jsmith-8-2**, set the following attributes:
 - i. **Lifecycle state**: switch to **Active (production)**
4. click **Save**

The **Person Object Template** is used for all users with **Person** archetype. It is part of midPoint built-in objects. We have been actually using almost from the beginning of the course to generate users' full names.



We are setting the mapping's lifecycle state directly to **Active**, without first going through the simulations. We can afford this in this particular case as there is no automatic synchronization with HR yet and this mapping won't affect any existing users in midPoint (**weak** strength).

We will still use simulations before creating the users.

We will create new test users in HR application.

In your browser with HR application:

1. click **Register user** and fill in the following attributes:
 - a. **First name**: **Louise**
 - b. **Surname**: **Callahan**
 - c. **Employee number**: **9000**
 - d. **Locality**: **White Stone City**
 - e. **Job**: **222#Export/Import Coordinator**
 - f. **EmpType**: select/keep **FTE**
 - g. **Status**: select/keep **In**
 - h. click **Register user**
2. click **Register user** and fill in the following attributes:
 - a. **First name**: **Andreas**
 - b. **Surname**: **Baker**
 - c. **Employee number**: **9001**
 - d. **Locality**: **White Stone City**
 - e. **Job**: **222#Export/Import Coordinator**
 - f. **EmpType**: select/keep **FTE**
 - g. **Status**: select/keep **In**

- h. click **Register user**
3. click **Register user** and fill in the following attributes:
 - a. **First name:** **Clara**
 - b. **Surname:** **Whiteherring**
 - c. **Employee number:** **9002**
 - d. **Locality:** **White Stone City**
 - e. **Job:** **222#Export/Import Coordinator**
 - f. **EmpType:** select/keep **FTE**
 - g. **Status:** select/keep **In**
 - h. click **Register user**
4. click **Register user** and fill in the following attributes (this user will have the same First name and Surname as the previous one):
 - a. **First name:** **Clara**
 - b. **Surname:** **Whiteherring**
 - c. **Employee number:** **9003**
 - d. **Locality:** **White Stone City**
 - e. **Job:** **222#Export/Import Coordinator**
 - f. **EmpType:** select/keep **FTE**
 - g. **Status:** select/keep **In**
 - h. click **Register user**
5. click **Register user** and fill in the following attributes:
 - a. **First name:** **Jacques**
 - b. **Surname:** **Smith**
 - c. **Employee number:** **9004**
 - d. **Locality:** **White Stone City**
 - e. **Job:** **222#Export/Import Coordinator**
 - f. **EmpType:** select/keep **FTE**
 - g. **Status:** select/keep **In**
 - h. click **Register user**
6. click **Export users to csv file**

In your browser with midPoint:

1. go to **Resources > All resources**

2. edit **HR** resource
3. click **Accounts** menu item
4. click **Reload** to reload the list of accounts from HR application CSV export file (midPoint is not aware of them as there is no automatic synchronization (yet))
5. search for accounts having **90** in **Name** field (or scroll to the last page of accounts)
6. click context menu for account **9000** and select **Import preview**
7. in **Select task execution mode** select: **Simulated production** and click **Select**



Simulated production mode will evaluate all **Active** (and **Deprecated**) configuration items, but there will be no permanent effects on data; we are only simulating.

8. midPoint will display information about new user **lcallaha** (and not **9000**) which would be created
9. click **Back**
10. click context menu for account **9001** and select **Import preview**
11. in **Select task execution mode** select: **Simulated production** and click **Select**



Simulated production mode will evaluate all **Active** (and **Deprecated**) configuration items, but there will be no permanent effects on data; we are only simulating.

12. midPoint will display information about new user **abaker2** (and not **9001**) which would be created (midPoint appends a number **2** because **abaker** user already exists in midPoint)
13. click **Back**

The username generator looks good! Let's create a scheduled reconciliation with HR.

1. click **Tasks**, then click **Create task** item in the context menu to open a simple task creation wizard for HR accounts
 - a. click **Reconciliation Task** tile
 - b. keep **Simulate task** value **OFF**
 - c. click **Create task** and fill in the following details:
 - i. **Name: HR Reconciliation**
 - d. click **Next: Resource objects**
 - e. click **Next: Schedule**
 - f. in **Schedule** page, set the following:
 - i. Set **Interval: 60** (seconds)

- g. click **Next: Distribution**
- h. click **Save & Run**
2. go to **Users > Persons** and check the new users (no AD accounts have been created for them yet)
3. to display only those users, you may want to use midPoint's query language:
 - a. in search panel above the user list, click ▼ and select **Advanced**
 - b. paste the following query to the input box:

```
personalNumber startsWith "900"
```

- c. click **Advanced** to apply the query
4. the resulting users should match the information in the following table:

HR empnum / midPoint personalNumber	midPoint username	midPoint fullName	Notes
9000	lcallaha	Louise Callahan	No uniqueness issues
9001	abaker2	Andreas Baker	Iterated, because abaker (Alice Baker) already exists
9002	cwhitehe2	Clara Whiteherring	Iterated, because cwhitehe (Charles Whitehead) already exists
9003	cwhitehe3	Clara Whiteherring	Iterated, because cwhitehe (Charles Whitehead) and cwhitehe2 (Clara Whiteherring) already exist
9004	jsmith3	Jacques Smith	Iterated, because jsmith (John Smith) and jsmith2 (Joseph Smith) already exist

5. to switch to basic search and stop using the query, click ▼ and select **Basic** in the search panel
6. go to **Audit Log Viewer** and check what the reconciliation tasks did

- a. look for **Event type: Add object** operations for **Channel: Reconciliation**



The username generator in **Person Object Template** generates values usable as Active Directory **sAMAccountName** values (strings shorter than 20 characters).

The reconciliation task is scheduled and will look for new/updated data in HR resource each minute.

LAB 8-2: Automate Active Directory Account Creation For All Persons

Estimated Time: 10 min.

In this lab, we will configure midPoint to create AD accounts automatically.

In most cases, midPoint roles and/or organizations are used for provisioning, but we have no roles yet. On the other hand, we have already assigned **Person** archetype automatically to each user created from HR resource. We will use **Person** archetype to create AD accounts as a *birthright* of each user created from HR data.

In your browser with midPoint:



1. go to **Archetypes** › **All archetypes**
2. edit **Person** archetype
3. go to **Inducements** › **Resource**
4. click **New**
 - a. select **AD**
 - b. click **Next: Resource object type**
 - c. click **Next: Entitlements**
 - d. click **Next Mappings**
 - e. click **Save settings**
5. click **Back** as the archetype has been already saved automatically after the previous step
6. wait for the next regular reconciliation with HR resource, it will add the AD accounts for the new users (otherwise full recomputation is needed)
7. check the users created earlier and their Active Directory DNs either by checking users and their accounts or using **AD LDAP browser**

midPoint username	midPoint fullName	AD DN	Description
lcallaha	Louise Callahan	cn=Louise Callahan,ou=users,dc=example,dc=com	No AD DN uniqueness issues
abaker2	Andreas Baker	cn=Andreas Baker,ou=users,dc=example,dc=com	No AD DN uniqueness issues
cwhitehe2	Clara Whiteherring	cn=Clara Whiteherring,ou=users,dc=example,dc=com	No AD DN uniqueness issues
cwhitehe3	Clara Whiteherring	cn=Clara Whiteherring (cwhitehe3),ou=users,dc=example,dc=com	Iterated, because cn=Clara Whiteherring,ou=users,dc=example,dc=com already exists (for user cwhitehe2 (Clara Whiteherring)).
jsmith3	Jacques Smith	cn=Jacques Smith,ou=users,dc=example,dc=com	No AD DN uniqueness issues



The distinguished name is made unique in AD's outbound mapping for **dn** attribute by using a simple Groovy script. The value is either **CN=Full Name**, if the Full Name is unique or **CN=Full Name (username)** if it is not.

Let's check if there are any persons without AD account:

1. go to **Users > Persons**
2. in search toolbar, locate **Users without account** search criteria
 - a. click  button (tooltip: **Property settings**) to open a popup window:
 - i. in **Name**: click the  button and select **AD** resource
 - b. check the ☐ for **Users without account** to apply the search criteria

There should be no users without AD resource accounts.

To stop using the search criteria, uncheck the checkbox for **Users without account** in search toolbar.

By the previous configuration, we instructed midPoint to create accounts in AD resource for all users with **Person** archetype. Users in midPoint are kept forever even for former employees. AD

accounts are configured to be disabled for users in Long-term leave or Former employee HR state and deleted later for Former employee state. This will be demonstrated later.

The new users created by midPoint have no passwords. They cannot log in to midPoint. Their AD passwords were randomly generated using a weak (one-time) activation outbound mapping in AD resource. For the sake of this training, we assume the users will visit helpdesk to reset their AD account passwords.

midPoint can be configured for authentication using Active Directory. It can also be used to change the passwords in Active Directory using its self-service interface. This configuration is out of scope of this training.

LAB 8-3: Automate Active Directory Group Membership For All Persons

Estimated Time: 10 min.

In this lab, we will update midPoint provisioning configuration for AD resource to make all accounts of Person users members of a fixed pre-existing group.

The group membership management (called **association** in midPoint) is already prepared to be used in our AD resource from the resource template. We will review this configuration first.

In your browser with midPoint:

1. go to **Resources** › **All resources**
2. edit **AD** resource
3. click **Schema handling** menu item
4. notice the object type definition **AD Group** in **Proposed** lifecycle state



Do not change the configuration of **AD Group** object type. It is required by the association configuration, but we will not use it in this training in any other way.

5. click **Accounts** menu item
6. click **Configure**, then click **Associations** item in the context menu
 - a. the **adGroup** association for group's **member** attribute is configured in **Proposed** lifecycle state, ready for simulations.
7. click **Exit wizard**

As the configuration is in **Proposed** lifecycle state, even if we have already scheduled reconciliation for HR resource, nothing bad will happen. You **don't** need to stop the scheduled task!

We will configure **Person** archetype to put all accounts to AD's **cn=all-users** group.

1. go to **Archetypes** › **Person**
2. edit **Person** archetype
3. click **Inducements** › **Resource**
4. edit **AD** resource inducement
 - a. click **Construction Associations** tab
 - i. click **+** button

- ii. in **Grant entitlements / Group membership** popup click on group **cn=all-users,ou=groups,dc=example,dc=com** or click **Reload** first if no groups are displayed
- iii. click **Done**
- b. click **Done**
5. click **Save**

We will simulate what will happen for a single account, as usual.

1. go to **Resources > All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. click context menu for account **9000** and select **Import preview**
 - a. in **Select task execution mode** select: **Simulated development** and click **Select**



Simulated development mode will evaluate all **Active** and **Proposed** configuration items, but there will be no permanent effects on data; we are only simulating. In our particular case, the only **Proposed** configuration is the association configuration in AD resource.

5. **cn=Louise Callahan,ou=users,dc=example,dc=com** AD resource account has a new indication *Projection entitlement changed*. Clicking the account simulation details will reveal a new association with group **cn=all-users** is going to be made
6. click **Back** to get to the list of processed objects
7. click **Back** to get to the list of HR accounts

We can run a simulated import or reconciliation task from HR resource to see what will happen for all users:

1. click **Tasks**, then click **Create task** item in the context menu to open a simple task creation wizard for HR accounts
 - a. click **Import Task** tile
 - b. toggle **Simulate task** to **ON**
 - c. click **Create task** and fill in the following details:
 - i. **Name:** **Import from HR - development simulation**
 - d. click **Next: Resource objects**
 - e. click **Next: Execution**
 - f. in **Execution options** page, set the following:

- i. select **Mode:** **Preview**
- ii. select **Predefined:** **Development**
- g. click **Next: Distribution**
- h. click **Save & Run**



Running simulated import task with **Development** configuration will evaluate all **Active** and **Proposed** configuration items, but there will be no permanent effects on data; we are only simulating.

2. click **Defined Tasks** menu item
3. edit the task **Import from AD - development simulation** and wait for the task completion (task status: closed)
4. click **Show simulation result**
5. the Simulation results show:
 - i. all 5 recently created AD accounts are going to be added to **cn=all-users,ou=groups,dc=example,dc=com** group (click **More info** in **Projection entitlement changed** tile to see more details)

Simulation looks OK for all 5 AD accounts. Let's activate the association configuration.

1. go to **Resources** › **All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Associations** item in the context menu
 - a. switch **adGroup** association lifecycle state to: **Active**
5. click **Save association settings**
6. wait for next regular reconciliation with HR resource, it will add the AD accounts for the new users to the **cn=all-users** group

To check the account membership after the reconciliation with HR finishes:

1. go to **Users** › **Persons**
2. edit any of the 5 recent users, e.g. **lcallaha**
3. click **Projections** menu item
4. click **AD** account
5. scroll down to **Associations** container
6. **AD Group Membership** should include the value: **cn=all-users,ou=groups,dc=example,dc=com**

All existing AD accounts before midPoint deployment were already members of the group. All newly created AD accounts for people from HR will be automatically members of the group from now on.

LAB 8-4: Enforcing AD Account Data

Estimated Time: 15 min.

In this lab, we will test how midPoint enforces the values provided by its policies. We already know that midPoint can automatically detect orphaned account and delete them. But what about unauthorized AD account changes?

We will stop scheduled reconciliation with HR resource as it would fix *some* inconsistencies automatically, and we would like to explain what's going on.

In your browser with midPoint:

1. go to **Resources** › **All resources**
2. edit **HR** resource
3. click **Defined Tasks** menu item
4. edit task **HR Reconciliation**
5. click **Suspend** to suspend the task

We will delete one AD account directly in AD LDAP browser - such action is certainly possible, as AD administrator may, in error or not, delete account managed by midPoint.

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. edit **cn=Alexander Freeman**
4. click **Delete this entry**
5. confirm by clicking **Delete**

AD account was deleted.

Now we will try to update some AD account attributes outside midPoint.

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users** or click **Refresh** in the tree
3. edit **cn=Alice Baker**
 - a. change the following attributes:
 - i. **1: Silver City**

- ii. **givenName: A1**
- b. click **Update object**
- c. click **Update object**
4. expand **ou=groups**
5. edit **cn=all-users**
6. scroll down in the right panel and click **(modify group members)**
7. in the right part, in the list of **Group members**:
 - a. select **cn=Alice Baker,ou=users,dc=example,dc=com**
 - b. click **<<< Remove selected**
 - c. click **Save changes**
 - d. click **Update object**

After we have made some changes in AD outside midPoint, we will run reconciliation with AD - first in simulation mode.

In your browser with midPoint:

1. go to **Resources > All resources**
2. edit **AD** resource
3. click **Defined Tasks** menu item
4. edit and run **Reconciliation with AD - production simulation** task using click **Run now** and wait for the task completion (task status: closed)
5. click **Show simulation result**
6. the Simulation results show:
 - a. 1 object **afreeman** to be updated in midPoint:
 - i. link to newly created AD account is to be added
 - b. 1 object **cn=Alexander Freeman,ou=users,dc=example,dc=com** to be activated (created) in AD:
 - i. all attributes are populated by AD outbound mappings
 - ii. account will be added to **cn=all-users,ou=groups,dc=example,dc=com** group (because of policy in **Person** archetype)
 - c. 1 object: **cn=Alice Baker,ou=users,dc=example,dc=com** to be updated in AD with the following details:
 - i. **Locality** attribute will be changed to **White Stone City** (because of data in HR)
 - ii. **Given Name** attribute will be changed to **Alice** (because of data in HR)
 - iii. account will be added to **cn=all-users,ou=groups,dc=example,dc=com** group (because of

policy in **Person** archetype)

If the reconciliation with AD would be scheduled, it would automatically do the changes presented in the simulation.

We will run the reconciliation manually:

1. get back to **Defined Tasks**
2. edit and run **Reconciliation with AD (real)** task again using **Run now** and wait for the task completion (task status: closed)
3. go to **Audit log viewer** and verify the executed changes there (1 account should be created and 1 account should be modified)
4. go to **Users > Persons**
5. edit **abaker** user
6. click **Projections** menu item
7. edit **AD** account
8. verify the **Locality** and **Given Name** attributes and **AD Group Membership** association have been updated to the same values as in simulation
9. click **Back**
10. edit **afreeman** user
11. click **Projections** menu item
12. edit **AD** account
13. verify the account has been created and its attributes populated



List of projections also shows a message about *dead shadow(s)* for user **afreeman**. Dead shadows contain metadata about the (now deleted) accounts midPoint is aware of. They will be automatically removed by midPoint's **Shadow Refresh Task** (default retention policy for dead shadows is: 7 days).

(Optional) In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. edit **cn=Alice Baker**
4. verify the attribute values in the account
5. verify that **cn=Alexander Freeman** account exists (has been re-created)

Now we will resume our scheduled HR reconciliation task.

In your browser with midPoint:

1. go to **Resources** › **All resources**
2. edit **HR** resource
3. click **Defined Tasks** menu item
4. edit task **HR Reconciliation**
5. click **Resume** to resume the task. The task will be executed immediately.

As a matter of fact, the scheduled reconciliation with HR helps us to maintain the attribute consistency even without running scheduled AD reconciliation. HR reconciliation task evaluates all HR accounts and their owners in midPoint and their AD accounts. As we are using **strong** mappings everywhere, any inconsistency in attributes is automatically fixed by the HR reconciliation task. Please note that HR reconciliation task *cannot* detect any orphaned accounts (without midPoint owner) in AD!

In real deployments, the reconciliation with AD should be scheduled to be executed automatically to detect any inconsistencies.

LAB 8-5: Handling HR Data Updates

Estimated Time: 5 min.

In this lab, we will verify that we can actually change data in HR application and that they will be picked up midPoint. We have already created new users, now let's check updates.

In your browser with HR application:

1. click **Show users**
2. edit **Geena Green (employee number: 1001)** entry using **Modify**
3. update the following fields:
 - a. **Locality:** Hot Lava City
4. click **Modify user**
5. click **Export users to csv file**

In your browser with midPoint:

1. wait for the next scheduled reconciliation with HR
2. edit user **geena**
3. check that user's **Locality** has been updated to: Hot Lava City
4. click **Projections** menu item
5. edit **AD** account
6. check that **locality** attribute has been updated to Hot Lava City

You can also check user-related audit log entries.

1. while editing **geena** user
2. click **History** menu item
3. click **Time** column value of the audit log entry with latest timestamp (by default displayed as the first entry)
4. midPoint audit log shows that both midPoint user and her AD account **cn=Geena Green,ou=users,dc=example,dc=com** were updated:

Item	Old value	New value
Locality	Small Red Rock City	Hot Lava City

We have seen that midPoint is correctly picking up updates of existing HR data just like the new entries.

LAB 8-6: Handling Long-term Leave

Estimated Time: 10 min.

In this lab, we will test midPoint behaviour for HR long-term leaves.

In this training, long-term leave stands also for parental leave etc. Such users and their accounts should be disabled.

In your browser with HR application:

1. edit user **Martin Knight (employee number: 1006)** by clicking **Modify**
2. change the following attribute:
 - a. **Status:** select **Long-term leave**
3. click **Modify user**
4. click **Export users to csv file**

Wait for the next scheduled reconciliation with HR.

In your browser with midPoint:

1. go to **Users › Persons**
2. search for and edit user **knight**
3. check the following:
 - a. User's **Lifecycle state** is **Suspended**
 - b. User's effective status (displayed in the summary panel) is **Disabled**
4. click **Projections**
5. edit **AD** account
6. scroll down to verify that **Administrative status** is **Disabled**

Inactive users from HR are inactive in midPoint and AD resource.

We will return the employee back to the active state now.

In your browser with HR application:

1. edit user **Martin Knight (employee number: 1006)** by clicking **Modify**
2. change the following attribute:
 - a. **Status:** select **In**
3. click **Modify user**

4. click **Export users to csv file**

Wait for the next scheduled reconciliation with HR.

In your browser with midPoint:

1. go to **Users › Persons**
2. search for and edit user **knight**
3. check the following:
 - a. User's **Lifecycle state** is **Active**
 - b. User's effective status (displayed in the summary panel) is **Enabled**
4. click **Projections**
5. edit **AD** account
6. scroll down to verify that **Administrative status** is **Enabled**

When returning from long-term leave, user and his/her accounts in target systems are enabled.

LAB 8-7: Handling Leavers

Estimated Time: 10 min.

In this lab, we will test midPoint behaviour for former employees. Such users and their accounts should be disabled and their accounts should be deleted in the future automatically. We will use "disabled instead of delete" and "delayed delete" activation concepts of midPoint to first disable such users and their AD account and plan a delayed delete for their AD accounts.



The delayed delete interval is set for 5 minutes for this training.

In your browser with HR application:

1. edit user **Martin Knight (employee number: 1006)** by clicking **Modify**
2. change the following attribute:
 - a. **Status:** select **Former employee**
3. click **Modify user**
4. click **Export users to csv file**

Wait for the next scheduled reconciliation with HR.

In your browser with midPoint:

1. go to **Users > Persons**
2. search for and edit user **knight**
3. check the following:
 - a. User's **Lifecycle state** is **Archived**
 - b. User's effective status (displayed in the summary panel) is **Disabled**
4. click to **Projections**
5. click **AD account**
 - a. User's AD account is disabled
 - b. Trigger is set for user's AD account to be applied in 5 minutes from now (time of account disable when user entered **Archived** lifecycle state).
 - c. The trigger time is displayed when you hover the mouse pointer over the AD account icon
 - d. This trigger will be used to delete the AD account.



The trigger is stored in midPoint Shadow object corresponding to the resource account. It is not stored in the user object nor in the real account in AD.

You can check accounts with triggers in **AD account notices** dashboard:

1. go to **Dashboards › AD account notices**
2. dashboard indicates how many accounts are using the account marks
3. click **More info** in **Users with accounts with triggers** tile to display the list of users with triggers for any of their account
4. click **More info** in **Accounts with triggers** tile to display just list of accounts with triggers
 - a. all accounts with triggers on any resource are displayed (in our particular case, we can have triggers only for accounts in AD resource)

Wait 5 minutes.

After 5 minutes have elapsed, wait for the next scheduled execution of **Trigger Scanner** task.

In our particular case, the HR reconciliation task may process the triggers earlier as it runs each minute. If our HR reconciliation task was running in longer intervals, you could either wait for the **Trigger Scanner** task or run it manually:

1. go **Server tasks › System tasks**
2. click **Trigger Scanner** task.
3. this task is automatically scheduled each 5 minutes. Information about last task run is either in task's summary panel or visible in **Operational attributes**
4. to force running the task immediately, click **Run now** and wait for the task completion (task status: closed). Please note that **Trigger Scanner** will act only on objects that have their triggers in the past.



In our particular case, HR reconciliation will process the trigger earlier than **Trigger Scanner** task.

After 5 minutes have elapsed and either **Trigger scanner** or **HR Reconciliation** task has run, check the user again:

1. go to **Users › Persons**
2. click **knight** user
3. click **Projections**
4. user's AD account should be deleted

You can also check the **Users without account** search criteria:

1. go to **Users › Persons**
2. in search toolbar, locate **Users without account** search criteria

- a. click  button (tooltip: **Property settings**) to open a popup window:
 - i. in **Name**: click the  button and select **AD** resource
 - b. check the ☐ for **Users without account** to apply the search criteria
3. user **knight** should be in the list as midPoint has deleted his AD account

To stop using the search criteria, uncheck the checkbox for **Users without account** in search toolbar.

Of course, you can also check users without AD accounts in **AD account notices** dashboard:

1. go to **Dashboards › AD account notices**
2. dashboard indicates how many users are without AD accounts
3. click **More info** in **Users without AD accounts** tile
 - a. all users without AD accounts displayed

midPoint has automatically deleted AD account for former employee with a delay. This would allow administrators to transfer some important data (e.g. mailbox) before the account is deleted. It will also prevent an immediate account deletion in case the data in HR is incorrect.

LAB 8-8: Adding A New Outbound Mapping

Estimated Time: 10 min.

In this lab, we will demonstrate how an AD outbound mapping can be added to already existing configuration. We will still need and use simulations.

In your browser with midPoint:

1. go to **Resources** > **All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Mappings** item in the context menu
 - a. click **Outbound mappings (to Resource)**
 - b. use **Add outbound** button to create a new mapping:

Name	Source	Expression	To resource attribute	Lifecycle State
mapping-initials	givenName familyName (You need two source attributes here)	Script	initials	Proposed

- c. click **Show script** for the **initials** attribute mapping
 - i. paste the following code:

```
basic.uc(  
    basic.stringify(givenName)?.take(1) +  
    basic.stringify(familyName)?.take(1)  
)
```

- ① uppercase the concatenation of...
- ② first letter of user's **givenName** property converted to String
- ③ first letter of user's **familyName** property converted to String

- ii. click **Done**
5. click **Save mappings**

Now we are ready to run the simulated reconciliation.

1. click **Defined Tasks** menu item
2. edit **Reconciliation with AD - development simulation** task
3. click **Run now** and wait for the task completion (task status: closed)



Simulated development mode will evaluate all **Active** and **Proposed** configuration items, but there will be no permanent effects on data; we are only simulating.

4. click **Show simulation result**
5. the Simulation results show:
 - a. there will be resource objects affected (click **More info** in **Resource objects affected** tile to see details) - AD attribute **initials** is being populated

We will switch the new simulated mapping to **Active** lifecycle state.

In your browser with midPoint:

1. go to **Resources > All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Mappings** item in the context menu
 - a. click **Outbound mappings (to Resource)**
 - b. edit the mapping **mapping-initials** and set:
 - i. **Lifecycle state: Active (production)**
5. click **Save mappings**

Wait for the next scheduled run of reconciliation with HR. Then you can verify the mapping has been applied.

1. go to menu **Users[Persons]**
2. edit user **geena**
3. click **Projections** menu item
4. click user's **AD** account
5. the **initials** attribute should contain the following value: **GG** (Geena Green)

You can also check the account attributes in AD resource using LDAP browser.

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. click any account and verify the **initials** attribute is populated

We have successfully created a new outbound mapping for AD resource. Simulations were again helpful - even if the solution is actually deployed.

LAB 8-9: Adding New Attribute Provisioning From HR to AD

Estimated Time: 10 min.

In this lab, we will import another attribute from HR for users and let it provision to AD resource. We will need two mappings: one inbound mapping to get HR data to midPoint and one outbound mapping to populate AD resource account.

In your browser with **HR application**:

1. click **Show users**
2. notice how **Job** attribute is displayed. The value contains job code and job title concatenated with **#**. We will start with importing the value as it is and improve it later.

We will add the inbound mapping first.

In your browser with midPoint:

1. go to **Resources > All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Mappings** item in the context menu
 - a. use **Add inbound** button to create an additional mapping:

Name	From resource attribute	Expression	Target	Lifecycle State
job-to-title	job	As is	title	Proposed

5. click **Save mappings**

We would add a new outbound mapping for AD now, but we will realize a suitable mapping from midPoint **title** property to AD's **title** attribute is already present in AD resource in **Draft** lifecycle state (because it was copied from the resource template).

1. go to **Resources > All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Mappings** item in the context menu
 - a. click **Outbound mappings (to Resource)**

- b. edit **mapping-title** mapping and set:
 - i. **Lifecycle state: Proposed (simulation)**

5. click **Save mappings**

Both mappings are in **Proposed** lifecycle state, so they will not influence the scheduled reconciliation task.

Now we are ready to run the simulated import from HR resource.

1. go to **Resources > All resources**
2. edit **HR** resource
3. click **Defined Tasks** menu item
4. edit **Import from HR - development simulation** task
5. click **Run now** and wait for the task completion (task status: closed)



Simulated development mode will evaluate all **Active** and **Proposed** configuration items, but there will be no permanent effects on data; we are only simulating.

6. click **Show simulation result**

7. the Simulation results show:

- a. there will be resource objects affected (click **More info** in **Resource objects affected** tile to see details) - AD attribute **title** is being populated
- b. the list of modified objects also includes Users objects in midPoint (**Title** property is being populated). Click **View processed objects** to see also the users.
- c. some AD accounts already contain values for **title** and will be overwritten:
 - i. **cn=Brad Carpenter,ou=users,dc=example,dc=com**
 - ii. **cn=Jimmy Taylor,ou=users,dc=example,dc=com**
 - iii. **cn=Peter Hunter,ou=users,dc=example,dc=com**
 - iv. **cn=Diane Davis,ou=users,dc=example,dc=com**
 - v. **cn=Patrick Anderson,ou=users,dc=example,dc=com**
- d. for other AD accounts we are simply adding a new **title**

We will switch the new simulated mappings to **Active** lifecycle states.

In your browser with midPoint:

1. go to **Resources > All resources**
2. edit **HR** resource

3. click **Accounts** menu item
4. click **Configure**, then click **Mappings** item in the context menu
5. edit the mapping **job-to-title** and set:
 - i. **Lifecycle state:** **Active (production)**
6. click **Save mappings**

Then navigate to AD resource.

1. go to **Resources > All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Mappings** item in the context menu
 - a. click **Outbound mappings (to Resource)**
 - b. edit the mapping **mapping-title** and set:
 - i. **Lifecycle state:** **Active (production)**
5. click **Save mappings**

Wait for the next scheduled run of reconciliation with HR. Then you can verify the mapping has been applied.

1. go to **Users > Persons**
2. edit user **geena**
 - a. notice the property **Title** and its value
3. click **Projections** menu item
4. click user's **AD** account
 - a. notice the **title** attribute should contain the same value as in HR application and midPoint user

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. click any account and verify the **title** attribute is populated

We have populated yet another value from HR to AD through midPoint. The values do not look very nice as they contain some internal HR codes, but we will improve that in the following lab - we will show how to safely exchange mappings in production.

LAB 8-10: Exchanging Inbound Mapping

Estimated Time: 10 min.

In this lab, we will demonstrate how mapping can be safely exchanged for another one. As our system is already in production, we need to be extra safe. We need to use simulations, just like before.

In the previous lab, we have seen that the **job** attribute in HR application actually contains a code, which is something we want to avoid. We want to show **CEO** instead of **124#CEO**. For the sake of the previous lab, it was OK, but now we need to do better.

We will parse the **job** attribute during import and store only the value after **#** separator using a simple Groovy script.

For the first time, we will use lifecycle state to deprecate the existing mapping to allow it still to be evaluated during scheduled HR reconciliation, while we will prepare a new proposed mapping for simulations. Then we will switch these two mappings.

In your browser with midPoint:

1. go to **Resources** > **All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Mappings** item in the context menu
5. edit the mapping **job-to-title** and set:
 - i. **Lifecycle state:** **Deprecated**
6. use **Add inbound** button to create a new mapping for **job** attribute:

Name	From resource attribute	Expression	Target	Lifecycle State
job-to-title-nice	job	Script	title	Proposed

- a. click **Show script** for the **job-to-title-nice** attribute mapping
 - i. paste the following code:

```
def separator = '#'

if (input == null || input.indexOf(separator) == -1) {
    return input
} else {
    return input.tokenize(separator)[1]
}
```

ii. click **Done**

7. click **Save mappings**



The script parses the value using '#' character and returns the second item. For **123#CEO** it returns **CEO**. To be on the safe side, we will take care of anomalies too:

- **CEO**: returns **CEO**
- empty string: returns empty string
- null: returns null

The new mapping is in **Proposed** lifecycle state, so it will not be used by the scheduled HR reconciliation. We can simulate the configuration change safely.



We won't make any change to AD's outbound mapping for **title** attribute. That one will use the midPoint property value once we correct it in midPoint.

We will run the simulated import from HR resource.

1. go to **Resources > All resources**
2. edit **HR** resource
3. click **Defined Tasks** menu item
4. edit **Import from HR - development simulation** task
5. click **Run now** and wait for the task completion (task status: closed)



Simulated development mode will evaluate all **Active** and **Proposed** configuration items, but there will be no permanent effects on data; we are only simulating. At the same time, the real scheduled reconciliation task executed all **Active** and **Deprecated** configuration items, so the old configuration is still in production.

6. click **Show simulation result**

7. the Simulation results show:

- a. there will be resource objects affected (click **More info** in **Resource objects affected** tile to see details) - AD attribute **title** is being updated
- b. the list of modified objects also includes Users objects in midPoint (**Title** property is being updated). Click **View processed objects** to see also the users.



You can improve your script expression and run simulated import without worries and any impact on real users and their AD accounts while the mapping is in **Proposed** lifecycle state.

We have seen what will happen. We will now switch the mappings.

In your browser with midPoint:

1. go to **Resources > All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Mappings** item in the context menu
5. edit the mapping **job-to-title** and set:
 - a. **Lifecycle state: Archived**
6. edit the mapping **job-to-title-nice** and set:
 - a. **Lifecycle state: Active (production)**
7. click **Save mappings**

Wait for the next scheduled run of reconciliation with HR. Then you can verify the mapping has been applied.

1. go to menu Users[Persons]
2. edit user **geena**
 - a. notice the property **Title** and its value: it should be updated to the new format
3. click **Projections** menu item
4. click user's **AD** account
 - a. notice the **title** attribute should contain the same value as in HR application and midPoint user

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**

3. click any account and verify the **title** attribute is updated correctly

We have succeeded in exchanging mappings using lifecycle state and simulations during real operation (scheduled reconciliation with HR was not suspended in the process). This way you could improve your configuration and still see what would happen thanks to the simulations.

The mapping in **Archived** lifecycle state can be eventually removed.

This concludes the Module 8 labs.