



# MidPoint Deployment: First Steps [MID301]

## *Student Lab Guide - Module 7*

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 7: Enable Provisioning to Target Systems** ..... **3**

    LAB 7-1: Reviewing Active Directory Resource Provisioning Configuration..... 3

    LAB 7-2: Active Directory Provisioning Simulation..... 5

    LAB 7-3: Active Directory Provisioning ..... 7

# Module 7: Enable Provisioning to Target Systems

## LAB 7-1: Reviewing Active Directory Resource Provisioning Configuration

**Estimated Time: 5 min.**

In this lab, we will review the provisioning configuration of AD resource which has been copied from the resource template.

The provisioning configuration is either in **Proposed** or **Draft** lifecycle states, so the resource is not yet ready for normal use.



Please do not change any resource configuration while reviewing it.

In your browser with midPoint:

1. go to **Resources** › **All resources**
2. edit **AD** resource
3. click **Accounts**

We will review outbound attribute mappings now. These mappings are already in place from the resource template.



Please do not change any resource configuration while reviewing it.

1. click **Configure**, then click **Mappings** item in the context menu
2. click **Outbound mappings (to Resource)** to display the outbound mappings
3. there are several outbound mappings prepared for future use, all of them are in **Draft** lifecycle state, so they are effectively disabled. The configuration is typical for a target Active Directory resource

These mappings are already in place from the resource template.

Click **Exit wizard** to get back to account list.

We will review activation outbound mappings now. These mappings are already in place from the resource template.



Please do not change any resource configuration while reviewing it.

1. click **Configure**, then click **Activation** item in the context menu
2. click **Outbound**
3. there are three outbound activation mappings, all of them in **Draft** lifecycle state, so they are effectively disabled:
  - a. mapping **set-account-status-based-on-midpoint-user** will be later used to enable/disable AD account based on midPoint user status
  - b. mapping **Disable instead of delete** will be later used to disable AD account instead of deleting it if the user has no "reason" to have an account there
  - c. mapping **Delayed delete** will be later used to delete AD account after it has been disabled for configured time if the user has no "reason" to have an account there.
    - i. click **Settings** to display the time configuration for the delayed account deletion (please do not make any changes)
4. click **Exit wizard** to get back to the account list

We will review credentials outbound mappings now. These mappings are already in place from the resource template.



Please do not change any resource configuration while reviewing it.

1. click **Configure**, then click **Credentials** item in the context menu
2. click **Outbound**
3. there are two outbound credentials mappings, all of them in **Draft** lifecycle state, so they are effectively disabled:
  - a. mapping **initial-password-generate** will be later used to generate a random *initial* password (using a *weak* mapping) for AD account (as the account cannot be passwordless). This password won't be stored and will be unknown to the user; we assume the user will activate his/her AD account by visiting the company's helpdesk
  - b. mapping **password-change** will be later used to allow password changes from midPoint to Active Directory



We will not allow end-user access not password changes via midPoint in this training.

Click **Exit wizard** to get back to account list.


The resource created from resource template is ready to be used for provisioning simulations.

## LAB 7-2: Active Directory Provisioning Simulation

### Estimated Time: 10 min.

In this lab, we will re-use some of the outbound mappings for Active Directory which were preconfigured in the resource template, and we will simulate the provisioning first. This step is very important as there might be data inconsistencies in Active Directory and midPoint (based on HR data,) and we don't want to have any unexpected attribute changes.

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. select the following **outbound** mappings (there are more mappings prepared in the resource template, but we - as in real life - will not need to use all of them):
    - i. **mapping-dn**
    - ii. **mapping-cn-weak**
    - iii. **mapping-displayName**
    - iv. **mapping-sn**
    - v. **mapping-givenName**
    - vi. **mapping-uid**
    - vii. **mapping-l**
    - viii. **mapping-employeeNumber**
  - c. click  button (tooltip: **Change lifecycle state**) in the table header and select **Proposed (simulation)**
  - d. click **Apply changes**
  - e. click **Save mappings**

We will also update the configuration for activation outbound mapping(s) to see if midPoint is going to change any account's status:

1. click **Configure**, then click **Activation** item in the context menu
2. click **Outbound**
  - a. for all outbound mappings, switch lifecycle in upper right corner to **Proposed (simulation)**

- b. click **Save settings**

We will also update the configuration for credentials (password) outbound mapping(s) to see if midPoint is going to change any account's password:

1. click **Configure**, then click **Credentials** item in the context menu
2. click **Outbound**
  - a. for all outbound mappings, switch lifecycle in upper right corner to **Proposed (simulation)**
  - b. click **Save settings**

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)
4. click **Show simulation result**
5. the Simulation results show:
  - a. 5 accounts are going to be renamed (DN is being changed) - as AD DN contains user's **fullName** - if users had incorrect DN/CN in AD, they will be now corrected/renamed, e.g. **cn=Ema Jones** instead of **cn=Emma Jones**
  - b. 2 users are being deactivated (disabled) because of incorrect data in AD (their accounts should be disabled and are not): **cn=Jane Anderson** and **cn=Laura Shepherd** are enabled in AD, but are on **Long-term leave** in HR
  - c. AD **employeeNumber** attribute is being updated for Ana Lopez
  - d. no passwords are going to be changed
  - e. no accounts are going to be deleted

This is the time to analyze the results of the simulation. Make sure to check all entries in the simulation results. Are the changes expected? Are the changes good or bad? Thanks to the simulation, nothing has been executed yet, we have time to think and fix the situation.

Usually you will either let midPoint to execute the changes in Active Directory, or fix the data in HR. It is also possible to update the mappings to provide some conditional behaviour (outside of scope for this training). You could also mark some AD accounts as "Do not touch" and resolve these exceptions later.

In general, the simulation results show that midPoint is trying to fix the target system data using HR data - which we consider more authoritative and thus better, at least in this particular lab.


## LAB 7-3: Active Directory Provisioning

### Estimated Time: 10 min.

In this lab, we will turn on provisioning to Active Directory after successful simulation from previous lab.

We will switch all simulated mappings of attributes, activation and credentials 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. select the following **outbound** mappings:
    - i. **mapping-dn**
    - ii. **mapping-cn-weak**
    - iii. **mapping-displayName**
    - iv. **mapping-sn**
    - v. **mapping-givenName**
    - vi. **mapping-uid**
    - vii. **mapping-l**
    - viii. **mapping-employeeNumber**
  - c. click  button (tooltip: **Change lifecycle state**) in the table header and select **Active (production)**
  - d. click **Apply changes**
  - e. click **Save mappings**

We will also update the configuration for activation outbound mapping(s):

1. click **Configure**, then click **Activation** item in the context menu
2. click **Outbound**
  - a. for all outbound mappings, switch lifecycle in upper right corner to **Active (production)**
  - b. click **Save settings**



We will also update the configuration for credentials (password) outbound mapping(s):

1. click **Configure**, then click **Credentials** item in the context menu
2. click **Outbound**
  - a. for all outbound mappings, switch lifecycle in upper right corner to to **Active (production)**
  - b. click **Save settings**

We will run the simulated reconciliation one last time. All configuration is already in **Active** lifecycle state.

1. click **Defined Tasks** menu item
2. edit and run **Reconciliation with AD - production simulation** task using click **Run now** and wait for the task completion (task status: closed)
3. click **Show simulation result**
4. the Simulation results show:
  - a. 8 objects to be updated in AD just like before

Finally, let's run the real reconciliation.

1. click **Back** until you get to **Defined tasks** page
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 check what has happened (8 AD accounts modifications should be displayed)
  - a. click the value in **Time** column to display the change from audit log
  - b. click the value in **Target** value to display the object in its current state
  - c. each event is recorded multiple times. For example, try to check what has happened for user **alopez** (and her account **cn=Ana Lopez,ou=users,dc=example,dc=com**):
  - d. event stage **Request** contains the information about what was requested from midPoint (in the case of reconciliation, you will not find much information here)
    - i. event stage **Execution** contains the information about what midPoint has executed as seen from the **Model** component perspective (User and his/her account). **Employee number** change is recorded here.
    - ii. event stage **Resource** contains the information about what midPoint has executed as seen from the **Provisioning** component perspective (account). **Employee number** change is recorded here.

If you want, you can also check the accounts in AD.

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. click any account from the previously updated ones, for example:
  - a. **cn=Ana Lopez** should have her **employeeNumber: 1002**
  - b. **cn=Jane Anderson** and **cn=Laura Shepherd** should be disabled (simulated by **roomNumber: disabled**)

From now on, provisioning to AD resource is active for all attributes with mappings with **Active** lifecycle status, account activation status and credentials.

Automatic synchronization between HR and midPoint is not yet configured.

This concludes the Module 7 labs.