



How to automate the synchronization of AD and metadata

Manage users in AD, loading of users and groups into metadata and regular, automatic checking of rights

Agenda

- 1** Initial situation
- 2** The tool of choice
- 3** Preparation in AD
- 4** The implementation in SMC
- 5** Let's automate it
- 6** Regular checks

Agenda

- 1** Initial situation
- 2 The tool of choice
- 3 Preparation in AD
- 4 The implementation in SMC
- 5 Let's automate it
- 6 Regular checks

Initial situation

- ▶ Manual user administration
- ▶ Maintenance of users through separate user administration
- ▶ No comparison when user information changes
- ▶ No regular checks of user rights
- ▶ Lots of old entries in metadata
- ▶ Frequent coordination with user administration required
- ▶ Special cases or problems still had to be solved by SAS-admins
- ▶ Applications for rights are mainly made by email

Agenda

- 1 Initial situation
- 2 The tool of choice**
- 3 Preparation in AD
- 4 The implementation in SMC
- 5 Let's automate it
- 6 Regular checks

The tool of choice - METACODA

- ▶ Already in use as a test version
- ▶ Brings all those functions we were looking for, right the moment we needed them

What's New in Metacoda Plug-ins 5.0?

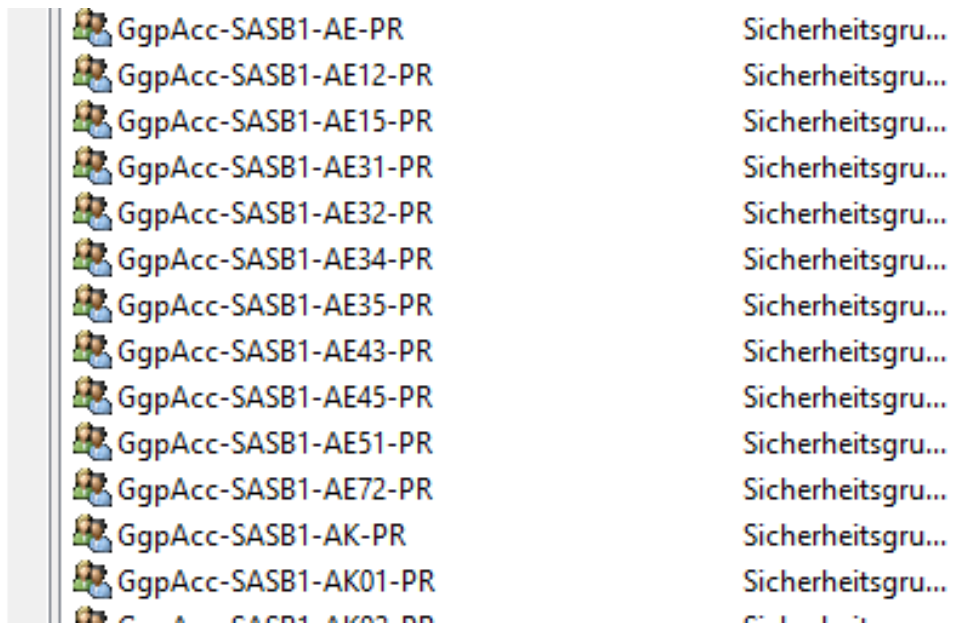
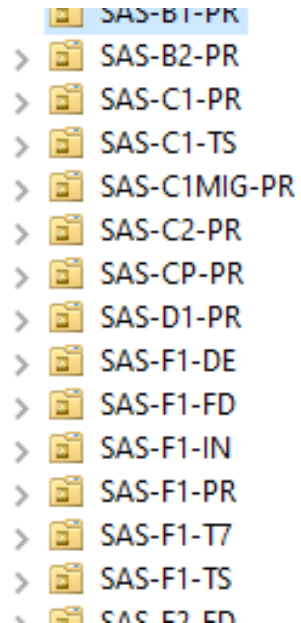
- **Easily Sync Active Directory Users & Groups into SAS Metadata:** the new Metacoda Identity Sync plug-in allows you to easily synchronise identities from Microsoft Active Directory (AD) and other SAS environments into SAS metadata, without needing to write SAS code.
- **Documentation from Interactive Security Testing:** where the Metadata Security Testing Framework previously generated test failure reports in batch mode, you can export an HTML or CSV file of test failures directly from the interactive Test Runner plug-in now too.
- **New Recommended Practice Tests:** the Metadata Security Testing Framework can now help you to enforce the 'Golden Rules' for SAS metadata security. A new series of tests help you to enforce the use of Access Control Templates (ACTs) and limit the use of Access Control Entries (ACEs), and enforce the use of groups and limit the use of users in access controls (whilst allowing for some exclusions). You can find out more about the new recommended practice tests on platformadmin.com.
- **Enhanced Exports:** as some of the most requested enhancements, the Identity Permissions Explorer and Object Permissions Explorer now allow effective permission reports to be exported in HTML and CSV format. You can also export effective permission tests to run in the testing framework too.
- **Inspect SAS Workspace Servers:** the new [Metacoda Workspace Inspector Plug-in](#) allows you to quickly inspect workspace server execution environments. You can run small code fragments, review the SAS log, check pre-assigned libraries and test the availability of table contents without leaving SAS Management Console.
- **Support for Multiple SAS Software Versions:** Metacoda Plug-ins 5.0 is supported for use with SAS software versions 9.4, 9.3 and 9.2 (including SAS Visual Analytics) at all maintenance levels. If you still have any legacy SAS 9.1.3 SP4 installations we still have Metacoda Plug-ins 1.0 available too.
- **New Licensing Bundles:** **Starter** if you just want to do identity synchronization; **Basic** if you want all the time-saving metadata security perspectives provided by the reviewers and explorers; and **Enterprise** if you want everything including the confidence-boosting automated Metadata Security Testing Framework.
- **Automatic Upgrades for Metacoda Customers:** if you're already a customer, we'll be sending you your new V5 licenses. The Metacoda Plug-ins 5.0 R1 installation packages are now available for download from support.metacoda.com.

Agenda

- 1 Initial situation
- 2 The tool of choice
- 3 Preparation in AD**
- 4 The implementation in SMC
- 5 Let's automate it
- 6 Regular checks









Preparation in AD – Orga-based permissions

- ▶ One OU for all SAS-OUTs
- ▶ One OU per SAS-environment
- ▶ One AD-group per organisation unit (AE12, AE15, ...) and one per parent organisation unit (AE, AK, ...)



Preparation in AD – Rolebased permissions

- ▶ One AD-group per SAS-role
- ▶ Also an AD-group for some software components

 GgpAcc-SASC2-HU00-CIStudio-PR
 GgpAcc-SASC2-HU00-DA-PR
 GgpAcc-SASC2-HU00-DC-PR
 GgpAcc-SASC2-HU00-DE-PR
 GgpAcc-SASC2-HU00-DIN-PR
 GgpAcc-SASC2-HU00-DS-PR
 GgpAcc-SASC2-HU00-PR
 GgpAcc-SASC2-HU00-VV-PR

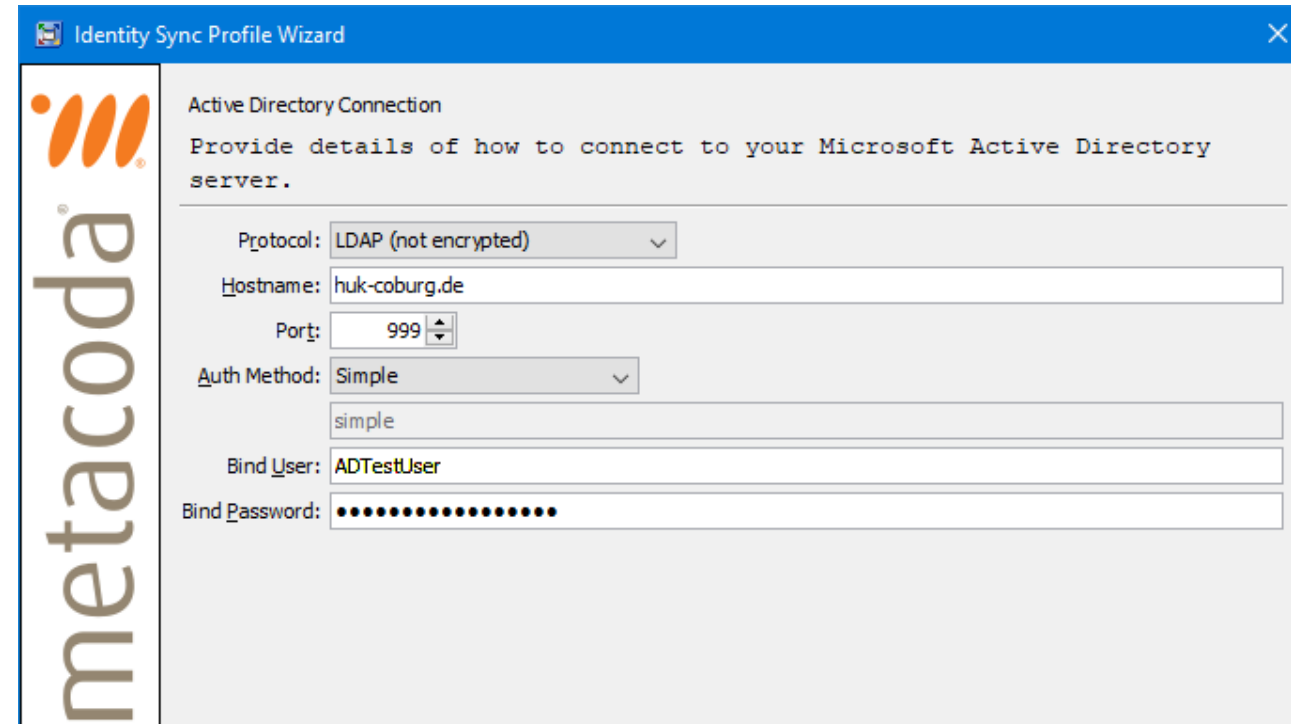
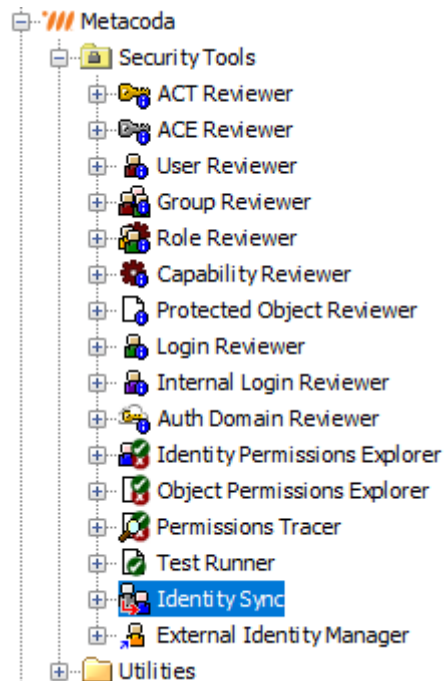
Sicherheitsgru...	Berechtigt für das SAS CI Studio
Sicherheitsgru...	HU00 - SAS Data Analyst
Sicherheitsgru...	HU00 - SAS Data Versender
Sicherheitsgru...	HU00 – SAS Data Entwickler
Sicherheitsgru...	HU00 – SAS Data Abteilung IN
Sicherheitsgru...	HU00 – SAS Data Spezialist
Sicherheitsgru...	HU - HUK24
Sicherheitsgru...	HU00 - VA-Report Viewer

Agenda

- 1 Initial situation
- 2 The tool of choice
- 3 Preparation in AD
- 4 The implementation in SMC**
- 5 Let's automate it
- 6 Regular checks

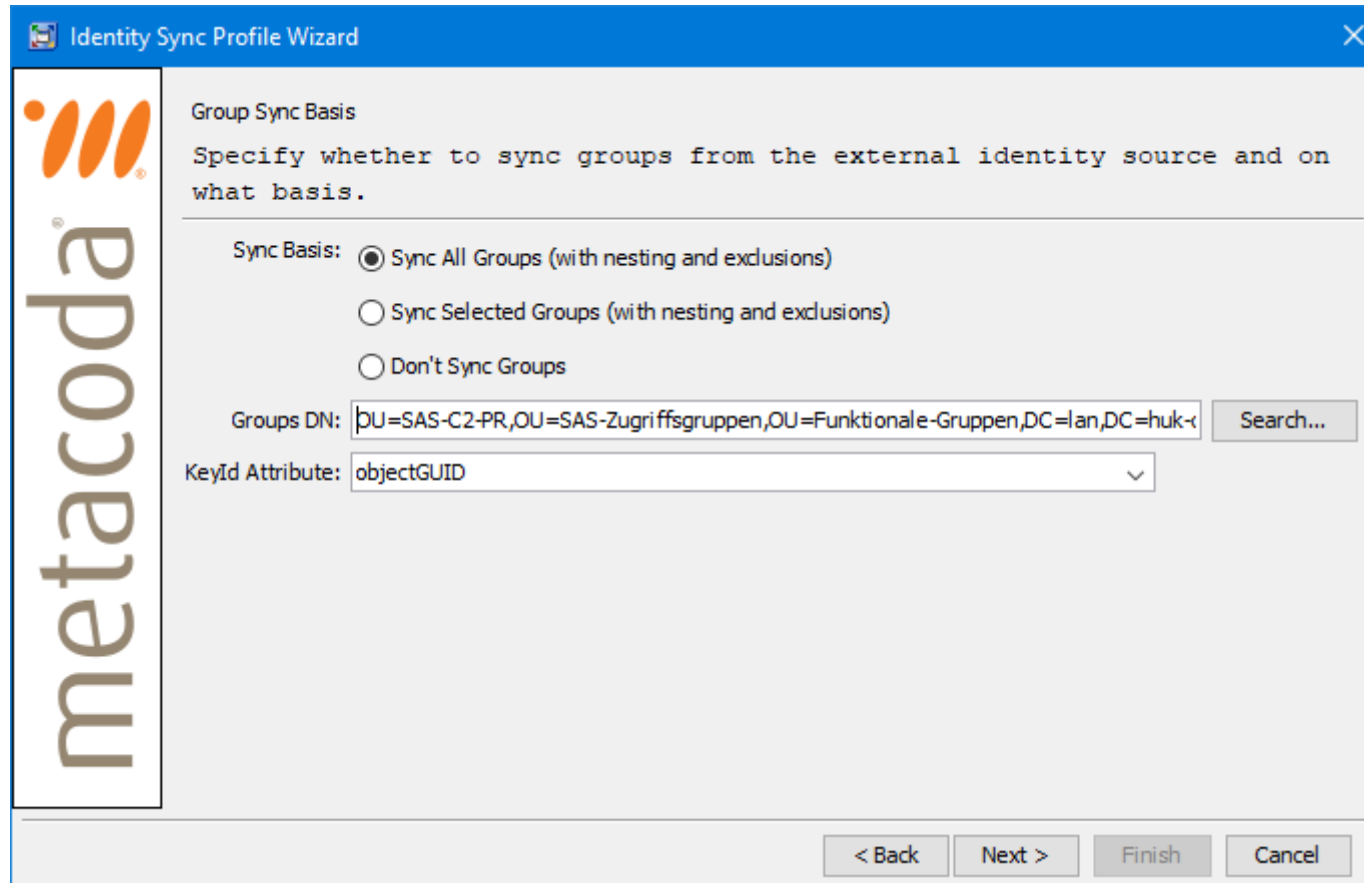
The implementation in SMC

- ▶ Install the plugin into SMC
- ▶ Create a new idsp – identity sync profile with the wizard
- ▶ An AD-user with read rights is needed



Setup the idsp using the wizard

- All groups of the selected OU should be synced



Identity Sync Profile Wizard

metacoda

Group Sync Basis
Specify whether to sync groups from the external identity source and on what basis.

Sync Basis: ☒ Sync All Groups (with nesting and exclusions)
☐ Sync Selected Groups (with nesting and exclusions)
☐ Don't Sync Groups

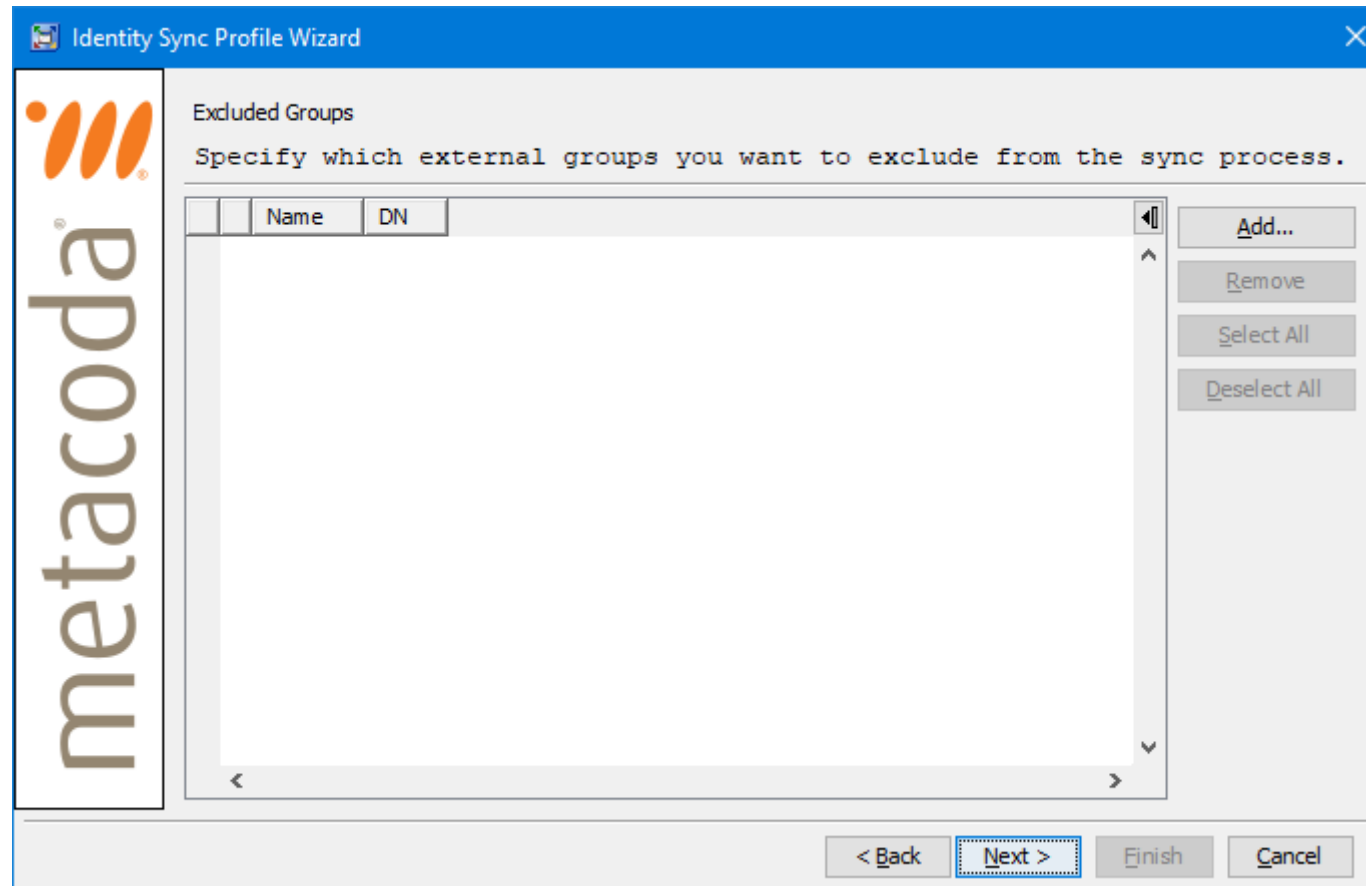
Groups DN:

KeyId Attribute:

< Back Next > Finish Cancel

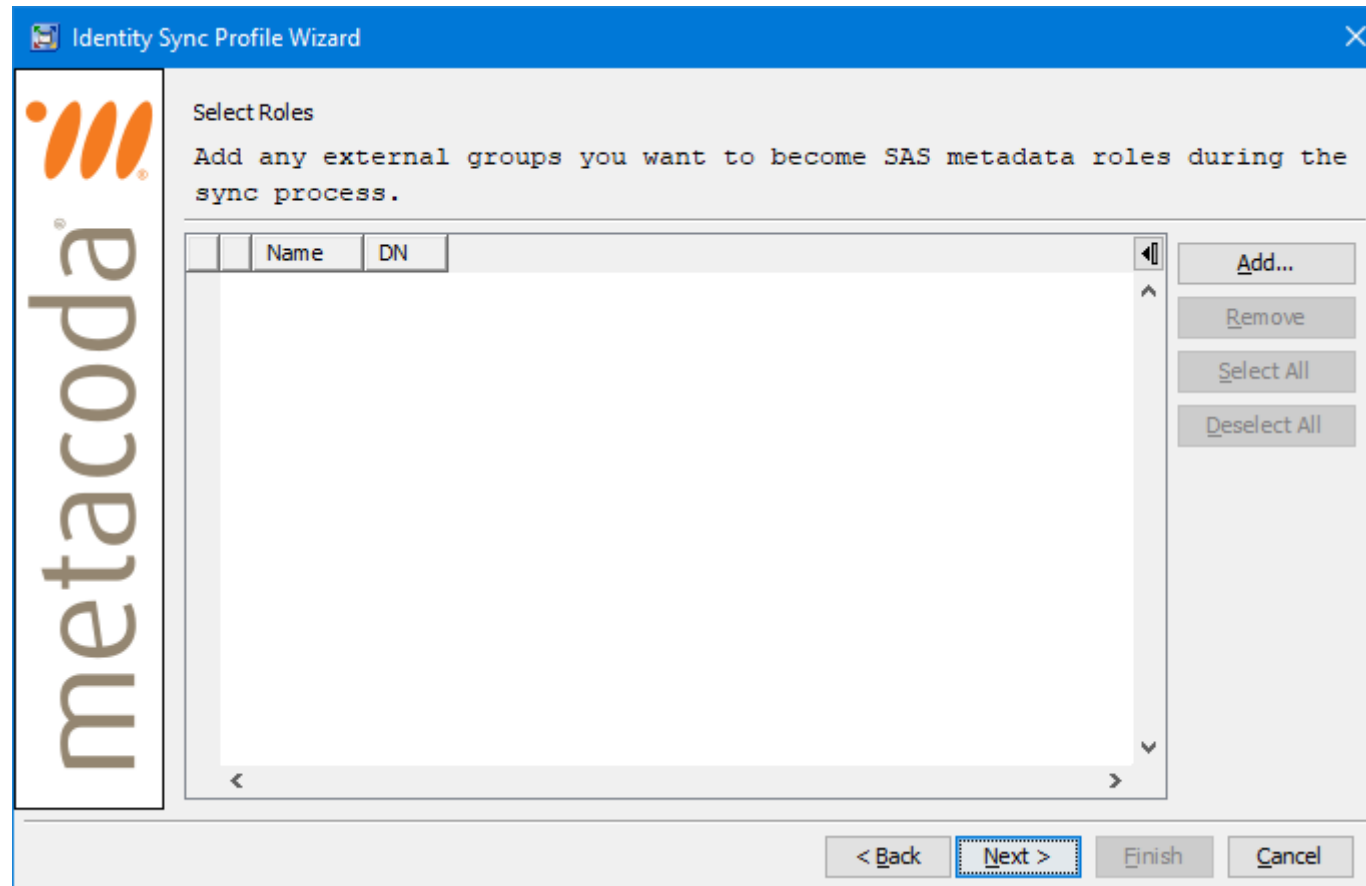
Setup the idsp using the wizard

- No exclude needed, since the structure in AD already is fine



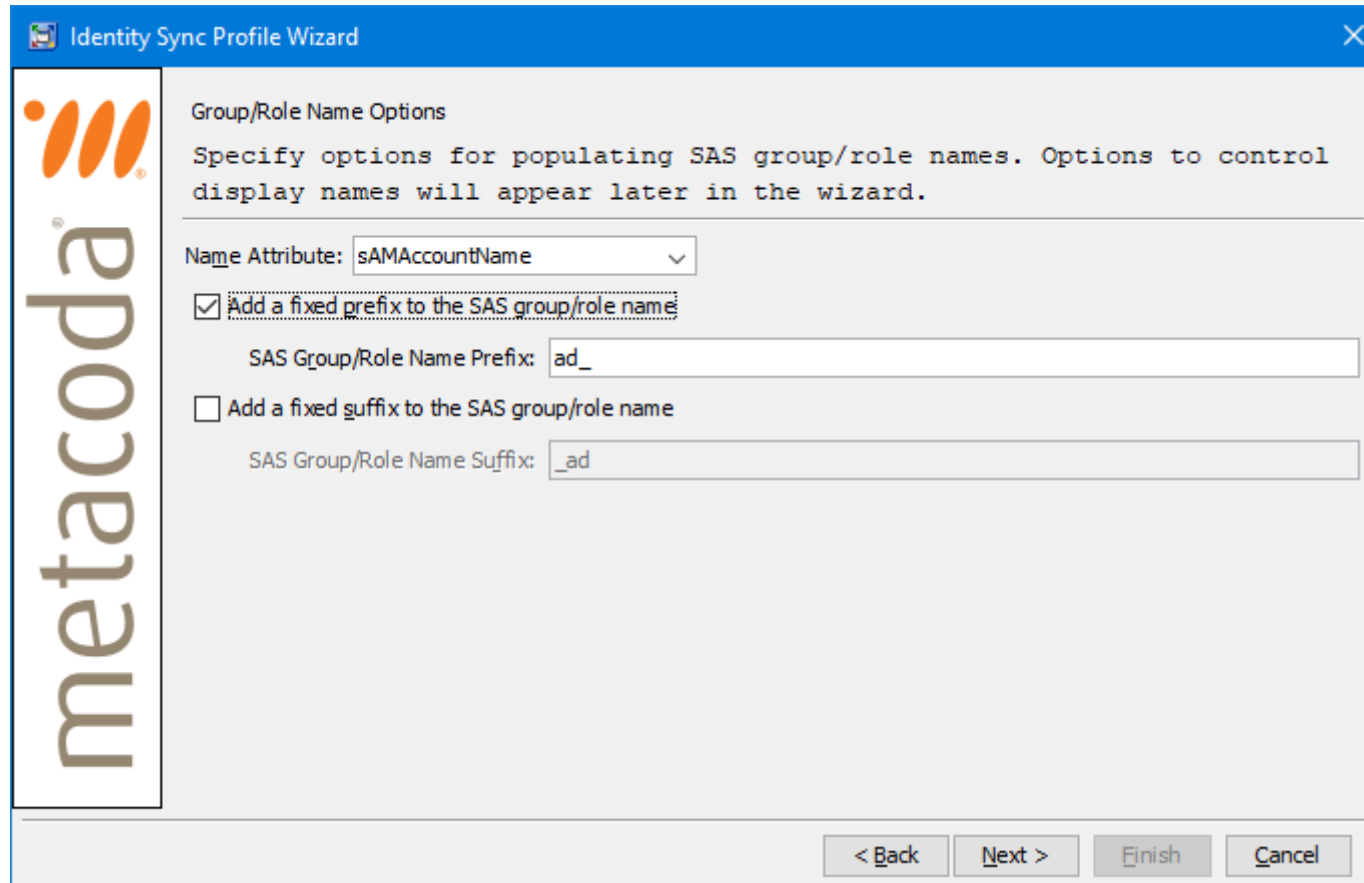
Setup the idsp using the wizard

- Ability to create SAS roles from AD groups



Setup the idsp using the wizard

- ▶ Which AD-attribute should be used for the Name Attribute
- ▶ Do you need a Pre- or Suffix?



The screenshot shows the 'Identity Sync Profile Wizard' window. On the left is a vertical sidebar with the 'metacoda' logo. The main area is titled 'Group/Role Name Options' and contains the following text: 'Specify options for populating SAS group/role names. Options to control display names will appear later in the wizard.' Below this, there are two sections. The first section is 'Name Attribute:' with a dropdown menu showing 'sAMAccountName'. The second section has two checkboxes. The first checkbox, 'Add a fixed prefix to the SAS group/role name', is checked, and below it is a text field for 'SAS Group/Role Name Prefix' containing 'ad_'. The second checkbox, 'Add a fixed suffix to the SAS group/role name', is unchecked, and below it is a text field for 'SAS Group/Role Name Suffix' containing '_ad'. At the bottom right are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Identity Sync Profile Wizard

Group/Role Name Options

Specify options for populating SAS group/role names. Options to control display names will appear later in the wizard.

Name Attribute: sAMAccountName

☒ Add a fixed prefix to the SAS group/role name

SAS Group/Role Name Prefix: ad_

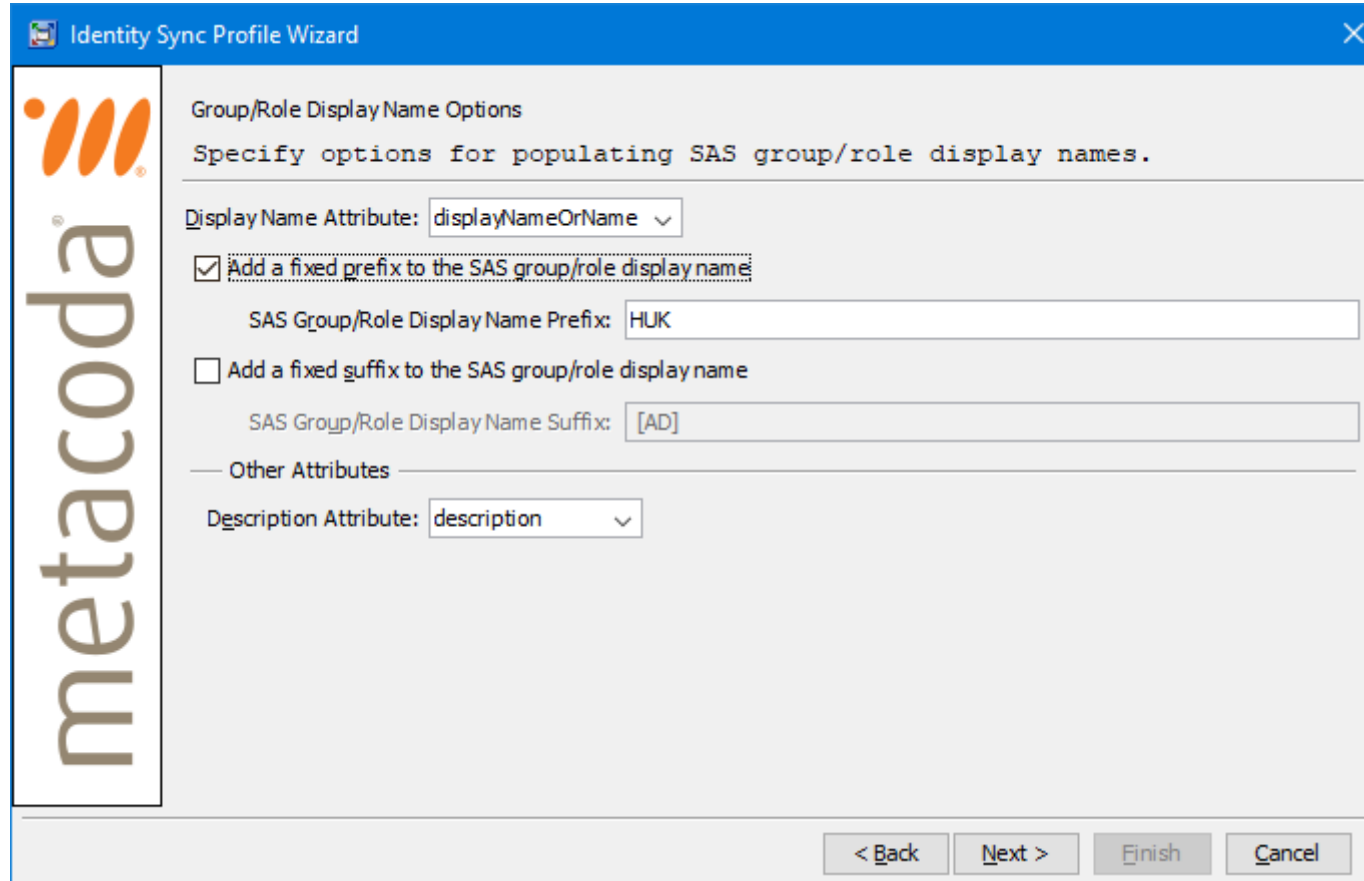
☐ Add a fixed suffix to the SAS group/role name

SAS Group/Role Name Suffix: _ad

< Back Next > Finish Cancel

Setup the idsp using the wizard

- Setting the Display Name and Description attribute



Identity Sync Profile Wizard

Group/Role Display Name Options
Specify options for populating SAS group/role display names.

Display Name Attribute:

☒ Add a fixed prefix to the SAS group/role display name

SAS Group/Role Display Name Prefix:

☐ Add a fixed suffix to the SAS group/role display name

SAS Group/Role Display Name Suffix:

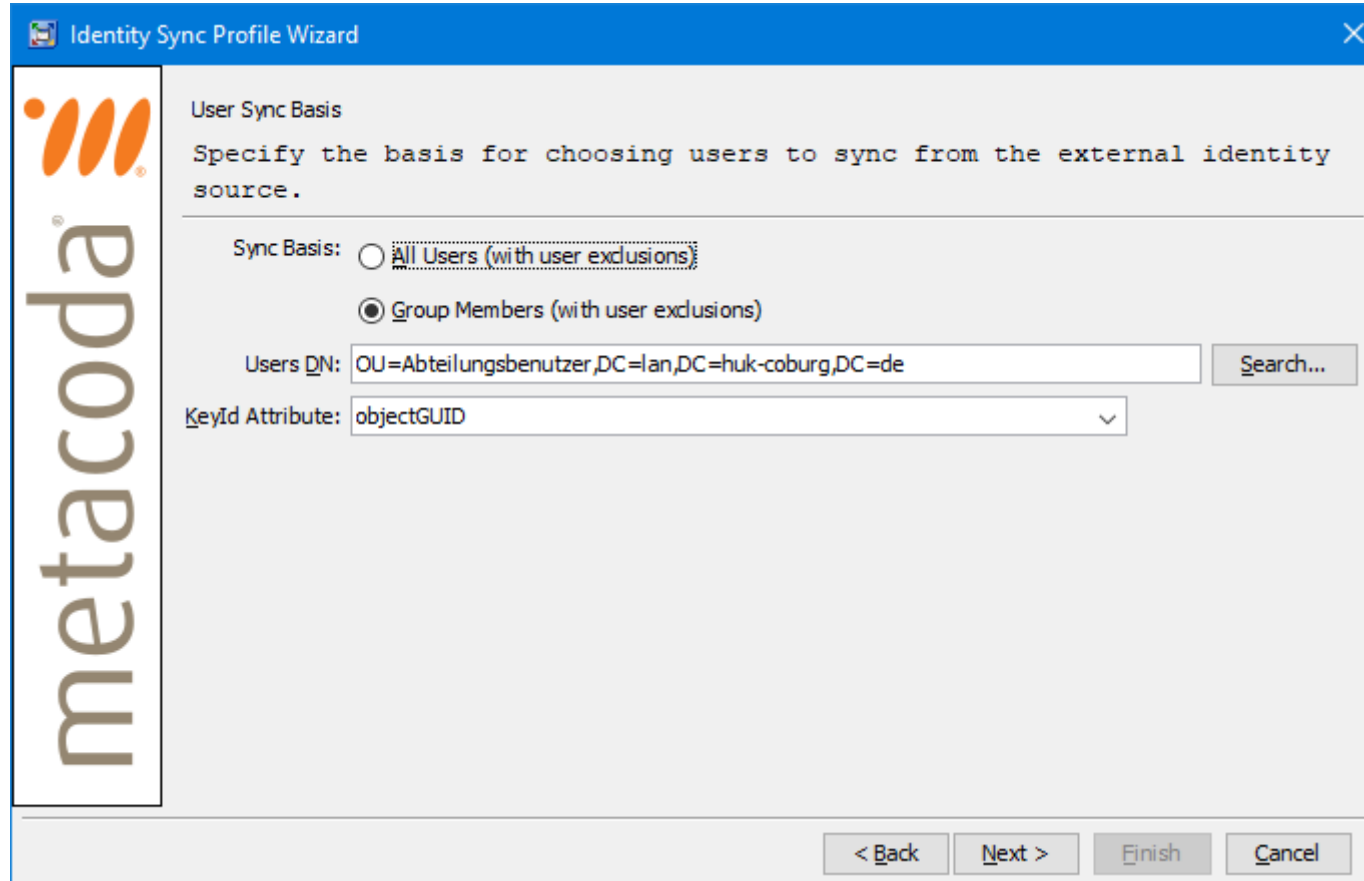
Other Attributes

Description Attribute:

< Back Next > Finish Cancel

Setup the idsp using the wizard

- ▶ Choose which users should be synced
- ▶ At HUK, all users are in one OU, so we only want to sync the group members



Identity Sync Profile Wizard

metacoda

User Sync Basis

Specify the basis for choosing users to sync from the external identity source.

Sync Basis: ☐ All Users (with user exclusions) ☒ Group Members (with user exclusions)

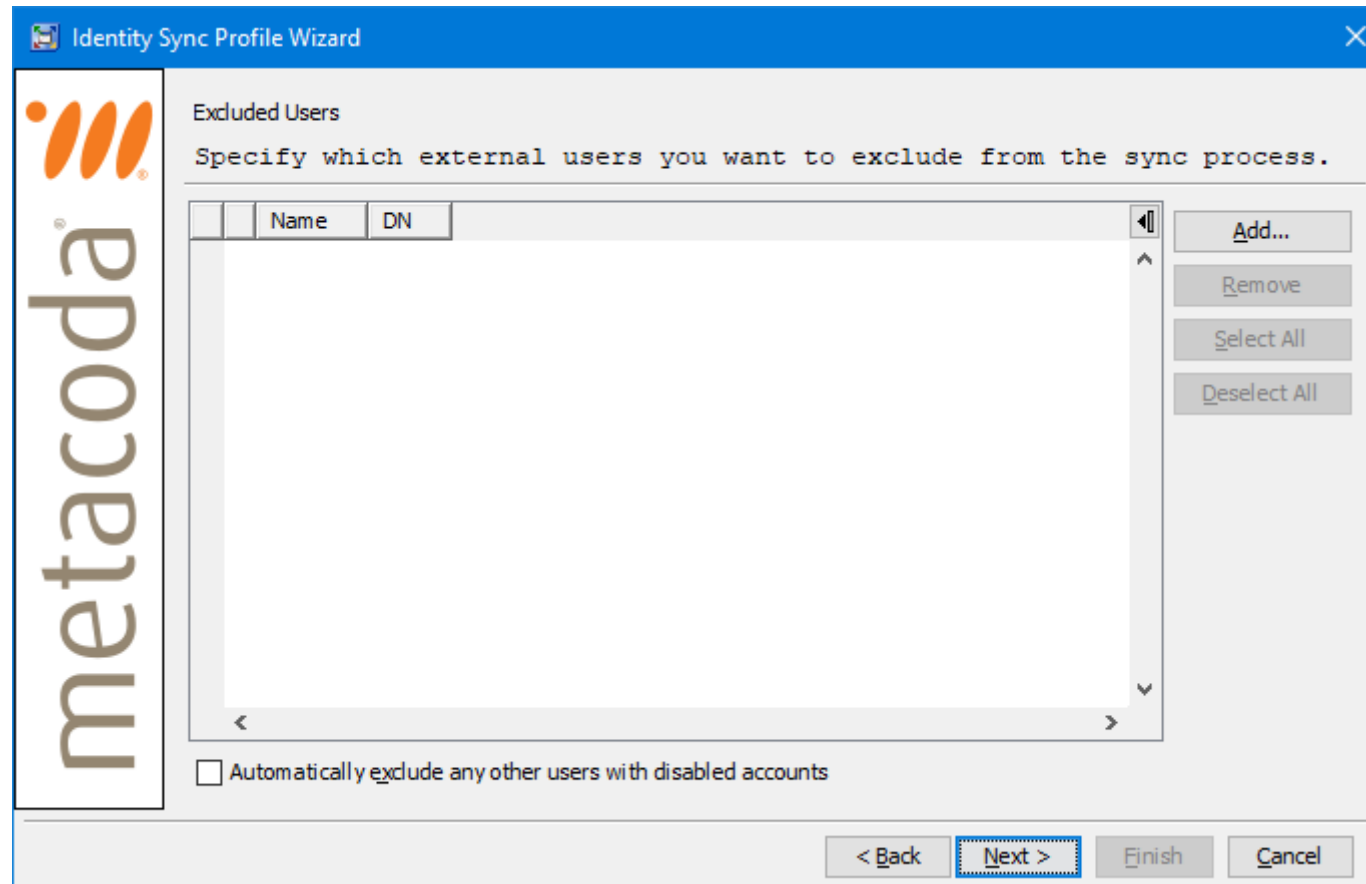
Users DN: OU=Abteilungsbenutzer,DC=lan,DC=huk-coburg,DC=de Search...

KeyId Attribute: objectGUID

< Back Next > Finish Cancel

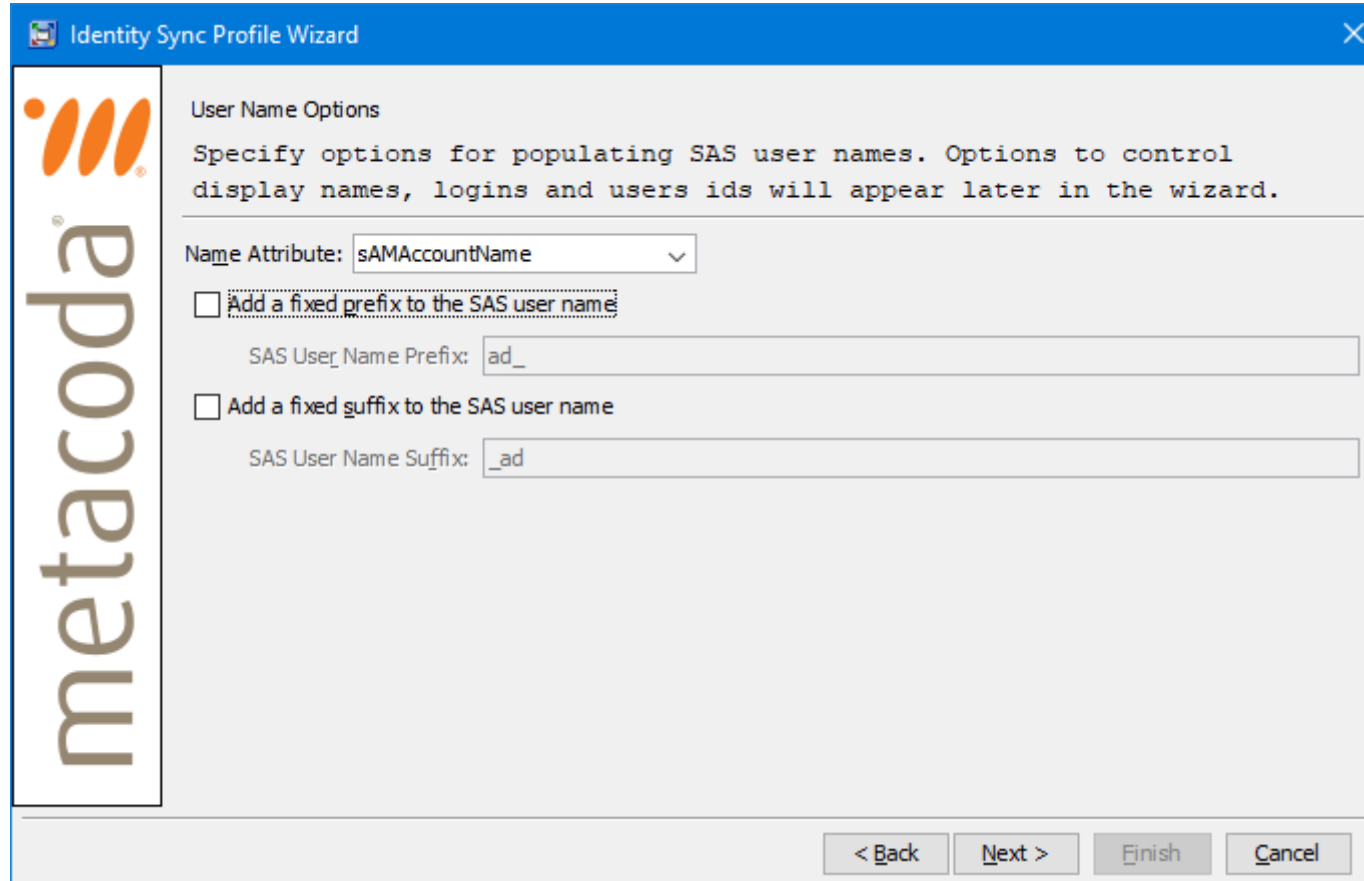
Setup the idsp using the wizard

- You can exclude users as well



Setup the idsp using the wizard

- Same as for groups - User-Name, Pre- und Postfix



The screenshot shows the 'Identity Sync Profile Wizard' window. On the left is a vertical sidebar with the 'metacoda' logo. The main area is titled 'User Name Options' and contains the following text: 'Specify options for populating SAS user names. Options to control display names, logins and users ids will appear later in the wizard.' Below this, there is a 'Name Attribute' dropdown menu set to 'sAMAccountName'. There are two checkboxes: 'Add a fixed prefix to the SAS user name' (unchecked) and 'Add a fixed suffix to the SAS user name' (unchecked). The 'SAS User Name Prefix' field contains 'ad_' and the 'SAS User Name Suffix' field contains '_ad'. At the bottom right are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Identity Sync Profile Wizard

User Name Options

Specify options for populating SAS user names. Options to control display names, logins and users ids will appear later in the wizard.

Name Attribute: sAMAccountName

☐ Add a fixed prefix to the SAS user name

SAS User Name Prefix: ad_

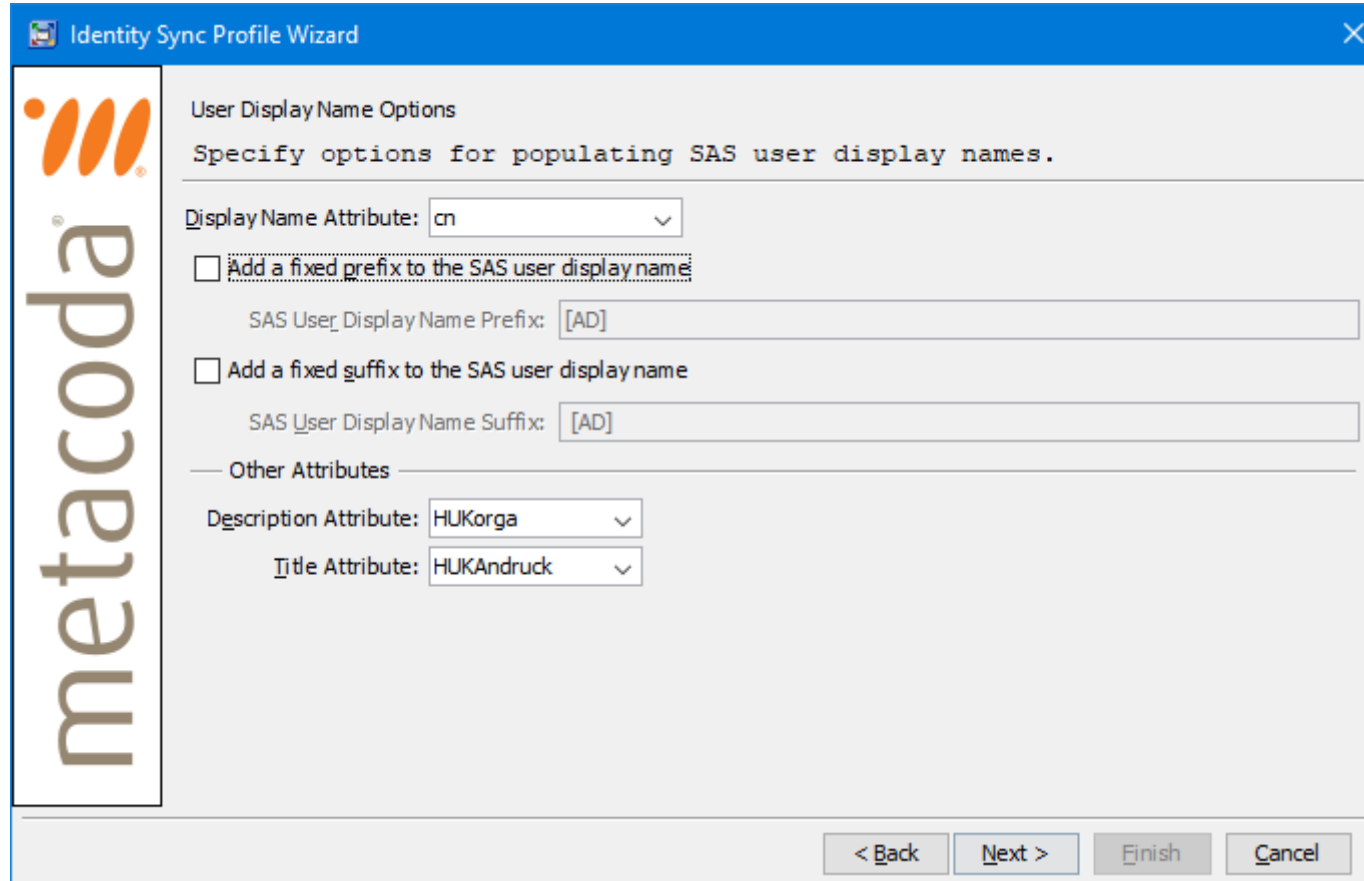
☐ Add a fixed suffix to the SAS user name

SAS User Name Suffix: _ad

< Back Next > Finish Cancel

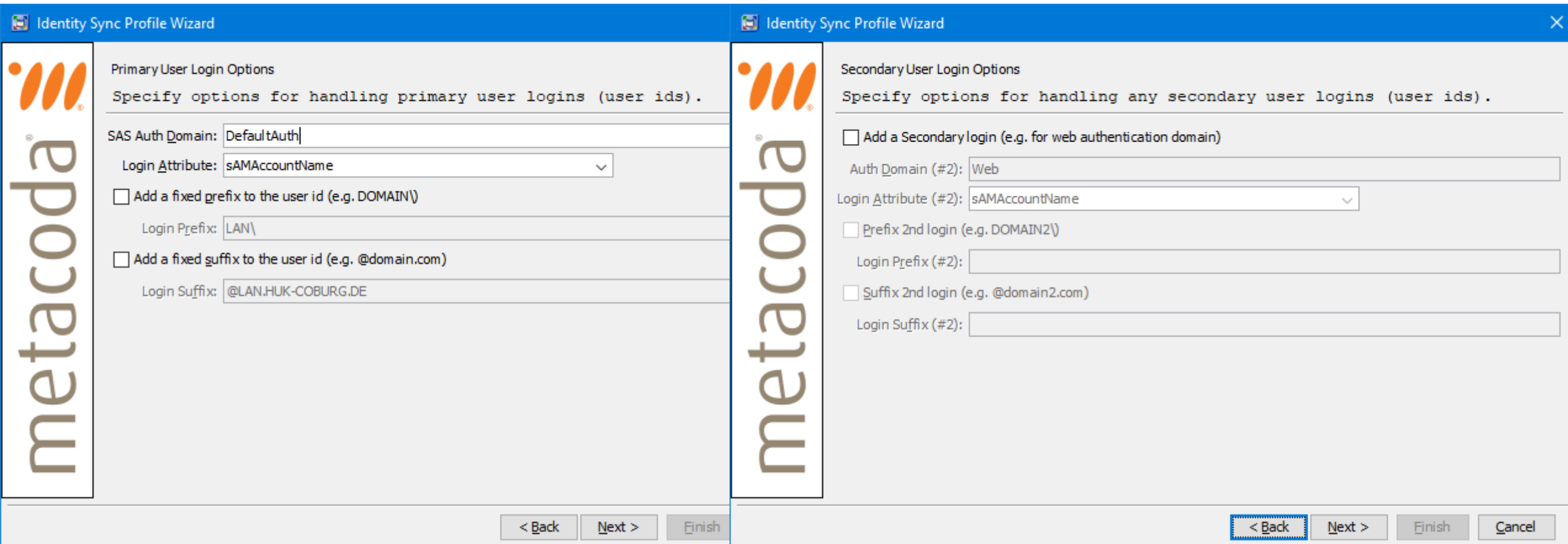
Setup the idsp using the wizard

- ▶ Select AD-attribut for Display Name, Description and Titel
- ▶ All AD-attribut-fields are preset with the standard AD attributes but at the same time free text field, so your own attributes are also possible



Setup the idsp using the wizard

- Choose of Auth Domain, Pre- and Suffix for user id and if needed a second auth domain



Identity Sync Profile Wizard

Primary User Login Options
Specify options for handling primary user logins (user ids).

SAS Auth Domain: DefaultAuth|

Login Attribute: sAMAccountName

☐ Add a fixed prefix to the user id (e.g. DOMAIN\)

Login Prefix: LAN\

☐ Add a fixed suffix to the user id (e.g. @domain.com)

Login Suffix: @LAN.HUK-COBURG.DE

< Back Next > Finish

Identity Sync Profile Wizard

Secondary User Login Options
Specify options for handling any secondary user logins (user ids).

☐ Add a Secondary login (e.g. for web authentication domain)

Auth Domain (#2): Web

Login Attribute (#2): sAMAccountName

☐ Prefix 2nd login (e.g. DOMAIN2\)

Login Prefix (#2):


☐ Suffix 2nd login (e.g. @domain2.com)

Login Suffix (#2):

< Back Next > Finish Cancel

Setup the idsp using the wizard

- An all the other attributes, that should be filled




Identity Sync Profile Wizard

User Email Options
Specify options for populating SAS user email addresses.

☒ Populate User Email Address

Email Type: work

Email Attribute: mail




Identity Sync Profile Wizard

User Phone Options
Specify options for populating SAS user phone numbers.

☒ Populate User Phone Numbers

Phone Type/Label	AD/LDAP Attribute
Work: Office	HUKTelefon
Fax: Office Fax	HUKFax
Mobile: Mobile	HUKMobile
Home: Home	none
Pager: Salutation	HUKanrede
IP Phone: IP Phone	none

< Back Next >



Identity Sync Profile Wizard

User Location Options
Specify options for populating SAS user locations.

☒ Populate User Locations

Location Type: HUK

Address Attribute: HUKstrasse

City Attribute: HUKOrt

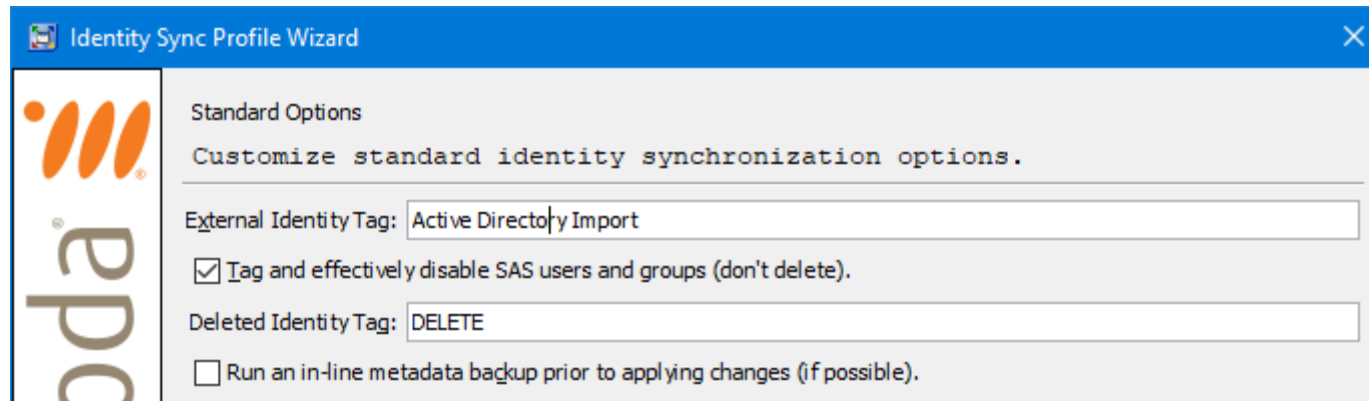
Area Attribute: HUKStandort

Post Code Attribute: HUKplz

Country Attribute: none

Setup the idsp using the wizard

- ▶ External Identity Tag is being filled aswell
- ▶ Login and group membership of users, that are no longer member of a synchronised AD-group, will be deleted and the Display Name gets a TAG like “DELETE”
- ▶ An optional metadata backup can be activated



Identity Sync Profile Wizard

Standard Options
Customize standard identity synchronization options.

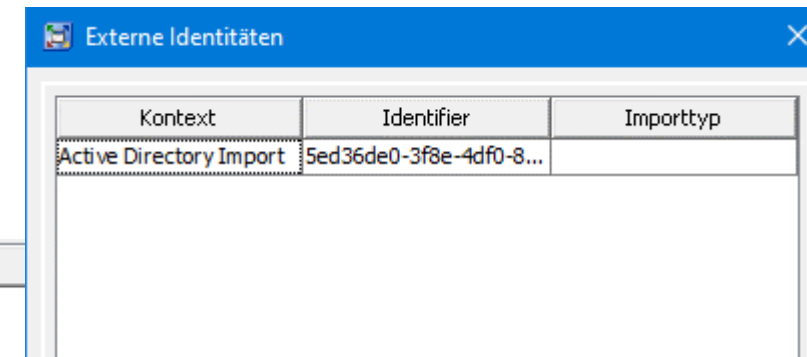
External Identity Tag: Active Directory Import

☒ Tag and effectively disable SAS users and groups (don't delete).

Deleted Identity Tag: DELETE

☐ Run an in-line metadata backup prior to applying changes (if possible).

Benutzer, Gruppe oder Rolle	Beschreibung	Jobtitel
[DELETE] Max Mustermann - TU123456	TE2A	Abteilung Test

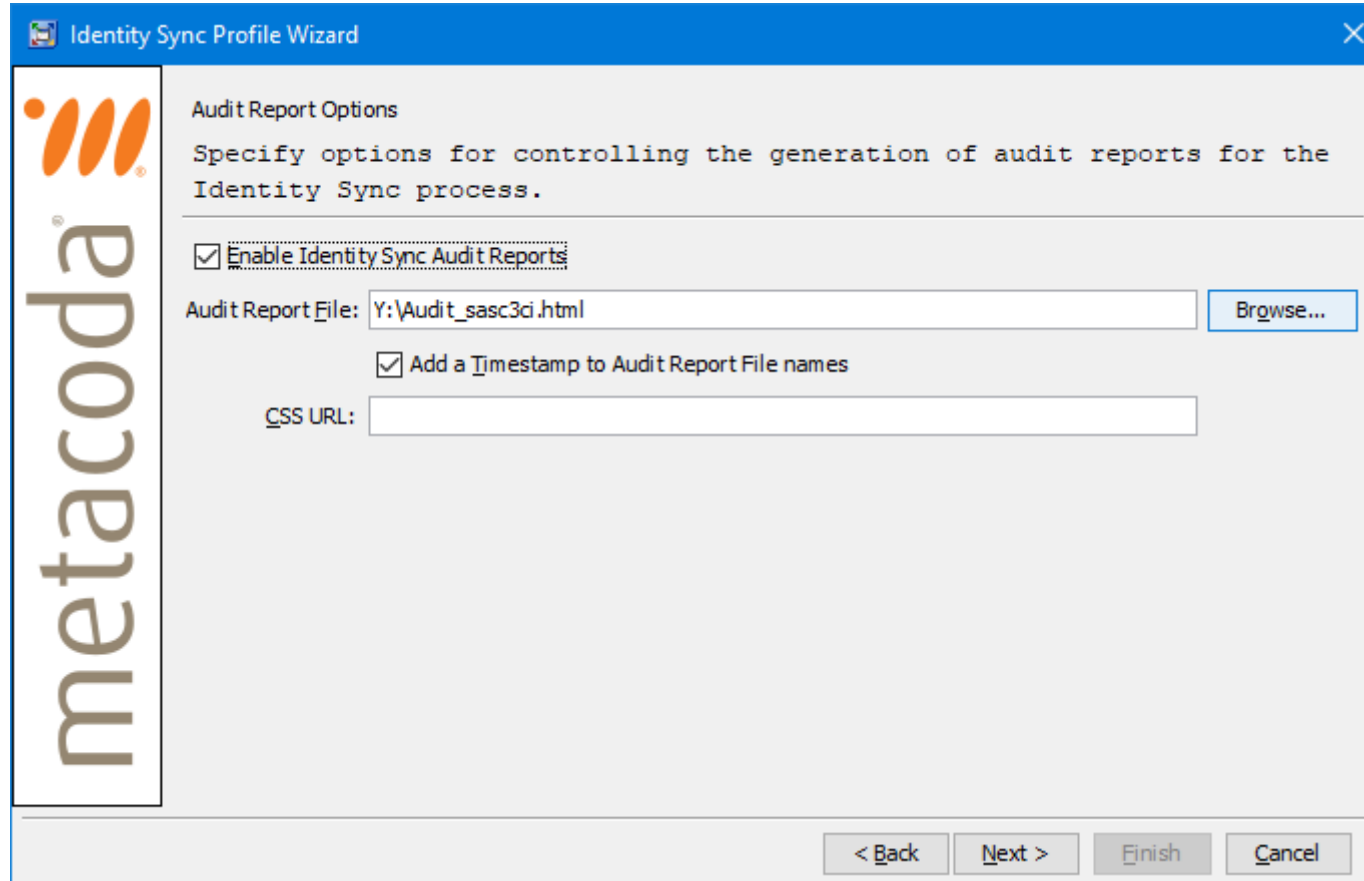


Externe Identitäten

Kontext	Identifier	Importtyp
Active Directory Import	5ed36de0-3f8e-4df0-8...	

Setup the idsp using the wizard

- A report with all the changes can be created



The screenshot shows the 'Identity Sync Profile Wizard' window. On the left is a vertical sidebar with the 'metacoda' logo. The main area is titled 'Audit Report Options' and contains the text: 'Specify options for controlling the generation of audit reports for the Identity Sync process.' Below this, there is a checkbox labeled 'Enable Identity Sync Audit Reports' which is checked. Underneath is a text field for 'Audit Report File:' containing the path 'Y:\Audit_sasc3ci.html', followed by a 'Browse...' button. Another checkbox labeled 'Add a Timestamp to Audit Report File names' is also checked. Below that is a text field for 'CSS URL:'. At the bottom of the window are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Identity Sync Profile: W:\Prz-SAS-IB\IB62\sy053\SASC3CI-PR.idsp

Server: SASCIMAS - Logical Workspace Server

Groups (35) Users (288) Memberships (1.112) Logins (275) Emails (264) Phones (908) Locations (250) Domains (0) Exceptions (82) Validation (0) Failures (0)

	Action	Name	DisplayName	Description	Group Type
1	+ Add Group	ad_GgpAcc-SASC2-IB34-PR	HUK GgpAcc-SASC2-IB34-PR	IB - Anforderungs- u. Rechteservice	
2	+ Add Group	ad_GgpAcc-SASC2-HU00-VV-PR	HUK GgpAcc-SASC2-HU00-VV-PR	HU00 - VA-Report Viewer	
3	+ Add Group	ad_GgpAcc-SASC2-AE41-PR	HUK GgpAcc-SASC2-AE41-PR	AE - Planung und Konzeption	
4	+ Add Group	ad_GgpAcc-SASC2-HU00-DIN-PR	HUK GgpAcc-SASC2-HU00-DIN-PR	HU00 - SAS Data Abteilung IN	
5	+ Add Group	ad_GgpAcc-SASC2-AE44-PR	HUK GgpAcc-SASC2-AE44-PR	AE - Provisions- und Kampagnenmanagement	
6	+ Add Group	ad_GgpAcc-SASC2-HU00-DC-PR	HUK GgpAcc-SASC2-HU00-DC-PR	HU00 - SAS Data Versender	
7	+ Add Group	ad_GgpAcc-SASC2-PZ01-PR	HUK GgpAcc-SASC2-PZ01-PR	PZ - Innendienst Betriebliche Versorgungslösungen	
8	+ Add Group	ad_GgpAcc-SASC2-HU00-DE-PR	HUK GgpAcc-SASC2-HU00-DE-PR	HU00 - SAS Data Entwickler	
9	+ Add Group	ad_GgpAcc-SASC2-IN16-PR	HUK GgpAcc-SASC2-IN16-PR	IN16 - Internetbearbeitung	
10	+ Add Group	ad_GgpAcc-SASC2-IN17-PR	HUK GgpAcc-SASC2-IN17-PR	IN17 - Internetbearbeitung	
11	+ Add Group	ad_GgpAcc-SASC2-IN14-PR	HUK GgpAcc-SASC2-IN14-PR	IN14 - Internetbearbeitung	
12	+ Add Group	ad_GgpAcc-SASC2-IB62-PR	HUK GgpAcc-SASC2-IB62-PR	IB - DB-/DC-Systeme Service Produkte	
13	+ Add Group	ad_GgpAcc-SASC2-IB11-PR	HUK GgpAcc-SASC2-IB11-PR	IB - Storage- und Backup-Management	
14	+ Add Group	ad_GgpAcc-SASC2-HU00-CIStudio-PR	HUK GgpAcc-SASC2-HU00-CIStudio-PR	Berechtigt für das SAS CI Studio	
15	+ Add Group	ad_GgpAcc-SASC2-HU00-DA-PR	HUK GgpAcc-SASC2-HU00-DA-PR	HU00 - SAS Data Analyst	
16	+ Add Group	ad_GgpAcc-SASC2-AE82-PR	HUK GgpAcc-SASC2-AE82-PR	AE - Dokumentenmanagement & Basiskomponenten	
17	+ Add Group	ad_GgpAcc-SASC2-HU00-DS-PR	HUK GgpAcc-SASC2-HU00-DS-PR	HU00 - SAS Data Spezialist	
18	+ Add Group	ad_GgpAcc-SASC2-HU00-PR	HUK GgpAcc-SASC2-HU00-PR	HU - HUK24	
19	+ Add Group	ad_GgpAcc-SASC2-PR	HUK GgpAcc-SASC2-PR	SASC2-User	
20	→ Update Group	ad_GgpAcc-SASC1-AE63-PR	[DELETE] HUK GgpAcc-SASC1-AE63-PR	AE - Business Intelligence I	
21	→ Update Group	ad_GgpAcc-SASC1-MA-MO-PR	[DELETE] HUK GgpAcc-SASC1-MA-MO-PR	Berechtigt Marketing für SAS MO	
22	→ Update Group	ad_GgpAcc-SASC1-WMRD-PR	[DELETE] HUK GgpAcc-SASC1-WMRD-PR	WMRD - Distributed Marketing User	
23	→ Update Group	ad_GgpAcc-SASC1-PR	[DELETE] HUK GgpAcc-SASC1-PR	SASC1-User	
24	→ Update Group	ad_GgpAcc-SASC1-MA21-PR	[DELETE] HUK GgpAcc-SASC1-MA21-PR	MA - Marketing Grundsatzfragen	
25	→ Update Group	ad_GgpAcc-SASC1-MA21-CI-PR	[DELETE] HUK GgpAcc-SASC1-MA21-CI-PR	Berechtigt MA21 für SAS CI	
26	→ Update Group	ad_GgpAcc-SASC1-MA41-CI-PR	[DELETE] HUK GgpAcc-SASC1-MA41-CI-PR	Berechtigt Marketing für SAS CI	
27	→ Update Group	ad_GgpAcc-SASC1-AE65-PR	[DELETE] HUK GgpAcc-SASC1-AE65-PR	AE - Business Intelligence II	
28	→ Update Group	ad_GgpAcc-SASC1-AE44-PR	[DELETE] HUK GgpAcc-SASC1-AE44-PR	AE - Provisions- und Kampagnenmanagement	
29	→ Update Group	ad_GgpAcc-SASC1-MA2A-PR	[DELETE] HUK GgpAcc-SASC1-MA2A-PR	MA21 - Marketing Grundsatzfragen	
30	→ Update Group	ad_GgpAcc-SASC1-AE41-PR	[DELETE] HUK GgpAcc-SASC1-AE41-PR	AE - Planung und Konzeption	
31	→ Update Group	ad_GgpAcc-SASC1-AK-PR	[DELETE] HUK GgpAcc-SASC1-AK-PR	AK - Aktivist Komposit	

What do we have now?

- ▶ Manual user administration → Still manually, but now by SAS-admins with just one click
- ▶ Maintenance of users through separate user administration → Automated
- ▶ No comparison when user information changes → Automatic
- ▶ No regular checks of user rights → Process still manual
- ▶ Lots of old entries in metadata → Done
- ▶ Frequent coordination with user administration required → Not needed anymore
- ▶ Special cases or problems still had to be solved by SAS-admins → Special cases and problems reduced to a minimum
- ▶ Applications for rights are mainly made by email → Applications are made via HUK's own ordering process

Agenda

- 1 Initial situation
- 2 The tool of choice
- 3 Preparation in AD
- 4 The implementation in SMC
- 5 Let's automate it**
- 6 Regular checks

Let's automate it – With the SAS Metacoda Batch Interface

- ▶ Allows automation of AD synchronization
- ▶ In addition, it offers various checks to control metadata security
- ▶ Must have access to an SMC (no problem thanks to GPFS)
- ▶ Initial configuration somewhat complex, afterwards "no" adjustments are necessary
- ▶ The previously created idsp is used - an easy-to-edit XML
- ▶ Technical users who are registered in the metadata must be excluded from the sync
- ▶ Automate via crontab:
Metacoda AD-Sync and Security-Check
- ▶ `15 0 * * * /gpfs/sasconf/config/grid/misc/3rdparty/metacoda/sasc3ci/SASC3CI_AD_SYNC.sh >>/dev/null 2>&1`


```

<SyncException tableName="IdGrps" filter="upcase(name) = &quot;DATA MANAGEMENT BUSINESS USERS&quot;;" desc="Data Management Business Users"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;DATA MANAGEMENT EXECUTIVES&quot;;" desc="Data Management Executives"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;DATA MANAGEMENT POWER USERS&quot;;" desc="Data Management Power Users"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;DATA MANAGEMENT STEWARDS&quot;;" desc="Data Management Stewards"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;DATA MANAGEMENT: OPERATION&quot;;" desc="Data Management: Operation"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;DATA MANAGEMENT: PROCESS ORCHESTRATION&quot;;" desc="Data Management: Process Orchestration"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;DATA REMEDIATION: ISSUE ADMINISTRATION&quot;;" desc="Data Remediation: Issue Administration"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;DATA REMEDIATION: ISSUE MANAGEMENT&quot;;" desc="Data Remediation: Issue Management"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;DATA REMEDIATION: ISSUE VIEW&quot;;" desc="Data Remediation: Issue View"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;ENTERPRISE GUIDE: ADVANCED&quot;;" desc="Enterprise Guide: Advanced"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;ENTERPRISE GUIDE: ANALYSIS&quot;;" desc="Enterprise Guide: Analysis"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;ENTERPRISE GUIDE: OLAP&quot;;" desc="Enterprise Guide: OLAP"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;ENTERPRISE GUIDE: PROGRAMMING&quot;;" desc="Enterprise Guide: Programming"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;HOME: ADMINISTRATION&quot;;" desc="Home: Administration"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;HOME: USAGE&quot;;" desc="Home: Usage"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;JOB EXECUTION: JOB ADMINISTRATOR&quot;;" desc="Job Execution: Job Administrator"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;JOB EXECUTION: JOB DESIGNER&quot;;" desc="Job Execution: Job Designer"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;JOB EXECUTION: JOB SCHEDULER&quot;;" desc="Job Execution: Job Scheduler"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;JOB EXECUTION: JOB SUBMITTER&quot;;" desc="Job Execution: Job Submitter"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;JOB MONITOR: OPERATION&quot;;" desc="Job Monitor: Operation"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;MANAGEMENT CONSOLE: ADVANCED&quot;;" desc="Management Console: Advanced"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;MANAGEMENT CONSOLE: CONTENT MANAGEMENT&quot;;" desc="Management Console: Content Management"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;META: OPERATORS ROLE&quot;;" desc="Metadata Server: Operation"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;META: UNRESTRICTED USERS ROLE&quot;;" desc="Metadata Server: Unrestricted"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;META: USER AND GROUP ADMINISTRATORS ROLE&quot;;" desc="Metadata Server: User Administration"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;PROCESS ORCHESTRATION: JOB ADMINISTRATION&quot;;" desc="Process Orchestration: Job Administration"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;PROCESS ORCHESTRATION: JOB DEVELOPMENT&quot;;" desc="Process Orchestration: Job Development"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;PROCESS ORCHESTRATION: JOB EXECUTION&quot;;" desc="Process Orchestration: Job Execution"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;PUBLIC&quot;;" desc="PUBLIC"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;SAS GENERAL SERVERS&quot;;" desc="SAS General Servers"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;SAS STUDIO: REPORT CONSUMER&quot;;" desc="SAS Studio: Report Consumer"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;SAS STUDIO: USAGE&quot;;" desc="SAS Studio: Usage"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;SAS SYSTEM SERVICES&quot;;" desc="SAS System Services"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;SAS_EV_APPSERVER_TIER&quot;;" desc="SAS Environment Manager App Server Tier Users"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;SAS_EV_GUEST&quot;;" desc="SAS Environment Manager Guests"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;SAS_EV_SUPER_USER&quot;;" desc="SAS Environment Manager Super Users"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;SASADMINISTRATORS&quot;;" desc="SAS Administrators"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;SASUSERS&quot;;" desc="SASUSERS"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;TASK MANAGER: TASK ADMINISTRATION&quot;;" desc="Task Manager: Task Administration"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;TASK MANAGER: TASK MANAGEMENT&quot;;" desc="Task Manager: Task Management"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;TASK MANAGER: TASK VIEW&quot;;" desc="Task Manager: Task View"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;THEME DESIGNER FOR FLEX: ADMINISTRATION&quot;;" desc="Theme Designer for Flex: Administration"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;TSADMIN&quot;;" desc="Table Server Administrators (9.2)"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;VISUAL ANALYTICS DATA ADMINISTRATORS&quot;;" desc="Visual Analytics Data Administrators"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;VISUAL ANALYTICS USERS&quot;;" desc="Visual Analytics Users"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;VISUAL ANALYTICS: ADMINISTRATION&quot;;" desc="Visual Analytics: Administration"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;VISUAL ANALYTICS: ANALYSIS&quot;;" desc="Visual Analytics: Analysis"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;VISUAL ANALYTICS: BASIC&quot;;" desc="Visual Analytics: Basic"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;VISUAL ANALYTICS: DATA BUILDING&quot;;" desc="Visual Analytics: Data Building"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;VISUAL ANALYTICS: REPORT VIEWING&quot;;" desc="Visual Analytics: Report Viewing"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;VISUAL DATA BUILDER ADMINISTRATORS&quot;;" desc="Visual Data Builder Administrators"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;WEB REPORT STUDIO: ADVANCED&quot;;" desc="Web Report Studio: Advanced"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;WEB REPORT STUDIO: REPORT CREATION&quot;;" desc="Web Report Studio: Report Creation"/>
<SyncException tableName="IdGrps" filter="upcase(name) = &quot;WEB REPORT STUDIO: REPORT VIEWING&quot;;" desc="Web Report Studio: Report Viewing"/>
<SyncException tableName="Logins" filter="upcase(userid) = &quot;SVCSASTUHU&quot;;" desc="svcSASTuHU"/>
<SyncException tableName="Person" filter="upcase(keyid) = &quot;999C324D-709F-465D-B7F0-751F0B3CA064&quot;;" desc="svcSASTuIB"/>
<SyncException tableName="Person" filter="upcase(keyid) = &quot;EF451B09-3600-485A-8836-C980192E831D&quot;;" desc="svcSASTuIB"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;LSFADMIN&quot;;" desc="LSF Administrator"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;LSFUSER&quot;;" desc="LSF User"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;SAS&quot;;" desc="SAS Installer"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;SASADM&quot;;" desc="SAS Administrator"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;SASDEMO&quot;;" desc="SAS Demo User"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;SASEVS&quot;;" desc="SAS Environment Manager Service Account"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;SASGUEST&quot;;" desc="SAS Guest User (9.1.3)"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;SASRMDT&quot;;" desc="SAS Data Remediation Services User"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;SASSEARCH&quot;;" desc="Search Interface to SAS Content User"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;SASSRV&quot;;" desc="SAS General Servers"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;SASTRUST&quot;;" desc="SAS Trusted User"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;SASWBADM&quot;;" desc="SAS Web Administrator (9.1.3)"/>
<SyncException tableName="Person" filter="upcase(name) = &quot;WEBANON&quot;;" desc="SAS Anonymous Web User"/>

```

What do we have now?

- ▶ Manual user administration → Automated
- ▶ Maintenance of users through separate user administration → Automated
- ▶ No comparison when user information changes → Automatic
- ▶ No regular checks of user rights → Process still manual
- ▶ Lots of old entries in metadata → Done
- ▶ Frequent coordination with user administration required → Not needed anymore
- ▶ Special cases or problems still had to be solved by SAS-admins → Special cases and problems reduced to a minimum
- ▶ Applications for rights are mainly made by email → Applications are made via HUK's own ordering process

Agenda

- 1 Initial situation
- 2 The tool of choice
- 3 Preparation in AD
- 4 The implementation in SMC
- 5 Let's automate it
- 6 Regular checks**

Regular checks

- ▶ Metacoda AD-sync writes all changes to the report
- ▶ Metacoda Security Test enables current metadata to be checked against a template
- ▶ Both run automatically via the Metacoda Batch Interface
- ▶ Sends Mail when an “Error”/Mismatch occurs
- ▶ Security Test runs weekly

Regular Checks – Metacoda AD-Sync



Metacoda Identity Sync Audit Report



Summary Report

Overview

Date/Time	15Sep2020:00:15:25
Client Operating System User Id	svcsasc3
Source Identity Environment	Microsoft Active Directory Server: lan.huk-coburg.de
Target Identity Environment	SAS Metadata Server: sasc3cim.lan.huk-coburg.de:16061
SAS Metadata Identity	SAS Administrator
SAS Workspace Identity	[same as SAS metadata identity]
Identity Sync State	Source/target identity changes have been applied.
Configured Sync Exceptions/Exclusions?	Yes (82)
Source Groups Extracted?	Yes (19)
Source Users Extracted?	Yes (41)
Target (SAS Metadata) Identity Changes Required?	Yes
... Validation Errors?	No (0)
... Target Group Changes?	Yes (2) : 0 group(s) added, 2 group(s) updated, 0 group(s) removed
... Target User Changes?	Yes (10) : 0 user(s) added, 10 user(s) updated, 0 user(s) removed
... Target Group/Role Membership Changes?	No (0) : 0 membership(s) added, 0 membership(s) removed
... Target Login Changes?	No (0) : 0 login(s) added, 0 login(s) removed
... Target Email Changes?	No (0) : 0 email(s) added, 0 email(s) updated, 0 email(s) removed
... Target Phone Changes?	No (0) : 0 phone(s) added, 0 phone(s) updated, 0 phone(s) removed
... Target Location Changes?	No (0) : 0 location(s) added, 0 location(s) updated, 0 location(s) removed
... Target Auth Domain Changes?	No (0) : 0 domain(s) added, 0 domain(s) updated, 0 domain(s) removed
Failures when Applying Changes?	No (0)

Identity Changes

Group/Role Changes


#	Action	Name	Display Name	Description	Group Type	Old Name	Old Display Name	Old Description
1	 Update Group	ad_GgpDel-AZ01179-HU00	[DELETE] HUK GgpDel-AZ01179-HU00	Abordnungsgruppe gültig vom 13.05.2019 bis zum 29.02.2020		ad_GgpDel-AZ01179-HU00	[DELETE] HUK GgpDel-AZ01179-HU00	Abordnungsgruppe gültig vom 13.05.2019 bis zum 29.02.2020
2	 Update Group	ad_GgpDel-AZ01185-HU00	[DELETE] HUK GgpDel-AZ01185-HU00	Abordnungsgruppe gültig vom 01.08.2019 bis zum 14.03.2020		ad_GgpDel-AZ01185-HU00	[DELETE] HUK GgpDel-AZ01185-HU00	Abordnungsgruppe gültig vom 01.08.2019 bis zum 14.03.2020

User Changes

Regular Checks – Metacoda Security Test



Metacoda Plug-ins: Security Testing Framework Report



Metadata Security Test Failures
Some metadata security tests have failed.
Details of the individual failures are provided below.

Summary

Started:	13Sep2020 00:30:08
Finished:	13Sep2020 00:30:19
Elapsed:	10 seconds
Tests Run:	173,990
Tests Failed:	12

Details

#	Test	Reason
1	ACTs/ACT('Customer Intelligence Template')/Objects/complete	The test specifies a COMPLETE set of protected objects for the Access Control Template (ACT) 'Customer Intelligence Template'. The test has failed because the ACT was actually found to be applied to an additional 2 unspecified objects. Additional test failures will occur for each unspecified object.
2	ACTs/ACT('Customer Intelligence Template')/Objects/complete/+Selection campaign '/HUK24/HUK24CI/HUK24_Context/2020/H24_Servicemailing_KFZ_Rueckerstattung'	The test specifies a COMPLETE set of protected objects for the Access Control Template (ACT) 'Customer Intelligence Template'. The test has failed because the ACT was also found to be applied to the unspecified Selection campaign '/HUK24/HUK24CI/HUK24_Context/2020/H24_Servicemailing_KFZ_Rueckerstattung'.
3	ACTs/ACT('Customer Intelligence Template')/Objects/complete/+Selection campaign '/HUK24/HUK24CI/HUK24_Context/2020/H24_KWK_HR_JW_2020'	The test specifies a COMPLETE set of protected objects for the Access Control Template (ACT) 'Customer Intelligence Template'. The test has failed because the ACT was also found to be applied to the unspecified Selection campaign '/HUK24/HUK24CI/HUK24_Context/2020/H24_KWK_HR_JW_2020'.
4	Users/User('AZ01179')/displayName	Mismatched displayName found. Expected <"[DELETE]"> but got <"[DELETE] Max Mustermann - TU123456">.
5	Users/User('AZ01179')/desc	Mismatched desc found. Expected <"[REDACTED]"> but got <"TE2A">.
6	Users/User('AZ01179')/title	Mismatched title found. Expected <"Abteilung [REDACTED]"> but got <"Abteilung Test">.
7	Users/User('')/DirectGroupMemberships/complete	The test specifies a COMPLETE set of DIRECT group memberships for the user 'i [REDACTED]'. The test has failed because they were actually found to be a direct member of an additional 1 unspecified group. Additional test failures will occur for each unspecified group.
8	Users/User('HU00-VV')/DirectGroupMemberships/complete/+ad_GgpAcc-SASC2-HU00-VV-PR'	The test specifies a COMPLETE set of DIRECT group memberships for the user 'i [REDACTED]'. The test has failed because that user was also found to be a direct member of the unspecified group 'ad_GgpAcc-SASC2-HU00-VV-PR'.
9	Users/User('')/Capabilities/Capabilities('Visual Analytics 7.5:/Add and View Comments')/granted	The test has failed because the capability was found to be granted when the test specified it should have been NOT granted.
10	Users/User('')/Capabilities/Capabilities('Visual Analytics 7.5:/Personalization')/granted	The test has failed because the capability was found to be granted when the test specified it should have been NOT granted.
11	Groups/Group('ad_GgpAcc-SASC2-HU00-VV-PR')/DirectMembers/complete	The test specifies a COMPLETE set of DIRECT members for the group 'ad_GgpAcc-SASC2-HU00-VV-PR'. The test has failed because there were actually found to be an additional 1 unspecified member. Additional test failures will occur for each unspecified member.
12	Groups/Group('ad_GgpAcc-SASC2-HU00-VV-PR')/DirectMembers/complete/+user 'i [REDACTED]'	The test specifies a COMPLETE set of DIRECT members for the group 'ad_GgpAcc-SASC2-HU00-VV-PR'. The test has failed because the user 'i [REDACTED]' was unspecified but was found to be a direct member of that group.

SAS Software distribution

- ▶ SAS-Software packed using NetInstall/DSM
- ▶ Authorization is based on AD
- ▶ Application uses the same process, we use for the rights (AD-Sync)
- ▶ Users order the software and the rights in one process and get both till the next day

Further Information

- ▶ 30-day free test of metacoda available <https://www.metacoda.com/en/products/security-plug-ins/>
- ▶ Using SAS-Macro to write your sync by yourself
<https://documentation.sas.com/?docsetId=bisecag&docsetTarget=n0l2hp5m00a1z2n1b598q4pknfih.htm&docsetVersion=9.4&locale=en>