One Identity

Identity Manager Implementation Certification (#IM-IC)

Student Lab Manual

September - 2022

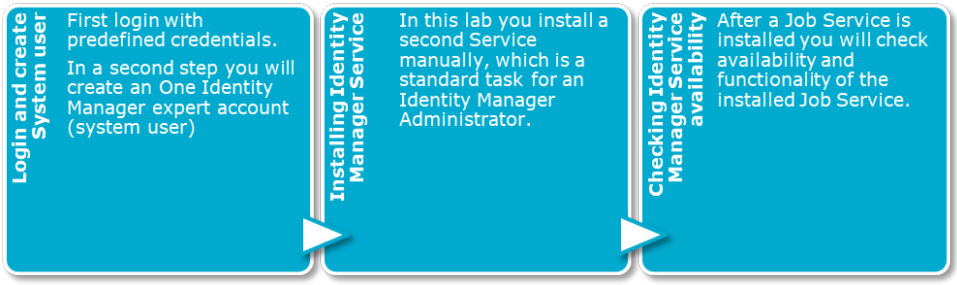
Table Of Content

skip table of contents

Hide table of contents

Lab Exercise: Add Identity Manager Service (IM-INS-02)

Exercise Overview



In this lab you install the Identity Manager Service for Active Directory. The lab includes instructions on how to configure the Server Service on the AD server and how to check the service availability.

> **NOTE:**
> The Identity Manager Service on the DB server was installed earlier, automatically, using the Installation Wizard. This lab shows how to install (or add) an Identity Manager Service manually.

What you need to know

- You should have the images open and running for this lab.
- You need the installation resources stored on i: = \\IAMS10\install. To take the right software version please ask your trainer.

User credentials required for this lab

Affected Machines	IAMS01,IAMS02,IAMS03,IAMS04, IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin
Identity Manager service account	
Username	iam\svc_1im_service
Password	I.4Madmin
SQL Connection	
Username	svc_1IM_SQL
Password	I.4Madmin
Identity Manager - system user	
Username	[your system user] or training
Password	I.4Madmin

Estimated Time To Complete This Lab: **20 minutes**

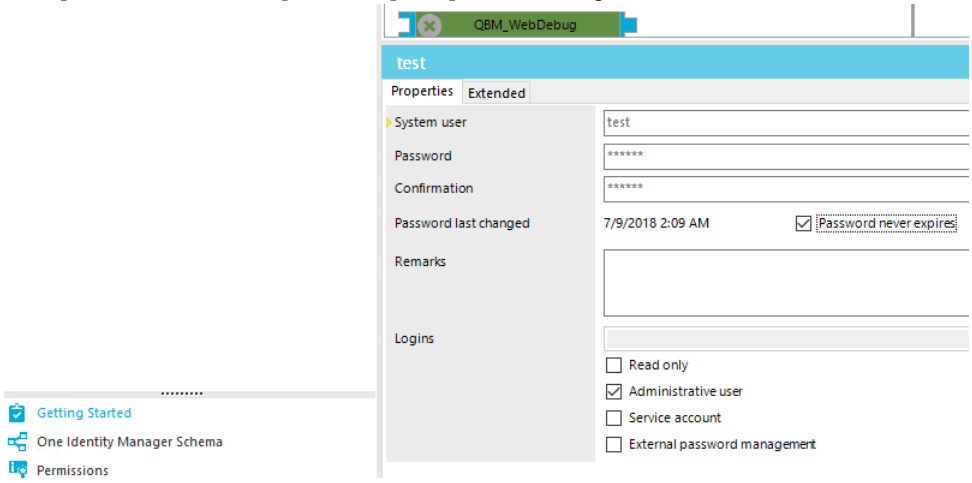
Lab Exercise

Login and create system user

- Logon to the Admin Workstation (IAMW01) as IAM\administrator
- Run **Launchpad** from the Start menu.
  - Connection: ***IAMS02\IAMDB***
  - Authentication method: ***System user***
  - User: ***Training***
    ([your system user] if database was manually installed)
  - Password: ***I.4Madmin***
    ([your system user password] if database was manually installed)

NOTE:
System user and password maybe was predefined during initial installation (typically not part of a course). If this was not the case, please use System user: Training, Password: I.4Madmin to sign in. We try to use Launchpad to start any other admin front-end in order to simplify the login process.
Each Identity Manager - System User is like an account for Identity Manager but can act as well like a role to assign Identity Manager entitlements. IAG experts working with Identity Manager typically gets their personalized System user. This account will now be created.

- Start **Designer** from **Launchpad**, click **Manager system users** from **Configure** tab (**RUN** button).
  In Designer:
- Select **Getting started**
- Click on **Create system user** to create your Identity Manager account
  - Note your system user name.
  - Note your system user password.
  - Click **[OK]**.
- On the property form:
  - Password never expires: ***checked***
  - Administrative user: ***checked***
- Click **[Commit to database]** and click **[Save]** to store changes



- Close Designer. You are now able to login with your personalized System user.

NOTE:
There are more ways to create a system user. In this scenario we created a system user with super admin privileges (Administrative user). In difference to a standard system user, this account collects continuously nearly all permissions. This type of user is only for experts. In a productively used environment this type of system users should be closely monitored for security reason.

Installing Identity Manager Service

- In Launchpad select One Identity Manager Service for database from the Installation overview tab and click [Run].

NOTE:
Two ways to add an Identity Manager Job Service using Launchpad:

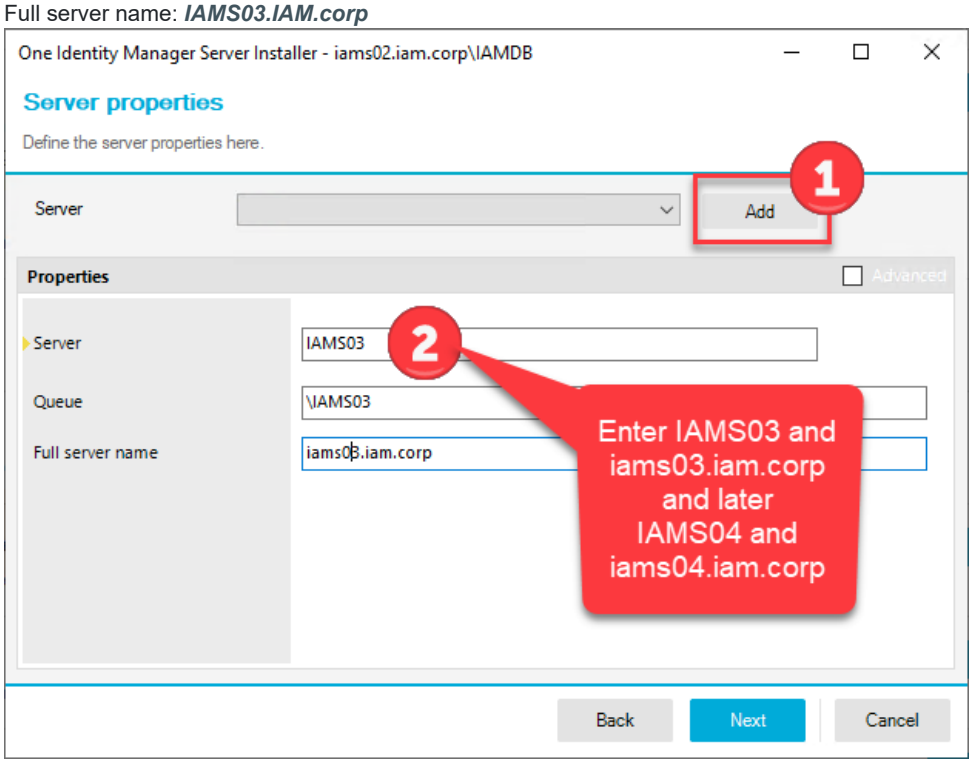
- Installation overview / One Identity Manager Service for Database
- Configure / Add or modify a job server

In case of adding a Job Service to an installation you can use both options. We prefer to use the first option in this lab, because the wizard getting started, can be used easily and straight forward.
Please note: The first option allows to select an already in the database inserted Job service. BUT it is possible to add a NEW service as well!

S T O P

→ START with a click on **[Add]!**→ (1) in the picture below.

- In Identity Manager Server Installer
  - Click **[Next]**
  - If necessary, select a connection and login with your system user credentials (normally all was set automatically).
  - Click **[Next]**
  - Click **[Add]** Define Server Properties:
    - Server: ***IAMS03***
    - Queue: ***\IAMS03***
    - Full server name: ***IAMS03.IAM.corp***



  - Click **[Next]**
  - From the **Machine roles** tab
    - select:
      - Job Server,
      - Active Directory,
      - Microsoft Exchange
      - SCIM
    - Click **[Next]**
  - From the Server functions tab
    - Keep all the default selections
    - Click **[Next]**
  - In **Service settings**
    - select queuex

        - Set Process request interval 30

> **NOTE:**
> In a production environment we try not to stress the database with many requests from many services all the time. Because of this, 90 seconds is a proper default to re-query the database. In a development environment, waiting on job execution in front of a monitoring tool, 90 seconds can be a bit long. Because of this, and only for a development environment, we configure this value to 30 seconds (few server services only). Any values below 30 seconds might lead to handshake problems and increases the service reaction time.

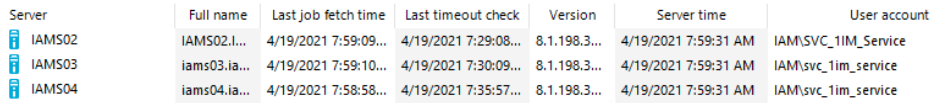
        - Click **[Next]**.
    - Answer the question to install the software now remotely on the server with **[Yes]**.
    - Select the install source if needed
        - Browse for folder **I:\OI-Manager\[Name of the current product and version] (\\IAMS10\Install\OI-Manager\[Name of the current product version we use in this training])**
        - Click **[OK]**
        - Wait until a green checkmark to appear. Click **[Next]**.
    - On **Server access** configure
        - Computer: ***IAMS03***
        - User: ***IAM\SVC_1IM_Service***
        - Password: ***I.4Madmin***
        - Click **[Next]**.

> **NOTE:**
> During the installation, it is possible that a positive answer is required to grant the permission to **login as a service** for the above specified user.

- Click **[Next]** and **[Finish]** to end the wizard.
- Repeat the same steps (2-3.) to install a server service on **IAMS04 (IAMS04.IAM.corp)**. This time you need to configure flags for **LDAP Directories, SharePoint** and **SCIM**. If there are questions, your trainer will like to answer them.

Checking Identity Manager Service availability

- From **Launchpad** start **Manage/Check system status** to start Jobqueue Info in order to monitor our system and check the health of our installed Identity Manager Service.
- In Jobqueue Info
    - Select tab **Job Server**
    - Click into the **Job Server** dialog and press **F6** to reload the entries and **F5** to refresh the status (optionally you can use the context menu).



Server	Full name	Last job fetch time	Last timeout check	Version	Server time	User account
IAMS02	IAMS02.I...	4/19/2021 7:59:09...	4/19/2021 7:29:08...	8.1.198.3...	4/19/2021 7:59:31 AM	IAM\SVC_1IM_Service
IAMS03	iams03.ia...	4/19/2021 7:59:10...	4/19/2021 7:30:09...	8.1.198.3...	4/19/2021 7:59:31 AM	IAM\svc_1im_service
IAMS04	iams04.ia...	4/19/2021 7:58:58...	4/19/2021 7:35:57...	8.1.198.3...	4/19/2021 7:59:31 AM	IAM\svc_1im_service

> **NOTE:**
> The server icons for IAMS02, IAMS03 and IAMS04 should return as blue icons after a few seconds. This indicates the Identity Manager server services are up and running.

        - Right click on **Server IAMS02** and select **Show in browser** from the context menu.
- In the fresh opened internet browser select **Log File** and follow all messages down to the end. You should see some green lines indicating that jobs were successfully processed.
- Step back to **Jobqueue Info** and repeat step 2.c and 3 for server IAMS03 and IAMS04.

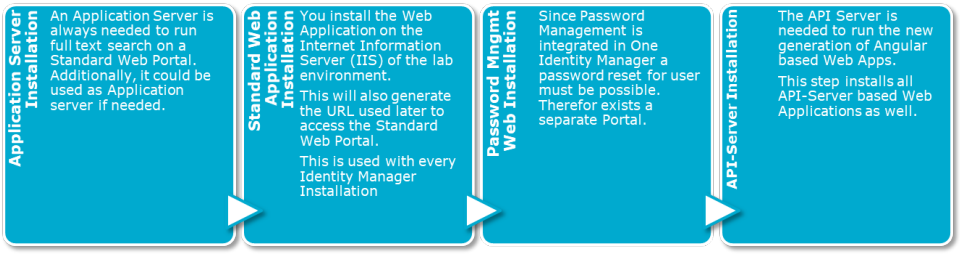
> **NOTE:**
> This time you may see an error talking about a dropped or missing HTML connection. This can be ignored.
> The encryption warning can also be ignored. In a training we will not work with encrypted connections or data.

Follow the messages to the end. You should see the same green lines as before. This is because of a timing issue during the installation.

Lab Exercise Complete

Lab Exercise: Installation Web Applications (IM-INS-03)

Exercise Overview



In this lab you will install several One Identity Web Applications on your IIS Server.

What you need to know

- You should have the images open and running for this lab.
- You need the installation resources stored on i:=\\iams10\install. Your trainer will tell you which setup set to take.

User credentials required for this lab

Affected Machines	IAMS03, IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin
SQL Connection	
Username	svc_1IM_SQL
Password	I.4Madmin

Estimated Time To Complete This Lab: **30 minutes**

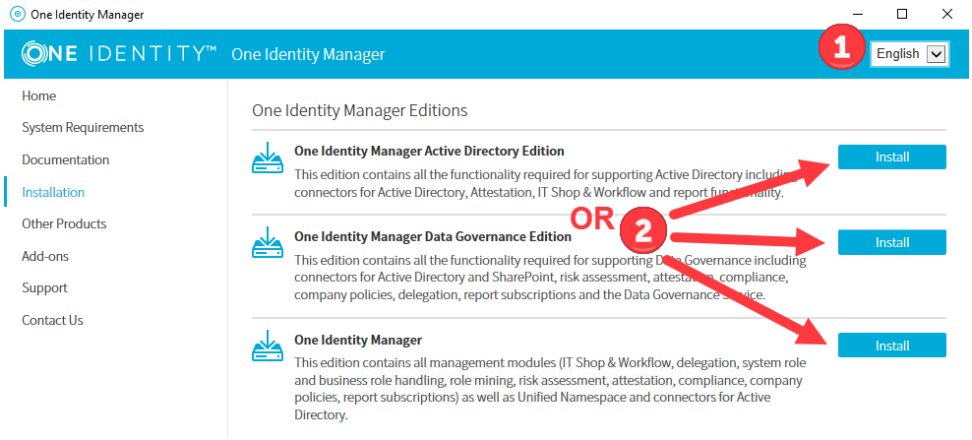
Lab Exercise

Application Server Installation

> **NOTE:**
> The Identity Manager Application Server is a REST based Web Application. You can install many of these Applications and run them as well in a Cluster if you like. In any basic training we install just one Application Server. This Application server is used to enable the full text search capability of the Standard Web Portal.
> The installation of Web Applications happens locally on server IAMS03. There is no remote capability to install these Web applications until today (missing but necessary OS API calls for security reasons).

- Switch to the App Server (IAMS03) and logon as IAM\administrator.
- Open Windows Explorer. Expand the following path I:=\\IAMS10\install and find the Identity Manager installation directory (Note: There may be more than one installer directory. If in doubt which to select, ask your instructor).
- Run **autorun.exe**.
- Click several times onto the upcoming error message
- Install **Web based components** in **Installation**.
- In the **Web Installer…**
  - Click on **Install application server**
  - Click **[Next]**

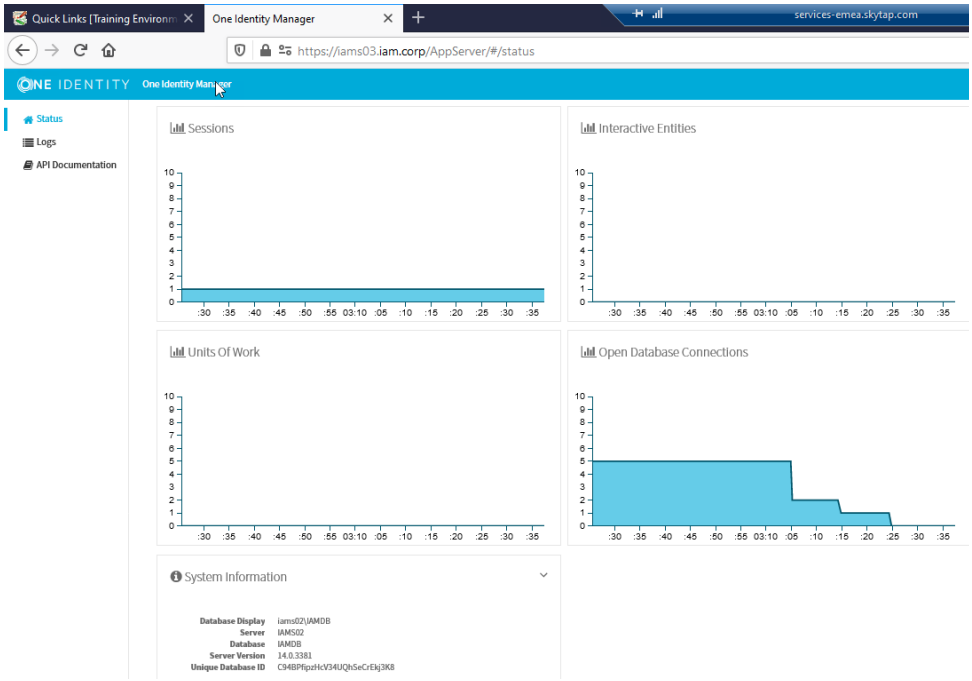
- If no connection to IAMS02/IAMDB exists, click on **Add new connection**. If a connection to IAMS02/IAMDB exists, select this connection and continue with d.
  - Select **SQL Server** from **Connections**
  - Click **[Next]**.
  - Server: ***IAMS02***
  - Leave Windows authentication UNCHECKED
  - User: ***SVC_1IM_SQL***
  - Password: ***I.4Madmin***
  - Select Database: ***IAMDB***
  - Click **[Finish]**.
- Connect to the One IM Database (IAMDB)
  - Authentication method: ***System user***
  - User: ***[Your user] or Training***
  - Password: ***[Your password] or I.4Madmin***
- Click **[Next]** and configure **Select setup target**
  - Application name: ***AppServer***
  - IIS target path: ***Default Web Site***
  - Enforced SSL: ***checked***
  - Setup dedicated application pool: ***checked***
  - Web authentication: ***Windows authentication (single sign-on)***
  - Database authentication: ***SQL authentication***



NOTE:
Only if prompted specify SQL account to connect to the database svc_1im_sql, I.4Madmin.

- Click **[Next]**
- Keep defaults on **Assign machine roles**
- Use the already existing session token certificate
  - Session token certificate Use existing certificate
  - Select certificate: ***Subject: CN=iams03.iam.corp,…***
    (take the first similar entry in the list)
- Click **[Next]**
- Use **Set update credentials** defaults
- Click **[Next], [Next]** and **[FINISH]**

- On your Workstation IAMW01 start your Internet Browser
  - Enter URL: ***https://iams03.iam.corp/AppServer***
    (Optional you can select **Quick Links** → **Identity Manager** → **Application** Server from the Environment documentation which gets started with each installed Internet Browser)
  - In the login mask enter the following credentials if prompted:
    - User Name: ***iam\administrator***
    - Password: ***I.4Madmin***
  - In the Portal login mask enter system user credentials:
    - User: **[Your account]**
    - Password: **[Your Password]**

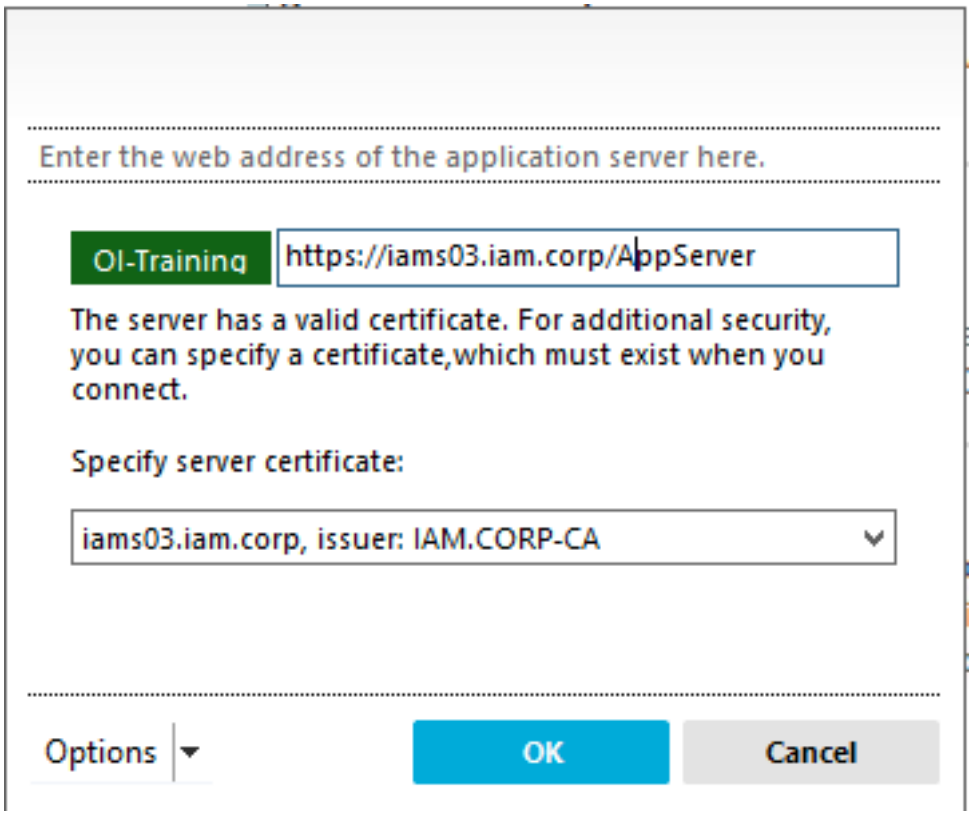


Standard Web Portal Installation

- Switch to the App Server (IAMS03). If needed logon as IAM\administrator.
- Open Windows Explorer. Expand the following path I:=\\IAMS10\install and find the Identity Manager installation directory.
- Run **autorun.exe**.
- Select **Install** of **Web based components** on tab **Installation**.
- In the **Web Installer…**
  - Click on **Install Web Portal**
  - Click **[Next]**
  - Logon using your system user account (remember, it's not the first time doing this).
  - On **Select setup target…**
    - Application name: ***IdentityManager***
    - IIS target path: ***Default Web Site***
    - Check: ***Enforce SSL***
    - Check: ***Setup dedicated application pool***
    - Web authentication: ***Anonymous***
    - Database authentication: ***SQL authentication***

> **NOTE:**
> Enforce SSL needs a Default Web Site installed with HTTPS binding. We use the **Anonymous authentication** to be able to login with different dedicated users, which is standard for a development or test environment (a production configuration would use typically Windows authentication and single sign-on).

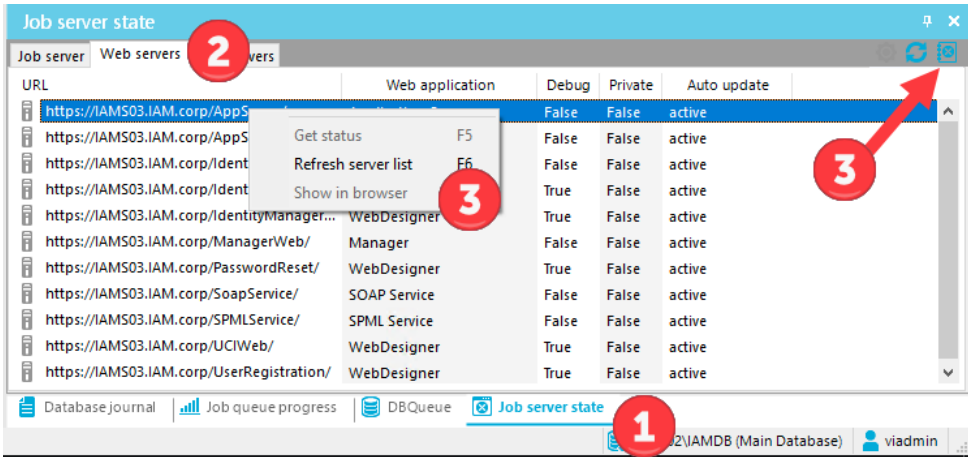
    - Click **[Next]**.
  - On **Select application server**
    - Click **Select application server**
    - Enter URL: ***https://iams03.iam.corp/AppServer***
      You should see something green.
    - Specify server certificate: ***IAMS03.IAM.corp*…***
    - Click **[OK]**
    - Click **[Next]**



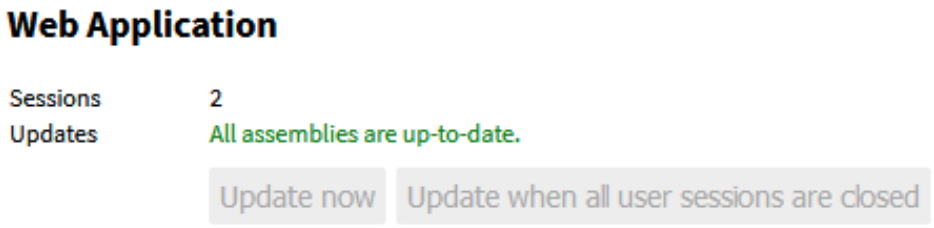
    - On **Select setup target**
        - Accept configuration defaults.
        - Click the small icon next to **Authentication for sub project is missing**.
            - In the sub-form select VI_UserRegistration_Web
            - User: **[your user]**
            - Password: **[your system user password]**
            - Click **[OK]**.

> **NOTE:**
> You might get asked about a URL for notifications. If such a question appears, select always the URL to your Standard Web Portal (https://.../IdentityManager).

        - Click [Next], [Next] and [Finish] to close the wizard.
- Switch to your workstation and use **Launchpad: Manage/Check system** status to open Jobqueue Info.
    - Select **Job server status** on right lower
    - Select tab **Web servers**
    - Right click into the list and select **Refresh server list** (optionally you can use **F6** like before in **Job server**)
    - Right click the entry which represents the portal you installed and select **Show in browser** (if this is not available you can as well use the marked icon on the tabs right upper side, '3' in the picture below).



- On the monitoring site of your Standard Web Portal, you see that all your assemblies are up to date. This is also a good place to upgrade your Web Application (Identity Manager Service Pack or Upgrade).



- Shorten the portal Https://*/monitor#* by deleting the end of the URL beginning with "//". You will now get the real portal site.

NOTE:
Currently we can't log in, because we do not have any permitted identities in the system we can use, but you should see a One Identity Manager login mask.

Password Reset Web Installation

NOTE:
This installation looks very similar to the last installation. Please read instructions carefully, because there are small but important configuration differences.

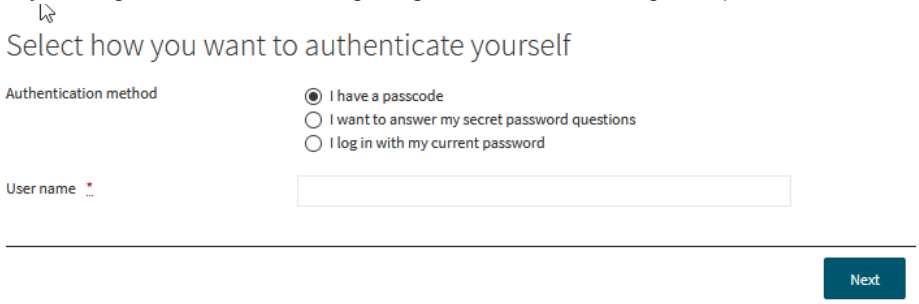
- Switch to the App Server (IAMS03). Logon as IAM\administrator if needed.
- Open Windows Explorer. Expand the following path I:=\\IAMS10\install and find the Identity Manager installation directory (Note: There may be more than one installer directory. If in doubt which to select, ask your instructor).
- Run **autorun.exe**.
- Select **Install** of **Web based components** on tab **Installation**.
- In the **Web Installer…**
  - Click on **Install Web Portal**
  - Click **[Next]**
  - Logon using your system user account (remember, it's not the first time doing this).
  - On **Select setup target…**
    - Application name: ***PasswordReset***
    - IIS target path: ***Default Web Site***
    - Check: ***Enforce SSL***
    - Check: ***Setup dedicated application pool***
    - Web authentication: ***Anonymous***
    - Database authentication: ***SQL authentication***

NOTE:
Enforce SSL needs a Default Web Site installed with HTTPS binding. We use the **Anonymous authentication** to be able to login with different dedicated users, which is standard for a development or test environment (a production configuration would use **Windows authentication**).

        - Click **[Next]**.
    - On **Select application server**
        - Click **Select application server**
        - Enter URL: ***https://iams03.iam.corp/AppServer***
          You should see something green.
        - Specify server certificate: **IAMS03.IAM.corp*…**
        - Click **[OK]**
        - Click **[Next]**
    - On **Select setup target**
        - Web project: ***QER_PasswordWeb***.
        - Click **[Next]**
    - On Application token type in some text (for example: ***PasswordWebToken***)

NOTE:
The application token is like a password to secure the installation. After you defined a token you should store the text somewhere securely. Once you like to install another Password Reset Web instance you need this token again. The token hash is stored in the Database and in the Application web.config. For security reasons you cannot get a token cleartext from somewhere (beside your own secured notes).
You can create a new token during each Installation of another Password Reset Web but you will disable all other Password Reset Webs using another token.
Yes of course it is as well possible to change the token in a web.config and the database (for example for a token reset or if you need to create a new one). Therefore, you will use the Identity Manager Web Portal command line tool: bin\WebDesigner.ConfigFileEditorCMD.

    - Click **[Next]**
    - You get prompted to configure a Base URL for email notifications. This is a URL in the footer of your email communication. This should always point to your Standard Web Portal. Take the default!
    - Click **[Next], [Finish]** to close the wizard.
- Switch to your workstation and use **Launchpad: Manage/Check system** status to open Jobqueue Info.
    - Select **Job server state** on right lower
    - Select tab **Web services**
    - Right click into the list and select **Refresh server list**
    - Right click the entry which represents the portal you installed and select **Show in browser** (if this is not available you can as well use the marked icon on the tabs right upper side).
    - After you see the Monitor site of the selected portal and you ensured the assemblies are up to date, shorten the URL by deleting the end of the URL beginning with "//". You will now get the portal site.



API Server Installation

NOTE:
In the previous part of these labs we installed the App Server as a prerequisite for the Standard Web Portal, the Std.

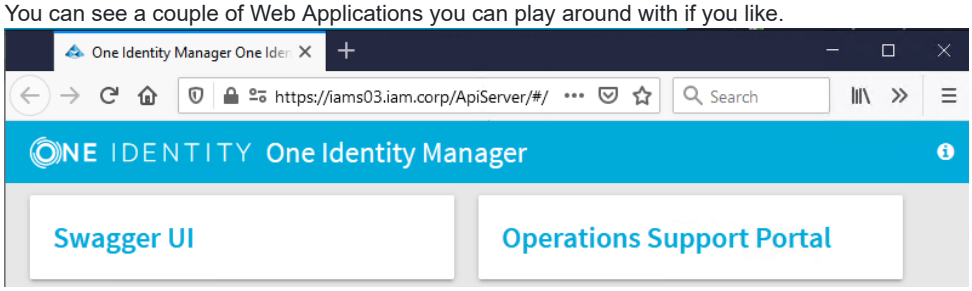
Web Portal and a Password Reset Portal. Beside the App Server this is a selection of Web Portals based on Web Designer technology (a One Identity proprietary technology to develop fast Web Portals). Since version Identity Manager 8.1 we started to switch all portals to a new Angular based technology. Therefore, we need another specific REST based Web Service which is named the API Server. This step will install the API Server and all currently available API Server based portal

- Switch to the App Server (IAMS03). Logon as **IAM\administrator** if needed.
- Open Windows Explorer. Expand the following path **I:=\\IAMS10\install** and find the Identity Manager installation directory (Note: There may be more than one installer directory. If in doubt which to select, ask your instructor).
- Run **autorun.exe**.
- Select **Install** of **Web based components** on tab **Installation**.
- In the Web Installer…
  - Click on **Install API Server**
  - Click **[Next]**
  - On **Installation source** keep the defaults and click **[Next]**
  - On **Select setup target…**
    - Application name: ***ApiServer***
    - IIS target path: ***Default Web Site***
    - Check: ***Enforce SSL***
    - Check: ***Setup dedicated application pool***
    - Web authentication: ***Windows authentication***
    - Database authentication: ***SQL authentication***
    - Click **[Next]**.
  - On **Select application server**
    - Click **Select application server**
    - Enter URL: ***https://iams03.iam.corp/AppServer***
      should see something green.
    - Specify server certificate: ***IAMS03.IAM.corp*…***
    - Click **[OK]**
    - Click **[Next]**
  - Use the already existing session token certificate
    - Session token certificate: ***Use existing certificate***
    - Select certificate: ***Subject: CN=API Server,…***
  - Click **[Next]**
  - On **Assign machine roles** keep the defaults and click **[Next]**
  - Use **Set update credentials** defaults
  - Click **[Next]**
  - On Application token type in the same token, you used above (for example: ***PasswordWebToken***)
  - Click **[Next], [Next]** and **[FINISH]**

NOTE:
Now the API Server is installed. To get the Api Server based Web Portals functional you need to compile the angular based content stored in the database. Because this takes some time, the compilation option is initially deactivated. Let's activate and compile this content.

- Switch to your Workstation IAMW01.
- In **Launchpad** start Designer (**Configure / Change system settings**)
- In Designer
  - Select **Edit configuration parameters** from **Getting Started**
  - Expand **QBM/HtmlDevelopment**
  - Compiler: ***checked***
  - **[Commit to database], [Save]** and exit Designer.
- In **Launchpad** start Database compiler (**Change & Extend/Compile the database**)
  - Click **[Next]**
  - Sign in with **[Your user]**
  - From the dropdown select **Scripts including all dependencies**
  - Use the bio break to discuss the reason to have a **Database compiler** with your trainer. Don't worry we will discuss

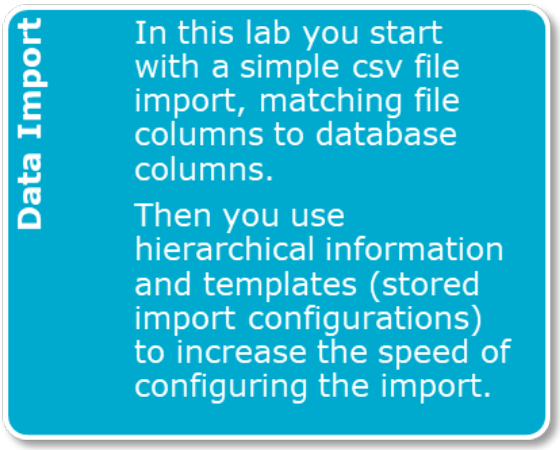
this later in the training again. This step needs some time.
    - After all is compiled, click **[Next]** and **[Finish]**
- Switch to **Launchpad: Manage/Check system** status to open Jobqueue Info.
    - Select **Job server state** on right lower
    - Select tab **Web services**
    - Right click into the list and select **Refresh server list**
    - Right click the entry which represents the API Server you installed and select **Show in browser** (if this is not available you can as well use the marked icon on the tabs right upper side).
    - You can see a couple of Web Applications you can play around with if you like.



Lab Exercise Complete

Lab Exercise: Import of Authoritative Resources

Exercise Overview



In this lab you import Authoritative Sources into Identity Manager

NOTE:
In a typical IAM project we have two options to import data.

- >We can use the **Synchronization Editor**
  (typically for recurring imports happens scheduled based and managed by IAG personal) or:
- We can use the **Data Importer**
  (typically used for single shot imports to integrate a given set of data into the system, often used by project developers or Identity Manager implementors).

Both import types do have its place in an Identity Manager installation. At this stage of the training and in the following Lab we focus on the Data Importer because we currently need Costcenter, Locations and Departments as fast as possible to be able to connect our main target systems. In later labs we will focus on the Synchronization Editor and the Synchronization Engine in a single topic.
→ **In a real IGA project you need to decide which import type is the best option depending on the use case, planned recurrence, operating personnel and implementation costs.**

What you need to know

- You should have the images open and running for this lab.
- Additional Lab content stored in the Lab folder T:\courses\IdentityManager\labs\IM-BSC-01 (T: = \\IAMS02\Training):

User credentials required for this lab

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin

Estimated Time To Complete This Lab: **60** minutes

Lab Exercise

Data Import

- From **Launchpad**, run **Configure/Configure a data import**.
- When the Data Import Wizard starts.
  - Click **[Next]**.

- Click **[Next]** again to perform the database login.
  Username and password should be preconfigured.
  If not, sign in with your System User Account
    - Username: ***user name created during the installation of Identity Manager***
    - Password: ***password used for user creation***
- Click **[Next]**.
- Skip loading an import definition file by clicking **[Next]**.
- Select **[Import CSV file]**.
- Click **[Next]**.
- Select from the IM-BSC-01_DATA_Location.csv file from the LAB folder structure T:\courses\IdentityManager\Labs\IM-BSC-01
- Click **[Open]**.
- The imported text appears in the window. File encoding will usually say utf-8 or Unicode.
- Click **[Next]**.
- As you can see in the **Example data** preview, the first line contains not a record. Configure the Number of lines in **Number of lines in header** to 1.
- Set Columns identified by Delimiter (typically keep the default).
- Click **[Next]**.
- On the next page configure the Delimiter to “Semicolon” (typically keep the default).
- Click **[Next]**.
- Step past the next window by clicking **[Next]**. This option is only used if you want to select a subset of the import data.
- In **Match target tables and columns**
    - Select Locality from the Target table drop down list
    - Click on the wizard icon on the right side of the window ().

> **NOTE:**
> An auto-mapping is performed using the header information.
> These mappings must still be **reviewed manually**.
> Auto-mapping makes it easier for you to map all the CSV columns to the database columns. Understand that this only works if the CSV column names are similar or equal to DB column names because, even within Identity Manager, there is no artificial intelligence implemented.

    - Perform the manual corrections
- Column **Ident_locality** is ok but must select **“Use as Key column”**. To do so click the drop down from **Ident_locality** and select the suitable checkbox.
- Step to the column mapped to **UID_DialogCountry** and drop down the mapping box.

> **NOTE:**
> A 'uid_' field means that a database UID is expected as data. As you easily can see the data contains only short text strings outlining country codes. You need to remap the automatically set column. Your selection will determine a column in a related table (therefore, you need to expand the previous mapped field) containing these codes. Data Importer will use this selection to identify the matching record (database UID).
> To know the right column, you need to know your database model or at least to look into your database to identify the right column by comparing your import data values with column value examples. In this lab we let you know which is the right column '**DialogCountry.Iso3166_2**'.

- Expand the **UID_DialogCountry** database field (expand means to click on the small plus in front of the entry)
    - Select **Iso3166_2** target column (this is the column matching to your strings)
        - The remaining fields should all be mapped correctly. Set column **Treelevel** to **not assigned**, this data is not needed to create your location structure.
        - Now take a second look at the columns to ensure all your changes registered correctly.
        - Click **[Next]**.
    - Ignore this time **Specify hierarchy** because the location structure is flat.
    - Click **[Next]**.
    - Leave **Insert new data record** and **Update existing data records** checked.

WARNING:
Sometimes you are only working with a subset of the records that exist in the target system. If the “Delete records that no longer exist” option is selected, you must also use “The Condition for target objects” field to properly identify the records to be deleted. This is to prevent records from accidental deletion.
Use case example: The data subset may include all employees from the sales department. You do not want all the users from the engineering department (and all other departments) to be deleted. You only want the users who are gone from sales to be deleted from the target system.

- Click **[Next]**.
- Skip Connection variables by clicking **[Next]**.
- Saving the import definition.

NOTE:
Checking **Save the import definition file** will save the import configuration. This is often helpful because when running the same kind of import again, you need to enter the configuration steps again. In our example the information already exists in your share so you can uncheck the functionality.

    - Un-check **Save import definition file**
    - Ensure the **Import data** option is checked.
    - Ensure the Create import script option is checked.
      Name the script: ***CCC_Import_Locations***
    - Leave **Add script to tag** empty.
    - Click **[Next]**.
  - A message box appears, asking you if you want to compile the database. Click **[No]**.
  - The data import progress page appears, and the data import starts.
- When completed, click **[Next]**, then click on the tiny blue link Start another import to continue with costcenter and department information.

NOTE:
In our previous import we stepped through the complete manually import process. This was to outline this technology. Now we will use predefined imports just to quickly get data we need. First, we will perform a costcenter import followed by the department import.

- Your **Data Importer** should show the form Loading an **import definition file**. If this is not the case remember what you have learned to start the Data Importer and sign in und step through until this page appears.
- Use the three dots to select from the **IM-BSC-01** lab folder an
  Import definition file: ***IM-BSC-01__DEF_DataImporter_CostCenter.xml***
- Step through, using **[NEXT]** until you get asked for a data source.
- Select: ***IM-BSC-01__DATA_Costcenter.csv***
- Step through, using **[NEXT]** and note that each setting is now preconfigured. Stop at **Specify hierarchy**.
  - On the **Specify hierarchy** form
    - Check **Sort by hierarchy** (should be already selected)

NOTE:
In our example costcenter and department structure is a hierarchical tree structure. Because of this we want to import this structure from the beginning as a hierarchical structure. One thing to know: If you activate this feature any values stored in the Key column or Parent key column must be unique (clean data source). Otherwise, you will get an error message.
If you don't use this feature you need to run the import two times to create all entries with a first run and a tree structure with a second run. Truly better to use the feature!

    - Key column: ***FullPath***
      (default, already set)
    - Parent key column: ***UID_ParentProfitCenter*** → ***Fullpath***

(default, already set)
    - Click **[Next]** until you need to compile the database.
    - Answer the **Do you want to compile database?** Question with **No**.
- Click **[Next]** and **Start another import**.
- This time we will import the department structure.
    - On form **Loading an import definition file** select from the lab folder
        - Import definition file: ***IM-BSC-01_DEF_DataImporter_Department.xml***
    - Click **[Next]** until it is time to select the import file.
        - Import file: ***IM-BSC-01__DATA_Department.csv***
        - Click **[Open]**
    - Click **[Next]** until you see the **Do you want to compile the database?** message
    - This time (last import) click **[Yes]** to compile the database.

> **NOTE:**
> Time for another bio break or cup of coffee. The compilation with Angular based Web Portals included, takes a while.

    - Click **[Next]** to perform the import.
    - Click **[Next]** and **[Finish]** to close the Data Importer.
- 11. In **Launchpad** open **Manage/Display and maintain content data** to open **Manager** for checking import results.
    - To expand the whole tree of Organizations expand the Departments/Hierarchical view.

> **NOTE:**
> You should see a hierarchical tree of departments.

    - In Organizations and expand Cost center/Hierarchical view

> **NOTE:**
> You should see a three level structure of department codes, controlling areas and cost centers. This is usual for a lot of companies.

    - In Organizations select Locations and expand Hierarchical view.

> **NOTE:**
> There should be a flat list of locations available.

- Now let's look into the import definition files we used.
    - Open DEF_DataImporter_Department.xml in Notepad++ and step through the content

> **NOTE:**
> Notice the defined **ScriptName**, the global configuration in section **LineProvider** and **FieldStrategy**, the defined mappings in the **columns** section and the hierarchical information starting with **Definition=FK(….**
> Definition files are used to store an import configuration for reuse later.
> For example: on an update.

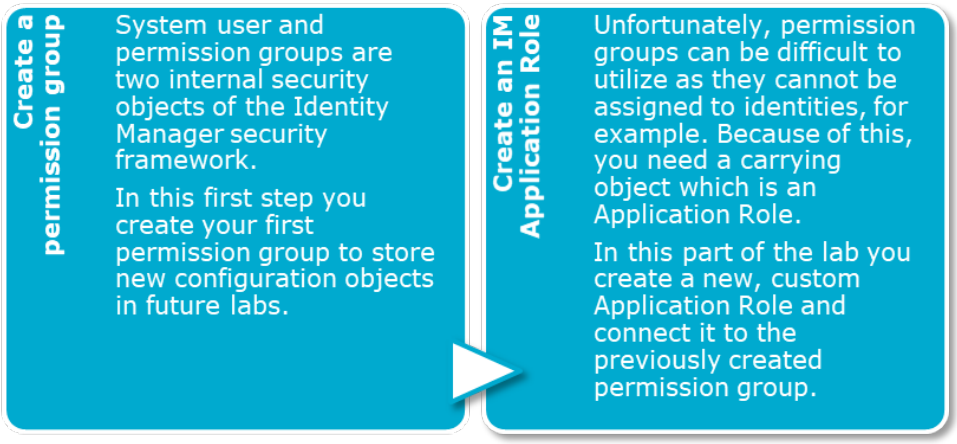
IM-BSC-01_DEF_DataImporter_Department.xml

```
<ImportDefinition Table="Department" Mode="Insert, Update" ScriptName="CCC_Import_Department">
  <LineProvider Name="Hierarchy" KeyIndex="2" ParentIndex="5">
    <LineProvider Name="CSV" Encoding="utf-8" Culture="" TimeZone="W. Europe Standard Time" HeaderLines="1">
      <FieldStrategy Name="Delimiter" Delimiter=";" MaskedByDoubling="False" StringBoundaryChars="" IgnoreEmptyLines="True" />
    </LineProvider>
  </LineProvider>
  <Columns>
    <Column Definition="CustomProperty01" IsKey="False" FixValue="" SourceColumn="CustomProperty01" ConvertScript="" />
    <Column Definition="DepartmentName" IsKey="False" FixValue="" SourceColumn="DepartmentName" ConvertScript="" />
    <Column Definition="FullPath" IsKey="True" FixValue="" SourceColumn="FullPath" ConvertScript="" />
    <Column Definition="ShortName" IsKey="False" FixValue="" SourceColumn="ShortName" ConvertScript="" />
    <Column Definition="" IsKey="False" FixValue="" SourceColumn="treelevel" ConvertScript="" />
    <Column Definition="FK(UID_ParentDepartment).FullPath" IsKey="False" FixValue="" SourceColumn="UID_ParentDepartment &gt; Full
    <Column Definition="FK(UID_ProfitCenter).FullPath" IsKey="False" FixValue="" SourceColumn="UID_ProfitCenter &gt; FullPath" Co
    <Column Definition="" IsKey="False" FixValue="" SourceColumn="UID_ProfitCenter &gt; CustomProperty01" ConvertScript="" />
    <Column Definition="CustomProperty02" IsKey="False" FixValue="" SourceColumn="CustomProperty02" ConvertScript="" />
  </Columns>
  <Variables />
</ImportDefinition>
```

Lab Exercise Complete

Lab Exercise: Add Permission and Application Role (IM-SEC-01)

Exercise Overview



In this lab you create system permissions and add them to an Identity Manager application role. This is done as a prerequisite for the customization labs.

> **NOTE:**
> In many parts of Identity Manager customization and configuration options you need to assign permissions to new objects to make them visible or usable to specific identities or identity groups.
> Out of the box existing permission groups or Application roles can't be used for this, because as predefined and upgradeable standard objects they can't be modified. Because of this it is necessary to create a set of custom permission objects, from now on can be used to manage access to extensions and addons we will develop in this system and this training.

What you need to know

- You should have the images open and running for this lab.

User credentials required for this lab

Affected Machines	IAMS01,IAMS02,IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin
Identity Manager - system user	
Username	[your system user] or training
Password	I.4Madmin

Estimated Time To Complete This Lab: **10** minutes

Lab Exercise

Create a permission group

- Open Launchpad and start the tool to configure Identity Manager (**Designer**). Wait for the full interface to be loaded. (Wait for the Getting Started page to appear)
- Select **Permissions** from the Main Menu

- Select **Permissions groups** from the **Permissions** navigation pane.
- Right-click in the list pane and click on **New** in the popup selection. You will get a grid displayed below which allows to enter some values. Configure as follows:
  - Permissions group: ***CCC_Dialog_And_Schema_Extensions***
  - Only use for role-based authentication: ***True***
- Commit to database and save all changes to the report change label.

> **NOTE:**
> New permission groups could have scripts associated with them. Therefore, we must recompile the database. Because of this it is helpful to temporarily deactivate the compilation of Angular Web Portals which cost a lot of time.

- In Designer select Base Data and expand the section General in the Treeview.
  - Select **Configuration Parameter** and expand **QBM/HtmlDevelopment**
  - Turn off (uncheck) parameter **Compiler**.
    Remember we did the opposite with this Configuration parameter before, to compile the Web Projects explicitly.
- From the Database menu Compile database using scripts including all dependencies configuration.
  You will see this time the compiler will do its job much faster as during the last two times. Don't wonder there are web projects getting compiled. These are the Web Designer technology-based web projects are getting always be compiled.

Create an Identity Manager Application role

> **NOTE:**
> To make the new permissions groups accessible, they must now be associated with an application role. There are no out-of-the-box application roles for this, so we must create one.

- Use Launchpad to open the main data administration tool.
- Select One Identity Manager Administration from the Main Menu.
- Right click Custom in the navigation pane and select New from the context menu.
  - Application role: ***Dialog and Schema extensions***
  - Permissions group: ***CCC_Dialog_And_Schema_Extensions***
  - Click **[Save]**

> **NOTE:**
> You now have a permission group in Identity Manager with the necessary additional permissions and an application role that allows assignment of the permission role to identities. Please keep in mind that, in a production environment, life is not that easy, and you typically deal with more, sometimes nested, permission groups and more application roles. If there is an error message indicating, you cannot save because of a missing flag: **IsRoleBasedOnly** please return to Designer and set the flag as described in step 4b in the section above.

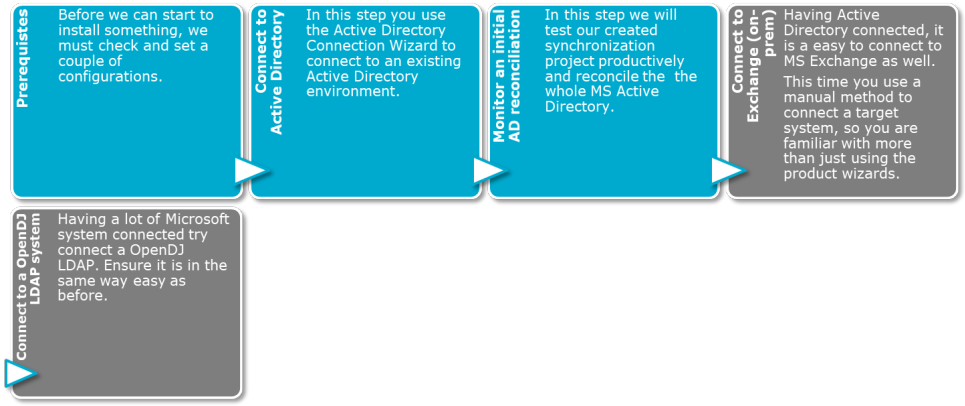
- Select the new object. Maybe you need to switch the treeview
  - Select **Create dynamic role** from the **Tasks** list
    - Object class: ***Person***
    - Click Edit SQL icon ()
    - Condition: ***1=1***
  - Click **[Save]**.

> **NOTE:**
> This will assign all employees to this role. Employees are currently not available in this system. The condition allows to assign them automatically to the role once they exist.

Lab Exercise Complete

Lab Exercise: Connecting Basic Target Systems (IM-CBS-01)

Exercise Overview



In this lab you connect several standard target systems.

> **NOTE:**
> To check your LDAP objects you can use the pre-installed Softerra LDAP Browser on your Admin Workstation.

What you need to know

- You should have the images open and running for this lab.
- Additional Lab content stored in the Lab folder T:\courses\IdentityManager

User credentials required for this lab

Affected Machines	IAMS01,IAMS02,IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin
AD synchronization account	
Username	iam\svc_1im_ad
Password	I.4Madmin
MS Exchange synchronization account	
Username	iam\svc_1im_ex
Password	I.4Madmin
LDAP synchronization account	
Username	svc_LDAP_1im
Password	I.4Madmin
SQL Connection	
Username	svc_1IM_SQL

Password	I.4Madmin

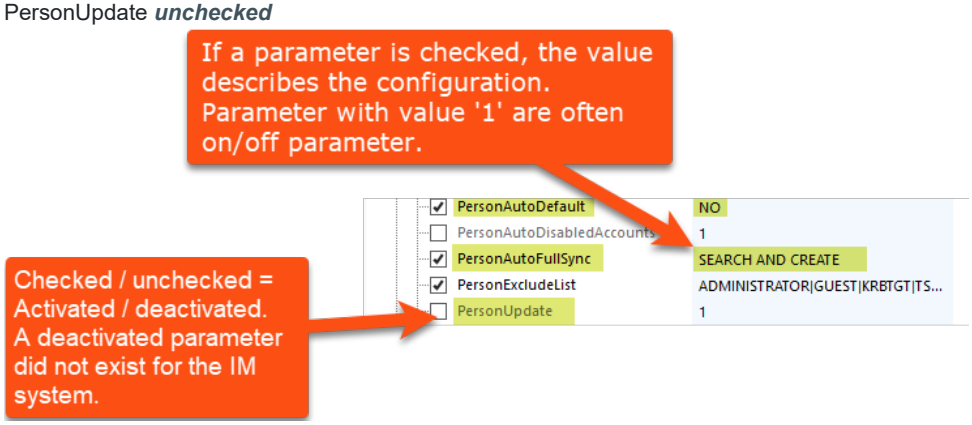
Estimated Time To Complete This Lab: **45 minutes**

Lab Exercise

Prerequisites

NOTE:
In an earlier lab we have connected authoritative sources to Identity Manager using the Data Importer. This is more for IGA project development or single shot imports.
In this lab we use the Synchronization Editor to configure a Standard connector. Typically, a connector is used for a well known Target System such as Microsoft Active Directory. These includes as well generic data sources like LDAP, CSV, ADO.NET or a generic API connect like PowerShell connect.
A connector is typically the fastest way to connect a target system if it is natively supported. In difference to this, if you build a connector from scratch, this could very fast become very expensive (depending on the target data model and complexity).
To build a connector from scratch will be done in another lab.
Before we can start, we should **doublecheck** some **already set** prerequisites just to become aware of.

- From the Launchpad open **Configure/Change System Settings** a **Designer** will be started.
  (In cases where your **Designer** did not show up Configuration parameters, from the **Getting started** page select **Edit configuration parameters**.)
  - Expand tree: **TargetSystem\ADS**
    - PersonAutoFullsync ***checked***
    - PersonAutoFullsync ***Search and Create***
    - PersonAutoDefault ***checked***
    - PersonAutoDefault ***No***
    - Exchange2000 ***checked***
    - PersonUpdate ***unchecked***



  - Expand tree: **TargetSystem\LDAP**
    - PersonAutoDefault ***checked***
    - PersonAutoDefault ***No***
    - PersonAutoFullSync ***checked***
    - PersonAutoFullSync ***Search***
  - To activate MS Exchange synchronization later, we also must set a default mail domain.
    Expand the configuration tree to QER\Person
    - DefaultMailDomain ***checked***
    - DefaultMailDomain ***IAM.corp***
  - It is also helpful to check the parameters to enable the Identity Manager software auto-update functionality. This helps prevent error messages on missing DLL's if you forget to select the installation option Select modules from database.
    Expand configuration tree Common
    - Autoupdate ***checked***

- Autoupdate *1*
- Autoupdate/AllowOutOfTimeApps *0*
- Autoupdate/ServiceUpdateType *Auto*

NOTE:
PersonAutoFullSync describes the behavior of how the system should handle a not existing identity (Person) object if, during reconciliation, an account in the Identity Manager database is created. In this configuration: An existing identity object is assigned or it gets created, if there is no such object in the database.
Please understand, in most IGA projects, HR (identity) data is imported from authoritative sources (SAP HR, Peoplesoft, etc.). During the initial synchronization, AD users are assigned to the existing Person objects (search). In our training scenario, we use the ability to create identities (Person objects) based on AD user accounts (create).
This is the second part of **SearchAndCreate**.
PersonAutoDefault This parameter describes the system behavior **if in Identity Manager** an account gets created (difference to the parameter above: It was for reconciliation). Here our configuration leads to “do nothing” which means no identities gets created or assigned to the new account objects.
Both configuration parameter, **PersonAutoFullSync** and **PersonAutoDefault**, exists for many target systems and have to be configured separately.
Exchange2000 is the parameter that indicates that MS Exchange can be connected. Sorry, half of the name (“2000”) is a bit misleading but never changed because of downward compatibility.
PersonUpdate controls the data flow between identities (person objects) and Active Directory account objects. Typically, Identity Manager controls an Active Directory. This means modifications of person object properties leads to modifications of AD account properties. In scenarios where no authoritative HR system is connected, this behavior can be inverted by checking this configuration parameter.
Use the description of a configuration parameter or the Identity Manager manual to learn about its effect. This configuration exists only for target system Active Directory.
DefaultMailDomain allows us to build the default email address for any person object. This is independent in how many systems an identity has mailboxes. All could be assigned to a person but only one address can be the default address.
AutoUpdate enables the feature where Identity Manager service and front-end binaries are automatically updated from the database. This prevents working with old software (on a system update or hotfix) and missing DLL's if, during an installation, the **select current installed modules from database** option is not used. We highly recommend activating this for every installation.
IMPORTANT: In this section, there were few actions to perform. However, these are essential principles of Identity Manager which you should remember. These (and all other) notes in the lab exercises could provide answers to the questions in the online certification assessment.

- Click **[Commit to database]** and **[Save]**.
- Close **Designer**.

Connect to Microsoft Active Directory

- From Launchpad start Installation overview/Target system type Active Directory (Data Synchronization section)

NOTE:
The front-end starting in the background is Synchronization Editor. Launchpad directly starts a wizard from the Synchronization Editor to create an Active Directory synchronization project. From a principle there are two different ways to connect to Active Directory:
- Using the Identity Manager native AD connector
- Using Active Roles (separate product) to connect to Active Directory.

Which option to choose is depending on your needs and your licensed One Identity software. Both connection types do have pros and cons and which way to go should always be decided on your technical requirements.
A general IGA project suggestion could help:
“Depending on your needs, keep your system as simple as possible.”

- In this training we focus on native Identity Manager!
  Because of this:

- Select **Active Directory Connector**
- Click **[Next]**

> **NOTE:**
> In a few circumstances you may not be permitted to access Active Directory using your workstation. In these cases, using a remote connection server may be an option. This is a generic question and typically more useful if you try connecting SAP, Notes or SharePoint etc. (target systems, needs additional installed software to become connected). This means that for this CONFIGURATION a locally installed Synchronization Editor uses a remote server service to connect to the selected target system instead of using the local machine.

- We do not require a remote server connection.
  - Leave **Connect using remote connection server** unchecked.
  - Click **[Next]**.
- Select an Active Directory Domain from the list box. Happy you, it should be pre-selected.
  - Domain: ***IAM.corp***
  - Click **[Next]**.
- In the Credentials form, an Active Directory account to access Active Directory during the synchronization process must be specified. This is the admin account the Synchronization Engine will use to interact with the target system.
  - User: ***SVC_1IM_AD***
  - Password: ***I.4Madmin***
  - Domain: ***IAM.corp***
  - Click **[Test]** and continue after the green light. In all other cases, correct your input above and try again.
  - Click **[Next]**.
- Configure connection options (**THIS IS IMPORTANT**, don't skip):
  - Secure ***checked***
  - Server ***bind checked***
  - Domain Controller ***IAMS01.iam.corp***
  - Port ***389***
  - Click **[Test]** and continue after the green light. In all other cases correct your input above and try again.
  - Click **[Next]**.
- Review the default configuration.

> **NOTE:**
> Connector features allow to opt-in additional features.
> Currently for AD you can get back previous deleted objects from an AD recycle bin (must be supported by your AD configuration). You may be allowed to handle RAS or TS properties. Keep the default.

- Click **[Finish]**.
  Now an Active Directory Synchronization projects gets auto configured. This is based on a template for connecting Active Directory we selected at the begin.
- If needed configure the database connection. If you get not prompted just skip this step and its subs (default).
  Typically only the password must be set.
  - Server: ***IAMS02***
  - Windows authentication: ***un-checked***
  - User: ***SVC_1IM_SQL***
  - Password: ***I.4Madmin***
  - Database: ***IAMDB***
  - Click **[Next]**.
- The schema is loaded from Active Directory and Identity Manager. Please be patient until the wizard returns and click **[Next]**
- Configure a target system access restriction (keep default, select **Read/write access to target system. Provisioning available**).

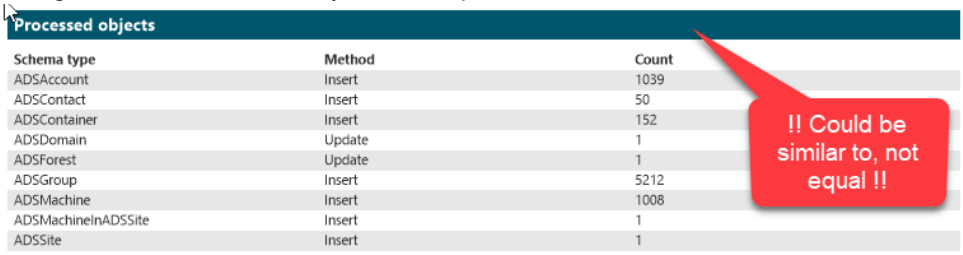
- Click **[Next]**
- Now configure the responsible Identity Manager Job-server to access the configured Active Directory domain. Select this server from the drop-down box.
  - Synchronization server: ***IAMS03***

> **NOTE:**
> The responsible (and only) Active Directory Domain Controller in our lab environment is IAMS01.IAM.CORP. It is not common to install an Identity Manager Job-service on a target system host. Instead, we will use server IAMS03 as the server to remotely connect to IAMS01 (Synchronization server).
> Technically, it is possible to install an Identity Manager Job-service on a Windows Domain Controller. In such a scenario the Domain Controller becomes a Job-server as well.
> In this lab exercise you can't choose this option because there is not an Identity Manager service installed on IAMS01 yet.

  - Click **[Next]**.
- Please notice the tiny checkbox **Activate and save the new synchronization project automatically** at the end of the wizard. It let you know that the synchronization project is automatically saved and activated. Without this option checked, it is necessary to do this manually before the Synchronization Project can be used (additionally steps to perform). Leave the configuration checked and Click **[Finish]**.
- Answer the database is not encrypted warning with **[Yes]**.
- Excellent, you connected Active Directory. Please continue to get some data in, during your first synchronization.

Run and monitor an initial AD reconciliation

- From Launchpad start Manage/Check system status. This will open JobQueueInfo.
- Check that the Identity Manager system is in idle mode.
  - Click into form Job queue and press [F5] until there are no more jobs in Job queue
  - Select DBQueue from the right lower tabs and ensure the field is empty.
- Switch back to Synchronization Editor
  - Select Start up configurations from the already open Active Directory synchronization project we just created.
  - Press [SIMULATE…] to get an idea what will happen during the initial reconciliation.
    - Answer the loosing performance warning message with [Yes]
    - Have a look at the steps passed through during the simulation, good to know that they exist.
  - Watch the report that is created. There are several data creation actions planned for the Identity Manager Database. This is exactly what we expect for an initial reconciliation.



Processed objects

Schema type	Method	Count
ADSAccount	Insert	1039
ADSContact	Insert	50
ADSContainer	Insert	152
ADSDomain	Update	1
ADSForest	Update	1
ADSGroup	Insert	5212
ADSMachine	Insert	1008
ADSMachineInADSSite	Insert	1
ADSSite	Insert	1

  - Close the report.
  - Click on **[Run]** to perform the synchronization
    - Answer the question to start the synchronization on Identity Manager service with **[Yes]**
    - Click **[OK]** to confirm the synchronization is started.
  - Switch back to **JobQueueInfo**.
    - Right click **Job queue** in tab **Job queue** and select **Monitor Job queue**.

> **NOTE:**
> You can watch the **FullProjection** job processing for a while.

  - Select the **Job Server Status** tab from the right lower part of the window.
  - Right click server **IAMS03** and select **Show in Browser** from the context menu.

- In the browser front-end (which is getting started with a delay) select Executing instance for queue \IAMS03 from the Home page
- Select the slot containing the keyword **…FullProjection…** . You can now see more detailed information about the process and refresh this view (press **[F5]**) from time to time to get an update. Once the **Slot is empty**, proceed.

- Switch to **JobQueueInfo** and follow all synchronization post processes (**Job queue** is empty as well, this can take a while).
- Use **Launchpad** to start Identity Manager Manager (**Manage/Display and maintain content data**).
- In **Manager** we will check what was reconciled and which data was created
  - Select Main tab: **Active Directory**
    (bottom left of the screen)

    (Depending on your screen resolution you might need to select it from the more button )
  - Expand: **Hierarchical view/IAM.corp**

> **NOTE:**
> You should see a proper container structure

  - Select: **Groups**:
    (Be careful meant is **Groups** in parallel to **Hierarchical view**)

> **NOTE:**
> A little over 5000 groups should be available. This could lead to a filter box, Press [Show all].

  - Select: **User Accounts**

> **NOTE:**
> A little over 1000 accounts should be available

  - Expand: **Mailboxes**

> **NOTE:**
> It looks like there is no information stored underneath mailboxes which is easy to explain, because we don't have connected Microsoft Exchange yet.

  - Select **Employees** from the Main tabs
  - Select **Employees** in the **Navigation tree**

> **NOTE:**
> There are a little over 1000 identity objects created

  - Select a single person object

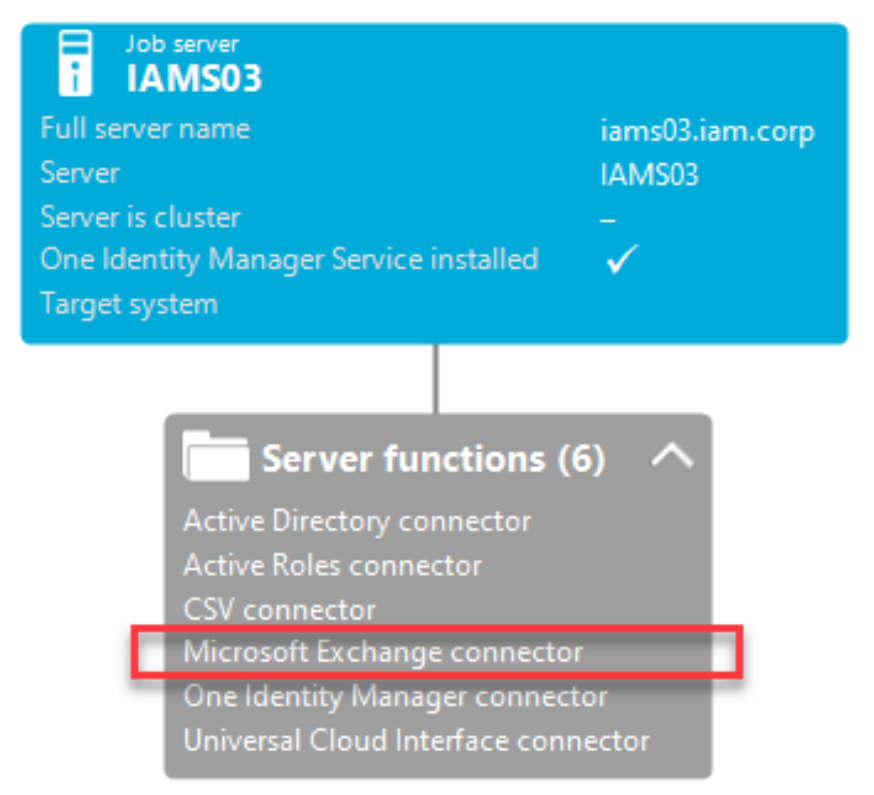
> **NOTE:**
> The overview will show you a person object surrounded with other assigned objects

Connect Exchange

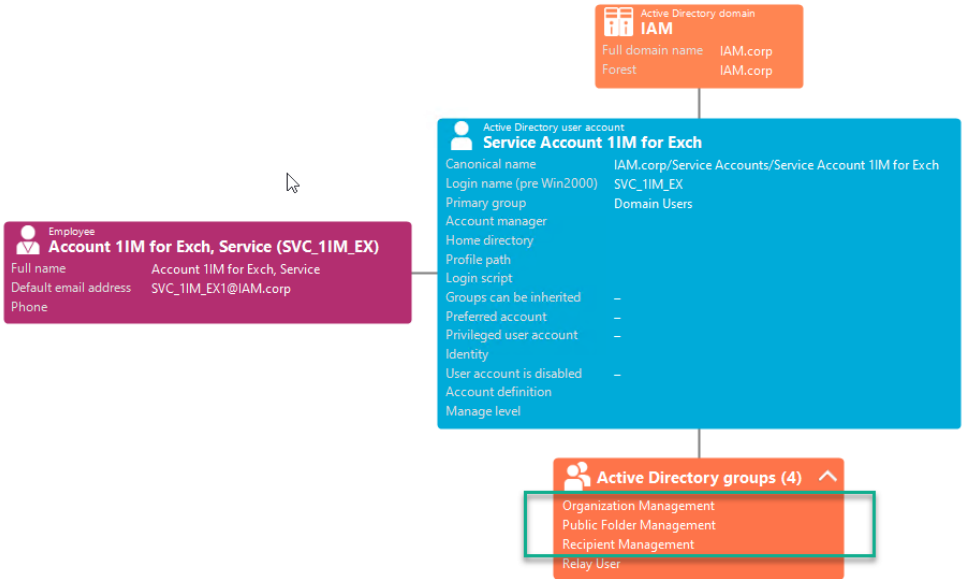
> **NOTE:**
> First we must ensure the Identity Manager system has identified an Exchange server.

- In the Manager, select **Active Directory** from the main tabs.
  - In the **Basic configuration data** section select **Server**.
  - Select (double-click on) **IAMS03** from the list of servers.
  - Select A**ssign server functions** from the **Tasks** list.

NOTE:
As you can see **Microsoft Exchange connector** is assigned to the server IAMS03. This was made during the remote installation of the Identity Manager Service by adding **Server roles** to the machine.
This step was showing you how to watch and assign server functions.
To view assigned functions only, you don't need this.
Use the **[← Back]** button to return to the overview.



- Our last check is the mandatory Exchange permissions which must be configured for a Microsoft Exchange synchronization user (described in the Identity Manager manual).
  These permissions are already set, but we will double check everything to get aware of these parameters.
  - Expand **Navigation** tree down to **Hierarchical view / IAM.corp / Service Accounts** and select **User accounts**.
    - In the list of accounts double click **Service Account 1IM for Exch**
  - The account must be a member of:
    - Organization Management
    - Public Folder Management
    - . Recipient Management



- Last step is to ensure that you can run PowerShell scripts on your system. This is typically not needed in this training environment (it's already set) but please doublecheck.
  - Start PowerShell as admin
    - Enter: ***Get-ExecutionPolicy***

NOTE:
You need the ability to run PowerShell commands to connect to the MS Exchange server.
The system should return with Unrestricted or with RemoteSigned. If this is not the case, use the command Set-ExecutionPolicy RemoteSigned to deactivate any script restriction from your PowerShell console. The same is necessary on a server used as a remote connection server for MS Exchange (for a MS Exchange server with an installed Identity Manager service, this is not necessary). You can sign onto the server and use the command above or type the following commands in your already open PowerShell console on the wks.

```
New-PSSession -ComputerName IAMS03     Enter-PSSession 1     Get-ExecutionPolicy     #
```

- From **Launchpad** start **Installation overview/Target system type Microsoft Exchange**.
  (If Synchronization Editor was already open, this happens in the background and there is no action to see on the screen. In this case, please switch to **Synchronization Editor**)
  - In **Create synchronization project** select **Microsoft Exchange 2013 Connector** and click [Next].
  - We don't need a remote connection server. Please click **[Next]**.
  - On **Select Microsoft Exchange server**
    - Server: ***IAMS01.IAM.corp***
    - Click**DNS query** until the light returns green. If it does not turn green, check your input and retry the query.
    - . Click **[Next]**
  - Enter connection credentials
    - Username: ***svc_1im_ex@iam.corp***
    - Password: ***I.4Madmin***
    - Click **[Next]**
  - We want to manage the **Entire organization**, please accept the default and click **[Finish]**.
  - Click on **[Next]**.
  - Select **Read/write access to target system. Provisioning available** and click **[Next]**.
  - Select **IAMS03** as **Synchronization server** and click **[Next]**.

NOTE:
Please remember we configured this server role before, installing the Identity Manager Service on server

IAMS03.

- Click **[Finish]** to store and activate the synchronization project.
- Read the information to handle linked mailboxes and click **[OK]**.
- Confirm saving the synchronization project to an unencrypted database. Click **[Yes]**.

- In **Synchronization Editor**, select **Start up configuration** from the already open, MS Exchange synchronization project we just created.
- Start the initial synchronization just as you learned for Active Directory earlier.
- Monitor progress in **JobQueueInfo**.
- Once **Job queue** is empty again, switch to (or open) **Manager**.
  - Select **Active Directory** main menu.
  - Right click into the **Navigation** tree and select **Refresh view**.
  - Expand **Exchange system Administration**.

NOTE:
You should now see more folders than before, including:
IAM/Organization Configuration/Adress list/All Groups,
…/All Rooms,
IAM/Recipient configuration/Mailboxes/Discovery, etc.

- Switch back into **JobQueueInfo**
  - Select from **Job server status** the **IAMS03** entry with a right click.
  - Select **Show in Browser** from the context menu.
- In Browser step to **Log File**
  - Move to the logs end and find the green message which confirms that the MS Exchange synchronization ended successfully.
- Close all admin front ends.

Connect OpenDJ LDAP system

- From **Launchpad** start **Installation overview/Target system type LDAP**
  - There are many LDAP templates available. Select **LDAP Connector (Version 2)**
  - We **don't** need a remote connection server. Please click **[Next]**.
  - On **Create system connection…**
    - Server/Port: ***IAMS04.IAM.corp : 389***
      (The port should show the default)
    - Authentication method: ***Basic***
    - Username: ***cn=svc_LDAP_1im***
    - Password: ***I.4Madmin***
    - Encryption: ***None***
    - Protocol version: ***3***
    - Click **[Next]**
  - There are two ways to **Select the schema source**. You can load them from a LDAP server (default) or from a file (typically if the default option doesn't work).
    - Select **Load schema from LDAP server** from Source drop-down list.
    - Click the refresh button on left ( )
    - Look at **Schema parser errors**. If there are no errors, you can proceed. If there are some, you may need to start with a schema file.

    - Click **[Next]**
  - Now you should **select configuration preset**.

NOTE:
You can select between two general options. You can define the mapping and matching on your own (long and time consuming and you need to be a LDAP and Identity Manager pro) or you can use one of the predefined templates for

- Microsoft ADLDS,
- Oracle DSEE,
- Novell eDirectory,
- OpenDJ

and may be others. A default gets typically created depending on the schema that was loaded previously (this means very often you can just proceed with defaults like in this training).

    - Select: ***Use preset***
    - Selection: ***OpenDJ***
    - Click **[Next]**.
- After the schema is set, you may need to add **LDAP schema extensions**.
    - Expand **LDAP schema extensions**
    - Select **Return operational attributes**

NOTE:
As you can see some schema extensions was already loaded together with reading the schema. Please recognize also the ‘PLUS’ and ‘Trash bin’ buttons which allow to define such extensions manually if necessary.

    - Click **[Next]**.
- Enter **Search base** (a search base is typically also preselected by loading a proper schema. If not just select an entry from the drop-down)
    - Base DN: ***dc=iamldap,dc=corp***
    - Click **[Next]**
- For further testing and editing it might be helpful to save the connection locally on this machine.
    - Check: **Save connection locally**
    - Click **[Finish]**
    - Click **[Next]**
- **Select a project template**. Therefore, read the description of available templates first to get an idea where they are configured for.
    - Select **OpenDJ synchronization**
    - Click **[Next]**
- Select **Read/write access to target system**. Provisioning available and click **[Next]**.
- As Synchronization server select **IAMS04**
- Click **[Next]**.
- Click **[Finish]** and **[Yes]** to store and activate the synchronization project.

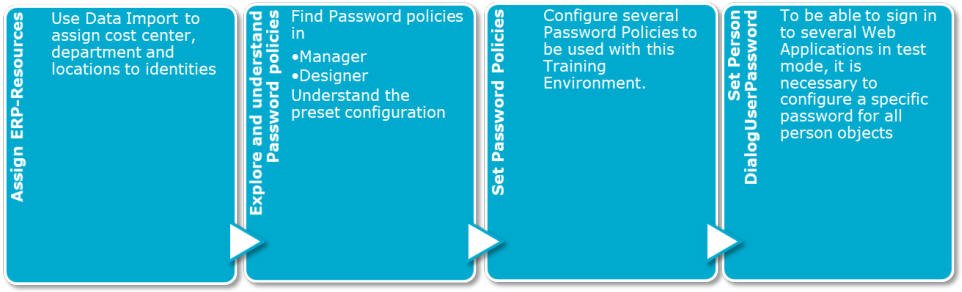
NOTE:
The according Identity Manager server service was installed before. This service was as well configured with the right server functions and roles to process with LDAP and SharePoint. In situations where available services getting used with new connected target systems or functions you must ensure that all features and roles are configured (**Designer** → **Basic Data** → **Installation** → **Job server** tabs **Server functions** and **Machine roles**).

- In **Synchronization Editor**, select **Start up configuration** from the already open, LDAP synchronization project we just created.
    - Start the initial synchronization just as you learned before.
- Monitor progress in **JobQueueInfo**.
- Once the job queue is empty again, switch to (or open) **Manager**.
    - Select **LDAP** main menu
    - Expand hierarchical view you should see many containers with LDAP user assigned.

Lab Exercise Complete

Lab Exercise: Password Policy Configuration and ERP-Resource Assignment (IM-CBS-02)

Exercise Overview



In this lab you will assign department, cost center and locations to identities. In a second step you will explore Password Policies and configure them to be used during this training.In this lab you will assign department, cost center and locations to identities. In a second step you will explore Password Policies and configure them to be used during this training.

> **NOTE:**
> The way to configure Password Policies is exact the way you will use in a real-life scenario. The configuration we will set, fits better to a Developer- or Test Environment which a Training Environment always should be.

What you need to know

- You should have the images open and running for this lab.
- Additional Lab content stored in the Lab folder T:\courses\IdentityManager (\\IAMS10\Training\courses \IdentityManager):

User credentials required for this lab

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin
Identity Manager - system user	
Username	[your system user] or training
Password	I.4Madmin

Estimated Time To Complete This Lab: **10 minutes**

Lab Exercise

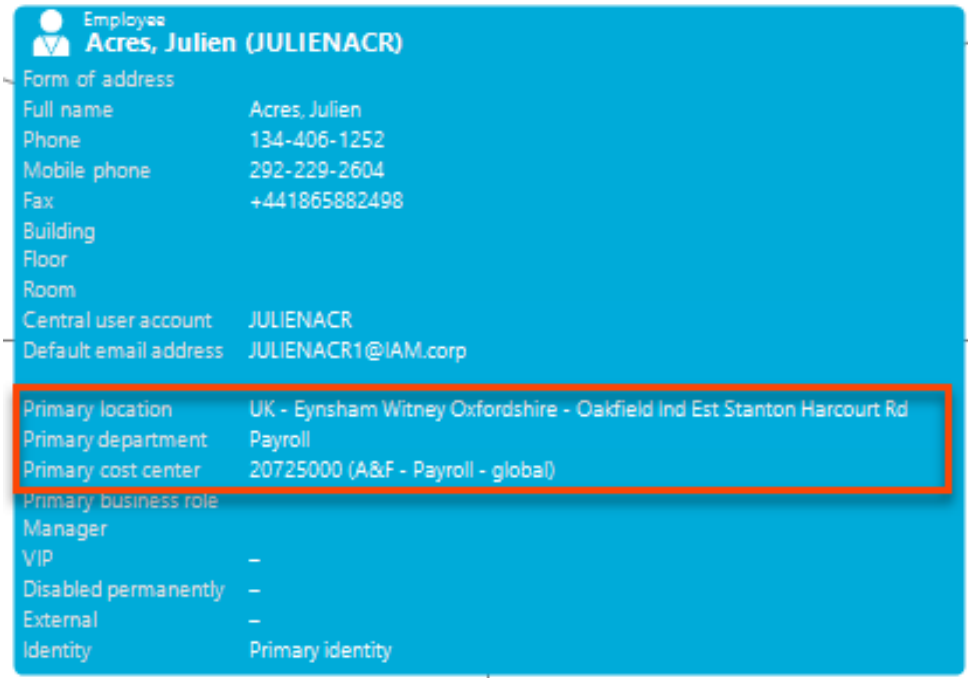
Assign ERP Resources

NOTE:
In a previous lab we connected some target systems to Identity Manager, and we imported Department, Cost center and Locations (Enterprise Resource Planning Data = ERP-data). All of this is important data but empowers and IAG system by being connected. In the following step we will assign imported ERP-data to employees. To speed this up we use another csv data import with an according definition file.

- Start **Data-Importer** for example using **Launchpad**.
- Click **[Next]**
- From the according lab folder
  (IM-CBS-02) open **Import definition file**: IM-CBS-02__Import_Def_Person2ERP_Assignment .xml.
- Click **[Next]**
- Select **Import CSV file**
- Click **[Next]**
- From the according lab folder
  (IM-CBS-02) open **Import file**: IM-CBS-02_Person2ERP_Assignment.xml
- Notice the preset configuration and click **[Next]**.
- **File structure**: Notice the preset configuration and click **[Next]**.
- **Defining the line structure**: Notice the preset configuration and click **[Next]**.
- **Line condition**: Notice the preset configuration and click **[Next]**.
- **Match target tables and columns**: Notice the preset configuration and click **[Next]**.
- **Specify hierarchy**: Notice the preset configuration and click **[Next]**.
- **Handling options for data sets**: Notice the preset configuration and click **[Next]**.
- **Connection variables**: Notice the preset configuration and click **[Next]**.
- Saving the import definition
  - Save import definition file: ***unchecked***
  - Import data: ***checked***
  - Create import script: ***unchecked***
  - Click **[Next]**
  - Notice the result and click **[Next]**
  - Click **[Finish]**

NOTE:
You should not see any errors. If there are some, they might result out of the data situation. Discuss this with your trainer.

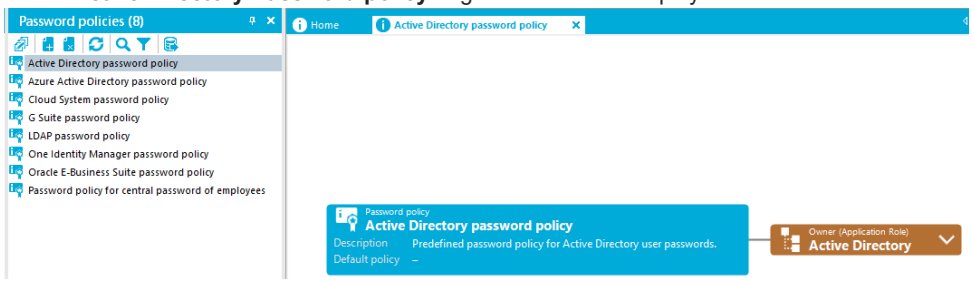
- Open **Manager** and select some identities (person objects). Now they should show a department, cost center and location assignment for nearly each identity.



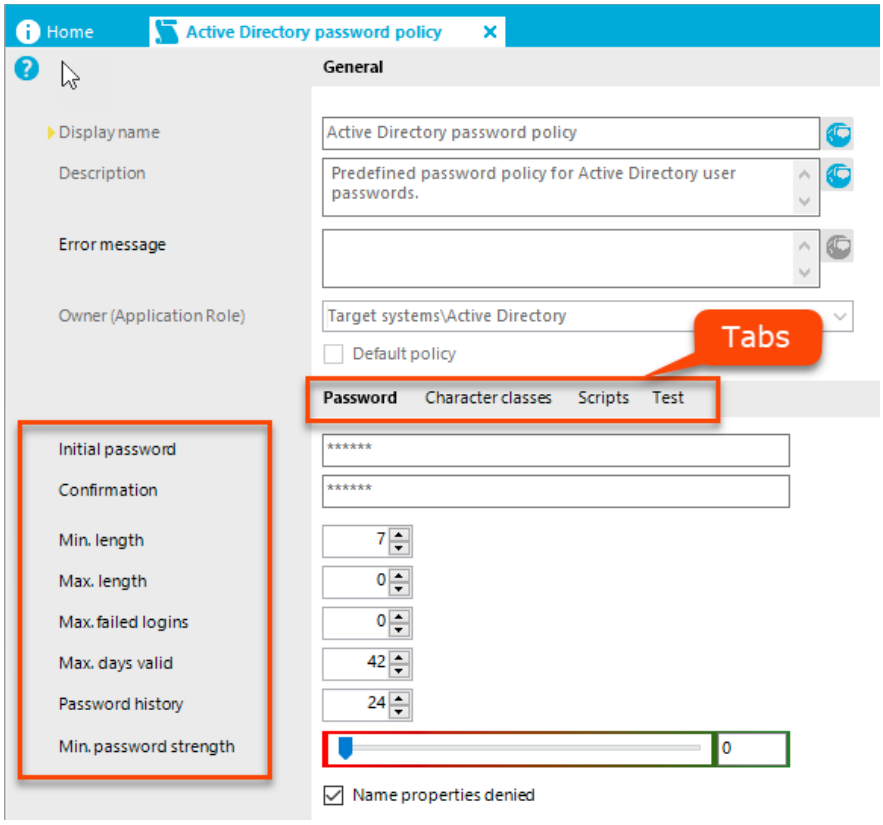
Explore and understand Password Policies

NOTE:
Password Policies can be configured in **Designer** and **Manager**. In difference to the **Manager** which shows **Password Policies** always as sub-node of a **Target System administration** section, **Designer** shows all Password Policies in one place and at one location (target system independent). From a Password Policy configuration perspective, there is no difference between both tools.

- Open **Manager** and sign in with your **system user** account. You might use the already open **Launchpad** to simplify things.
- Select target system **Active Directory** and expand filter **Basic configuration data**.
- Select filter node **Password policies**. In the list on right you should see several Password policies now.
- Select **Active Directory Password policy** to get the overview displayed.

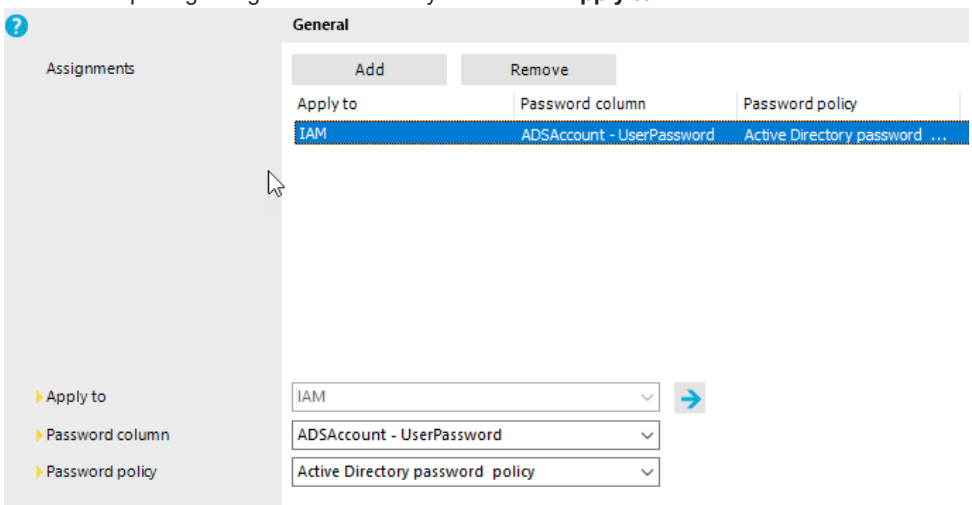


- Select Change main data from the Tasks list.



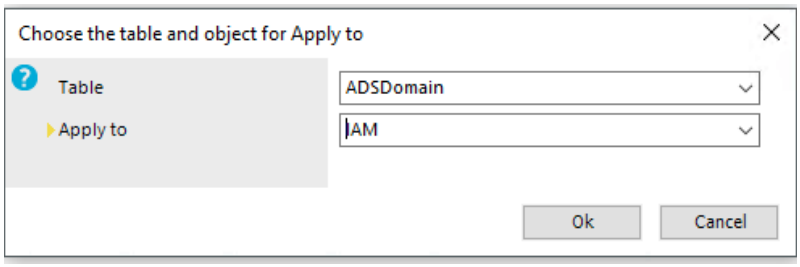
NOTE:
As you can see there are some fields write protected. This indicates that this is an out of the box object could not be modified like always. Nevertheless, there are some fields NOT write protected. In case of Password policies, you can change the configuration of a standard policy, but you can't change names, description or the owner. If you like to do this, you must create a custom password policy and assign it instead of the standard policy to an object.

- Select **Assign objects** from the **Tasks** list.
- In the form opening on right select the entry underneath **Apply to**.



If there is **no entry** in the list click **[Add]** to get a new one.

- Click the right arrow icon next to **Apply to**
  - Table: ***ADSDomain***
  - Apply to: ***IAM.corp***
  - Click **[OK]**



-
- Select password column: ***ADSAccount-UserPassword***
- Click **[Save]**

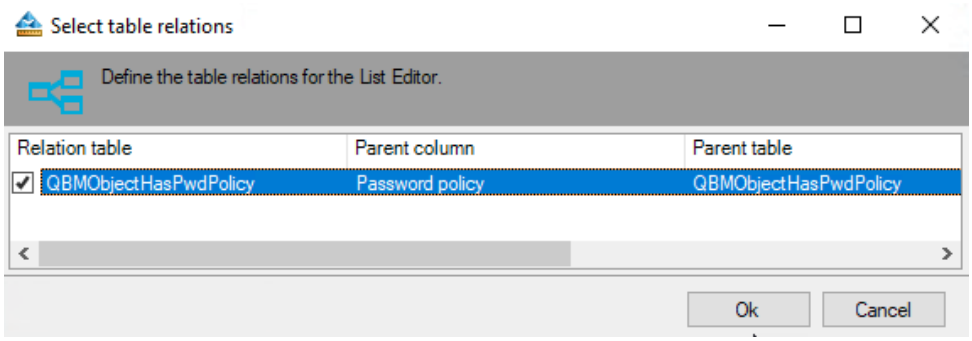
NOTE:
This is the place where the policy gets assigned to one, or more password fields in the database, the policy should be valid for. In the example above, you can see it is valid for a data field **ADSAccount.UserPassword**, which is the password of an Active Directory Account database object (remember we are talking about a database entry, representing a target system object).

Set Password policies

- Open **Designer** (you might use **Launchpad**) and sign in with your **system user** account.
- Select **Base Data** and expand **Security Settings**
- Select **Password policies**
- Ensure that one Password policy is selected

NOTE:
As you easily can see, it seems to be, you do not have the same capabilities as before. To assign the policy to objects is currently missing. This is a special feature of Designer where sometimes additional assignment capabilities gets hided to simplify things. Typically, you like to change the policy properties once the policy is assigned to an object.
Depending on the Identity Manager version you may see a **Password policy assignment** tab on right lower. In this case perform action 5. Just to get aware of this feature.

- To assign policies to objects, select from menu **View, Select table relations**.



  - Check/ensure: ***QBMObjectHasPwdPolicy***
  - Click **[OK]**
- Select tab **Password policy assignment**s that appeared on the bottom of the Designer if necessary.

NOTE:
As you can see, here you can assign a policy directly to an as password field marked data column of an Identity Manager table. Now you know two ways to configure Password policies. It is your choice which one you like to prefer. In this lab we make life simple as possible and continue in Designer.

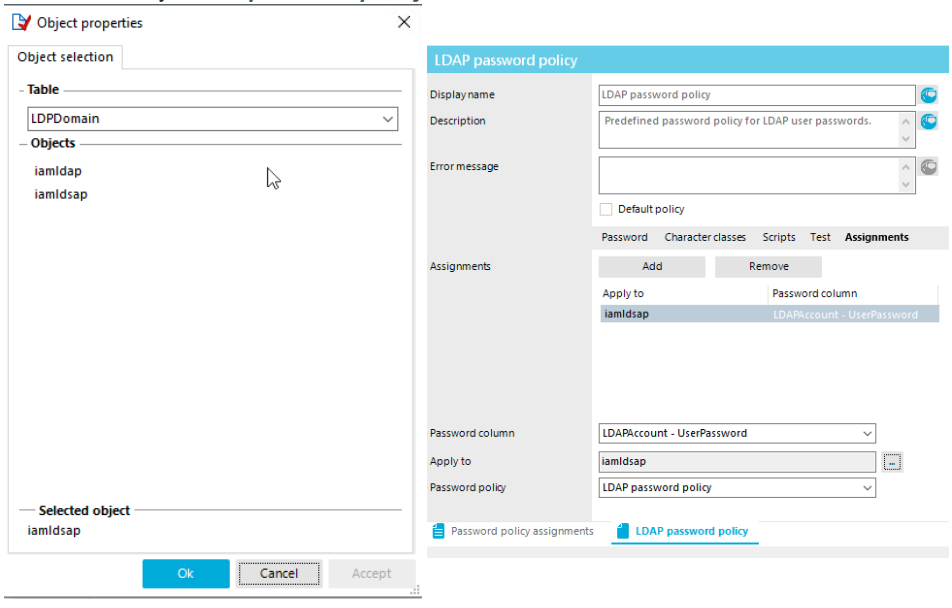
- In the **List Editor** select **Active Directory password policy** and switch to tab **Active Directory password**

policy on bottom of the **Designer**. Next step is to configure settings fitting to our Demo/Training environment.

- Initial Password: ***I.4Madmin***
- Min length: ***4***
- Max length: ***0***
- Max. failed logins: ***0***
- Max days valid: ***0***
- Password history: ***0***
- Min. password strength: ***0***
- Name properties denied: ***uncheck***
- Switch to tab **Character classes**
- Min. number of letters: ***1***
- Min. number of lowercase: ***1***
- Min. number of uppercase: ***1***
- Min. number of digits: ***1***
- Min. number of special characters: ***1***
- Max. identical characters in total: ***0***
- Max. identical characters in success: ***0***
- Permitted special characters: ***keep the default***
- Denied special characters: ***empty***

> **NOTE:**
> A huge number of properties to double check. In a real-life scenario your configuration should fit to the target system policy. Additionally, to know, 'value 0' is sometimes used to turn a policy off like for **Min. password strength** or **Min. password length**.

- Please redo steps all subs of the previous main step you did before, for the following Password policies. This is necessary to connect the other target systems.
  - Password policy for central password employees
  - One Identity Manager password policy
  - LDAP password policy
- Use tab **Assignments** to assign the LDAP password policy to the connected LDAP realm (LDAP password policy only!)
  - Password column: ***LDAPAccount - UserPassword***
  - Apply to: ***iamLDAP***
    - Klick on the tiny gray button
    - Table - select LDPDomain Object - klick on iamldap to select the entry
    - Klick on **[OK]**
  - Password Policy: ***LDAP password policy***

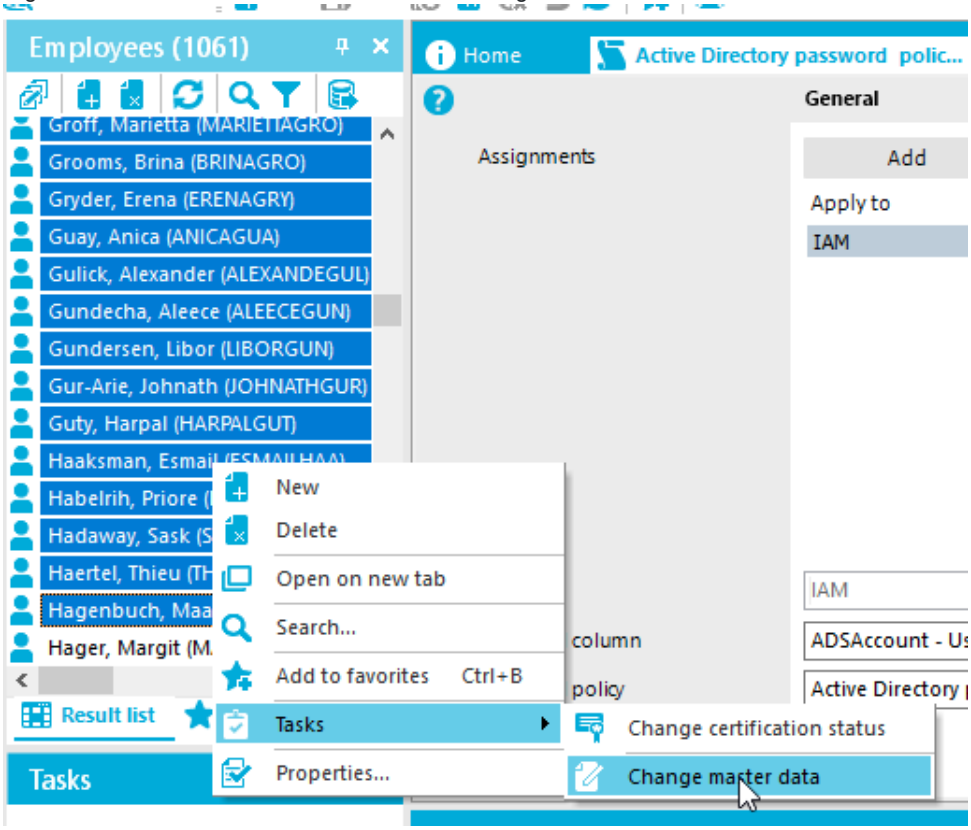


- Don't forget to **[Commit to database]**.

Set Person. DialogUserPassWord

NOTE:
To fully handle an initial password you must write a template (this will be shown later in this training) to get this password written into an object. If an initial password (in a password policy) is empty the system tries to generate a random password. This only works if there is a mechanism which allows to send this random password out to someone. Unfortunately, after an initial installation, we do not have these addresses or email sending enabled. We can also not deliver a static initial password. Because of this in a real-world scenario, a custom template must be used to configure the customer specific functionality. In this training, to simplify things for our more static training environment, we will just set these Person.DialogUser passwords once being valid for the whole training session.
Nevertheless, don't forget to set the initial password for each Password policy.

- Open **Manager** for example using Launchpad and sign in with your system user account.
- Select filter **Employees/Employees**. You should see about 1068 employees in your list.
- Perform the following actions in three equal sized blocks. An accurate block size is not important, but we recommend using similar sized blocks for an optimal performance. You can use **[Shift] + [right click]** to size your blocks like usual. With a determined group of objects:
  - Right click the marked block and select Tasks/Change main data



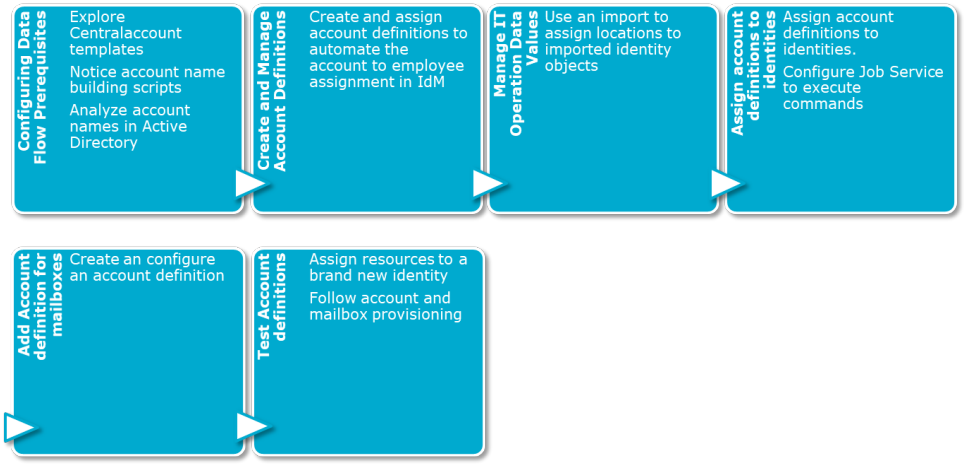
  - Switch to tab Miscellaneous
  - Enter in field System User Password - NOT in field Central password.
    - System user Password: ***I.4Madmin***
    - Confirmation (below): ***I.4Madmin***
    - Click **[Save]**
  - Repeat this for the rest of all objects (two more groups of selected objects (=blocks))

NOTE:
This allows you in the ongoing training to sign in to our Web portals using a person role-based authentication.

Lab Exercise Complete

Lab Exercise: New Hire Provisioning in Active Directory (IM-CBS-03)

Exercise Overview



In this lab you configure Identity Manager for AD and Exchange provisioning and automate the system to create an account and mailbox for a new employee.

What you need to know

- You should have the images open and running for this lab.
- Additional Lab content stored in the Lab folder (T:\courses\IdentityManager (\\IAMS10\Training\courses \IdentityManager):

User credentials required for this lab

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin

Estimated Time To Complete This Lab: **45 minutes**

Lab Exercise

Configure Data Flow Prerequisites

> **NOTE:**
> Each Identity Management Project requires some customization. At this time, we won't bother you with detailed knowledge of VB.Net or SQL scripting. Because of this, we provide the code to apply as pre-configured snippets. Please be aware that Identity Manager is a powerful solution framework with much out-of-the-box functionality, but you still need SQL and VB.NET knowledge for each project. In the following lab exercise, we explain the prerequisites to be checked and configured and show why this knowledge is required.

- One configuration which seldom fits out-of-the-box, is how to build account names. Requirements differ from customer to customer and from project to project. Following a modern IGA approach an Identity and Access Governance software (including Identity Manager) needs to drive connected target systems. For newly created accounts we must build a script to construct the account names. First, let's understand the out-of-the-box functionality:

- From **Launchpad** open **Configure/Change system settings**
- In **Designer** select **One Identity Manager Schema** from the main menu and expand **Templates**. This may initially take a while. Don't worry, Designer is loading many scripts.
- Expand **Default Templates/Person** and select the node: **Centralaccount**. If **centralaccount** is not in this list have a look into **Custom templates**.
- Select **Show column definition** from the **Tasks** list and in **Column properties** switch to the tab: **Value calculation**
- Have a look at the code (to ease reading, click at the tiny rectangle icon in the right lower edge of the value box).

You should see that the **Value** is built by calling the scripts: VI_AE_BuildCentralaccount or VI_AE_BuildCentralAccountGlobalUnique.

NOTE:
Depending on the environment you are using, the described changes are already made. Easy to figure this out by:

- The property **centralaccount** is located underneath of **Custom templates/Person**
- Instead of the scripts VI_AE_BuildCentralAccount and VI_AE_BuildCentralAccountGlobalUnique you will see similar named scripts starting with CCC_AE_.

In this case, please follow the next lines carefully. The explanations are more important as the steps to perform. Skip lines where there is something to do. Double check if everything was configured correctly.

- Close the Script editor pop-up form if needed.

- We are interested in understanding these scripts:
  - Select Script Library from the main menu.
  - Expand Scripts and select entry VI_AE_BuildCentralAccount
  - Select Edit VI_AE_BuildCentralAccount from the Task list
  - View the section displayed below:

```
   If Firstname.Length > 0 And Lastname.Length > 0 Then     accnt = Firstname & Las
```

NOTE:
As you can see, the account name (accnt) is built out of the firstname + first left character of the Lastname.

- Now let's check the existing **Person.Centralaccount** entries in our database.
  - Open **Object Browser** from the Start menu and login with your system user credentials.
  - From top menu **SQL** select **New SQL window**.
  - From top menu **SQL** select Load and open file IM-CBS-03__Analysis-Accountnames.sql from the IM-CBS-03 Lab folder.
  - Select the statement between “go” and “go” and click the **play** button or press (**F5**)

  - Ignore all service accounts and analyze how the **centralaccount** is build out of **firstname** and **lastname**.

NOTE:
You should see **centralaccount** is formed with **firstname** combined with the first 3 characters of the **lastname**. To ensure a unique value, we add a number at the end if an account name already exists. Also, remember that in Active Directory SAMAccount names should not be longer as 20 characters and we have the opportunity to add a prefix in front of the account name to specify, for example, an admin account (A_[account name]) if necessary. This is only a rough concept but let’s implement this now in the scripts we found above. In a real situation, you would discuss this with your customer and write a small proof-of-concept

first.

- For the lab implementation we will use predefined scripts, as mentioned.
  - Switch back into **Designer** and select **Script Library** from the main menu
  - Select **Create a new script** from the Task list
  - Open script file IM-CBS-03__Script_CCC_AE_BuildCentralAccount.vb with a text editor and copy the script content (starting with #If Not SCRIPTDEBUGGER Then…)
  - Paste the code into the large empty window in **Designer**.
  - Name your script (use the real script name e.g. **CCC_AE_Build…**)
  - Close the script window.
- Repeat steps a. to e. for script file:
  IM-CBS-03__Script_CCC_AE_BuildCentralAccountGlobalUnique.vb (name the record CCC_AE_BuildCentralAccountGlobalUnique)
- Remember, the scripts were called from a small template we viewed at the beginning of this lab. We must change this template to call our new scripts instead of the originals.
  - In Designer select **One Identity Manager Schema** from the main menu and expand **Templates**. Again, don't worry if this takes a while. **Designer** is loading scripts.
  - Expand **Default Templates/Person** and select node **Centralaccount**.
  - Select **Show column definition** from the Task list and in **Column properties**, switch to the tab: **Value calculation**
  - Replace the old script names using our new script names (it should be enough to replace "VI_" by "CCC_" for both scripts VI_AE_BuildCentralAccount and VI_AE_BuildCentralAccountGlobalUnique). After you have finished your work, the template should look like this:

```
… Value = CCC_AE_BuildCentralAccountGlobalUnique( GetValue("UID_Person").String, $
```

  - Use **[Commit to database]** on the upper left to store the two new scripts and modified template.
  - From the **Database** menu at the top of the application window, run Compile Database… and compile the database including all dependencies.

NOTE:
Now the system will generate similar account names to what we imported from Active Directory earlier.

- To double check this, we will use **Manager** and create a new identity (person object).
  - If **Manager** is already open, close it.
  - From **Launchpad** start **Manage/Display and maintain content data**.
  - Select **Employees** from the Main Menu in **Manager**.
  - Click on the **Employees** root node.
  - Click the blue paper with the plus in the Employees pane toolbar.

NOTE:
If you already created an identity having your name during this training, be creative and find another name instead.

  - Enter the following data:
    - First name: ***your first name***
    - Last name: ***your last name***
  - Click the **Organizational** tab
    - Primary Department: ***Accounting & Finance\Accounting\Australia***
    - Primary cost center: ***20\20100\20100060***

NOTE:
Both should be a leaf node. Remember this, you will need the information later.

- Click the **Address** tab
  - Configure a **Primary location** of your choice but starting with AU.
- Click **[Save]**
- Now step to the **Miscellaneous** tab and view the calculated value of **Central user account**. It should meet to our naming conditions. Remember this value also.

NOTE:
The identity you have created is similar to a record inserted by an HR system import, for example. Often, the HR system delivers no more information than first name, last name, cost center, department and location. Now we must implement a configuration structure to get missing information, such as AD container, Home server, Profile server, Mailbox Store, etc.

- At present we have accounts and identities (person objects) and they are linked together. From a data safety perspective this configuration cannot lead to any administrative data manipulation in the target system (maximum safety configuration).
  - In **Manager** select **Employees** from the main menu section and select just one employee record. You can choose any record you like, except the one you just created as part of this lab exercise.
  - In the overview pane, on the right side, you should see the **Employee** object in the middle and below, the associated Active Directory user account object. If this is not the case, select another employee object.
  - Click on the AD account object name. Now you see the **Active Directory user account** object in the middle.
  - Click on the AD account name again. A page with several input fields opens. We call this the **Main Data** page of the **Active Directory user account** object.

NOTE:
Please notice the fields: Employee, **Account definition** and **Manage level**. There is an employee linked to this account, but there is no account definition assigned and because of this, there is no level of automation assignment either. This means the account is **completely managed by the target system** and any modification of the person object (identity) will not reach or impact the account object. A situation that is very nice for an initial synchronization, ensuring that nothing adverse happens (other than the data creation in Identity Manager) but this configuration is not fitting to Identity Management behavior (remember IGA should drive a target system).
Last, but not least, please notice the flag **Groups can be inherited** near the bottom of the form. It is unchecked, which means IT Shop orders or role-based assignments will not take any effect on this account. Any group assignment to the employee will not lead to a permission change in Active Directory (again in case of IGA against all rules but secure in case of an initial installation - Imported data will not be automatically corrected in a second, automated step).

Create and manage Account definitions

- To manage the accounts linked to an identity in Identity Manager, we must create an account definition and define an automation level for these accounts.
  First step gets your **Manager** front-end up and running if it isn't already.

NOTE:
There are two ways to hit the target:
- We can just create an account definition on the Active Directory domain level. This will automatically assign the account definition and its associated automation level to any new account created during a reconciliation run from Active Directory.
- The second way is to create an account definition and assign it manually to the Active Directory account object. In this case, any new, reconciled account will only be created as a linked account and you must repeat the assignment for any new account (inserted by reconciliation) again as it was seen before. It is up to the customer to decide which behavior to configure. Our first scenario is more authoritative, but only optimal if the employee data quality is clean. Our second scenario is more secure, but needs manual actions to get a new account created in Active Directory ready for IGA. There is no problem to

change the initial selection later in the project.

- To create an account definition, in **Manager** select **Active Directory** from the main menu.
  - Expand **Basic configuration data / Account definitions** and select **Account definitions**.
  - Hit on the create new object icon just above the list box

  - Configure a new account definition.
    - Account definition: ***Std. user account Domain IAM***
    - User account table: ***ADSAccount***
    - Target system: ***IAM.corp***
    - Manage level (initial): ***Full managed***
    - Groups can be inherited: ***Yes***
    - Click **[Save]**.

NOTE:
The User account table together with the Target system specifies whether to create or manage Active Directory accounts for the domain IAM. The Manage level (initial) defines that any change on a related identity object will affect the AD account object, depending on the out-of-the-box implemented data flow rules (templates).
By the way, you initially only find the Managed level (initial) Full Managed and Unmanaged in Identity Manager. Full Managed means that all predefined attributes are affected and Unmanaged means that only mandatory predefined attributes are affected. Please don't make the mistake of taking the word Unmanaged literally. An automation level is managing your account. Only linked accounts are and keeps untouched by identity changes.
If you need a more detailed behavior between Full Managed and Unmanaged you can create as many custom levels of automation as you like.

- Please remember, Active Directory is not the only connected target system. **Please create an account definition for your connected OpenDJ LDAP system**. You can use the information from the main step above to do this. It's the same way as to create the account definition for Active Directory. Change the described steps and values above. This time it is the REALM: **iamldap** and you need to take an **ldapaccount** table to store the values in. If something becomes unclear discuss steps with your class.
- Before we can assign the account definition to new account/identity objects we must configure some standard parameters necessary for further management. These parameters are known as **IT Operating Data**.
  - In **Manager**, select the newly created account definition for Active Directory accounts.
  - Click **Edit IT operating data mapping** from the Tasks list.
  - Click **[Add]** to create a new IT Data configuration if not exists
    - Column: ***ADSAccount - IsGroupAccount***
    - Always use default value: ***checked***
    - Default Value: ***1***

NOTE:
We configured a fixed value to ensure that any permission ordered through IT Shop or provisioned through a role will now take effect for accounts with this assigned account definition.

- Click **[Add]** to create another **IT Data configuration**
  - Column: ***ADSAccount - UID_AdsContainer***
  - Source: ***Primary Department***
  - Default value: ***IAM.corp/Users***
  - Always use default value: ***unchecked***
  - Notify when applying default: ***checked***

NOTE:
We configured an AD container where the account lives, to be chosen depending on the department assignment. Also, we ensured that the default container, users, at the domain level is used if the employee is not assigned to a department (default).

  - Click **[Add]** to create another IT Data configuration
    - Column: ***ADSAccount - UID_Homeserver***
    - Source: ***Primary Location***
    - Default value: ***IAMS01***
    - Always use default value: ***unchecked***
    - Notify when applying default: ***checked***
  - Please configure the same for **ADSAccount - Uid_Profileserve**r. This time the **Default value** to configure is **IAMS03**.
  - Now press **[Save]** and confirm the message.
- Now we will repeat parts of this for our LDAP target system
  - In **Manager**, select the newly created account definition for LDAP.
  - Click **Edit IT operating data mapping** from the **Tasks** list.
  - Click **[Add]** to create a new IT Data configuration if not exists
    - Column: ***LDAPAccount - IsGroupAccount***
    - Always use default value: ***checked***
    - Default Value: ***1***
  - Click **[Add]** to create another IT Data configuration
    - Column: ***LDAPAccount - UID_LDAPContainer***
    - Source: ***Primary Department***
    - Default value: ***OtherAccounts (iamldap.corp/OtherAccounts)***
    - Always use default value: ***unchecked***
    - Notify when applying default: ***checked***
    - Click **[Save]**
- In our next steps we want to configure server IAMS01 as home- and profile server. You will remember from the earlier steps in the lab exercises that IAMS01 was added by the AD synchronization wizard and is available in the list of servers to be selected. It's time to confirm and assign the appropriate server roles now.
  - In **Designer**, switch to the main menu **Base Data** and select **Installation/Job server** from the **Navigation** tree.
  - Select the Job Server: **IAMS01**. Click on the **Job server 'IAMS01'** tab (bottom of the window) and configured as follows:
    - Server: ***IAMS01***
    - Full server name: **IAMS01.iam.corp**
    - Executing server: **IAMS03**
    - Queue: ***\IAMS01***
  - Click on the Server Functions tab and view the **Add assignments** section at the bottom of the front-end and ensure the following are assigned:
    - Home server
    - Profile server
    - Domain controller
    - Microsoft Exchange server

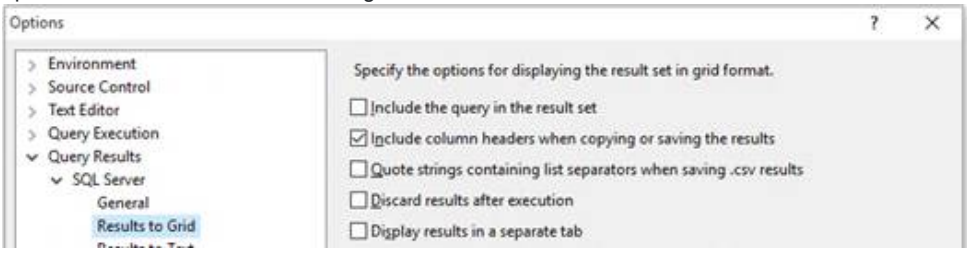
        - Click **[Commit to database]**
    - Close **Designer**

Manage IT Operating Data values

- In an earlier step we defined IT Operating Data to manage missing properties based on fixed values. Switch back to **Manager**.
- In **Manager** select **Organizations** from the main menu and expand **Departments** tree down to **Accounting & Finance\Accounting\Australia**.
- Select task **Edit IT operating data**
    - Click **[Add]**.
    - Click on the blue arrow beside **Effects on**
        - Table: ***TSBAccountDef***
        - Effects on: ***Std. user account domain IAM***
        - Click **[Ok]**.
    - Column: ***ADSAccount - UID_ADSContainer***
    - Value: ***IAM.corp/Company/Accounting***
    - Click **[Save]** and commit the message.
- Next step is to configure IAMS01 as Home and Profile Server
- Select **Locations:Hierarchical view/ AU - Bayswater VIC - 5 - 7 Waldheim Rd**, and select **Edit IT operating data**.
- Click **[Add]**.
- Click on the blue arrow beside **Effects on**
    - Table: ***TSBAccountDef***
    - Effects on: ***Std. user account domain IAM***
    - Click **[Ok]**
- Column: ***ADSAccount - UID_Homeserver***
- Value: ***IAMS01***
- Configure the same for ADSAccount - UID_Profileserver **but** configure **IAMS03** as profile server value.
- Click **[Save]**.

NOTE:
Now we have IT operating data configured for just one department and one location. To do the same for all other departments and locations, we will use an import. In a real world scenario, you would take the template records we created and use copy, paste and calculations in a spread sheet to build a csv file for import. In our training environment, with the previously imported department and location structure, and for this specific use case, we can use a SQL script to generate our csv. This is necessary because each environment includes some different UID's. This does not allow us to use a pre-created csv file.
Please note as well: In a real-world scenario, you must create and permission the necessary home and profile shares on each server you want to configure (or ensure they already exists and are accessible for your Identity Manager Service account).

- In order to generate the csv file, we must check the configuration of our SQL Management Studio first. It should already be configured but it is helpful to check this in our lab exercise. Open **Microsoft SQL Server Management Studio** from **START**.
    - Connect to Server IAMS02
    - In menu **Tools** select **Options…**
    - Ensure the following configuration is set: **Query Results → SQL Server → Results to Grid** shows the option **Include column headers when copying or saving results** is checked. If this is not checked, check the option and restart SQL Server Management Studio.



- Now we want to create the csv file. Open and run sql file IM-CBS-03_Script_Generate_IT-Data.sql in SQL Server Management Studio into a Data grid (Ctrl+D, Ctrl+E). Ensure you are running the script against the Identity Manager database. It should generate a long result list.
- Right-click into the data grid and perform Save Result As… and store the grid into a comma separated csv file named of your choice.

NOTE:
Running the query into a data grid is mandatory to get the result saved as a comma separated (csv) file. The option we set above generates the header. If this is not accurately done, you will have a csv file which cannot be imported as described below.
Please understand, to create this file is a little bit voodoo and not part of the training.
Please don't spend time in understanding the SQL script.
Voodoo like this is sometimes used by senior experts to initial fill data into an Identity Manager installation. The used SQL is always depending on the existing data situation and customer specific implementation/generation rules. In this case we used SQL to generate a CSV file, considering objects you created in labs before and we are using the API by using data importer to create more entries. This combination makes the change very stable and secure in difference to using SQL only.

- Open **Data Importer** (suggest using **Launchpad** again).
  - Select Import definition file: IM-CBS-03__Import_Def_IT_Operation_Data_2_Organization.xml
  - Select Import file you created and named before and complete the import.
  - Configure Save import definition file unchecked
  - Perform the import as you learned this before.

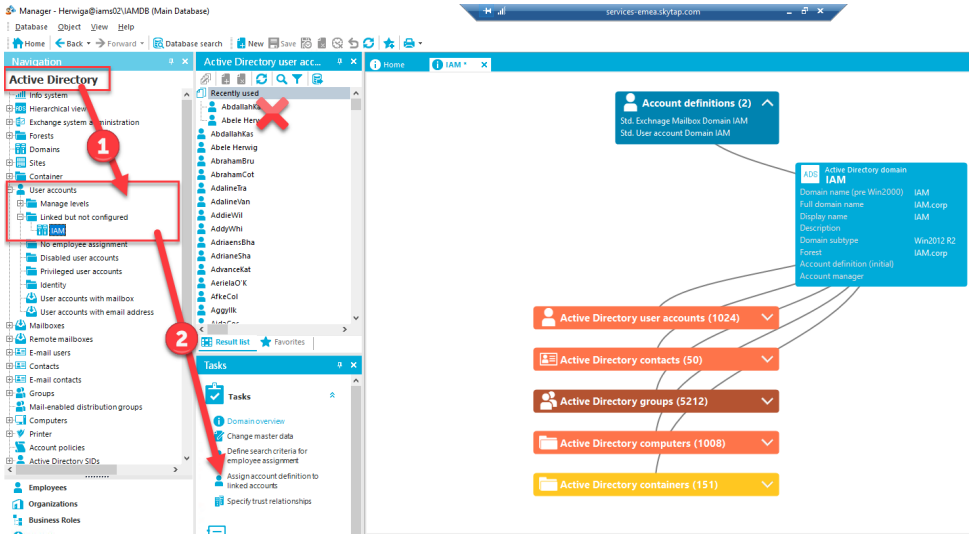
NOTE:
After performing many imports we assume that you can repeat this at any time using an import definition file. The description above only highlights important configuration steps.
During the import you may see up to 3 error messages. These messages appear to inform you, that it is not possible to insert the three records you already created manually, earlier in the lab exercise. These messages are OK and can be ignored.

- Use Manager to check a few department and location records, to see the assigned IT Operating Data. Now we are prepared to start using our account definitions.

Assign account definition to employees

NOTE:
Up to now, we have Active Directory accounts and identities in the Identity Manager database. They are only linked together which means that there is between accounts and identities (person objects) no data flow enabled. In this step we like to bring these accounts under control of a proper Identity Management.
In previous versions of Identity Manager, we assigned the account resource to the person object and that was the only account configured and set under control of the account definition. Issues arose if a person was configured with two and more different accounts from one target system (domain).
In Identity Manager there is a specific dialog we use to assign an account definition to people.

- In **Manager**, select **Active Directory** from the main menu and expand **User accounts/Linked but not configured**.
  - Click on **IAM**, the only domain that exists at present. (In a production environment there could be more than one domain in the tree.)



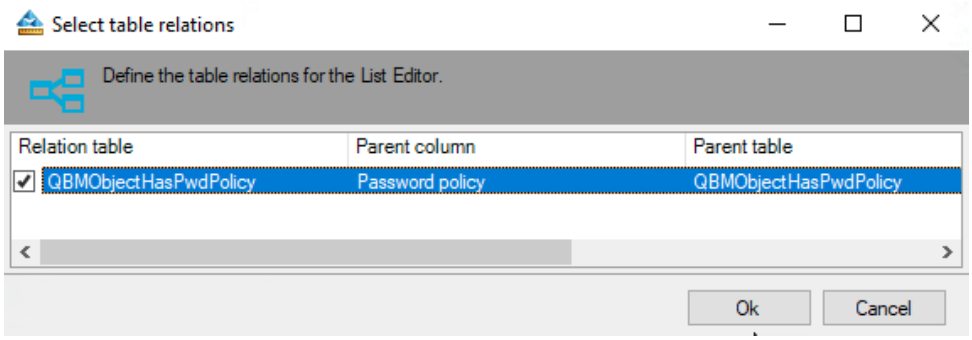
- Select **Assign account definition to linked accounts** from the Task list
- Use the only account definition: **Standard User Account domain IAM** (the name may differ to this, depending on your configuration before. Take your created Account definition for the Active Directory domain). A list of user accounts should then appear below the selection.
- Check the tiny box to the left of the first account (it should be AbdallahKas; The idea is to test this with one object to get an idea of related processes).
- Click **[Save]**.
- Open **Jobqueue Info** for monitoring.
- Use **Jobqueue Info** to follow the processes in Jobqueue and DB Queue.

NOTE:
The next steps show you to implement another Queue to your Identity Manager Job Service. We do this to allow to handle home directories. This is a typical task working with Identity Manager and adding functionality. LATER ON (and once you ensured the whole process works perfectly) you will configure the other AD accounts to become fully managed identities. Because of this you should not forget step 1a. to 1g., you will need this knowledge again. After the process of assigning the account definition, followed by a process to create an account, based on the assigned account definition, the last step is a process to create a home and a profile directory. You will probably see that these processes are sitting in the Job queue with nothing happening. The process steps are in Execution state, but the Start time is in the past and they didn't start. Please also see the Executing Server \IAMS01. Remember, we did not install the Identity Manager Service on this server. We have two options now:

- We can install another Identity Manager Service on IAMS01.
- We can install another queue on an existing Job Server.

The first option was already seen in Lab IM-INS-02. Now let's follow the second option and improve the Identity Manager service configuration on IAMS03, by adding another queue.

- Open a Skytap connection to your client IAMW01.



- Sign in and open Windows Explorer.
- Find the folder **C:\Program Files\One Identity\One Identity Manager** and start **JobServiceConfigurator.exe**
  - Open the file \\iams03\c$\program files\One Identity\One Identity Manager\JobService.cfg

- Select **Job destination** and click **[Insert]**
- Select **JobServiceDestination** and click **[Ok]**
  - Select the new entry **JobServiceDestination** and search for the **Queue** property
  - Replace **\%Computername%** by typing ***\IAMS01***
  - Replace **Process request interval (seconds)** configured to 90 by ***30***.

NOTE:
Please ensure that the mouse cursor leaves the last field after editing the value. (click on a different field)
You should see now two different **Job destinations** (named **queuex** and **JobServiceDestination**). One Queue property (in **queuex**) is configured to **\%Computername** and will take care of all job queue jobs showing the **\IAMS03** queue information. This is because **%Comutername%** represents the system environment variable computername and is set to the name of the server which is **IAMS03**. The second queue will take care on jobs for **\IAMS01**. We have now configured an Identity Manager Service with two different queues. We must ensure that the service account used to start the Identity Manager Service is permitted to do all file operations remotely on server **IAMS0**1. This is already configured by the Technical ENablement team. They also created the shares to access home and profile directories.

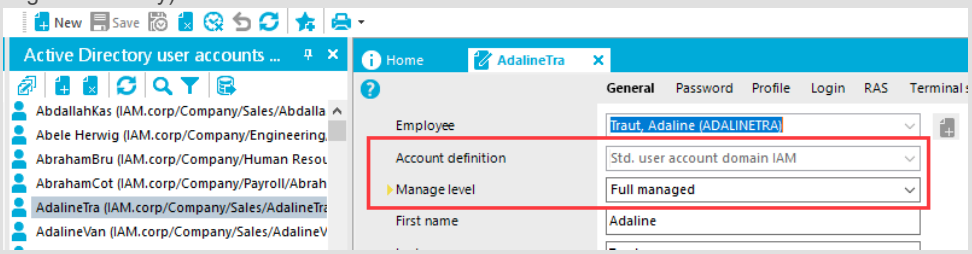
  - Save the configuration now using menu **File/Save**
- Open a Skytap connection to your server **IAMS03**. Open **SCM** now (e.g. from **RUN** start **services.msc**).
- Find **One Identity Manager Service** and restart the service.

- Switch back to your Workstation and follow the process execution in **Jobqueue Info**.
- If everything looks good now and Job queue is empty again we shall assign the same account definition to all other accounts except service and system accounts. Switch back to **Manager**.
- Now please remember everything you did in step 1. According to this use form **Assign account definition to linked accounts** to assign an account definition to all other accounts.
  - Select all accounts per the note below.

NOTE:
We only want to select accounts that are not service or system accounts. In our lab environment, they are the accounts residing below the Company OU (look at the path of each object, the OU is included). You may use **[Ctrl]+[A]** to select all accounts, then **[Ctrl]+[double click]** to deselect the service accounts. There should be ten service accounts to deselect - a group of two, a group of seven and a single account. Then click on a single selected check box to select all check boxes.

- Step page by page down the list and search for account names looking longer as the others or not stored in **IAM.corp/Company/…**.
  - De-select some **HealthMailbox…** accounts (two in all)
  - De-select some **Service Account…** accounts (eight in all)
  - . Click **[Save]**
- Sit back and relax, your system now starts some heavy work. You can follow using **Jobqueue Info**.

NOTE:
Awesome! We have now configured the appropriate account definition for each Active Directory account. This assigns the account definition and sets the automation level to Full Managed for each account. We are now ready for IGA. Take the Manager and to double check if accounts are switched to Full Managed now (remember there might be a delay).



If it was necessary to configure the account definition on the domain level (note above) and the Job queue is empty again, it is time to select the domain again and to remove the account definition from the domain master

data.

Adding MS Exchange mailbox account definition

NOTE:
Now we want to create an account definition to create mailboxes in the future. At present, there are only a few accounts equipped with mailboxes. We don't want to actually change this because we want to save space in the training environment. Instead, we will allow newly created employees to have the option to get a mailbox. This means we will create an account definition, but we will not assign it to all existing person objects like we did before for the AD account definition.

- In Manager select **Active Directory** from the main menu and expand the **Basic configuration data** section in the navigation pane.
  - Select **Account definitions**
  - Hit on the **Create new object** icon just above the list box.
  - Configure the new account definition (if it's not already done)
    - Account definition: ***Std. mailbox Domain IAM***
    - User account table: ***EX0MailBox***
    - Target system: ***IAM.corp***
    - Required account definition: ***Std. user account Domain IAM***
    - Level of automation: ***Full managed***
    - Click **[Save]**

NOTE:
The **Required account definition** must be set because you need an AD account first before you can start to create a mailbox and Identity Manager must know about this requirement.

- Select **Edit IT operating data mapping** from the Tasks list.
  - Click **[Add]** to add a mapping.
  - Column: ***EX0MailBox - UID_Ex0MailBoxDatabase***
  - Default Value: ***Mailbox Database 0089241127***
    (Select it from the list, it is the only existing entry)
  - Always use default value: ***checked***
  - Click **[Save]** and commit the message.
- Now let's assign the mailbox account definition to the domain. Select your Active Directory domain, using the **Domains** filter in the **Navigation** pane.
- Select **Change main data** from the **Tasks** list and select the **Exchange** tab.
  - Mailbox definition (initial): ***Std. mailbox domain IAM***
    (or the name of the definition you created in an earlier lab)
- Click **[Save]**

Test the auto-provisioning for new hires

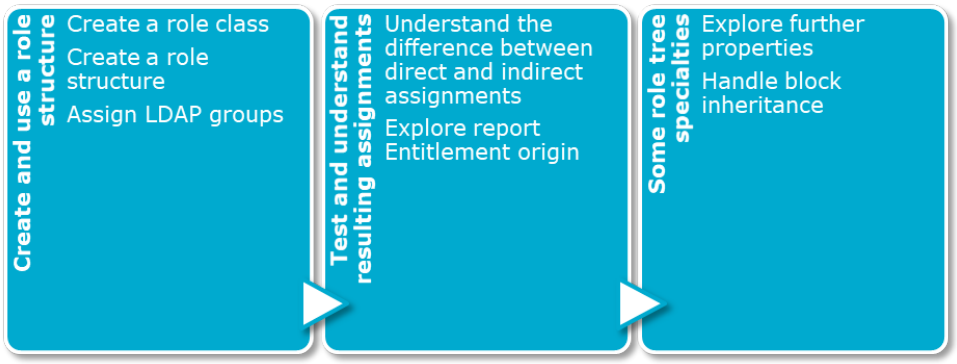
- Select **Employees** from main menu.
- Click the **Create a new object** icon in the employees **Result list** tool bar.
- Enter the following data:
  - First name: ***"enter a first name"***
  - Last name: ***"enter a last name"***
  - Click the **Organizational** tab.
  - Select a value for primary department from the drop-down tree (should be a leaf node for lab simplicity). Remember this name, you will need it later.
  - Select a value for primary cost center from the drop-down tree (again this should be a leaf node). Remember this name, you will also need it later.
  - Click the **Address** tab.
  - Configure a primary location of your choice.
  - Click **[Save]**.
- To get an AD account and a mailbox you need account definitions. Select your new employee and assign the

following account definitions.
    - Std. mailbox domain IAM
    - Std. user account domain IAM
    - Click **[Save]**.
- Start Jobqueue Info and observe the processes as they complete.

Lab Exercise Complete

Lab Exercise: Working with Roles (IM-ROL-01)

Exercise Overview



In this lab you create and manage role structures and view the advantage of roles for assigning permissions. We cover how to use an existing role structure as well as how to develop a new one.

NOTE:
Notes (gray boxes) are important in all labs. Please read them carefully some of them are as well considered in assessment tests. In this lab these boxes are essential to understand why you perform steps. The main purpose is to show you how roles are working and can be used to manage permissions (in this case for a simple, virtual document management system).
You can use Softerra LDAP Browser installed on your Admin Workstation to check your LDAP objects.

What you need to know

- You should have the images open and running for this lab.

User credentials required for this lab

Affected Machines	IAMS04, IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin
LDAP synchronization account	
Username	svc_LDAP_1im
Password	I.4Madmin

Estimated Time To Complete This Lab: **90 minutes**

Lab Exercise

Create and use a role structure

NOTE:
This lab and some others are used in different environments. To get not confused by working with more people together in one environment following the same lab description it is necessary to brand objects with a short prefix to identify the owned objects later. This prefix is named [Prefix] and gets typically created out of the first character of the students first name and last name. Please ensure that every student uses a different prefix. In a real-world

scenario this is nowhere seen, because typically you don't have 5 or more people fulfilling simultaneously the same job. remember and note your Prefix.

- In **Manager**, open **Business Roles** from the main menu.
- In the **Navigation** pane expand the node, **Basic configuration data** and select **Role classes**.
- Right click into white space of the **Result list** tab and select **New** from the context menu.
- Enter the following for the new role class:
  - Role class: ***[Prefix]_Doc Access Management***
  - Click **[Save]**.

NOTE:
In Identity Manager you can build up as many role trees as you like. Each role tree needs a root element, named role class. This role class is used to determine assignable resources and the resource inheritance within this role tree. If you mess up the inheritance, it is not possible to change this after the role class is saved for the first time. To change, this you must delete the role class and recreate it. Because of this, it makes sense to plan role classes properly before you start creating the object.

- In some white space in the Navigation pane right-click and select Refresh view from the context menu (only if you cannot see the created role-class. This is required because there is no auto-refresh in this front-end view).

NOTE:
Auto-refresh lowers the performance of the database because a large volume of data traffic is generated by the feature. Therefore auto-refresh is seldom seen in Identity Manager utilities.

- Click on **[Prefix]_Doc Access Management** in the **Navigation** tree.
- Select **Configure role assignments** from the **Tasks** list
- Check Assignments permitted (left column) and Direct assignments permitted (right column) for the following rows:
  - LDAP groups
  - Employees
  - Resources
  - Account Definitions
  - Click **[Save]**

NOTE:
To make objects assignable to the role structure you must configure this feature for each object class you like to handle. This is to limit the number of calculations DBQueueProcessor must perform to check the assignments by inheritance. We start with an empty selection on a new role class, which means nothing can be assigned to the roles.
Remember these steps if you miss a specific object class to assign to a role.
A role structure needs to be planned before you start an implementation. If this is your first experience with roles in Identity Manager, it is helpful to talk about how to simplify or speed up processes. Your Trainer is the right person to ask how objects in Identity Manager can be created easily. Just to give you an idea - the review of this lab with reading and implementing like here described took 30 minutes in total but don't stress yourself, this means only you might need a bit more exercise experience.
For this exercise:
→ There is a **virtual Documentation system** (does not exist in reality). → This system gets **managed by several LDAP permission** groups (exist in an OpenDJ LDAP structure on IAMS04, connected to Identity Manager). Look into **Manager: LDAP / Hierarchical view** and you will see:

- The LDAP container structure looks like the department structure
- The LDAP container names look like the **department.shortname**
- Each LDAP container contains three LDAP groups
  - Admin_*
  - Editor_*
  - Reader_*

In this example we like to implement a role structure which considers some roles for the United States (only US

departments or parents). This structure should look like:

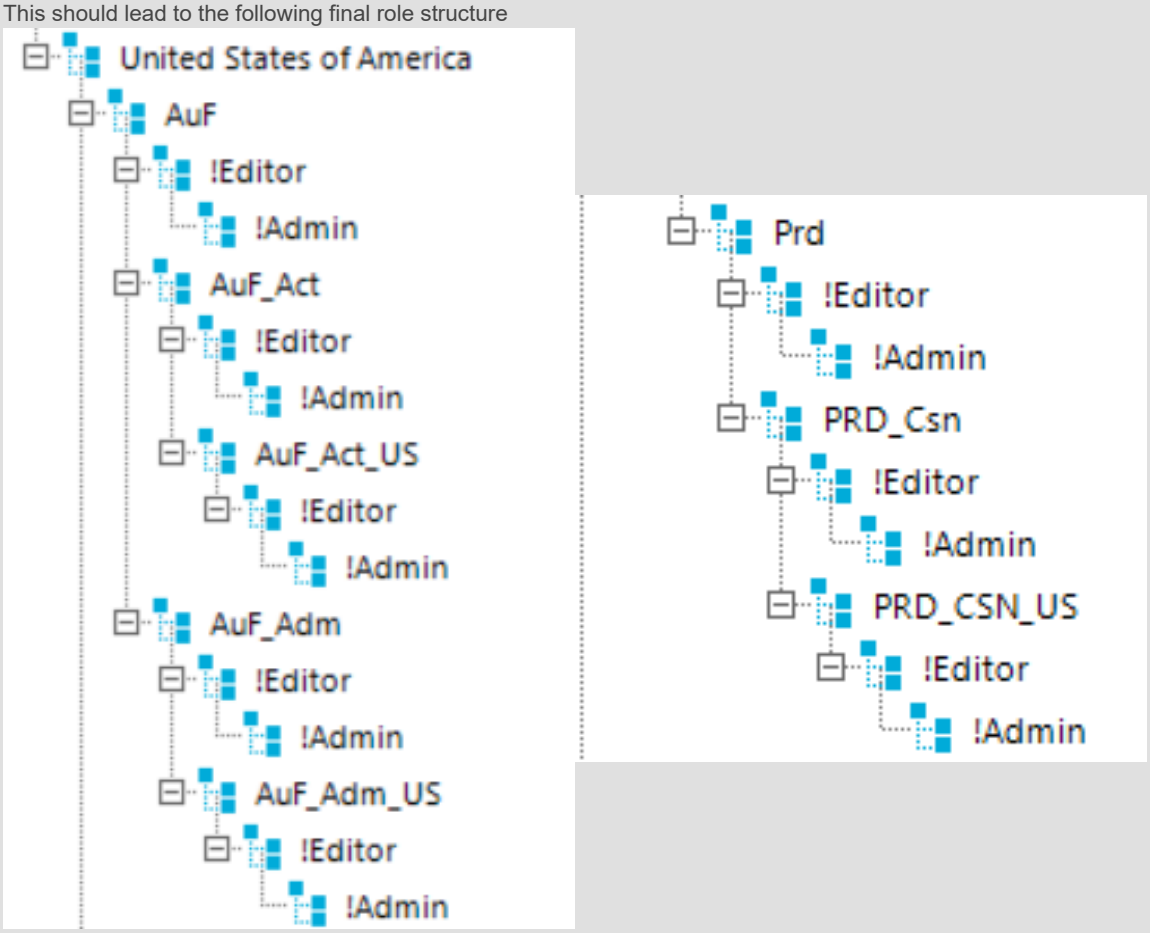
- United States of America
  - AuF
    - AuF_Act
      - AuF_Act_US
    - AuF_Adm
      - AuF_Adm_US
  - PRD
    - PRD_Csn
      - PRD_Csn_US

Additionally we make some assumptions:

- The plain department container will manage “Reader” permissions.
- For “Editor” and “Admin” privileges we like to implement additionally container.
- Admin should get all roles assigned to get all permissions available
- Our Documentation Tool only knows positive permissions (no deny permissions)
- Top down inheritance should help us as much as possible.
- In parent role structures only people located in US should be considered.
- Everybody in this company at least must have reading permissions to a node and his parents.
- Roles representing Editor / Admin privileges only should be marked.

Please discuss the role structure with your trainer and your class mates.

This should lead to the following final role structure



- To create this role structure, right click on **Hierarchical view** of the new created **Role class** and select **New** as you have already learned.
  - Name the new role: ***[Prefix] United States of America***
  - Click **[Save]**
- Create another new role underneath (it could be helpful to expand the parent element in the tree, see the child and right click the child to get a correct pre-configured new role).
  - Name it: ***[Prefix] AuF.***
  - Click **[Save]**

- Expand **Hierarchical view** in **Navigation** pane.
- Below each of the two roles you just created, create new sub-roles
  - Name: ***[Prefix] Auf_Act.***
  - Click **[Save]**
  - Name: ***[Prefix] Auf_Adm***
  - Click **[Save]**
- Please follow the picture above and create the rest of the role structure. Please remember as well, this picture doesn't show the right captions, you must add a prefix to each of your role names, this will help you in some courses to separate your roles from your colleagues. Two more hints:
  - Copy and paste can help to create roles having the same name.
  - Refresh tree-view and asterisk [*] on the num-pad can help to refresh and expands a sub-tree.
  - A nice order can help to speed work up
    - First create all non !* roles
    - Create all !Editor roles in non !* roles
    - Create all !Admin roles in !Editor roles

NOTE:
Permissions for these roles will be assigned through LDAP groups. These groups already exist. In the next step you will assign LDAP groups to this role structure.
Additionally these LDAP groups should be assigned to the according LDAP accounts of identities managed in these roles. This could mean that an identity without LDAP account should get one once he is assigned to one of the roles. Therefor an Account definition object must be as well assigned by this role structure.

- Select the top node of your role structure ([Prefix] United States of America).
  - Select **Assign account definitions** from the **Tasks** list
  - Assign the LDAP account definition to the role
  - Click **[Save]**
- Now we can start assigning permissions. Select the first second level node in **Hierarchical view** (should be AuF) and select **Assign LDAP groups** from the Tasks menu.
  - Select the according reader group and click **[Save]** to store the modification
    - Business role: ***AuF***
    - LDAP-group: ***iamldap / AuF / Reader_AuF***
    - Click **[Save]**
    - Business role: ***AuF_Act***
    - LDAP-group: ***iamldap / AuF / AuF_Act / Reader_AuF_Act***
    - Click **[Save]**
  - Repeat these steps accordingly until each container named like a department has its Reader_* group assigned.
  - Now let's assign LDAP groups to marked containers (!Editor, !Admin). This works accordingly to what we did before.
    - Business role: ***AuF / !Editor***
    - LDAP-group: ***iamldap / AuF / !Editor_AuF***
    - Click **[Save]**
    - Business role: ***AuF / / !Editor / !Admin***
    - LDAP-group: ***iamldap / AuF / !Admin_AuF***
    - Click **[Save]**
  - Repeat these steps accordingly for all other marked roles.

NOTE:
You might get the experience, that with all these technical names it is a bit complicated to select the right permissions. Additionally, it looks like, that creating a role structure and adding resources can be a bit painful if you try to do this initially.
Because of this, it might be easier to do this script based. You will find a couple of automation-features in Identity Manager making this possible. A proper naming might help as well. Therefore, exists on roles / departments / cost center / locations always properties for names and short names which could contain more technical AND user-friendly naming information.
To get the whole role structure a bit more looking friendly you can run the SQL script: **IM-ROL-01_Role-**

FriendlyNames.sql from the according lab folder (just open the script in **SQL Server Management Studio (SSMS)** after you selected the DB IAMDB, change the only variable by adding the name of your role class and execute the script using **[F5]**). Refresh the tree view in **Manager**. Now the display might help you to understand the intention of the script. You need once more to refresh the Hierarchical view of your role structure in Manager.
One more note to consider:
Playing around with SQL in Identity Manager is dangerous, because we don't take care of the Identity Manager object API. Something like this is only an option, if just a hand full of columns should be filled AND the data change should not have any effect on a connected target system. Better to be a super-hero with Identity Manager before you try to use something other else with an Identity Manager database as select … . Please understand, self-made inconsistencies can become very soon, very painful. **In any case a proper database backup should exist** before you try to do something like this with your production data.
Now it's time to assign identities to this role structure. Therefore, we need some **more assumptions:**

- **Reader should be assigned automated**
- **In each role only US employees should be considered**
- **Editors and Admins should be assigned manually**

- Select the **United States of America / AuF / AuF_Act / AuF_Act_US role** in the **Navigation** pane.
  - Click on **Create dynamic role** from the **Tasks** list.
    - Object class: ***Person***
  - Select **Use the where clause wizard** icon (2) that appears. Depending on the context where you navigate through sometimes you like to see the condition window instead of a wizard. In these cases, the db icon (1) can help you out.

  - In the popup window click on **At least one entry exists**.
  - Expand **Reference to other objects**
  - from the list select: ***Primary Department***
  - Click on **At least one entry exists**
  - Expand **Value comparison**
  - From the list select: ***Short name***
  - Click on the quotation marks behind **is equal to**
  - Enter role name: ***AuF_Act_US***
  - Click **[Next]** and watch people being considered
  - Click **[Next]** to see the generated SQL
  - Click **[Finished]** followed by **[Save]**

Note:
The SQL generated, might be a bit more complex or different to the SQL you have in mind. This is to get a better performance during execution.
The condition we created for this role considers only members of department AuF_Act_US. There is no further condition part necessary, because we know that department AuF_Act_US can only contain people from US. For parent roles we must consider this in a condition as well.

- Select the parent role **AuF_Act**
  - Click on Create dynamic role from the Tasks list.
    - Object class: ***Person***
  - Select **Use the where clause wizard** icon that appears.
  - In the popup window click on **At least one entry exists**.
  - Expand **Reference to other objects**
  - From the list select: ***Primary Department***
  - Click on **At least one entry exists**

- Expand **Value comparison**
- From the list select: ***Short name***
- Click on the quotation marks behind **is equal to**
- Enter role name: ***AuF_Act***
- Additionally, we need to prove people to live/work in US. Click the last **Add expression**. You should not click the previous one, because we don't want to specify another condition to determine the department we like to determine the location assigned to an employee to be done in the first level of this condition (in parallel to the department definition).
- Expand **Reference to other objects**
- From the list select: ***Primary Location***.
- Click on **At least one entry exists**
- Expand **Value comparison**
- From the list select: ***Location***
  (NOT the one with the key icon, this represents the UID we need the property containing a name)
- Click on **is equal to** at the end of the line and select **starts with**.
- Click on the quotation marks behind **starts with**
- Enter: ***US***
- Click **[Next]** and watch people being considered
- Click **[Next]** to see the generated SQL
- Click **[Finished]** followed by **[Save]**
- Copy the condition into your copy buffer (**[Ctrl]+[c]**).

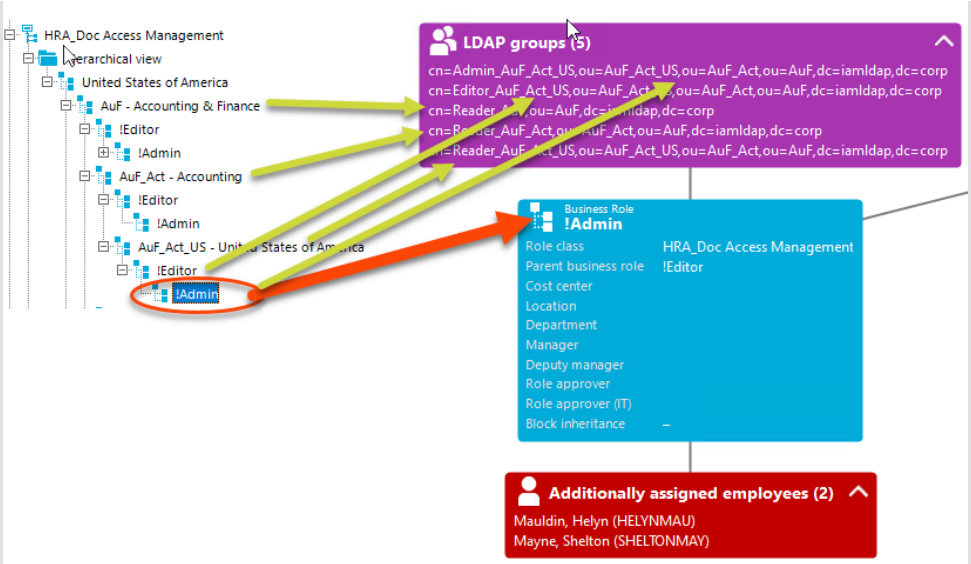
NOTE:
Why to step through all the steps as before, if we can copy and paste and modify the string a bit.
Please follow the steps carefully. You need to select the Object class first before you can paste and save the SQL!

- Select parent role AuF
  - Click on **Create dynamic role** from the **Tasks** list.
    - Object class: ***Person***
  - Paste the last created and copied where clause into field **condition**.
  - The only value should differ in this condition is departmentname. In the inserted string search for **AuF_Act** and replace it by **AuF**.
  - Click **Test condition** from the **Tasks** list and after getting some results, click **[Save]** to store the condition.
- Repeat steps above, as you like, to create similar results for Auf_Adm_US, Auf_Adm, PRD, PRD_CSN, PRD_CSN_US.
- In a last step assign one or two people from Parent roles manually to a !Editor and !Admin role. The entry Assign employees in the Tasks list is needed to do this. It is not necessary to do this for each of these roles but please only consider configured roles in the next steps.

Test and understand resulting assignments

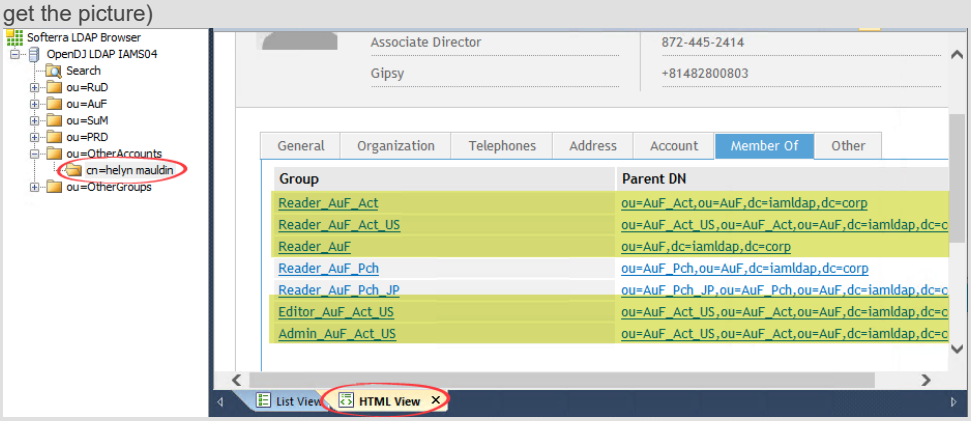
- Open Softerra LDAP Browser to check your LDAP objects hosted on IAMS04. This tool is installed on your admin workstation. There should be a connection pre-defined but you can use the following account to connect.
  - Login: ***cn=svc_LDAP_1im***
  - Password: ***I.4Madmin***
- Expand the tree and select an account and a group object to get a feeling for these objects.
  - In Manager select an !Admin role you have configured with employees before. For example use ***United States of America / AuF / Auf_Act / AuF_Act_US / !Editor / !Admin***.
  - Double-Check the group assignment in **LDAP Browser** on **IAMS04**

NOTE:
We expect to get a maximum set of permissions (LDAP-group assignments) for this role:
- Reader group for AuF by inheritance
- Reader group for AuF_Act by inheritance
- Reader group for AuF_Act_US by inheritance
- Editor group for AuF_Act_US by inheritance
- !Admin group for AuF_Act_US directly assigned



In this case user HELYNMAU must have all four groups assigned. A short look into Manager (selecting the LDAP account) shows the following Distinguishedname: ***cn=Shahid Fani, ou=SuM_Rsa_US, ou=SuM_Rsa, ou=SuM, dc=iamldap,dc=corp***.

This path leads to the following picture in LDAP (you must switch on ***View/Attribute view*** in this LDAP Browser to get the picture)

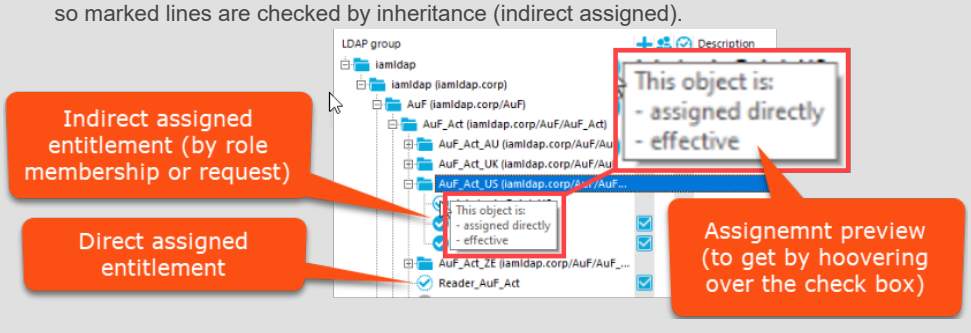


As you can easily see there are the expected and some other groups assigned. Time to figure out where these assignments came from.

- Before we can identify why these other LDAP groups are assigned, we must have a closer look at the assignment. In **Manager** for your selected role (in this example it is ***United States of America / AuF / Auf_Act / AuF_Act_US / !Editor / !Admin***) open **Assign LDAP groups**.

NOTE:

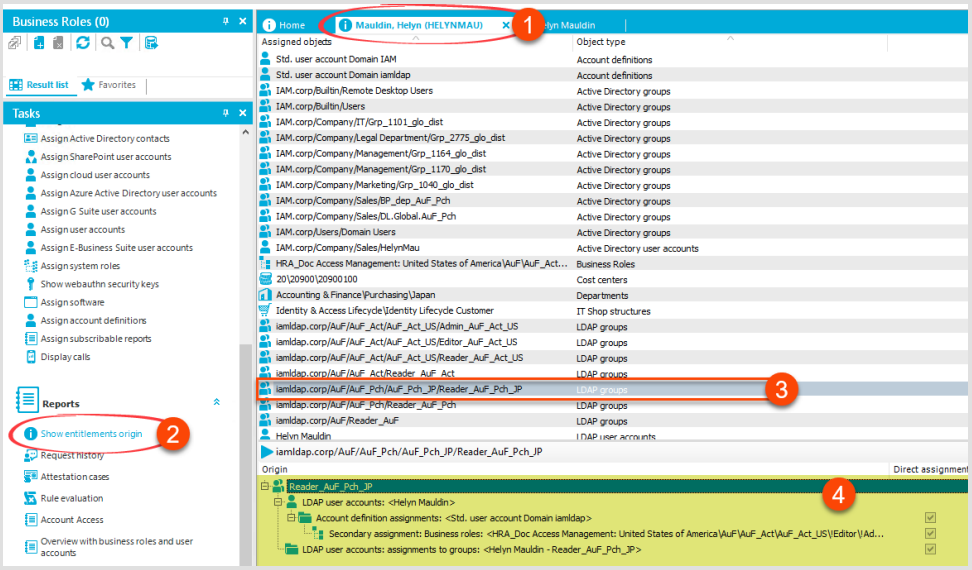
- There are two types of assignments, a white check in a blue circle and a blue check in a white circle. The white check assignments are caused by assignments happened in parent roles and are inherited to this role. The white check assignments are assigned manually right here in this place. This means in addition only the blue check assignment can be revoked in this place.
- This gets as well indicated by the white check in a blue square icon in the second column which indicates all so marked lines are checked by inheritance (indirect assigned).



In detail: Resources can be assigned manually and by inheritance. Second important information is to which object they are assigned to:
In our scenario an identity (person / employee) is assigned to a role (manually or automated (dynamic role) but as a direct assignment. The same is true for LDAP groups assigned to this role (as well a direct assignment). This leads by resource inheritance to LDAP-Account memberships in these LDAP groups (indirect assignment), because the identity is member of these roles. This means in this case, the LDAP account gets LDAP groups indirectly assigned via a role.
Now let's explore why this LDAP account do have more as the expected LDAP groups assigned. Yes, this could be caused by a manual assignment, but this is more seldom in an Identity Management System. In IAG we try to avoid entitlement assignments by direct assignments (because they don't reflect an assignment reason).

- In **Manager** find the employee who is assigned to our role (in this example: **Mauldien, Helyn**).
- Once you see the person overview of this user find and click **Show entitlements origin** in the **Tasks** list (the entry is in the **Report** section of the list) → (1), (2).
  - Look for entries where object type is **LDAP groups** (3).
  - Find a LDAP group which is not part of the expected group list above (3). In this case it is for example ***iamldap.corp/SuM/Reader_SuM***.
  - Double-click this entry and explore the detail pain (4)

NOTE:



As you can see:

- We started at a person object (identity).
- We selected the entitlement assigned to this identity we like to analyze.
- In the last line of the block you see the selected group which is (directly) assigned to the LDAP account or vice versa.
- The lines above show the other component of the assignment which is the LDAP-account. Here you can see two reasons to got this account assigned:

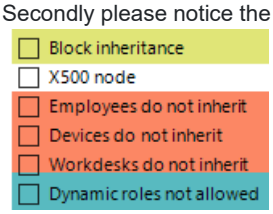
→ By a (direct) assigned Account definition
→ By being a member of the role structure **HRA_Doc_Access_Management** (remember we assigned the account definition to the root leaf of the tree which is the role **United States of America.**
This means that you need to revoke both reasons before there is no reason to have this LDAP account (or after losing it to deactivate this LDAP account).
Please notice **Entitlement origin** is an important part in an IAG system to answer an important question:
Why is this identity permitted?
During the ongoing training it could be of interest, to look from time to time into this view (for example if you work with IT Shop). You might find some other ways, how business resources can be assigned to identities.

Some role tree specialties

- In Manager select again one of your configured !Admin roles. In this example it is again: ***United States of America***

/ AuF / Auf_Act / AuF_Act_US / !Editor / !Admin

- Select Change main data from the Tasks list.
  - First have a look at the properties on four tabs of this object
  - Secondly please notice the flags exist for a role



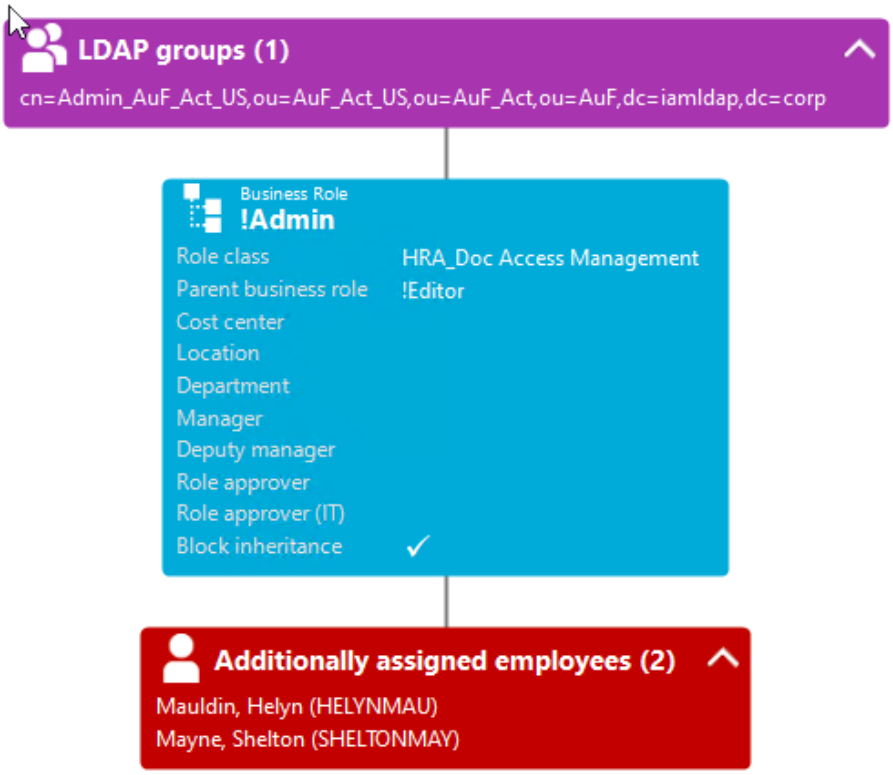
NOTE:

- **Block inheritance:** Is a configuration allows to block all inherited business resources from parents or to parents depending on the inheritance direction (top down / bottom up). This is what we will test in a second.
  *** do not inherit** allows us two more facts to understand:
  - 1. Beside of business resources like account definitions, resources, entitlements we can assign Employees, workdesks (hardware sets) and devices (hardware) as business resource user to a role.
  - 2. The flags mentioned allow to stop resource inheritance for a specific resource user and only for a role the flag is configured for.
- **Dynamic roles not allowed**: Exclude a role from getting configured by a dynamic role (people and/or workdesks and/or devices gets automatically assigned).

  - Open **Jobqueue Info** and sign in with your system user.
    - On tab **Job queue** right click filter **job queue** and select **Monitor job queue**. Your system will now auto-refresh the job queue. Please notice this can cost performance especially in circumstances where many jobs are listed in the job queue.
  - Switch back to Manager and set flag Block inheritance.
  - Press **[Save]**
  - Switch back to Job queue Info and see what results in the Job queue.

NOTE:
You should see a couple of jobs passing through. This is for a node at the end of a tree. Maybe you could get an idea what could happen, if there are many more people in more than one role underneath the role where block inheritance is set.
→ True, you easily can get a provisioning storm in your system. This is the reason why you should always be careful in moving role sub-trees or blocking the inheritance. Use these features only if necessary and monitor very closely your job queue during such operations.

- In a very last step have a look at the role overview of your configured role.



NOTE:
As expected all inherited LDAP groups are gone, only the direct assigned group is left. Take time to discuss this feature with your class:

- Can you find use cases for this?
- Can you find another role structure to solve this scenario without using this flag?

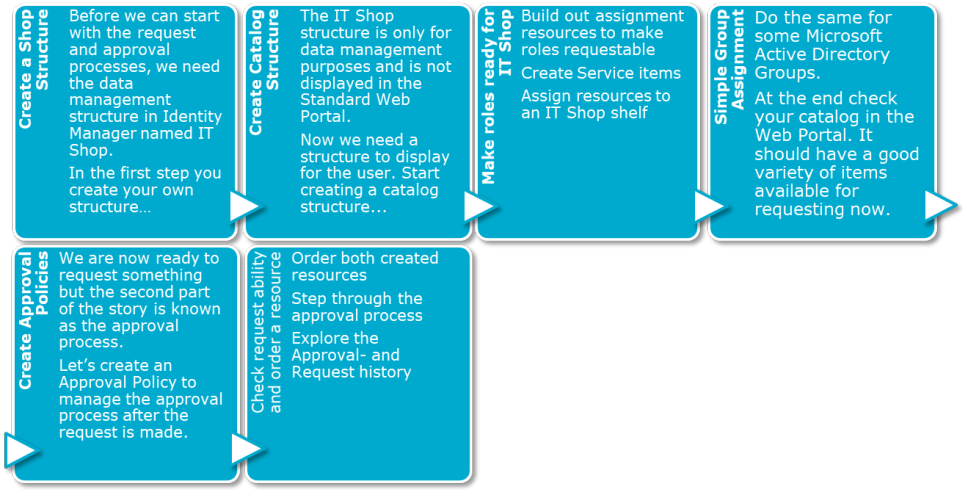
→ If yes, you should use this structure, because block inheritance is a performance expensive feature!

Lab Exercise Complete

Lab Exercise: IM-BIT-01 IT Shop Configuration and Administration

Exercise Overview

In this lab you create an IT Shop structure and work with typical business processes exploring request and approval configurations. This includes the development of two simple approval processes.



What You Need To Know

- You must have the images open and running for this lab.
- Additional Lab content stored in the Lab folder (T:\Courses\IdentityManager\Labs):

User credentials required for this lab

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin
Identity Manager - system user	
Username	[your system user] or training
Password	I.4Madmin

Estimated Time To Complete This Lab: **60 minutes**

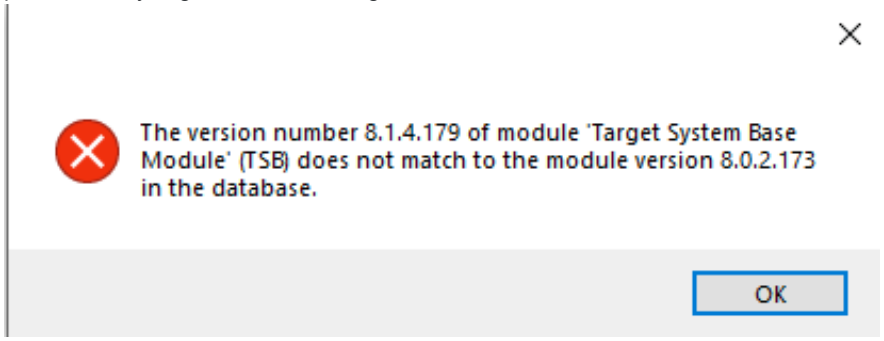
Lab Exercise

Prerequisites for INSTALLATION courses

NOTE:
These prerequisites can be skipped if you are working in a course without installation (in this case, continue with task: Create a Shop Structure below).
Please remember, in an installation course we start with an empty database. This means there are no business objects we can use for the next few labs. Because of this, we typically need to create some or can import some data.
In this example we use a third way to get some data into our system (we saw DB Importer, Synchronization Editor). This way is typically used to copy system configuration from one database to another. The mechanism is called Database transport. It can be used to transport a few dedicated business data objects, typically together with some

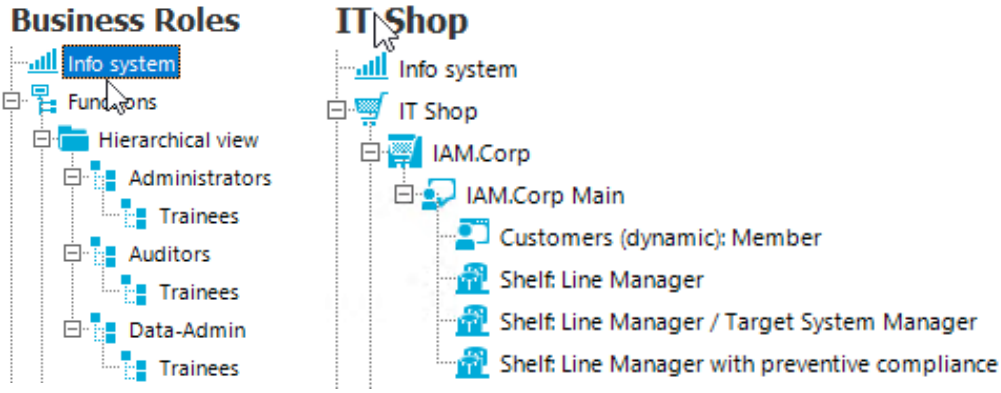
system configuration.

- >Start Transporter (from Launchpad start Change & Extend/Transport custom modifications)
  - >Select **Import a transport file**
  - >Click **[Next]** and **[Next]**
  - >From lab folder IM-BIT-01 select file: **IM-BIT-01_Roles-Business-Data.zip** and finish the transport. It is possible that you get an error message:

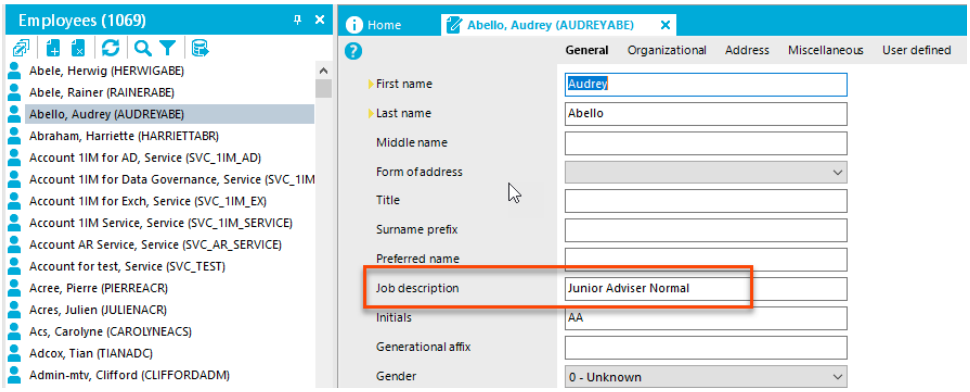


NOTE:
If you don't get the error message, please continue with step 3. If you see this or a similar error message this indicates that your transport was created with a previous Identity Manager version. In this case it is up to you to decide if your transport should be imported or not. In our example it is possible. The following steps are very often seen in IGA projects if you start with one version and later upgrade to another. This is the reason why we are showing this here.

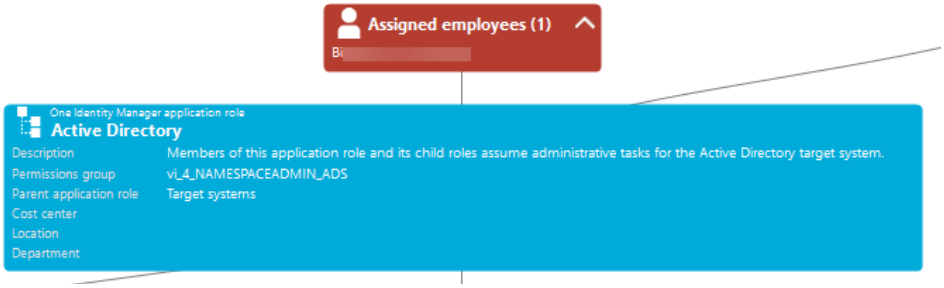
- Open your command shell (**[WIN]+[r]** → cmd → **[Return]**.
  - Navigate to your Identity Manager installation directory
    `cd /d "c:\Program Files\One Identity\One Identity Manager"`
  - Start Database transporter with switch /force
    `Transporter.exe /force`
  - Select Import a transport file
  - Click **[Next]** and **[Next]**
  - From lab folder **IM-BIT-01** select file: **IM-BIT-01_Roles-Business-Data.zip** and finish the transport.
- Repeat all steps to insert transport file: **IM-BIT-01_IT-Shop-Data.zip**. Now we do have a first IT-Shop imported and a small role structure.



- Next step is to add job title (***Person.Personaltitle***) to our imported identities (person objects). From lab folder **IM-BIT-01** open SQL file: **IM-BIT-01_Personaltitle.sql** in SQL Studio (**SSMS**, double-click should work).
  - Select the right database: ***IAMDB***
  - Run the file **[F5]**



- Now we need some responsible System manager in Identity Manager. In **Manager** select **One Identity Manager Administration**.
  - Expand node **Identity & Access Governance/Auditors** and add 3 random people (**Assign employees**).
  - Expand node **Target systems** and assign a random person (of your choice) to each role of
    - Application Role: ***Active Directory***
    - Application Role: ***LDAP***
    - Application Role: ***Exchange***



  - Now we must ensure the dynamic role membership re-calculation gets triggered. Switch back to **Business roles** and expand the **Basic Configuration data** section.
    - Select **Schedules**
    - Select **Dynamic roles check** from the **Schedules** list
    - Select **Start immediately** from the **Tasks** list
  - Now let's configure our imported IT-Shop structure by assigning imported Approval policies. Typically, the IT-Shop transport will do this but let's double-check. Select **IT Shop** from **Manager** main menu.
    - Expand: ***IT-Shop/IAM.Corp Main***
    - Select shelf: ***Shelf Line Manager***
    - Select **Assign approval policies** from the **Tasks** list
    - Ensure approval policy **Recipient's Manager** is assigned
    - Repeat these steps for shelfs (you will find according approval policies):
      - Shelf: Line Manager / Target System Manager
      - Shelf: Line Manager with preventive compliance

Configure email sender address

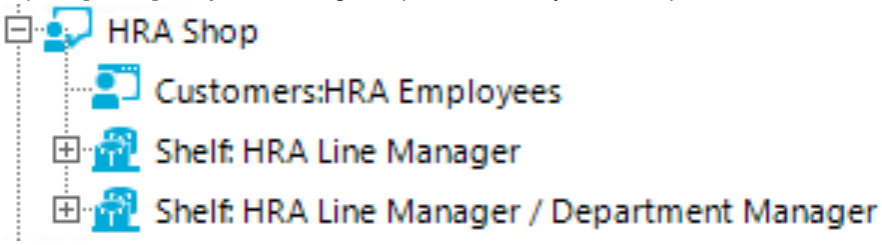
> **NOTE:**
> We connected MS Exchange as email system. Because of this Identity Manager tries to send out emails. Therefore, a sender address is needed. Unfortunately, this needs to be configured differently for some features. IT Shop does have its own sender address. Let's configure this to avoid FROZEN jobs in the Jobqueue later. Depending on your training and regarding to your training environment this might be preconfigured or not.

- Open Designer and login with your system user account. You can also use Lauchpad: Configure/Change system settings.
- In Designer you need to double check Configuration parameters.
  - Expand **QER\ITShop\DefaultSenderAddress**.
  - Value ***NOREPLY@iam.corp***

- Click **[Commit to database]** and **[Save]**.

Create a Shop Structure

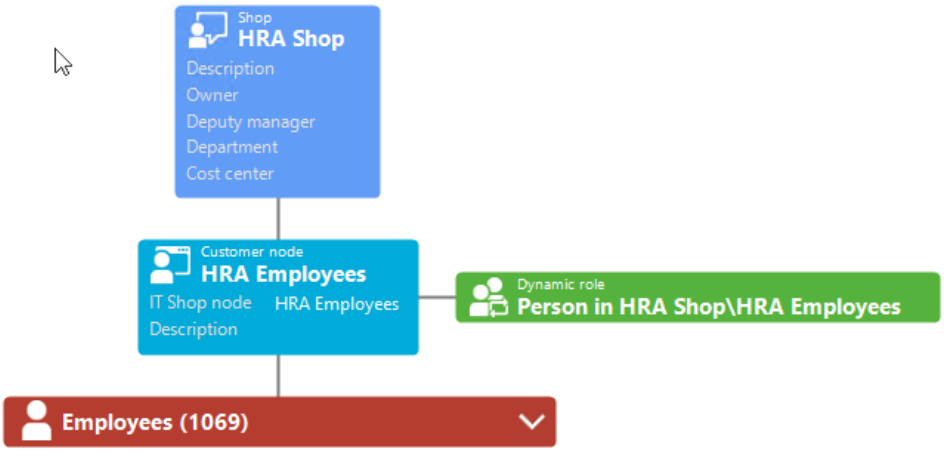
- Start Launchpad and select **Display and maintain content data**.
- In **Manager**, select IT Shop from the main menu and expand the first level of the tree. You should see two shops (IAM.Corp → IT Shop configured in this environment, **Identity & Access Lifecycle** → default IT Shop).
  We like to create a third one now.
- Select the **IT Shop** node in the navigation pane.
- Click the icon showing a paper and a plus (**Create a new object**) in the **IT Shop structures** pane tool bar
  - Name the IT Shop node: ***[Prefix] Shop***
  - For the IT Shop information field select: ***Shop***
  - Click **[Save]**
- Refresh the Navigation pane (you should remember how to do this).
- Select the **[Prefix] Shop** node.
- Right click the **[Prefix] Shop** node and select **new**.
  - Name the next IT Shop node: ***[Prefix] Employee***
  - For the IT Shop information field, select: ***Customer***
  - Click **[Save]**
- Right click the **[Prefix] Shop** node and select new again.
  - Name the IT Shop node: ***[Prefix] Line Manager***
  - For the IT Shop information field, select: ***Shelf***
  - Click [Save]
- Create another shelf
  - Name it: ***[Prefix] Line Manager / Department Manager.***
  - For the IT Shop information field, select: ***Shelf***
  - Click **[Save]**
- Expand **[Prefix] Shop** in the Navigation pane and view your IT Shop structure.



- Select the **Customers** node.
- Select **Create Dynamic Role**.
  - Select the database icon underneath of **Description**.
  - Click into the **Condition** field and enter the following: ***1=1***.

NOTE:
In SQL you are not able to write 'true' as a condition. Because of this we must implement a condition which is the equivalent to true in SQL syntax which is 1=1. With this condition, each person in the Identity Manager database can now access our IT Shop.

- Click **[Save]**.



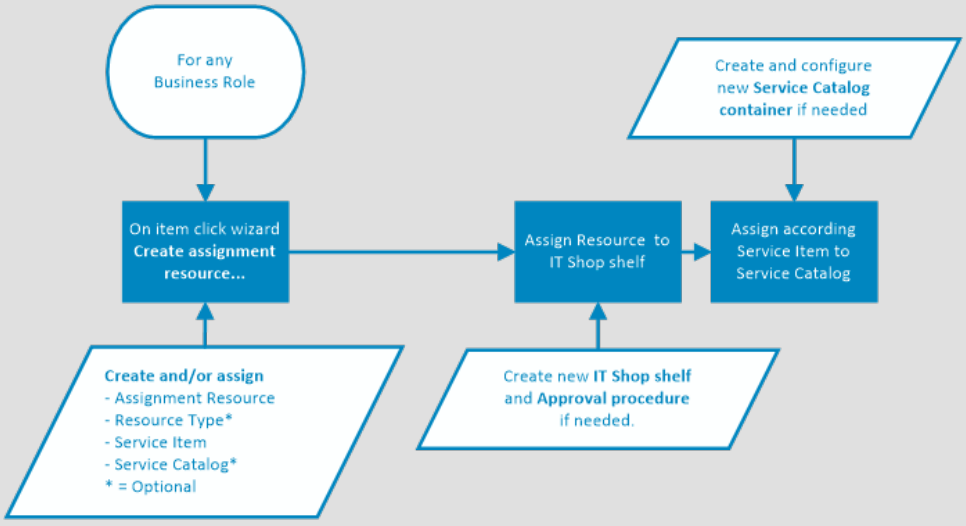
Create Catalog Structure

NOTE:
The IT Shop structure in Identity Manager is for administrative purposes. To organize items in IT Shop to get displayed in the Identity Manager Standard Web Portal, we need to create a catalog structure.
In the following steps you need some icons. The instructor will tell you where to find (Training Environment: ***T:\IAMS10\Training\courses\IdentityManager\Labs*** in the folder according to the lab). Here you can find some but feel free to download some small icons from Internet if you like instead.

- Expand the Basic configuration data node in the IT Shop Navigation pane.
- Right click on Service categories and select new from the context menu (be careful we mean Service categories underneath of Basic configuration data not the node Service Catalog above).
  - Service category: ***[Prefix] Function Roles***
  - Select the picture tab and add a picture from your Lab folder (set of keys)
- Click **[Save]**

Make roles ready for IT Shop

NOTE:
If you take a look into Business roles you will find a role-tree **Functions** which is part of the configuration of this environment. However, each of them shows a Trainee sub-role which we now want to make request-able in IT Shop. To meet this requirement, we must first re-configure these roles.
In difference to permissions or resources, roles cannot be directly added to IT Shop. To handle this the system exposes a task Create **assignment resource...** which automates all steps. The whole process looks like this:



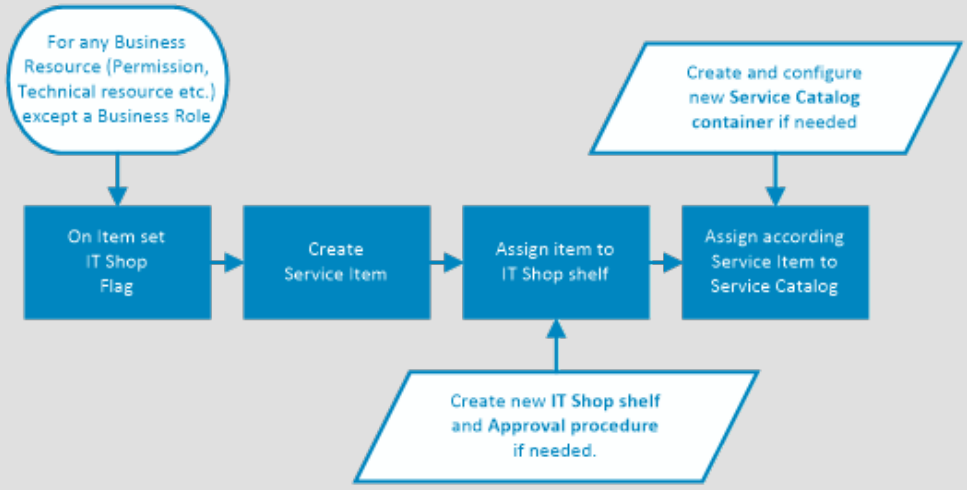
- Select **Business Roles** from the Main Menu.
- Expand **Functions** → **Hierarchical view** → down to the bottom (expand each sub node. You can use [*] from the num-pad).
- Right click **Hierarchical view** and select **New**.
  - Business Role: ***[Prefix] Project Controller***
  - Click **[Save]**
- Refresh view in **Navigation** (right click into the box)
- Right click the new entry and select **New** again.
  - Business Role: ***[Prefix] Trainees***
  - Click **[Save]**
- Select the **[Prefix] Trainees** role of the **[Prefix] Project Controller**.
- Select Create assignment resource from the **Tasks** list.
  - Click **[Next]**
  - Name the Resource: ***[Prefix] Project Controller Trainee***
  - Click **[Next]**
  - Name the Service item: ***[Prefix] Project Controller Trainee***
  - Select, **Select an existing service category**
  - Select Service category: ***[Prefix] Function Roles***
  - Click **[Next]**
  - Click **[Exit]**

NOTE:
Now, we do have a role which can be assigned to our IT Shop structure in one of the next steps.

- From the main menu select IT Shop.
- Expand IT Shop => [Prefix] Shop.
- Select [Prefix] Line Manager / Department Manager shelf.
- Click **Assign resources** from the **Tasks** list and select tab **Assignment resources**.
- Assign (Double-click) resource: ***[Prefix] Project Controller Trainee***
  (If you can't see the entry, ensure you selected tab 'Assignment resources' AND you expanded entry 'Functions').
- Click **[Save]**.

Simple Group Assignment

NOTE:
Now we will see the typical assignment of single resources (AD user accounts, groups & mailboxes). This process always looks like:



- Select **Active Directory** (ADS icon) from the main menu.
- Expand **Groups** in the **Navigation** pane.
- Right click **Global Groups** and select **New**

- Name: ***[Prefix]_Proxy_Internet_Access***
- Container: ***IAM.corp/Users***
- IT Shop: ***checked***

> **NOTE:**
> With IT Shop checked the Service item field is now mandatory. If you try to save the record before the field **Service item** is filled, you receive an error message.
> The Only use in IT Shop check-box is to prevent assignment through the Manager or Identity Manger tools. The request and assignment may only be performed through the IT Shop (web portal). Leave this flag un-checked!

- Click the blue plus icon right beside Service item
  - Service Item: ***[Prefix] Internet access for employees***
  - Click **[OK]**
- Click **[Save]**
- To assign the group to your IT Shop structure, switch to the IT Shop menu and expand the IT Shop tree you created before.
  - Select the shelf: ***[Prefix] Line Manager***
  - From the Tasks list select **Assign Active Directory Groups**
  - Assign AD group **[Prefix]_Proxy_Internet_Access**
  - Click **[Save]**

> **NOTE:**
> Now the group is request-able iPn IT Shop but it is necessary to place the according **Service Item** somewhere into the **Service catalog** to ensure the item gets visible in the Standard Web Portal.

- In the IT Shop Navigation pane expand the Service catalog structure.
  - Create a new service catalog container in the first level and name it (this is something you already did in the past).
    - Name it: ***[Prefix] Basic Employee Permissions***
    - Take picture: ***Paragraphs***
    - Click **[Save]**
  - Now use **Assign Service Item** from the Tasks list and assign the Service Item **[Prefix] Internet access for employees**.

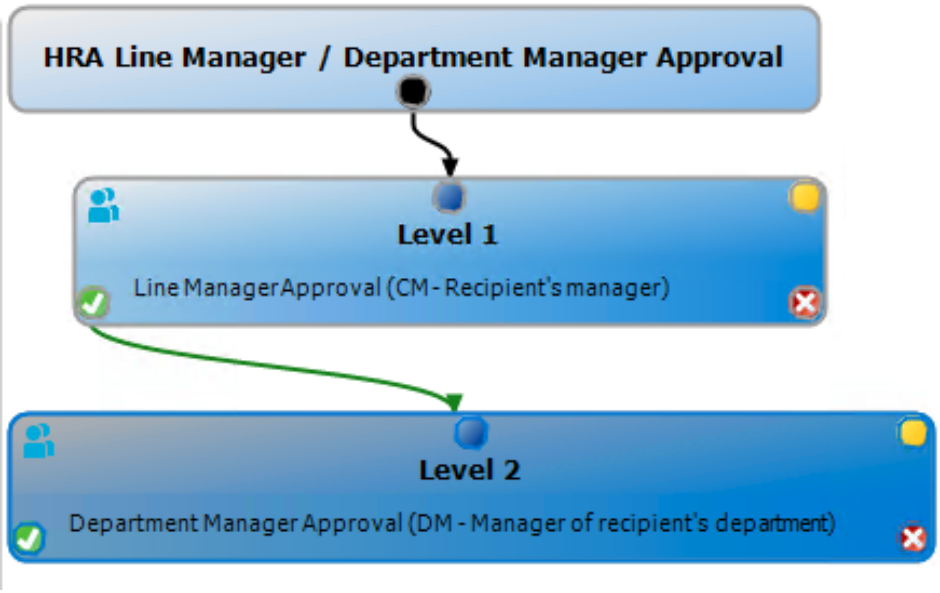
> **NOTE:**
> In a Web Browser you should see a new catalog icon in your Standard Web Portal containing one item. This means the item is now requestable but before we can run a request we need an approval policy.

Create Approval Policies

- From the Main Menu, select **IT Shop**.
- Expand **Basic configuration data.**
- Right click **Approval Policies** and select **New** from the context menu.
  - Approval policy: ***[Prefix] Line Manager Approval***
  - Click the icon right beside the field **Approval workflow**.
  - In the workflow editor double click on the new workflow rectangle and rename it: ***[Prefix] Line Manager Approval***.
  - Click **[Ok]**.
  - Add a new approval level.
  - Single step: ***[Prefix] Line Manager***
  - Approval procedure: ***CM-Recipient's Manager***
  - Click **[Ok], [Ok]**
  - Click **[Save]**.
- Repeat these steps for **[Prefix] Line Manager / Department Manager Approval.**

> **NOTE:**
> You need to define two approval levels in the approval workflow.

→ You need CM and DM approval steps
→ To connect the first with the second level expand the green check and connect the line that appears with the second level.

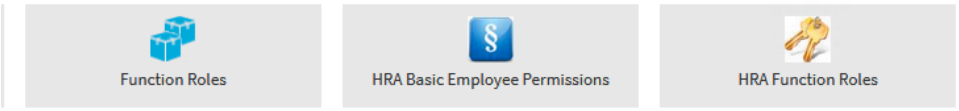


- Assign the approval policy to the appropriate IT Shop shelves.
  - Select the correct IT Shop shelf you created before
  - Assign the according Approval Policy
  - Remember two shelfs to configure

NOTE:
You should be able to complete this on your own based on what you have learned in earlier steps. Now is time to check our configuration...

Check request ability and order a resource

- Open Standard Web Portal in your Browser and login with an employee.
  - Browser / Quick Links / Standard Web Portal
  - Login for example as Harriall, I.4Madmin
- Select Start new request
  - You should see two more categories with colored icons



  - Each category should contain at least one item. If you can't see the picture below, double-check your IT Shop/shelf assignments.
- Select category: ***[Prefix] Function Roles.***
- Select item: ***[Prefix] Project Controller Trainee***
- Click **[Add to cart]** right bottom side
- In the gray box on right configure for your entry
  - Valid from: ***configure today***
  - Valid until: ***configure tomorrow***
  - Click the blue save icon underneath and submit.

NOTE:

As you can see we added a resource having a validity period assigned to give you access just for one day.

- From the menu select **Request/My Requests** and click **Start a new request**.
- Select **[Prefix] Basic Employee Permissions**
- Select line **[Prefix] Basic Employee Permissions**
- Click **[Add to cart]** right bottom side. Note the two items in your cart.
- Click **[Submit]** on bottom right.
- Select **View the request history**
- Check one of the entries and select the workflow tab. As you can see for both the next decision maker to approve is **Timtschenko, Alphen**. Don't worry, this could be another manager (memorize the account name).
- Sign out your requestor and sign in the decision maker (person icon on right upper)
  - Select **Pending requests**.
  - Check the two check marks in column Decision (for both entries, they need to become green)
  - Click **[Next]**
  - Click **[Save]**
- From the menu select **Request / My actions**
- Select **Approval history**
  - As you can see One item is assigned one item is canceled. If you don't see the status wait for some seconds and press **[F5]** to refresh.
  - Select the aborted item.
  - Look at the workflow. You can see that there was no decision maker the system was able to determine. This means in our two-step workflow (Line Manager / Department Manager) no department manager was configured. Check this using Manager and you will figure out this is the truth.

NOTE:
In circumstances where **Allmann, Harri** was not your requestor, it could be you see one assigned item and one pending item where you can see the next approver. Don't worry about it. You should take with you that a shopping cart can contain many items and they can have different workflows assigned.
To fix the problem with the aborted item exists several options:

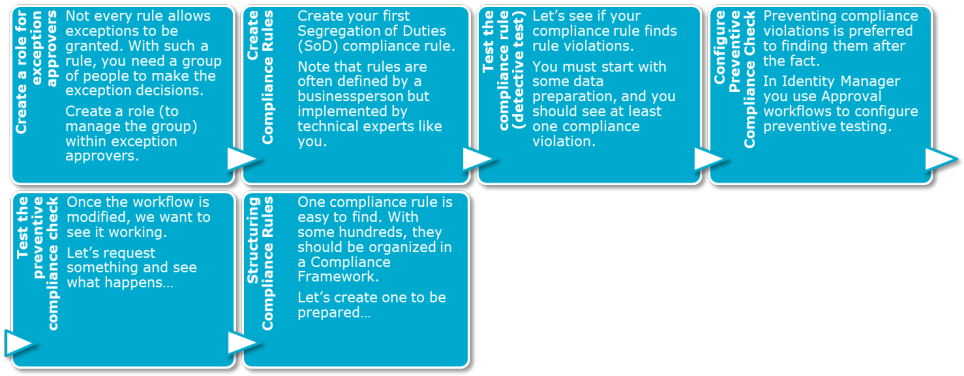
- Configure a department manager for the according users department.
- Configure members for the Chief Approver Team (an Application roll, members can approve everything).
- Configure fallback approvers in your approval workflow.
- …

Take this example to talk with your class about the different capabilities in Identity Manager to handle missing or unwilling or misconfigured approvers.

Lab Exercise Complete

Lab-Exercise IM-BCA-01: Preventive and detective Compliance

Exercise Overview



In this lab you create and validate a compliance rule and manage your compliance framework. This includes preventive and detective compliance checks.

What You Need To Know:

- You must have the images open and running for this lab.
- This lab is based on the results of the lab: ROL-1 Working with Roles.

User credentials required for this lab:

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin

Estimated Time To Complete This Lab: **45 minutes**

Lab Exercise

Configure email sender address

> **NOTE:**
> We connected MS Exchange as email system. Because of this Identity Manager tries to send out emails. Therefore, a sender address is needed. Unfortunately, this needs to be configured differently for some features. Compliance does have its own sender address. Let's configure this to avoid FROZEN jobs in the Jobqueue later. Depending on your training and regarding to your training environment this need to be preconfigured or not.

- Open **Designer** and login with your system user account. You can also use**Lauchpad: Configure/Change system settings** .
- In **Designer** you need to double check**Configuration parameters**
  - Expand**QER\ComplianceCheck\EmailNotification\DefaultSenderAddress**.
  - Value: ***mailto:NOREPLY@iam.corp***
  - Expand**QER\Policy\EmailNotification\DefaultSenderAddress** .
  - Value: ***mailto:NOREPLY@iam.corp***
  - If values were configured, click **[Commit to database]** and **[Save]**.

Create new roles for exception approvers and to deal with rules

- Start Launchpad and select **Display and maintain content data**.
- Select **Identity Audit** from main menu.
- Expand **Basic configuration data**
- Expand **Exception approvers** on the **Navigation** pane and create a new role.
  - Application role: ***[Prefix] Compliance and Security Officers***
    As you can see there is a role we later can use if we need exceptional approvers for compliance rules.
  - Assign and note a role member of your choice.
    Please note the centralaccount of your **Exceptional Approver**.

NOTE:
Now we will create/double-check two roles to deal with. These roles will not be needed in a real-world scenario (because there are some) but we must ensure that every student gets its own set of roles do deal with in an environment you share with your colleagues.

- Select **Business Roles** from the main menu and expand **Functions/Hierarchical view** structure.
- Add a single role underneath **Administrators** and **Auditors** and assign employees (there could be already a similar named role, just ignore it):
  - Each role name: ***[Prefix] Trainees***
  - Assign employees as you like, ensure that only one employee is member of both roles. Ensure that all these role members are NOT member of your **Compliance and Security Officers** role you created before.
    - Please note 1st employee, role one only (* we suggest to note the employees central account)
    - Please note 2nd employee, role one only *)
    - Please note 3rd employee, both roles *)
    - Please note 4th employee, role two only *)

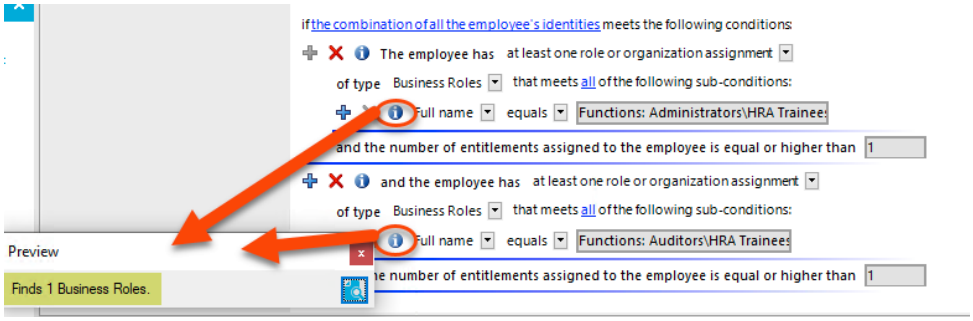
Create Compliance Rules

- In **Manager** switch back to **Identity Audit**.
- In the **Navigation** pane, right click **Rules** and select **New** from the context menu
  - Name the rule: ***[Prefix] SoD: Admin trainees must not be Auditor trainees***
  - Exception approval allowed: ***checked***
  - Exception approver: ***[Prefix] Compliance and Security Officers***
  - In section **Condition**
    - Click on the drop down arrow after **At least one entitlement**
      and select: ***at least one role or organization assignment.***
    - Click on the drop down arrow after **of type…**
      and select: ***Business Roles***
    - Click on the next drop down arrow in the line below after **…** and select: ***Properties / Full name.***
    - Type in: ***Functions: Administrators\[Prefix] Trainees***

NOTE:
You may right-click the affected role in the result list and copy the full name (display name: Full name, field name: Org.FullPath) information out of the **Properties** tab to insert it as described above. This works better than rewriting the name manually. To open an additional form without losing the changes in the rule, hold down the "ALT" key during the click action in the **Navigation** pane.

To double-check the condition, use the "I" icon nearest to the inserted fullname value (same line on left). It needs to return just one entry (the Trainee role).

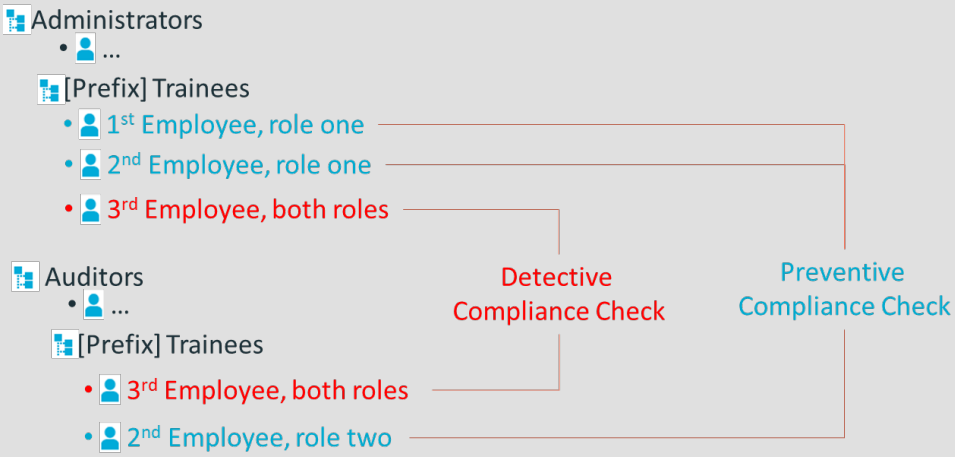
You might lose the focus of your rule. In this case you need to find the newly created rule again but it is not in the list of filter **Rules**. This is, because during editing it is a working copy. To find your rule again, expand **Rules** and select filter **Working copies of rules**.



  - Click on the first blue plus (located below **If the combination of all…**).
  - Repeat the steps above for Functions: Auditors\[Prefix] Trainees
  - Click **[Save]**
- Select **Enable working copy** from the tasks list.
- Click **[yes]** when prompted and confirm.

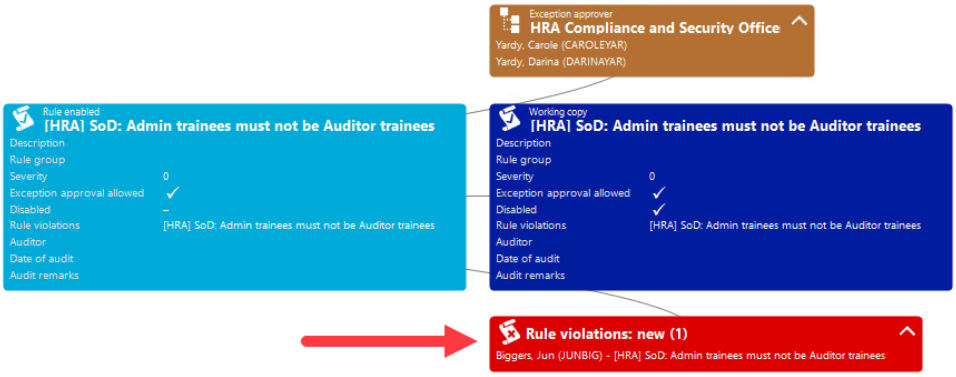
Test the compliance rule

NOTE:
Remember, the user who is member in both **[Prefix] Trainees** roles is to be used for the detective compliance check. You can use one of the other assigned users of role one for preventive compliance check by assigning the user to role two.



In this example we have assigned user **[3rd Employee, both roles]** both roles. This now creates a compliance violation we get with a detective check. Detective checks happens schedule based, let's speed this up.

- From the main menu select **Identity Audit** and expand **Basic configuration data**
  - Select **Schedules** .
  - Select **Compliance rule check** from the **Schedules** list
  - Select **Change main data**.
  - Notice the schedule is configured to run once per day.
  - For our lab purposes, select this entry again (double click to get the overview) and click **Start immediately** from **Tasks** list.
- Wait for the DB Queue Processor to complete the jobs (Jobqueue Info).
- View the rule overview for our compliance rule.
  - Notice the rule violations now appear.



NOTE:
If you need to edit the rule you must do it in the working copy. It is also not enough to click on **[Save]** to activate the changes. After saving, click on **Enable working copy** in the task list to activate it.

The screen shot above need to show another rule violation. Please have in mind it is depending on your data and should be different for each student in this class.

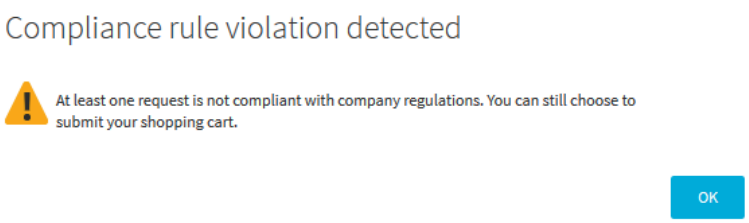
Configure Preventative Compliance Check

NOTE:
Preventative Compliance checks are better than detective checks as they prevent compliance violations before they occur when using the web portal.
Nevertheless, both checks are needed because you can bypass Identity Manager by using native administrative tools like "ADSI Edit" or "Active Directory Users and Computers". In this case a preventive check (you can find only in Identity Manager) can't prevent a violation. This is one of the reasons to have detective compliance checks available.
Preventive checks get implemented as part of an approval policy.

- In a first step we need to add our two newly created roles to the IT Shop to make them requestable. In **Manager** select **Business roles** and expand **Hierarchical view / Functions** down to your first created business role. Select the first role **Functions: Administrators / [Prefix] Trainees**
  - Select from the **Tasks** list **Create assignment resource**
  - Click **[Next]**
  - Assignment Resource: ***[Prefix] Basic administrator permissions for trainees***
  - Click **[Next]**
  - Service Item: ***[Prefix] Basic administrator permissions for trainees***
  - Service Category: ***[Prefix] Function Roles***
  - Click **[Next]**
  - Click **[Exit]**
- Repeat the previous steps for the second role. This is only necessary if this second role doesn't have an Assignment resource assigned.
  To create an assignment resource, use the following values:
  - Assignment Resource: ***[Prefix] Basic auditor permissions for trainees***
  - Service Item: ***[Prefix] Basic auditor permissions for trainees***
  - Service Category: ***[Prefix] Function Roles***
- Now the resources must be placed in IT Shop. Select **IT Shop** from the main menu.
  - Expand **IAM.Corp/IAM.CORP Main/Shelf: Line Manager** underneath the **IT Shop** filter.
  - Select shelf **Line Manager with preventive compliance**
  - Select **Assign Resources** from the **Tasks** list.
  - On the assignment form select tab **Assignment resource**
  - Assign the two **[Prefix] Basic …permissions…** resources
  - Click **[Save]**]

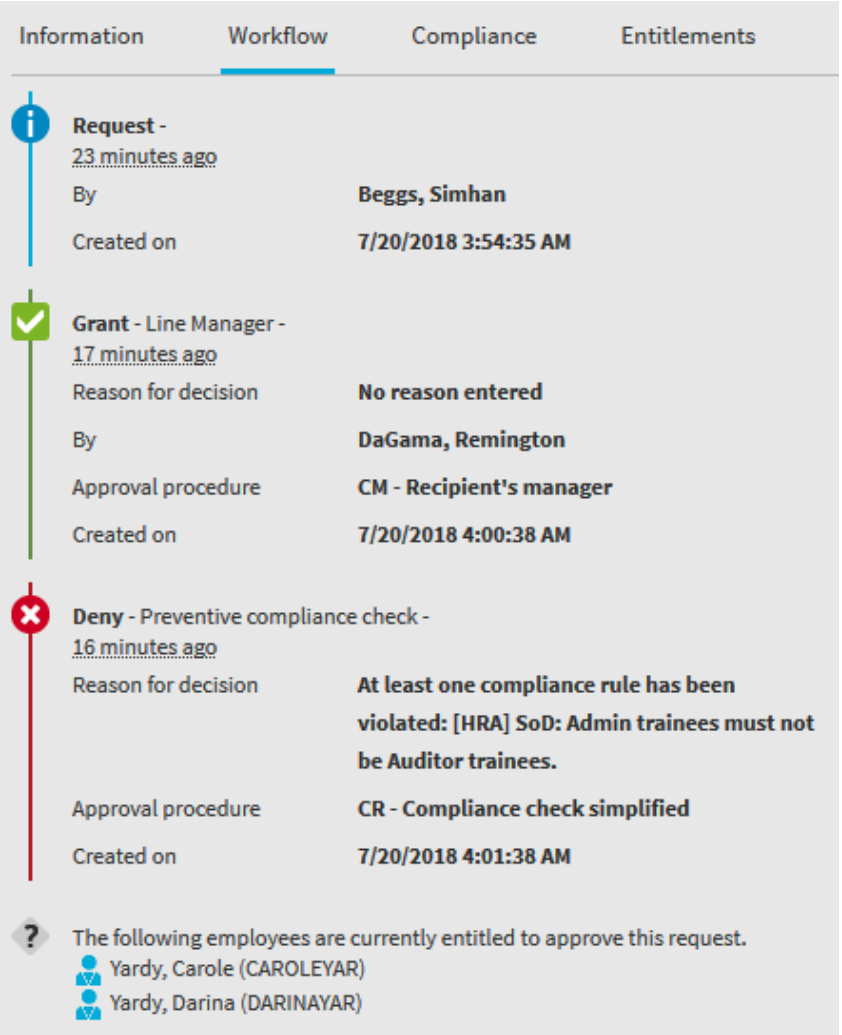
Test the preventative compliance check

- Logon to the web portal using one of the identities for preventive compliance checks (see above). Don't forget to remember in which **Trainees** role this person is located. In the following you should assign the opposite role to get your violation.
  - Select **Start a new request**
  - Select your **[Prefix] Function Roles** (in category **Function Roles**)
  - Check the box in front of the not assigned role.
  - Click **[Add to cart]** in this line located on right.
  - On the right lower side of your Shopping cart, you will find on left of the **[Edit]** and **[Submit]** button a drop-down field **[Actions]**.
    Click **[Actions]**
  - Select **Check shopping cart**
  - Please note the message **Compliance rule violation detected.**
  - Click **[OK]**



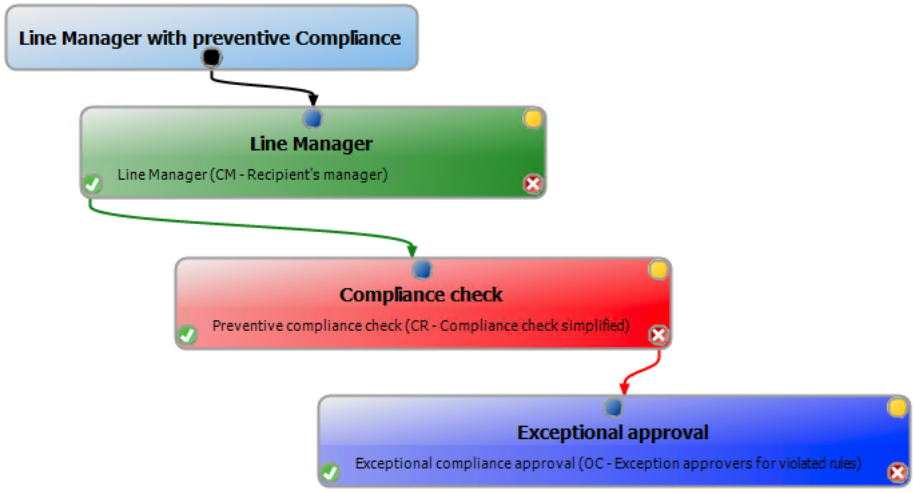
NOTE:
This is not the preventive Compliance check we are looking for. This is an upfront compliance test to signal the user that this shopping cart may lead to compliance issues.
It is still possible to submit this request. If the Line Manager approves the request, it will require a further exception approval from one of the compliance officers (CISO). Only if the exception approval is granted, this request will be finally granted.
A bit confusing is the system reaction if you directly click on **[Submit]** without using **[Actions]** first. In this case you will get the same error message, but the system will directly submit the compliance violation without giving a user a chance to correct the shopping cart. This is the default process, because users typically don't care about compliance issues they just request for resources and let decision makers making decisions.

- Click on **[Submit]** on right lower. You see the same message again, followed by **The request was successfully submitted** . See the note above.
- Select **View the request history** to show who must approve the request next (Details tab **Workflow**
  Note the approver centralaccount.
- Sign out the requestor and sign in as the approver.
  - You should be easily able to find the request. Please approve it by selecting the check on right and save the request.
  - Wait some seconds and select **Request / My actions** from the site menu.
  - Select **Approval History** .
- Select tab Workflow in the gray box on right. If you can't see a similar picture like displayed below, wait a bit and press F5 until it is displayed.



As you can see in this example, the approver did his job, the preventive compliance check denied but because we configured on the violated rule the exceptional approval option, now the members of role **[Prefix] Compliance and Security Officers** are the next approvers. This will work similar as all approvals we have seen before. Let's exit here. The workflow gets a bit better transparent, if we look in the workflow history in Manager (How to get there, is not part of the exercise) you can see:

Green → approved
Red → denied
Blue → currently to decide



Structuring Compliance Rules

- In the **Identity Audit** navigation pane of the Manager, expand **Basic configuration data** and right click **Compliance Frameworks**.
- **Select Newfrom the context menu.**
  - Compliance framework: ***[Prefix] Segregation of Duties***
  - Manager/supervisor: ***Rule supervisors***
  - Description: ***My SoD rules***
  - Click **[Save]**
- Click on **Assign rules** in the **Tasks** list
  - Assign the previously created rule to the framework
  - Click **[Save]**
- Right-click in the **Navigation** pane and select **Refresh view** and expand the Compliance framework. It seems to be there is no assignment.
- The reason is that this assignment happened to your rule working copy.
- Find the working copy in **Working copies of rules** (**Navigation** pane) and enable the copy. You will notice now it contains the rule.

Lab Exercise Complete

Lab-Exercise: IM-BCA-02 Attestation and Recertification

Exercise Overview

In this lab you build and implement an attestation policy.

What You Need To Know:

- You should have the images open and running for this lab.

User credentials required for this lab:

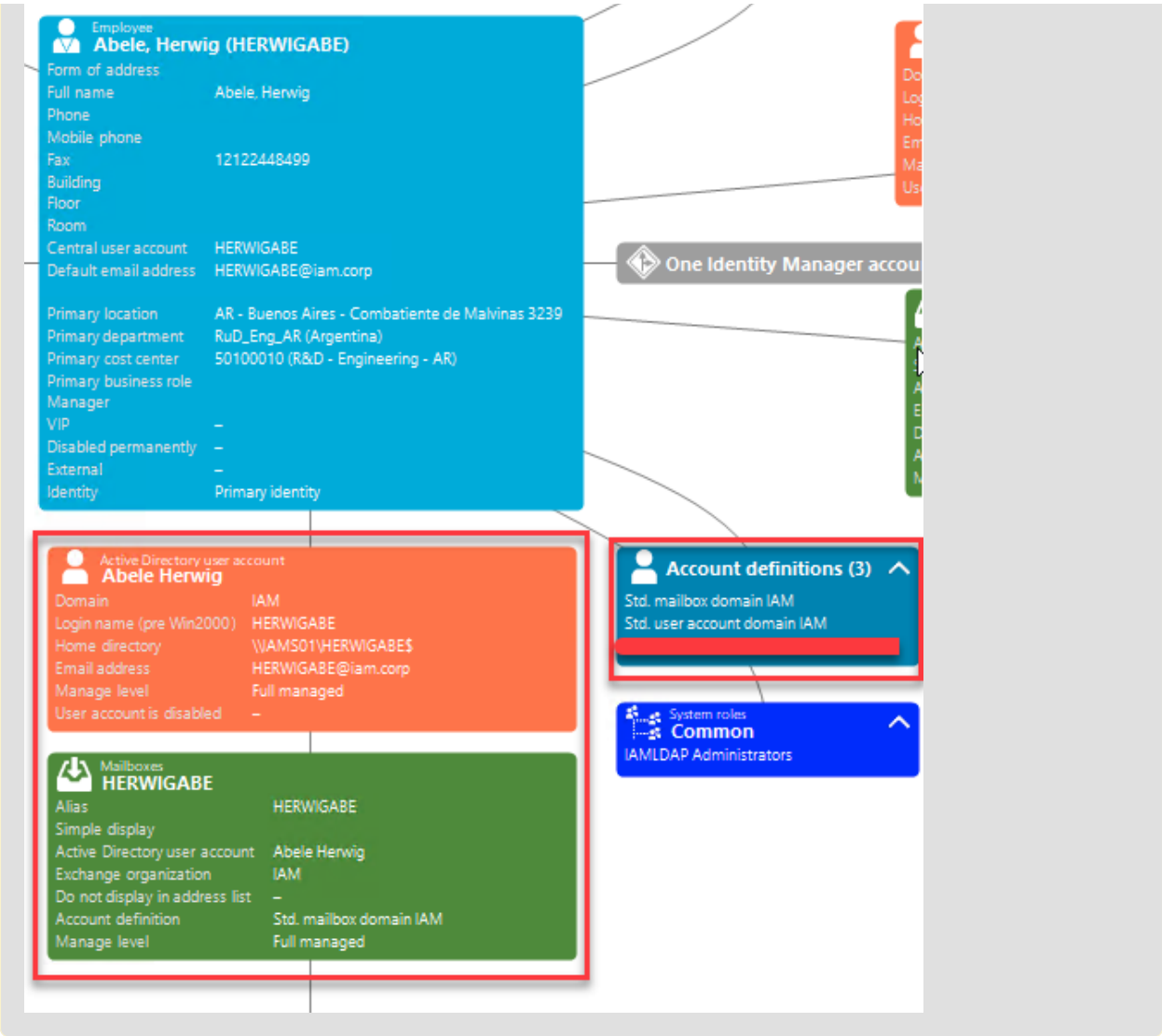
Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin
Identity Manager - system user	
Username	[your system user] or training
Password	I.4Madmin

Estimated Time To Complete This Lab: **40 minutes**

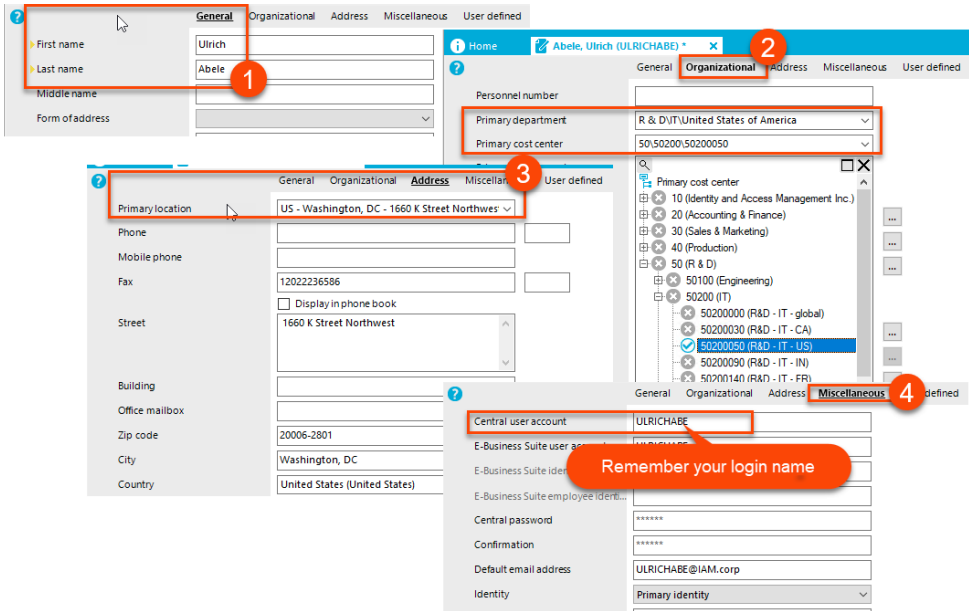
Lab Exercise

Create New Identity (Employee)

NOTE:
If you have **already inserted an employee with your name** into this environment and configured this employee with an AD account and a mailbox, **skip this section**. If not, please perform the necessary steps to create and provision an account. This employee object requires two account definitions along with an AD account in IAM and a mailbox in IAM.corp.



- Start Launchpad and select **Display and maintain content data**.
- Select **Employees** from main menu.
- Click the **Create a new object** icon in the employees **Result list** tool bar.
- Enter the following data:
  - First name: ***your first name***
  - Last name: ***your last name***
  - Click the **Organizational** tab.
  - Select a value for primary department from the drop-down tree (should be a leaf node for lab simplicity). Remember this name, you will need it later.
  - Select a value for primary cost center from the drop-down tree (again this should be a leaf node). Remember this name, you will also need it later.
  - Click the **Address** tab.
  - Configure a primary location of your choice.
  - Click the **Miscellaneous** tab.
  - Note the automatically generate **Central user account**, you will need it later.
  - System user password: ***I.4Madmin***
  - Confirmation: ***I.4Madmin***
  - Click **[Save]**

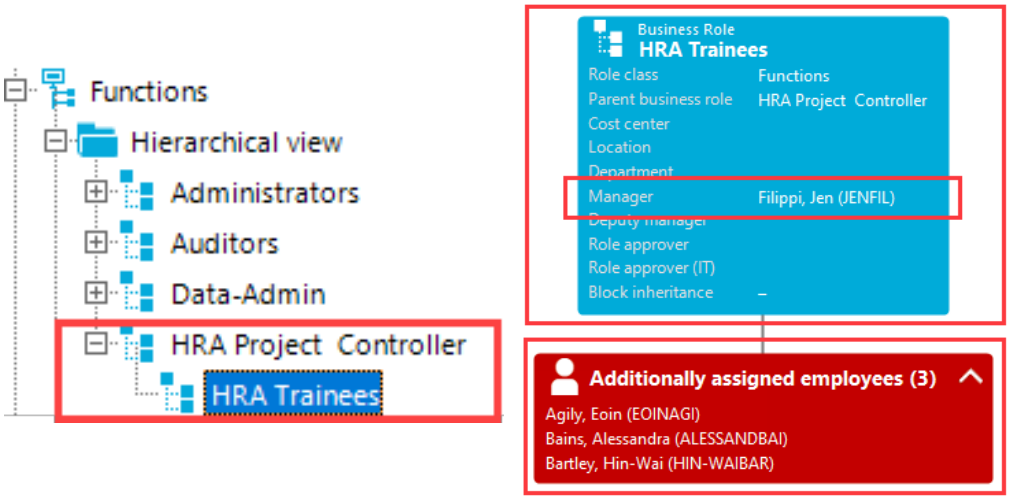


- To get an AD account and a mailbox you will need account definitions. Select your new employee and assign the following account definitions.
  - Std. mailbox domain IAM
  - Std. user account domain IAM
  - Click **[Save]**
- Start **JobQueueInfo** and observe the processes as they complete.

Create a Business role

> **NOTE:**
> Please check in **Manager / Business roles / Functions / Hierarchical view** if a role **[Prefix] Project Controller** exist. You could have created this before with another lab. If yes, you can skip the first 5 steps and their subs.
> **Caution: the 6th step and all below are needed in any case.**

- Select Business Roles from the Main Menu.
- Expand Functions -> **Hierarchical view** -> down to the bottom (expand each sub node. You can use **[*]** from the num-pad).
- Right click **Hierarchical view** and select **New**.
  - Business Role: ***[Prefix] Project Controller***
  - Click **[Save]**
- Refresh view in **Navigation** (right click into the box)
- Right click the new entry and select **New** again.
  - Business Role: ***[Prefix] Trainees***
  - Click **[Save]**
- Ensure there are people assigned to the **[Prefix] Project Controller/[Prefix]** Trainees role. If not assign two or more.
- Ensure the there is a manager configured for role **[Prefix] Project Controller/[Prefix] Trainees** and document this person (this manager should not be an assigned member to this role):



Authorize your user for Attestation Policy creation

NOTE:
To create Attestation policies, you need the role of Chief Information Security Officer (CISO)

- In Manager select Employees and search for your employee record (created in the last task or another lab).
- Select **Assign One Identity Manager application roles** from the **Tasks** list.
- Assign the following application roles:
  - Identity & Access Governance/Attestation/Administrators
  - Identity & Access Governance/Compliance & Security Officer
  - Click **[Save]**

NOTE:
These permissions are necessary to define attestation procedures (admin) and watch and manage attestation results (CISO).

Further, Attestation policies are easily to be created in the **Standard Web Portal**. (They can also be created in the **Manager** tool, but this is not recommended.)

Configure email sender address

NOTE:
We connected MS Exchange as email system. Because of this Identity Manager tries to send out emails. Therefore, a sender address is needed. Unfortunately, this needs to be configured differently for some features. Attestation does have its own sender address. Let's configure this to avoid FROZEN jobs in the Jobqueue later. Depending on your training and regarding to your training environment this might be preconfigured or not.

- Open **Designer** and login with your system user account. You can also use **Lauchpad: Configure/Change system settings**.
- In **Designer** you need to double check **Configuration parameters**.
  - Expand **QER\Attestation\DefaultSenderAddress**.
  - Value: ***NOREPLY@iam.corp***
  - Click **[Commit to database]** and **[Save]**.

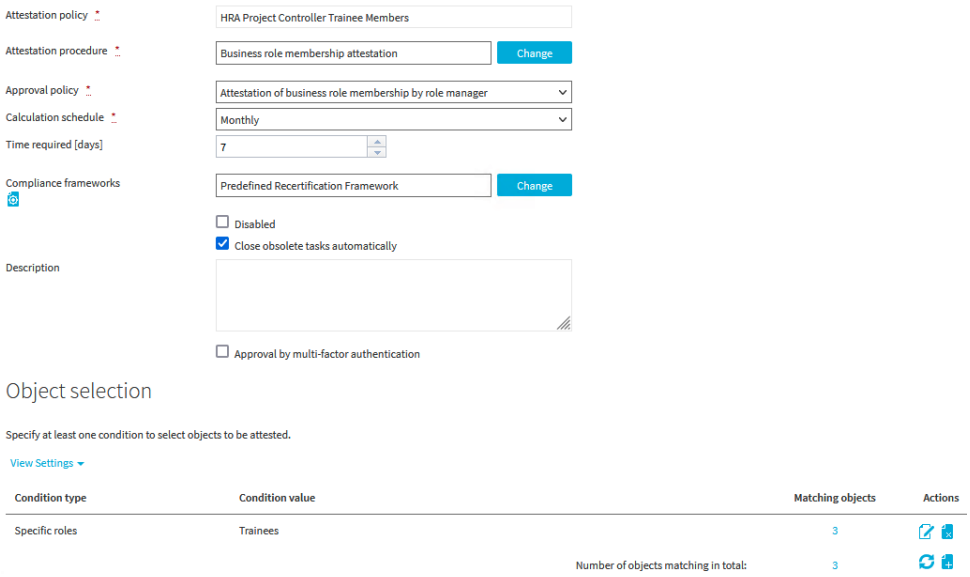
Create Attestation Policies

- Open your Web browser and start Standard Web Portal
  - **https://IAMS03.iam.corp/IdentityManager**

(better to use Quick Links from the documentation site)
- Sign in using your employee ID and your password

> **NOTE:**
> To find your actual ID, you can use the person overview form in Manager. Ensure the DBQueue Processor has finished its work before you try to logon to Manager.
>
> If you get a wrong user or password warning ensure:
> - Your **User Central account** is correctly written
> - You inserted a **System user password** during creating the identity object before. If you can't remember this just change the **System user password** on the **Miscellaneous** tab of the identity object to **I.4Madmin** (recommended for this training).

- In the web portal from the menu select **Attestation/Governance Administration** and click on **Attestation Policy Settings.**
- Click **[New attestation policy]** on the portals right lower corner.
- In the **Create New Attestation Policy** form:
  - Attestation policy: ***[Prefix] Project Controller Trainee Members***
  - Attestation procedure: ***Role memberships / Business role membership attestation***
  - Approval policy: ***Attestation of business role membership by role manager***
  - Calculation schedule: ***Monthly***
  - Time required (days): ***7***
  - Compliance framework: ***Predefined Recertification Framework***
  - Click on the tiny blue icon with the white plus inside in the **Object selection** ( )
    - Condition Type: ***Specific roles***
    - Select the **Functions / [Prefix] Project Controller / [Prefix] Trainees container**
    - Click **[Ok]**



- Click **[Create]**

Attestation Approval

> **NOTE:**
> The DBQueue Processor creates a scheduled process for the attestation cases. To speed this up for our lab exercise, we shall start the schedule manually.

- In **Manager** select **Attestation** from the main menu.

    - Expand **Basic Configuration data** and select **Schedules**.
    - Double click on **Monthly** in the **Schedules** list.
    - Select **Start Immediately** from the **Tasks** list and confirm.
- Switch back to the web portal and logoff the current user.

> **NOTE:**
> The employees responsible for the attestation are the senior managers assigned to the role we created before.

- Logon to the web portal as the role manager you noted above.
- You should immediately see **Pending attestations**
- Select **Pending Attestations** and review the entries by using the detail section on the right.
    - Deny Person1
    - Approve Person2 and all other people maybe in this list.
    - Click **[Next]**
- Note the yellow message informing about automatically deleted permissions and click on the message.
- Watch the role membership was prepared to become deleted. Close the pop-up form. This allows attestors a review about the consequences of the taken decisions.
- Click **[Save]** and **[Yes]** to save changes.

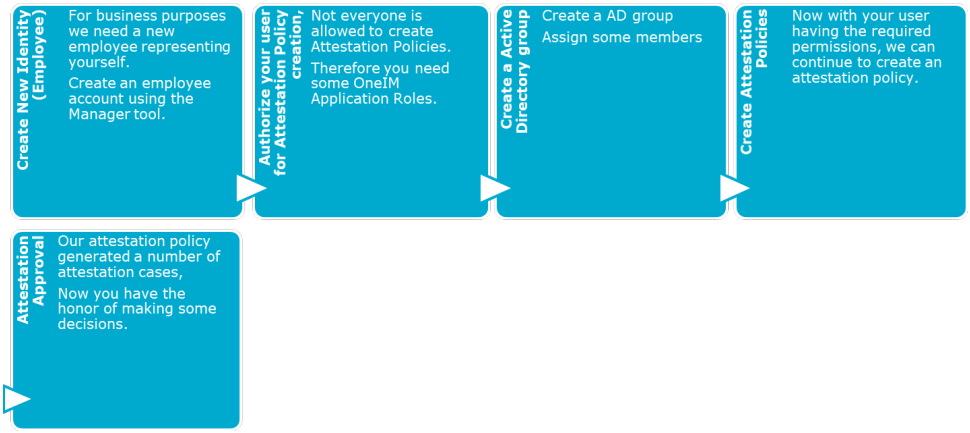
> **NOTE:**
> The out-of-the-box behavior of the system is to automatically remove the denied employee from the Business Role container. Be aware that before you can check this, you must wait on DBQueue Processor and the job engine. The tool to check the system is **JobQueueInfo**.

- In Manager check the appropriate Trainee role container to view the revised membership. You can watch Jobqueue to see the de-provisioning. Don’t forget finally to refresh the role overview in Manager to see the changes.

Lab Exercise Complete

Lab Exercise: IM-BCA-03 Simple Active Directory Group Attestation

Exercise Overview



In this lab we create a simple attestation policy acting as Compliance Information and Security Officer (CISO). We also see how to approve an attestation case

What You Need To Know:

- You should have the images open and running for this lab.

User credentials required for this lab:

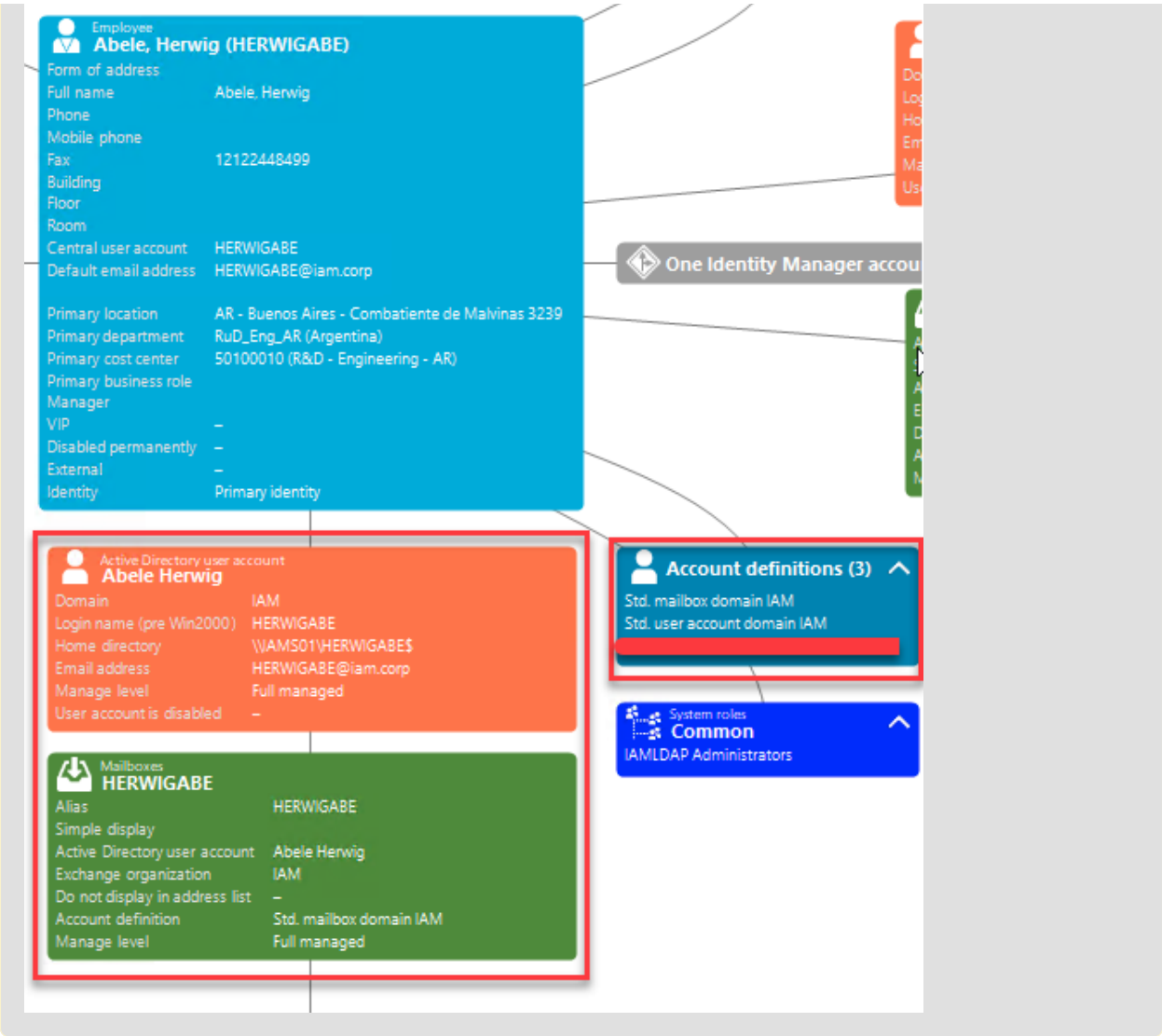
Affected Machines	IAMS01, IAMS02, IAMS03, IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin
Identity Manager - system user	
Username	[your system user] or training
Password	I.4Madmin

Estimated Time To Complete This Lab: **40 minutes**

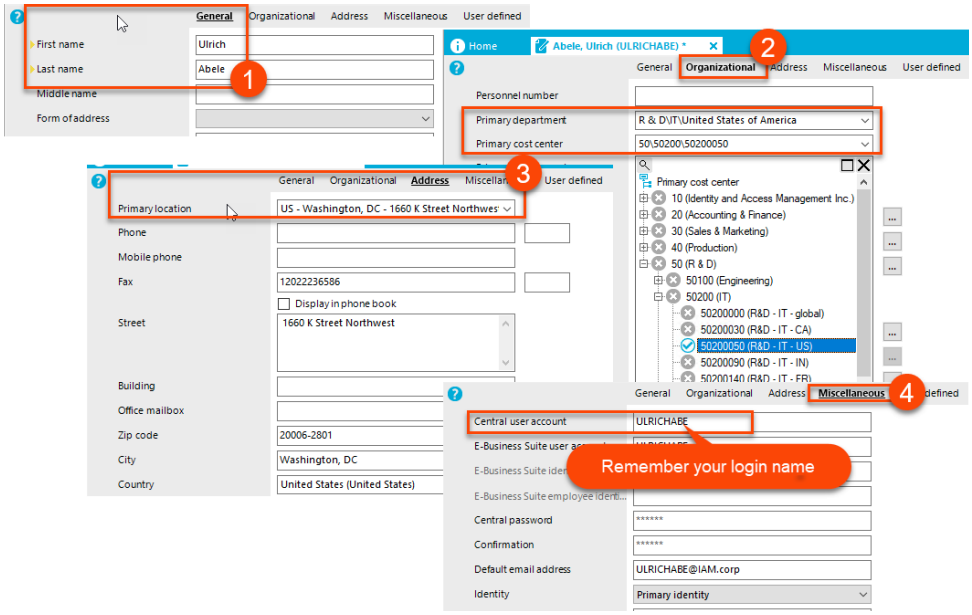
Lab Exercise

Create New Identity (Employee)

NOTE:
If you have **already inserted an employee with your name** into this environment and configured this employee with an AD account and a mailbox, **skip this section**. If not, please perform the necessary steps to create and provision an account. This employee object requires two account definitions along with an AD account in IAM and a mailbox in IAM.corp.



- Start **Launchpad** and select **Display and maintain content data**.
- Select **Employees** from main menu.
- Click the **Create a new object** icon in the employees **Result list** tool bar.
- 4. Enter the following data:
  - First name: ***your first name***
  - Last name: ***your last name***
  - Click the **Organizational** tab.
  - Select a value for primary department from the drop-down tree (should be a leaf node for lab simplicity). Remember this name, you will need it later.
  - Select a value for primary cost center from the drop-down tree (again this should be a leaf node). Remember this name, you will also need it later.
  - Click the **Address** tab.
  - Configure a primary location of your choice.
  - Click the **Miscellaneous** tab.
  - Note the automatically generate **Central user account**, you will need it later.
  - System user password: ***I.4Madmin***
  - Confirmation ***I.4Madmin***
  - Click **[Save]**



- To get an AD account and a mailbox you will need account definitions. Select your new employee and assign the following account definitions.
  - Std. mailbox domain IAM
  - Std. user account domain IAM
  - Click **[Save]**
- Start **JobQueueInfo** and observe the processes as they complete.

Authorize your user for Attestation Policy creation

> **NOTE:**
> To create Attestation policies, you need the role of Chief Information Security Officer (CISO). You may have done this in a previous lab. If you can remember just skip this section.

- In Manager select Employees and search for your employee record (created in the last task or another lab).
- Select Assign One Identity Manager application roles from the Tasks list.
- Ensure the following application roles are assigned:
  - Identity & Access Governance/Attestation/Administrators
  - Identity & Access Governance/Compliance & Security Officer
  - Click **[Save]**

> **NOTE:**
> These permissions are necessary to define attestation procedures (admin) and watch and manage attestation results (CISO).
>
> Further, Attestation policies are easily to be created in the **Standard Web Portal**. (They can also be created in the **Manager** tool, but this is not recommended.)

Configure email sender address

> **NOTE:**
> We connected MS Exchange as email system. Because of this Identity Manager tries to send out emails. Therefore, a sender address is needed. Unfortunately, this needs to be configured differently for some features. Attestation does have its own sender address. Let's configure this to avoid FROZEN jobs in the Jobqueue later. Depending on your training and regarding to your training environment this might be preconfigured or not.

- Open Designer and login with your system user account. You can also use Lauchpad: Configure/Change system settings.
- In Designer you need to double check Configuration parameters.
  - Expand QER\Attestation\DefaultSenderAddress.
  - Value: ***NOREPLY@iam.corp***
  - Click **[Commit to database]** and **[Save]**.

Create Active Directory group

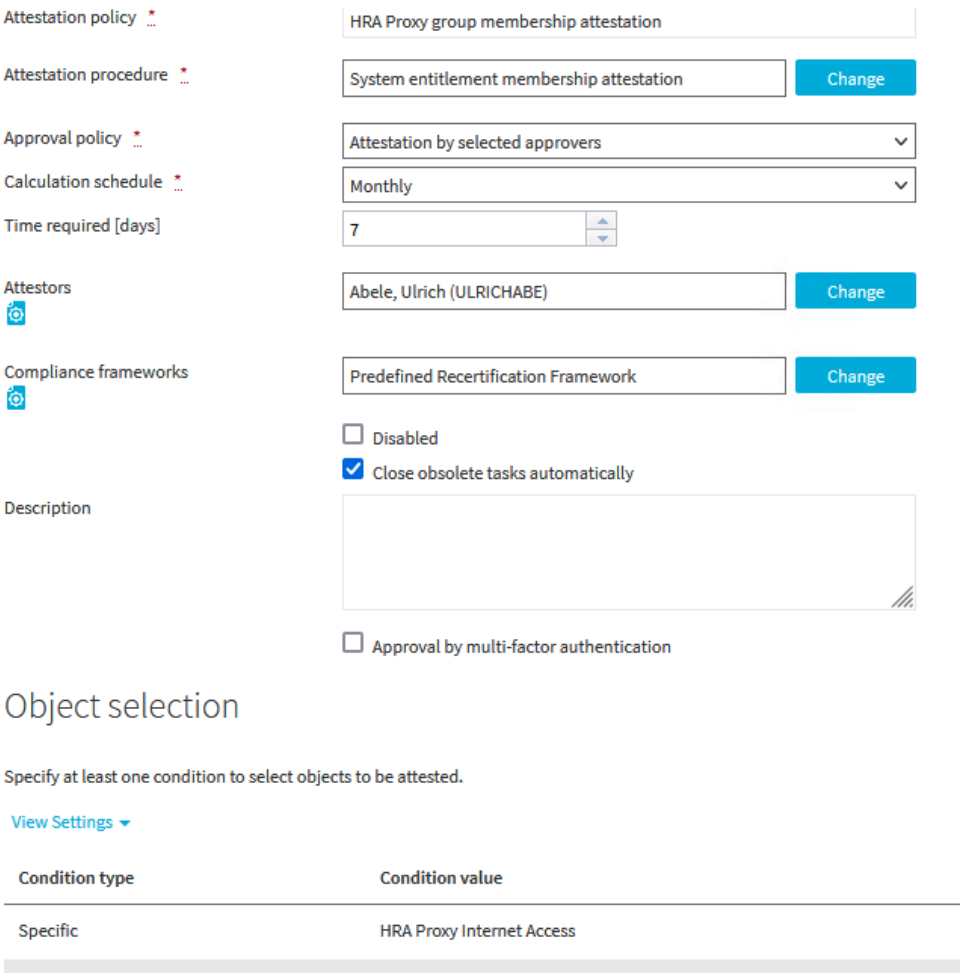
- In **Manager** select **Active Directory** from the Main Menu.
- Expand **Groups** in the Navigation pane.
- Right click **Groups** and select **New**
  - Name: ***[Prefix] Proxy Internet Access***
  - Container: ***IAM.corp/Users***
  - Click **[Save]**
- Select **Assign user accounts** from the **Tasks** list
- Assign two or more Active Directory accounts from a container underneath **Company**

Create Attestation Policies

- Open your Web browser and start Standard Web Portal
  - https://IAMS03.iam.corp/IdentityManager
    (better to use Quick Links from the documentation site)
  - Sign in using your employee ID and your password

> **NOTE:**
> To find your actual ID, you can use the person overview form in Manager. Ensure the DBQueue Processor has finished its work before you try to logon to **Manager**.

- From the site menu select **Attestation / Governance Administration**
- Select tab **Attestation Policy Settings**.
- Click **[New attestation policy]** on the portals right lower corner.
- In the **Create New Attestation Policy** form:
  - Attestation policy: *[Prefix] Proxy group membership attestation*
  - Attestation procedure: *System entitlement memberships / System entitlement membership attestation*
  - Approval policy: *Attestation by selected approvers*
  - Calculation schedule: *Monthly*
  - Time required (days): ***7***
  - Click **[Assign]** right beside the **Attestors** field.
    - Enter last name of your created user into the search box
    - Click the spyglass icon right beside
    - Select your created identity
    - Click **[OK]**
  - Compliance framework: ***Predefined Recertification Framework***
  - Click on the tiny blue icon with the white plus inside in the **Object selection**
    - Condition Type: ***Specific system entitlements***
    - Enter into the search box: ***[Prefix]***
    - Click the search (spyglass) icon
    - Select entry: ***[Prefix] Proxy Internet Access***
    - Click **[OK]**



- Click **[Create]]**

Attestation Approval

> **NOTE:**
> The DBQueue Processor creates a scheduled process for the attestation cases. To speed this up for our lab exercise, we shall start the schedule manually.

- In **Manager** select **Attestation** from the main menu.
  - Expand **Basic Configuration data** and select Schedules.
  - Double click on **Monthly** in the Schedules list.
  - Select **Start Immediately** from the Tasks list.
- Switch back to the Browser (**Standard Web Portal**) and select **Attestation / My Actions** from the site menu.
- Select **Pending Attestations**

> **NOTE:**
> In a real-world scenario the attestor often will not be the person who creates the attestation policy. To simplify the lab case, it makes sense to use the same user for both.

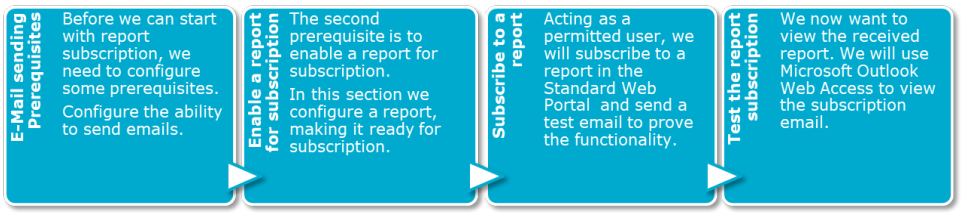
- Review the entries by using the detail section on the right.
  - Approve and deny members
  - Click **[Next]**
- 5. Click **[Save]** and **[Yes]** to save the changes

Lab Exercise Complete

Lab Exercise: Report Subscription (IM-BRP-01)

Exercise Overview

In this lab you enable mail delivery and subscribe to a report



What You Need To Know

- You must have the images open and running for this lab.
- AD Account SRV_1IM_EX must be member of the AD group Organization Management.

User credentials required for this lab

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin

Estimated Time To Complete This Lab: **20 minutes**

Lab Exercise

Prerequisites for sending email from Identity Manager

> **NOTE:**
> Before Identity Manager can send emails with subscribed reports, we must configure an account to send SMTP email to a MS Exchange server first. By default, Exchange does not permit anonymous SMTP traffic.

- Use **Launchpad** to launch change system settings. You should get a **Designer** started. Please ensure that only one Designer is started on your workstation.
- Wait for **Designer** to display the configuration parameter editor.
- Expand and activate **Common** → **MailNotification**
- Activate and configure the following parameters
  - AllowServerNameMismatchInCert: **checked**
  - DefaultAddress: ***the email address of your employee account***

> **NOTE:**
> The value can be copied from Manager.
> Typically, this is an administrator's or help desk mailbox, but we only have one mailbox enabled in our lab right now so let's use it. Please double check, that your identity has Active Directory Account and Mailbox assigned.

  - DefaultSender: ***NOREPLY@IAM.corp***
  - SMTPPort: ***25***
  - SMTPRelay: ***IAMS01***

NOTE:
DefaultSender exists more than once in the configuration parameter section of Identity Manager, each for a different purpose. We recommend searching for **"Enter email"** (without double quotes) starting with **Ctrl+F** in the **Configuration parameters** window.

    - Set the value NOREPLY@IAM.corp for the following configuration parameters:
        - QER\Policy\EmailNotification\DefaultSenderAddress
        - Common\MailNotification\DefaultSender
        - QER\RPS\DefaultSenderAddress
- Select Base data from **Designer** main menu and select **Installation / Job server** from the **Navigation** pane.
- Remember we do have physical Jobserver on IAMS02 and IAMS03 and there is another entry for IAMS01 (which is a virtual queue). We want to send mails using IAMS03. Please configure or double check:
    - Configure **Server function/SMTP** host for IAMS03
    - Remove the flag **Server function/SMTP** host from Server IAMS02
      (there is an according **Server function** tab at the bottom of the form of the middle form).
- **Commit to the database** and store the changes.

NOTE:
After installation, the only server that exists in the database (it's the DB server) gets the flag SMTP-Server automatically to ensure mail jobs can be sent. To simplify things, we recommend only to use one SMTP server.
When user accounts are created in AD, by default, the **User must change password on next logon** flag is set. This prevents the user from logging on to services like OWA before the password is reset. We shall uncheck this flag to avoid this issue.

- In Manager find your Active Directory and select User accounts.
- Find the related Active Directory account to your identity.
- Open the Main Data form and switch to tab Password.
    - Check: ***Password never expires***
    - Note, **Change password at next login** disappeared. Ensure it is unchecked.
    - Password: ***I.4Madmin***
    - Confirmation: ***I.4Madmin***
    - Click **[Save]**

Enable Report for Subscription

NOTE:
In Identity Manager, a report subscription can only be configured if the report is configured as available for subscription AND if an identity (person object) has permissions to subscribe this report.

- Use **Launchpad** to open **Manager**.
    - Select your identity in **Employees**.
    - Select **Assign One Identity Manager Application Roles** from the Tasks list
    - To make the configuration of report subscription available and manageable for your user expand **Identity & Access Governance** and assign the following Application roles
        - ./Report Subscription
        - ./Report Subscription/Administrators
    - Click **[Save]**
    - Select **Report Subscriptions** from the main menu.
    - Right click on **Subscribable reports** and select **New** from the context menu.

NOTE:
Each report In Identity Manager can be subscribed. Out-of-the-box, Identity Manager includes approximately 90 reports. You may also provide a new name for the report as it appears in the list.

- Name: ***[Prefix] Identity Permission Overview***
- Report: ***VI_Person_Overview_With_History***
  (Caution: Please don't select VI_Persons_*…)
- Click **[Save]**. A tab Parameters should be now available.
- Select tab **Parameters**
  - Select parameter Employee and configure
    Parameter type: ***User prompt***
  - Select parameter Minimum Date and configure
    Parameter type: ***User prompt***
- Click **[Save]**.
- Select **Assign to employees** from the **Tasks** list.
- Right-click in the list and assign all objects to the new report subscription.
- Click **[Save]**.

NOTE:
This allows all employee to subscribe to the report to display their own personal permissions overview.
In a production project a report subscription would typically be assigned to a business organization, or application role making the report available through a role assignment.

Subscribe to a report

- Open your web browser and select **Standard Web Portal** from **Quick Links**.
  - Logon with your employee account
  - Select **Settings** (right upper corner).
  - Select tab **Subscriptions**.

NOTE:
Now you may see some predefined already subscribed reports. In a production system there should be many of them.

  - Click [Add Subscription]
  - In the list of available reports please search for your report [Prefix] Identity Permission Overview.
    - Click on the Display filter icon.
    - Click the dropdown box All words and select Starts with.
    - Enter your [Prefix] into the empty first field.
    - Click **[Filter on]**
  - Now select your report and click [Next]
  - Enter the following info:
    - Schedule: ***Monthly report subscriptions***
    - Format: ***PDF***
    - Employee: ***select [your employee account]***
    - Please note: **Minimum date** is available to configure. To ensure in this environment to get enough data, we will let it unconfigured, but it is available.
  - Click **[Next]**
  - We do not need additional subscribers. Click **[Save]**
  - Click **[Close]**

Test the report subscription

- To test the subscription, select it first.
- Within the gray box on right, click on “Actions - Get report now”.

NOTE:
The next steps could only be performed if your test identity does have a mailbox assigned.

- Open another browser window
  - From the Home-Site (Documentation page) select **Quick Links** and **MS Outlook Web Access** in the

Administration section.
    - Logon using your AD user account.
    - Find the email with the attached pdf report file and enjoy the report.

> **NOTE:**
> We described this above, it is possible that you cannot logon or you get prompted to change your password. This is because of the default configuration of a new AD user: **User must change password on next logon**.

- Please use **Manager** to reconfigure this for **your** Active Directory account (this is the one you have created before and is equipped with a mailbox), we recommend to use **User cannot change password** and **Password never expires** in this training environment.

Lab Exercise Complete

Lab Exercise: Create and Attach report (IM-BRP-02)

Exercise Overview

In this lab you create and attach a custom report to the environment.

What You Need To Know

- You must have the images open and running for th is lab.
- Additional Lab content stored in the Lab folder (\\IAMS10\Training):
  - QDC_JobTitle_And_Members.mrt
  - QuestDemoCorp_300dpi_3cm.png

User credentials required for this lab

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin

Estimated Time To Complete This Lab: **60 minutes**

Lab Exercise

Creating a Report

NOTE:
Identity Manager supports development of custom report layouts. However, custom layout is not the focus of this lab.
The lab is divided into three parts like any report development:

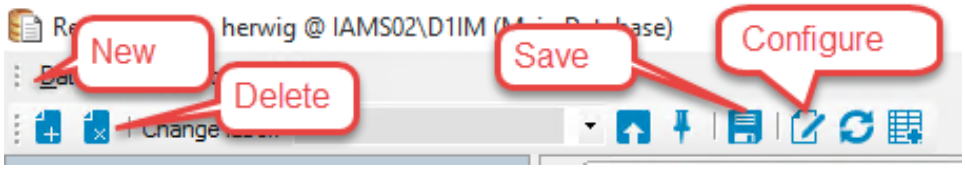
- Definition of the data sources.
- Integrating the data source into a layout
- Integrating the report into a front-end

- Use Launchpad to add or modify a report. The report editor works best if you sign in with your system user account.

NOTE:
On the left side of the Report Editor you should notice a number of existing reports. These existing reports can be used

as a template library for building new reports.

- Click on the new report icon on the left upper.

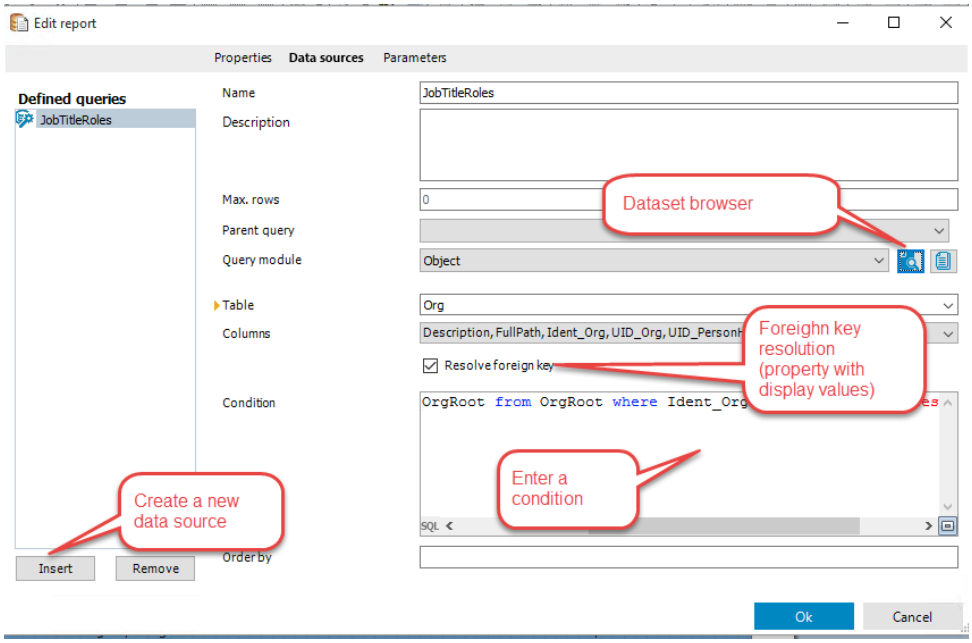


  - Name: ***CCC_FunctionRoles_and_members***
  - Display name: ***Function Role overview***
  - Base table: ***Org***
  - Category: ***Common***
  - Select the Data Sources tab
    - Name: ***FunctionRoles***
    - Query module: ***Object***
    - Table: ***Org***
    - Columns: ***Description, FullPath, Ident_Org, UID_Org, UID_PersonHead, UID_PersonHeadSecond*** (easiest way is to open the box and to use type ahead to find the columns. Use the space bar to assign the column to the list and click the “X” once you finished your selection).
    - Check the **Resolve foreign key** check box.

NOTE:
Typically in a relational database model Foreign Keys (FK's) and m:n member relations are used to generate references between data objects (or single records). Nearly everywhere the database developers use a type of unique identifier to securely identify their records which is mostly not human readable. Identity Manager for example is using GUID's (example: 0D7E327D-E2FA-42BC-9C65-A622C9206E1C).
They are very unique and easy to create but connecting records will in a connecting table not show any human readable information (see UID above). To get a user-friendly display name of a related record typically the related table must be loaded as well (to get all the human readable values).
The option **Resolve foreign key** loads to each identifier additionally a property with the display name of the related object into the data set of the parent table. Such a display name can be configured in Identity Manager for each table separately and must be a column of the connected table. For example:
[Person] → a table or object based on a table

- **uid_person (PK)**
  → UID of the current object
- **internalname***
  → Display name of the current object and its display value (*)
- **uid_personHead (FK, [Person])**
  → Manager of the current object
- **FK(uid_personhead),[Person].internalname****
  → Display name of the manager of the current object and display value of the related table object(**). This is a virtual property because there is no such column in the table [Person]. The property exists only in the object model if Resolve foreign key is checked.

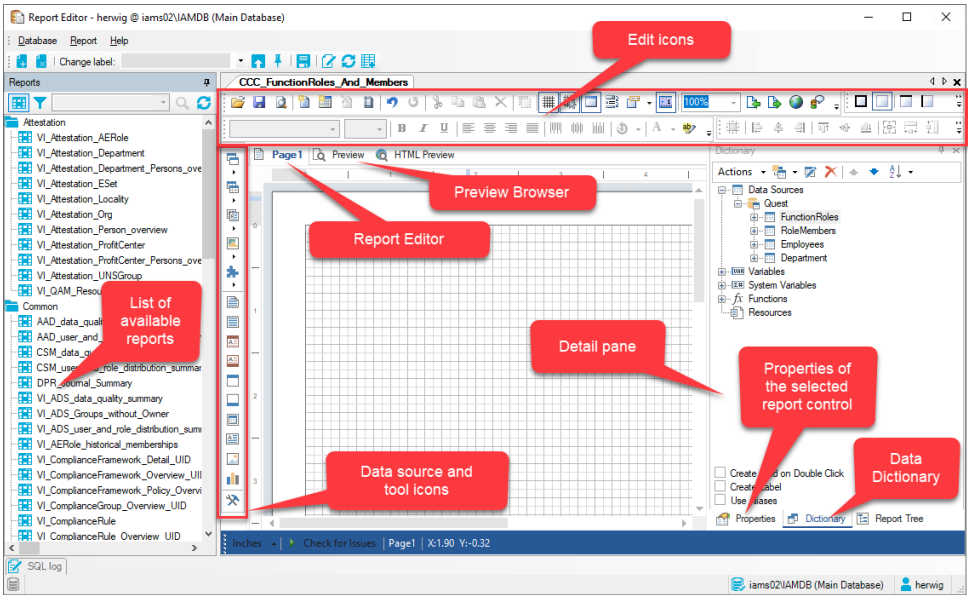
    - Insert the following into the Condition field (replace [Prefix] with yours):
      `UID_OrgRoot in (select UID_OrgRoot from OrgRoot where Ident_OrgRoot='Functions')`
    - Use the test icon (Dataset Browser) beside the **Query module** field (picture, **Dataset browser**) to check if your condition returns values.



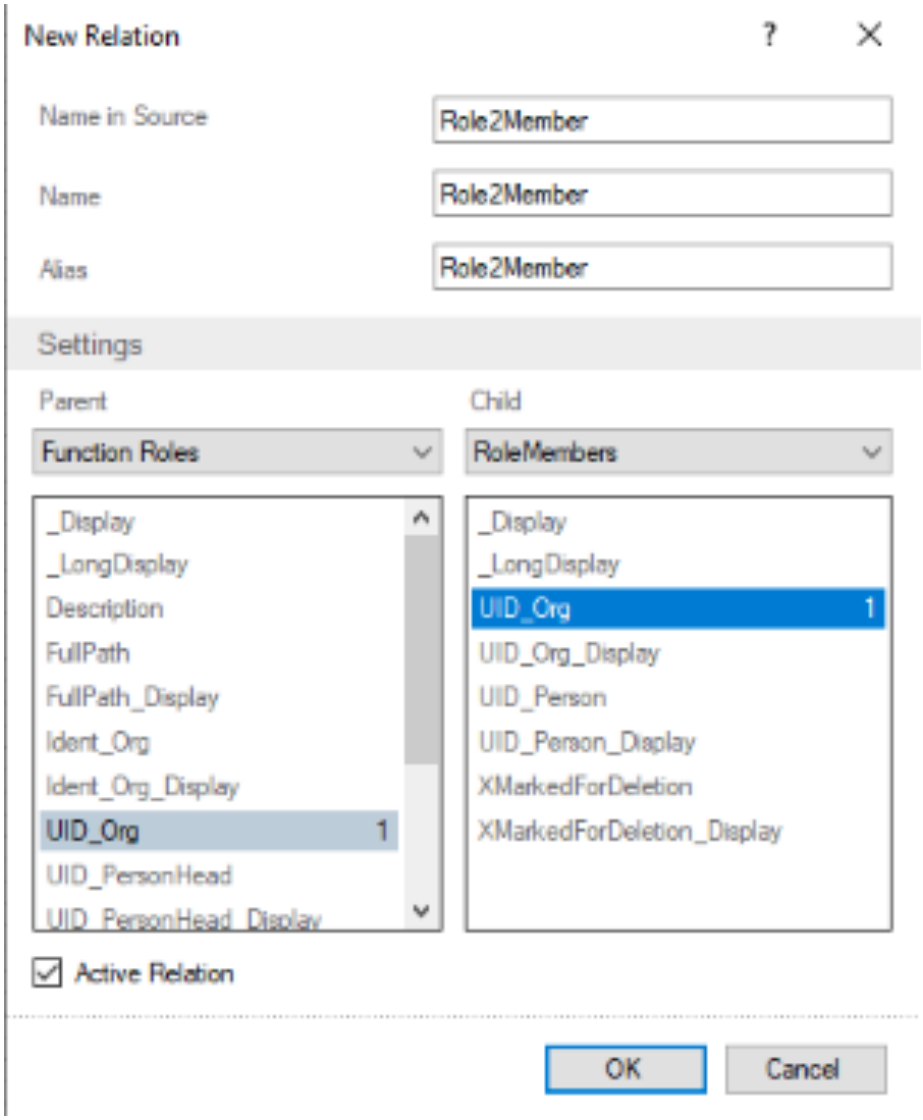
- Click **[Insert]** to create a new data sourceRole
  - Name: ***RoleMembers***
  - Query module: ***Object***
  - Table: ***PersonInOrg***
  - Columns: ***UID_Org, UID_Person***
  - Check the **Resolve foreign key** check box
- Click **[Insert]**
  - Name: ***Employees***
  - Query module: ***Object***
  - Table: ***Person***
  - Columns: ***FirstName, LastName, UID_Department***
  - Check the **Resolve foreign key** check box
- Click **[Insert]**
  - Name: ***Department***
  - Parent Query: ***..Employees***
  - Query module: ***Object***
  - Table: ***Department***
  - Columns: ***FullPath, UID_Department***
- Click **[Ok]**

- Now let's insert data relations into the report.

NOTE:
It is common in a report engine to design data relationships separately and not to take predefined relations from the data model. This makes the reports much more flexible because you may use self-defined relations, based on your self-defined data resources.
Before you can start it might be you see instead the Detail pane (see picture below), a three-button selection (Basic, Standard, Professional). The answer on this selection determines how many options (details) in the Detail pane you will see. The only valid answer is [Professional].

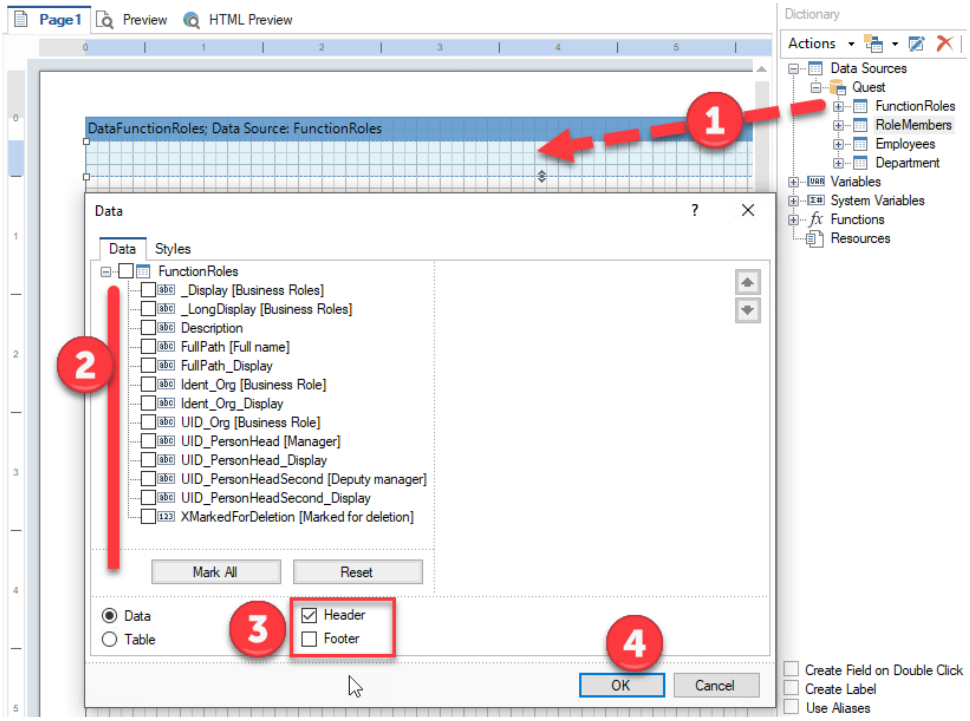


- In the **Dictionary** tab (right lower side), right-click on **Data Sources** (top right) and select New Relation….
  - Name in Source: ***Role2Member***
  - Name: ***Role2Member***
  - Alias: ***Role2Member***
  - Parent: ***FunctionRoles***
  - Child: ***RoleMembers***
  - Parent Columns: ***UID_Org***
  - Child Columns: ***UID_Org***
  - Active Relation: **checked**



    - Click **[OK]**
- In the **Dictionary** tab, right-click on **Data Sources** and select **New Relation…**.
- Name in Source: ***Member2Person***
- Name: ***Member2Person***
- Alias: ***Member2Person***
- Parent: ***Employees***
- Child: ***RoleMembers***
- Parent Columns: ***UID_Person***
- Child Columns: ***UID_Person***
- Active Relation: ***checked***
- Click **[OK]**
- In the Dictionary tab, right-click on Data Sources and select New Relation….
    - Name in Source: ***Person2Department***
    - Name: ***Person2Department***
    - Alias: ***Person2Department***
    - Parent: ***Department***
    - Child: ***Employees***
    - Parent Columns: ***UID_Department***
    - Child Columns: ***UID_Department***
    - Active Relation: **checked**
    - Click **[Ok]**
- Expand the Data Sources tree to view the added data sources and data relations (the relations are organized underneath the parent data sources).

- Drag and drop the FunctionRoles to the report editor pane.
  - In the popup window select:
    - Description
    - UID_PersonHead_Display
    - UID_PersonHeadSecond_Display
    - FullPath (FullName)
    - Check the Header check box

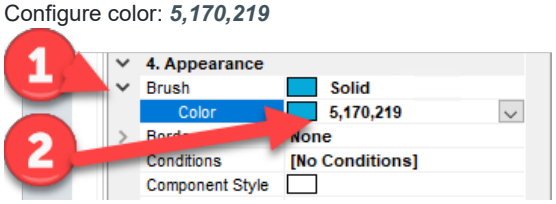


    vi. Click **[Ok]**
  - Select the **Preview** tab at the top of the layout pane.
  - Notice the list of roles that appear on the screen.
- Go back to the Edit page (labeled **Page1** on the tabs)
  - The first row on the layout is called the **Header band**.
  - The second row on the layout is called the **Data band**.

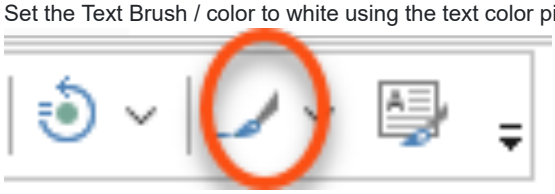
  - Click on the **Data band**
  - Expand the **Data band** to make it longer (down, click first the blue gray space on right of the data band title, use the bottom, middle selector of the element to expand).
  - Pull all the data fields, except FullPath, lower and expand the FullPath field all the way to the right side of the layout.
  - Select the FullPath data field and set the background color to blue.

    This is the quick way to do it. More control gives the next step.
  - Select the **Properties** tab.
    - Expand **Brush**

- Configure color: ***5,170,219***



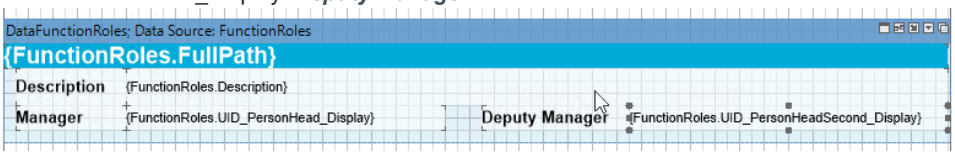
- Set the Text Brush / color to white using the text color picker in the editor tool bar



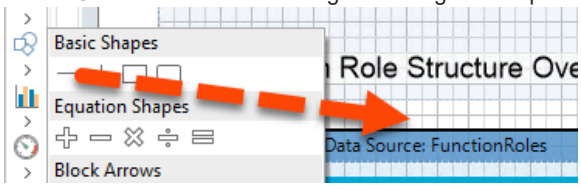
Yes, this time you selected from the collection of text layout icons (another toolbar).

- Font: ***Arial, 11pt, style=Bold***

- Pull the Description header field down below the FullPath field, slightly indented.
- Place the Description data field to the right of the header field and extend it to the right side of the layout.
- Place the Manager header field below the Description header so they are aligned on the left side.
- Place the **PersonHead_Display** data field to the right of the header field and extend it to the middle of the layout.
- Place the Assistant Manager header field to the right of the **PersonHead_Display** data field.
- Place the **PersonHeadSecond_Display** data field to the right of the header field and extend it to the right side of the layout.
- Rename the field labels
  (to do so, select each label with a double click and enter a new value)
  - PersonHead_Display: ***Manager***
  - PersonHeadSecond_Display: ***Deputy Manager***



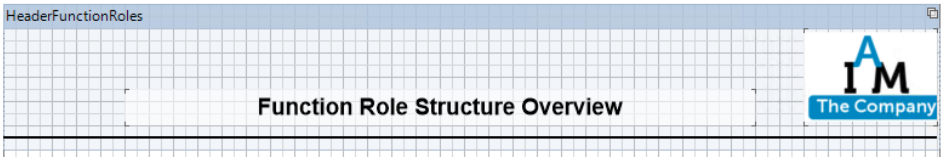
- Delete **FullPath_Display** field from the **Header band**.
  - Add a text field in the **Header band** (icon in the right tool bar).
  - Type in: ***Function Role Structure Overview***
  - Recolor the text field to black writing on transparent background with
    Font: ***Arial, 14, style=Bold***.
    (use the three dots to ease your life)
  - Add an image field to the **Header band**
    - Click the Image tool from the edit window tool column.
    - Click **Open** in the image popup.
    - Select the IAM logo (BRP-2_IAM_TheCompany.png from the LAB folder: T:\courses\IdentityManager\Labs\IM-BRP-02)
    - Click **[Ok]**
  - Move the image so it is aligned in the upper right corner.
  - On the properties tab for the image.
  - Multiple Factor: ***0.6***
  - Arrange and resize the logo shape to the upper right and expand your header band if necessary.
  - Select the title shape move it left beside the logo and increase shape and font size until it looks good.
  - Add a black line below the report title. This could be first time a bit tricky. Click on the shape logo first, then click AND HOLD the horizontal line logo and drag and drop it on your page.



  - Use Properties to configure the line size to 2 and the color to black if needed.

NOTE:
When you first draw the line, it may be its color is white. You must view its properties to change it to black.

- Your layout should look something like this.



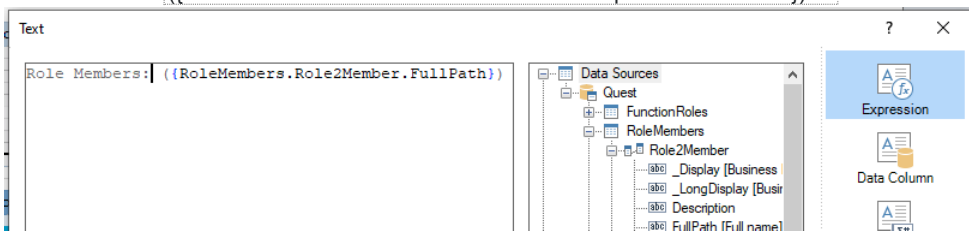
- From the **Dictionary**, drag the RoleMembers data source to the report layout (drop them below the other data source).
  - Select UID_Person_Display
  - Check the Header check box
  - Click **[OK]**
- Adjust the Header and Data bands for RoleMembers so the header fields start slightly indented below the JobTitleRoles data band.

NOTE:
We now must connect the two bands.

- Move the cursor to hover over the RoleMembers data band right.
  - Five Icons will appear on the right. 
  - Click on the first icon. A popup will display all the data sources with **RoleMembers** selected.
  - Click on the second icon and select the **Role2Member** relation.
  - Click on the third icon and select **DataFunctionRoles**
  - View the report in preview mode. You should now see the assigned people displayed below each Job title role.

NOTE:
To identify each name more accurately we shall now display the department info for each role member in parentheses after the name. We will also provide a summary line at the top of the list identifying the number of members in the list. To save space we will additionally display the list of members in two columns.

- Double-click in header-band **RoleMembers** the label field named **uid_Person_Display**.
  In the text Editor:
  - Select the **Expression** tab (on right)
  - Rename Text in the left window part to ...Role members
  - Expand tree in the middle to ../RoleMembers -> Role2Member/
  - Drag and drop FullPath **[Full Name]** into the edit window on left.
  - Separate both fields with a space.
  - Enclose the second field with brackets. It should look like this:
    Role members: ({RoleMembers.Member2Person.Person2Department.FullPath})

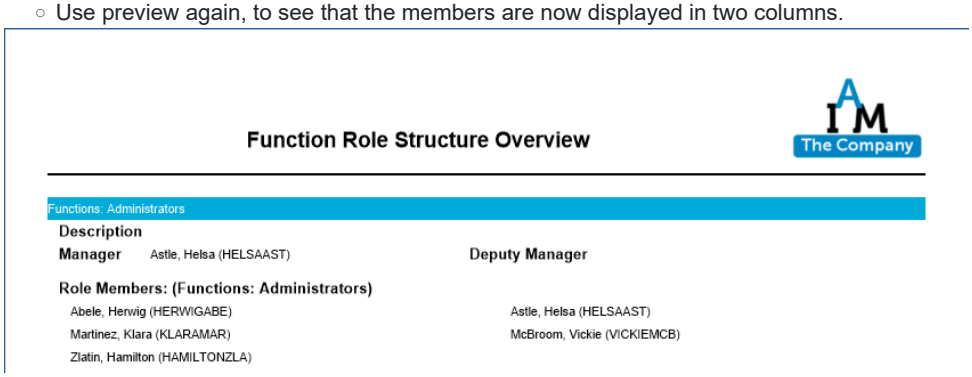


  - Click **[Ok]**

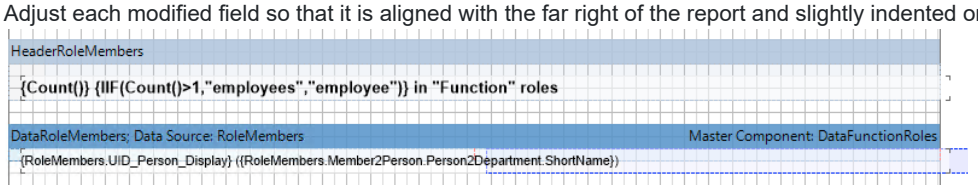
NOTE:
It might be, that you smash up something and this will lead to a red X replacing the complete Report Editor form. If this happens use the Report Tree tab (right lower) to select the

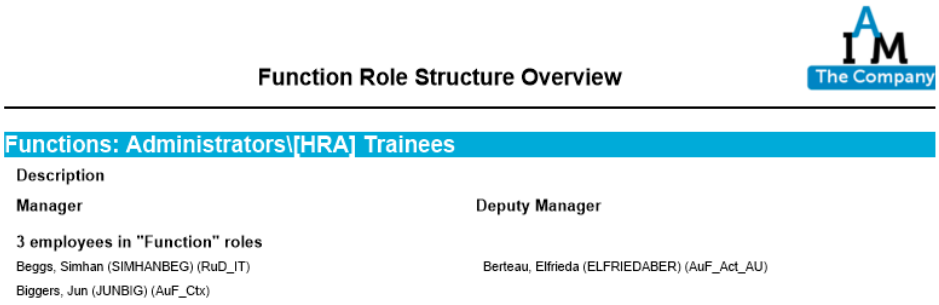
DataRoleMembers.DataRoleMembers_uid_person_Display element. Step to the **Properties** tab and use the Text property to edit or delete the value. Once this is done, save your report and restart the whole Report editor front-end. You should now see the **Report editor** window again. This procedure can accordingly always be used to solve this kind of problem.
The preview shows members with departments in parentheses.
In the next step we expand the layout a bit to show how to work with integrated programming elements.

- Click the second data band and edit the properties.
  - Columns: ***2***
  - Use preview again, to see that the members are now displayed in two columns.



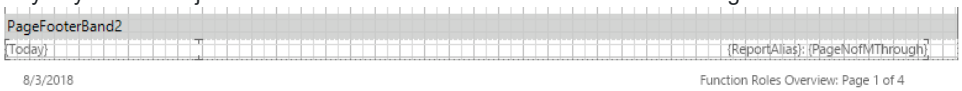
- Switch back to the Page 1 and double-click on the displayed field in the **RoleMembers** header band. The Text editor will open:
  - Ensure Expression is selected
  - Delete the displayed text in the Editor
  - Expand Functions → Totals → Count in the middle
    - Drag Count():Long to the text editor
    - Type a space behind the inserted value
  - Expand Functions → Programming
    - Drag IIf to the edit window after the Count function.
    - Configure the parameters as follows
      IIF(Count()>1,"Employees","Employee")
    - Add a space
    - Add text behind in Function roles
    - After configuring, the string should look like:
      {Count()} {IIF(Count()>1,"employees","employee")} in Function roles
    - Click **[Ok]**
  - Adjust each modified field so that it is aligned with the far right of the report and slightly indented on the left.



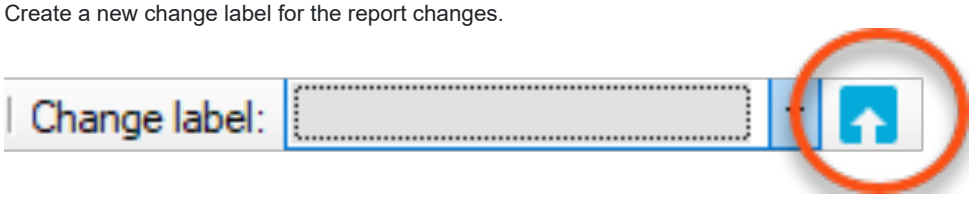


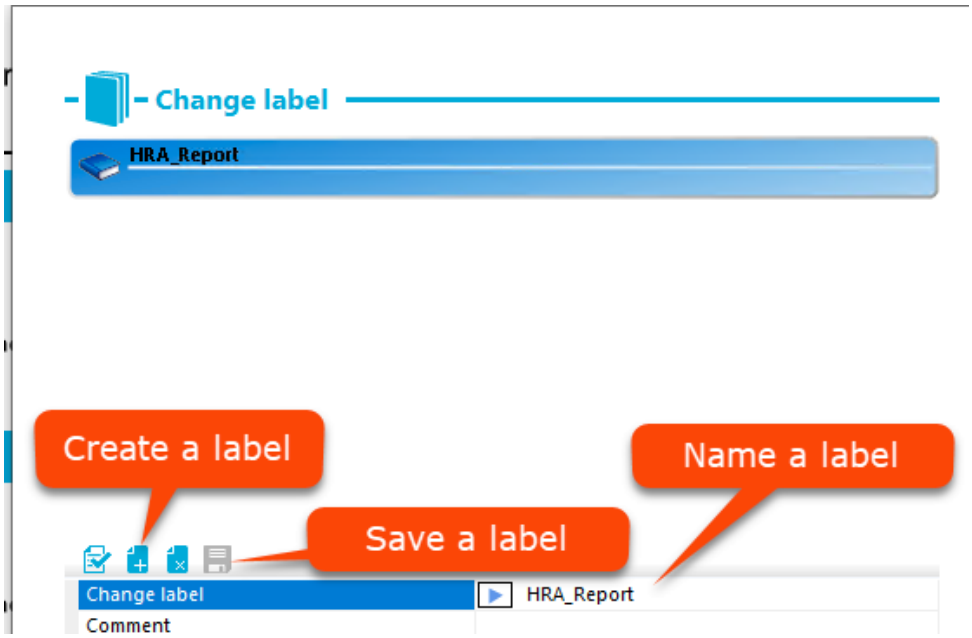
NOTE:
We now copy and re-use content from another report.

- Select any of the reports in the report list.
  - Select the Page Footer Band with a left click (ensure that the whole band is selected).
  - Copy the band (best to use right-click → copy for this action)
- Switch to your new report
  - Left click the report page background (no report control, important)
  - Paste the copied footer band into the report (best to use right-click → paste for this action).
  - Maybe you must adjust the size of the new footer band. Ensure that the right and the left values are displayed.



  - View the results in the preview page.
- Create a new change label for the report changes.





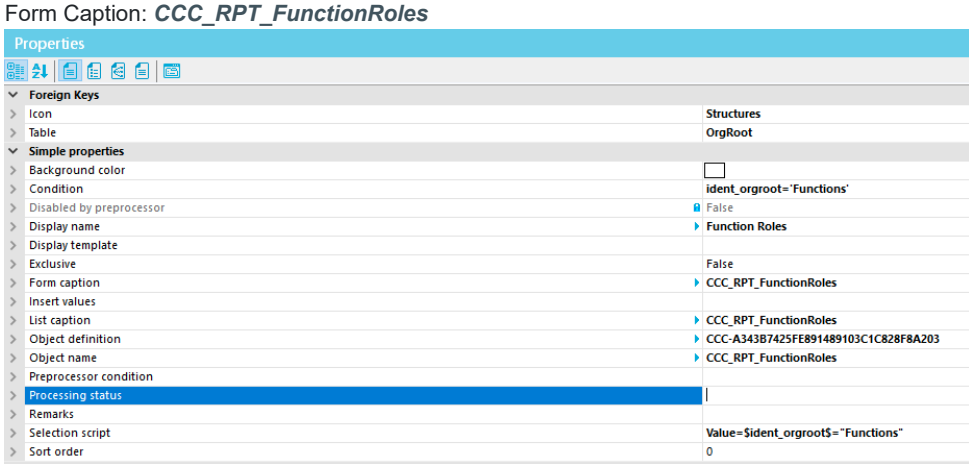
- Save the new report to the database. (Editor Tool bar at the top of the screen.)

Add the report to the Manager display (Prerequisites)

NOTE:
In Lab IM-SEC-01 we created a custom permissions group that now will be used to handle the Identity Manager permission.
To display the report only for the Job Title Role structure, we must also create a custom object definition before we can assign the report to the Manager front-end.

- Use **Launchpad** to open **Designer**.
- In a first step we need a managing wrapper around the pure report we created above. Select **User Interface** from the Main Menu
- Expand **Object definitions**
- Select **Custom objects**
- Right-click in the form on right and select **New**.
  - Icon: Structures
  - Table: OrgRoot

- Condition: `ident_orgroot='Functions'`
- Selection script: `Value=$ident_orgroot$="Functions"`
- Display name: ***Function roles***
- Object name: ***CCC_RPT_FunctionRoles***
- List Caption: ***CCC_RPT_FunctionRoles***
- Form Caption: ***CCC_RPT_FunctionRoles***



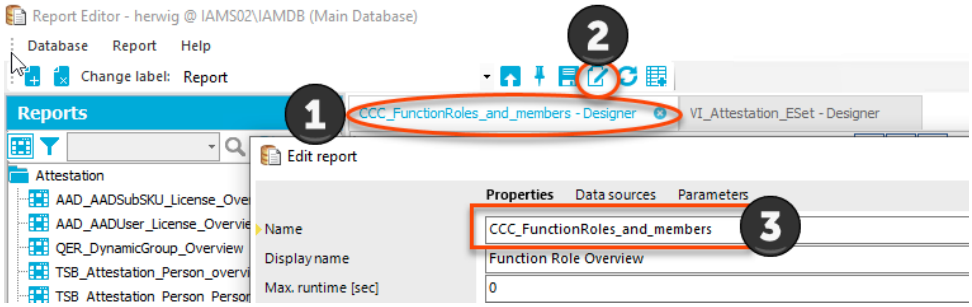
- Commit to database and save all changes to new Change label.

> **NOTE:**
> You can't use the same Change label as created in the Report Editor before, because this means storing incompatible change types. If you try it anyways, an error message will show you this immediately.
> New object definitions could have scripts associated with them. Therefore, we must recompile the database.

- From the Database menu, compile the database using defaults.

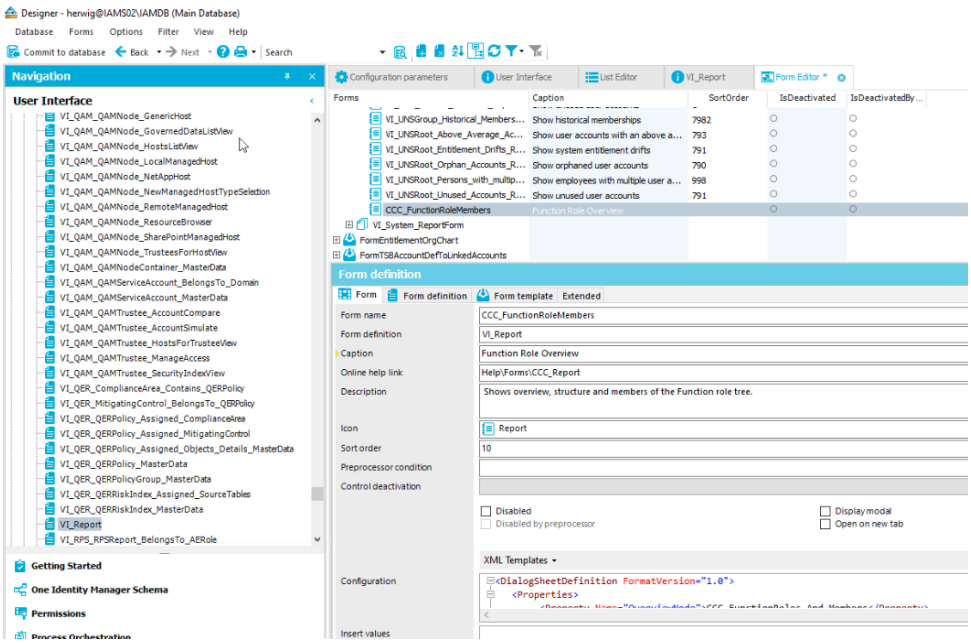
Add the report to the Manager front-end

- Now it's time to place the report-object in Manager.
  In **Designer / User interface**
- Expand **Forms**
- Expand **Form definitions**.
- Search for and select **VI_Report** (use **[Ctrl]+[F]** in **User Interface** use a double click to select)
- In the Task list select **Edit form definition VI_Report**
- Select Report form → **VI__Report** in the middle list and right-click the selected entry. There select Insert and configure the new report form definition.
- Form name: ***CCC_FunctionRoleMembers***
- Form definition: ***VI_Report***
- Caption: ***Function Role Overview***
- Description: ***Shows overview, structure and members of the Function role tree.***
- Icon: ***Report***
- Sort order: ***10***
- In the configuration section, you need some XML. There is a template available can be used but needs to be heavily modified. Because of this we suggest just to use a nearby template from another report. Please copy the **Configuration** from a report above or below this report entry. After inserting the value into your Configuration, it is easy to see what's to modify:
  - You don't need 'ReportParameter' such lines can be deleted if they exist
  - The 'ReportName' property needs the name of your report as value. This you can get from the Report editor.



- The finished xml code should look like this:

```
<DialogSheetDefinition FormatVersion="1.0">
 <Properties>
   <Property Name="ReportName">CCC_FunctionRoles_and_members</Property>
 </Properties>
</DialogSheetDefinition>
```



NOTE:
Now we have configured the form to make the report accessible. Let's assign the object to a permissions group, a front-end dialog and a Identity Manager App.

- Select the **Object Assignment** tab (bottom of the current form) → We want to be able to use the report task in Manager, only for Function Roles
  - Select: ***QER-T-OrgRoot - 0 - Function Roles***
    (could be named similar but near to this)
- Select the **Permissions group** tab → Somebody must be permitted to see the report.
  - Select: ***CCC_Dialog_And_Schema_Extensions***
- Select the **Program** tab → We want to use the report in Manager.
- Select: ***Manager***

- Commit to database using the report change label you created in Designer steps above.
- Compile the database.

NOTE:

Your report is based on object-based data queries.
To see the pure data you must have permissions on roles and employees. Therefore, we must increase the permission set of your user.

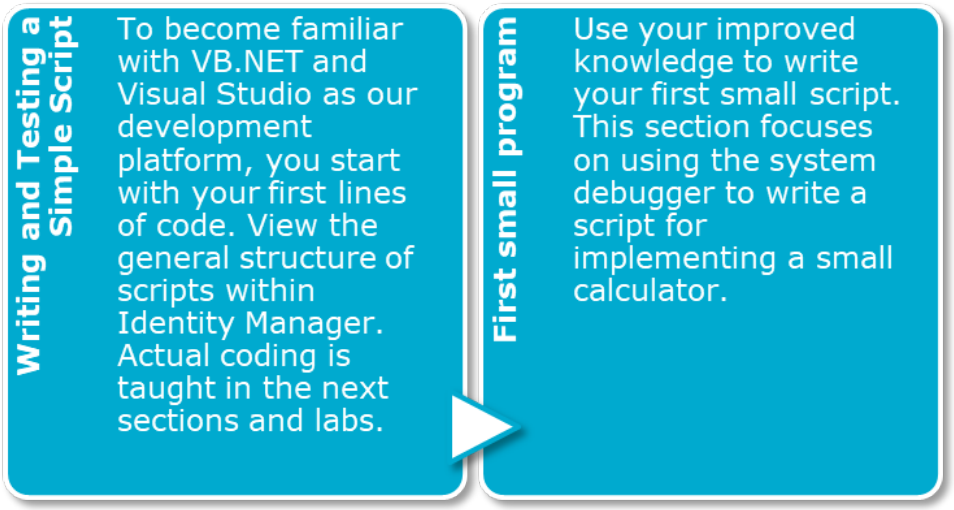
- Open **Manager** and logon using your system user account.
- Select your person employee object (created in an earlier lab).
- Click **Assign Identity Manager application roles** from the Tasks list.
  - Custom → Dialog and schema extensions
  - Identity Management → Business roles
  - Identity Management → Business roles → Administrators
  - Identity Management → Employees
  - Identity Management → Employees → Administrators
  - Click **[Save]**
- Check your success in **Manager**.
  Start or restart **Manager**.
- Sign in with your identity (Authentication method: **Employee (role based)**).
  - Menu Database/Close Connection
  - Menu Database/New Connection
    - Authentication method: ***Employee (Role based)***
    - User: ***[Your users central account]***
    - Password: ***[Your user password]***
      (May be, you forgot to set the password in previous labs, and you now can't login. Sign in again using your **system user**
      and step to your employee. On the **Miscellaneous** tab set the **Central user password** to **I.4Madmin** and try to login again. Using the training password is not mandatory but may help debugging your system by the trainer.)
- Select Business Roles from the main menu and select Functions

Lab Exercise Complete

Lab Exercise: Using the System Debugger

Exercise Overview

In this lab we cover how to use the System Debugger and you write your first VB.NET code. Remember writing code is usually the last option when customizing parts of Identity Manager. Nevertheless, in a standard Identity Management Project, it is common to do this. If this is your first time working with Visual Studio, this small lab should show you some basics on how to handle such a piece of software coding.



What you need to know

- You should have the images open and running for this lab.

User credentials required for this lab

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin

Estimated Time To Complete This Lab: **45 minutes**

Lab Exercise

Writing and Testing a Simple Script

> **NOTE:**
> System Debugger is not a standalone tool. It is a development solution for .NET that requires a Developer Environment before starting. Therefore, Visual Studio .NET is installed on the admin workstation. This solution can also work with Microsoft Visual Studio Code or other development tools, for example SharpDevelop.

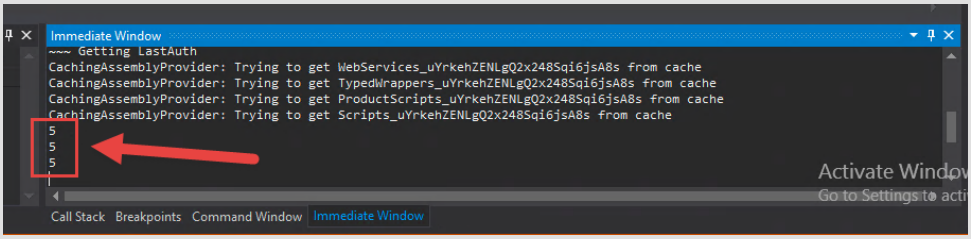
- Open **System Debugger** from the admin workstation Start Menu (All Apps → One Identity → System debugger). If you get prompted to select a Visual Studio version select the most current one.
- Press **F5** to open the System Debugger dialog and connect to the data base. If the front-end want's to start in elevated mode, accept.
- In **System Debugger** select **Create New Script** in the **Script** menu.
- Select the option **Public Sub** because we don't need to return a value this time and
  - Name the new procedure: ***[Prefix]_PoorCalculator***.
- Click **[Ok]** and **[Ok]** again.

- At the End of the file **CustomerScripts.vb** find code looking like **“Public Sub [Prefix]_PoorCalculator()”** and **“End Sub”**.
- Replacing the line **'Enter script code here'** with the following code. We suggest typing the code into the editor just to get a feeling for the editor and its functions.

```
    Dim var1 As Integer   Dim var2 As Integer   Dim result As Integer   Dim StrResult As String
```

- Press **F5** to start **System Debugger** and connect to database.

NOTE:
→ Normally you work with database objects. In this simple script, connecting the database is not necessary, but cannot ignored.
→ The script name **[Prefix]_*** is not typical for a custom script. In a real-world scenario, you will use CCC_* to identify custom scripts. In this training we must account for the fact that several people are developing a similar script which makes it necessary to name the script with a personal prefix. ** PLEASE DON'T DO THIS IN A NORMAL PRODUCTION IAG PROJECT, YOU WILL LOSE YOUR CHANGES ON A PRODUCT UPGRADE! **
→ The script execution may give you the feeling that nothing happened. Please carefully watch the Immediate Window to find a result.



- Click on **[Run]** and look at the Output Window where you can see the output of the result.
- Use menu **Library/Exit** (optionally you can use the “X” on upper right) to close System Debugger.
  Please have in mind, you can only edit scripts in this solution if the System Debugger tool it's closed (no code gets executed).
  If it looks like you can't edit script code close this tool first.
- Make some code changes to get other results and to modify the output string.
  - Change the values for var1 and var2.
  - Test your script again (F5).

NOTE:
Debug.Print() prints a string into the **Immediate Window**. You can combine strings and/or string variables with a “+”.
For example: “My result is: “+ StrResult.
Try this in your code.

- After modifying the code start System Debugger to test it. Open System Debugger as described above.
  - Test the **[Run]** button on the **System Debugger** main form
  - Test the **Run in debug method** option. Step through the script using **“Debug/Step into”** option **[F11]**.
- Insert a breakpoint into the script (click into the column in front of a line number) and test without **Run debug method** again.

NOTE:
In this exercise we want to implement a tiny calculator for +, -, *, /, ^ and ! (factorial) including basic error handling. Typically, the instructor will start the exercise (first steps) with you. Then you should try to finish the script on your own. If you run in trouble use the sample listing for help. This exercise is to give you an idea how to use Visual Studio and to work with the debugger and breakpoints. In addition, you should get an idea of how to test a script.
We suggest that beginners implement everything except factorial and more advanced coders use their experience to implement the factorial component.
→ There is not one correct solution. As long as the script calculates correctly and is stable, your solution is correct. If you need some code samples, remember there is the internet with many examples for VB.net that are only a simple

search away.

- Start implementing what you have learned, following your instructor's advice.
- After writing the code press F5 and see what happens.
- Use Run debug method and Breakpoints to debug your script

Lab Exercise Complete

EXAMPLE Code Listings

This is just an example. Any other working version showing the right results, is a valid sulotion as well.

Poor Calculator

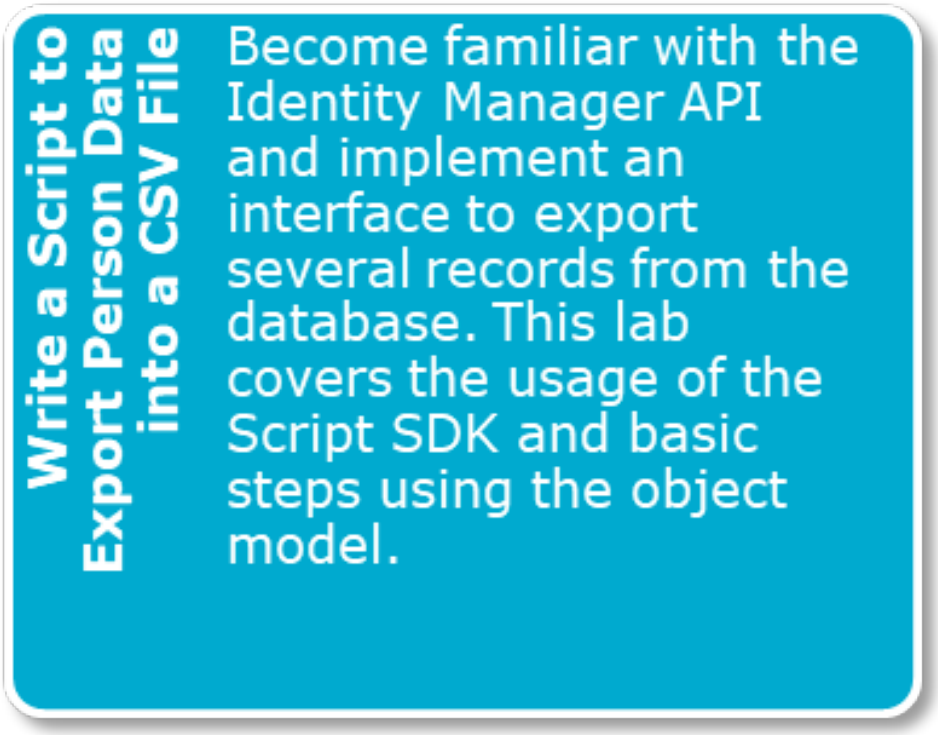
```
   Public Sub HRA_PoorCalculator () '   INITIAL Version   'Variable   Dim var1 As Integer = 2   Dim
```

Advanced Calculator

```
   '--> Calculator for +, -, /, *, 1, !   Function HRA_PoorCalculator(var1 As Double, var2 As Doubl
```

Lab Exercise: People Export via Interface Script (IM-BTS-02)

Exercise Overview



There are many ways to export data from One Identity Manager. This scripting option would only be used in exceptional cases in a production system, but this lab provides a good example of how to work with the Identity Manager API and the Script SDK based on a simple use case. How to use the API and SDK is the focus, rather than the specific use case example.

What you need to know

- You should have the images open and running for this lab.

User credentials required for this lab

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin

Estimated Time To Complete This Lab: **45 minutes**

Lab Exercise

Writing a Script to Export Person Data into a CSV File

NOTE:
Depending on the programmer skills in this training audience this could be a demo (development by the instructor in front of the class) or a real development exercise. Please discuss the approach with your instructor. To copy and past the demo script is not realy helpful because this exercise should beside the development capabilities show three facts:

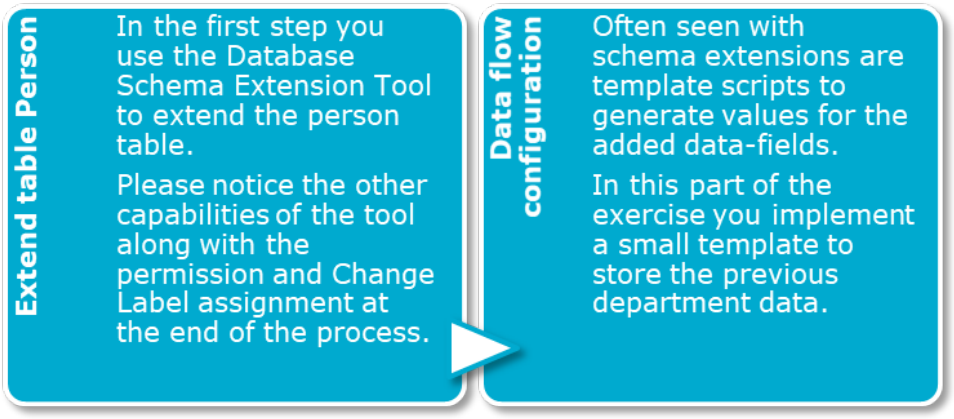
→ Code development is most flexible but most expensive (time consuming) from a project perspective.
→ Successful code development needs more additional skills than any other configuration in Identity Manager.
→ dentity Manager is equipped with a verry rich featured, verry professional API can be used additional to all the from Microsoft available API features.
All people in an IGA project should be aware of this. This makes this lab suitable and helpful for any kind of audience in introduction courses! To become a coding professional, you need much more experience as only these two small scripts in IM-BTS-01 and IM-BTS-02.

- Open System Debugger and create a new script and
  - name it: ***[Prefix]_Export_Person***
  - Script type: ***public sub***
- Start scripting with your instructor and then finish the script by yourself. If you need inspiration, look at the file **HRA_Export_Personen.vb**.
- Use **System Debugger** as you did in the previous lab.
- Use the following hints:
  - Actual time in VB: ***now()***
  - Use the Identity Manager script SDK as often as possible.
  - Query a single value: ***Session.Source.GetSingleValue(Of String)("UID_ADSContainer", strUID_ADSContainer, ValType.String)***
    or in a second step use dictionaries.
  - Collection objects (a hand full of data) are not created with properties (only PK and display)
  - Single objects are huge but get created with all properties.
  - To generate a time stamp, use an existing vb.net function from the script library containing **"isodate"** in its function name.
- After the script is tested and functioning use **[F5]** to run the System Debugger again.
  - Make sure your script is selected.
  - Use the correct option from the script menu to save the script in the database.

Lab Exercise Complete

Lab Exercise: Schema Extension (IM-DSE-01)

Exercise Overview



In this lab you extend the Identity Manager schema and data flow to store additional content.

What you need to know

- You should have the images open and running for this lab.

User credentials required for this lab

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin

Estimated Time To Complete This Lab: **20 minutes**

Lab Exercise

Extend table Person

> **NOTE:**
> Schema extensions must be planned carefully. Extensions cannot be automatically revoked as this can cause data loss within the database. Manual revocation is permitted but must also be carefully planned.

- From Launchpad start **Change & Extend → Extend the One Identity Manager Schema**.
  - Click **[Next]**
  - Click **[Next]**
  - Select **Extend Table**
  - Click **[Next]**
  - Select table: ***Person***
  - Click **[Next]**
  - Click on the new icon to add a column
    - Column Name: ***[CCC_]UID_PrevDepartment***
      (the prefix is automatic, do not retype it)
    - Select: ***Foreign key column***
    - From table: ***Department***
    - Click **[Ok]**

- Enter the **Display name** for the new column: ***Previous department***
- Click **[Next]**

> **NOTE:**
> We must add the schema extension to a permission group to enable users or administrators to use the extension.

- In the first field select CCC_Dialog_And_Schema_Extensions granting read and write permissions.
- Click [Next]
- Add new change label [Prefix]_WebDevelopment_Schema

> **NOTE:**
> Please remember the [Prefix]_ is your personal prefix. Even in a real project we recommend using a personal prefix for a change label to identify the developer of the feature tagged with this label. This allows the Change manager to identify the developer later for questions.

- Click **[Next]**
- Click **[save to file]**

> **NOTE:**
> This is done for documentation purposes. It is heavily recommended to keep accurate documentation of all schema extensions made to your IAG project. Note as well the Attach statements to an existing file option at the bottom left of the form.

- Click [Next]
- Click [Yes] in the popup to make the changes in the database. Possibly followed by a [Next] if you see active and disappearing DB calculation steps.
- Click [Yes] in the next popup to compile the database.
- After the compiler completes, wait for DBQueue Processor to finish.

- Click [Next] and [Finish] to complete the wizard.

Data flow configuration

> **NOTE:**
> The new field we just added to the schema contains the name of a person's previous department. We will use a template for populating this value.

- In **Launchpad** start the main configuration tool (Designer). If Designer is already open please reopen the connection to ensure the new schema extension is loaded and recognized.
- Select **One Identity Manager Schema** from the Main Menu.
- Expand **Tables/Type: Table** from the navigation pane.
- Select the **Person** table.
- Click on **Show table definition** in the **Tasks** list
- Select the new column: ***CCC_UID_PrevDepartment***.
- Select the **Value calculation** tab in the **Column properties**.
  - Overwrites Checked
  - Enter the following in field Template:

```
$UID_Department[C]:bool$ then     Value = $UID_Department[o]$   end if
```

- Commit to database using a NEW change label ***[Prefix]_WebDevelopment***

> **NOTE:**

You cannot use the **[Prefix]_WebDevelopment_Schema** change label because you must insert schema extensions first before you start inserting features based on these extensions. We heavily recommend creating at least two (or more) transports for a maintenance window. The first transport contains only the schema extensions. The second (and/or other) transport contains all other changes.

- Compile the database using the default settings.
- To get the right permissions to work with employees as a role-based authenticated person (employee) we must first assign some Application roles to our employee which we created earlier.
- In **Manager** select **Employees** in the main menu and **Employees** in the **Navigation** pane.
  - Select [your employee] you created in an earlier lab (the one showing your name)
  - Select **Assign One Identity Manager application roles** from the **Tasks** list.
  - Ensure the following roles are assigned to [your employee]
    - Base roles/Administrators
    - Base roles/Employee Managers
    - Identity Management/Employees
    - Identity Management/Employees/Administrators
    - Click **[Save]**
  - Wait until DBQueue Processor ended the calculation by cleaning the DBQueue you can watch in Jobqueue Info.

NOTE:
Now we want to test this new template using Manager. We suggest not using Launchpad to start Manager this time. Use the Start menu instead. If Manager is already open, please close and re-open the front-end to ensure all new software assemblies are loaded.

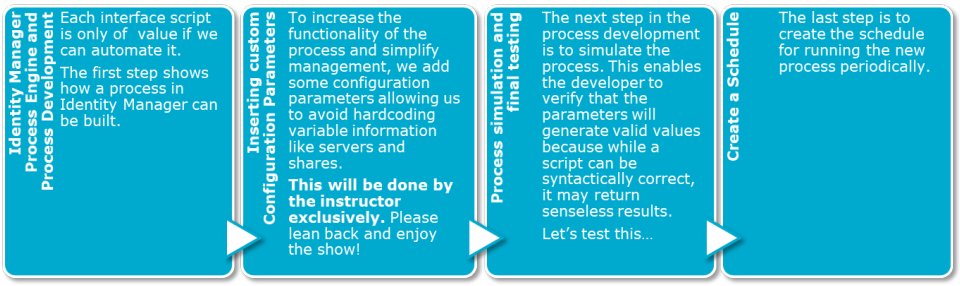
- Start Manager and logon using your employee. Therefore, you must use Employee (role based) authentication. Remember in test mode no password is needed (if you are a fast worker, it is possible to login before 9d. happened. Please ensure that all calculation jobs are done).
  - Go to the main data page for your employee account.
  - You should now see a new tab in the main data called **Custom**.
  - Select the Organizational tab, memorize the current **Primary department** value and change **Primary department** to: ***R & D\Engineering\Argentina***.
  - And **Primary cost center** to ***50\50100\50100010***
  - Select the **Address** tab and change **Primary location** to ***AR - Buenos Aires - Combatiente de Malvinas 3239***
  - Select the Custom tab and view the value of the **Previous department** field.
- Click **[Save]**

NOTE:
Now you can start booking flights because you moved your employee to Argentina. Be careful, this virtual company is not reimbursing expenses 😊.

Lab Exercise Complete

Lab Exercise: IM-BFP-01 Create a Fulfillment Process

Exercise Overview



In this lab you automate a person record export. You will create and test a short process and learn how to use the Process Editor. The lab covers how to use the process engine which is common for many customizations. The lab helps show the difference between the scripting and the process engine allowing you to understand the effort required for each customization method.

What You Need To Know

You should have the images open and running for this lab.

User credentials required for this lab

Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin

Estimated Time To Complete This Lab: **45 minutes**

Lab Exercise

Automation Prerequisites

- Open **SQL Server Management Studio (SSMS)** and run the contents of the following file. It is in the associated lab folder on you T: drive.
  - IM-BFP-01__Script_PersonData_for_Export.sql

NOTE:
This displays the data that we will export on a regular schedule through a process.

Results | Messages

	FirstName	LastName	Department	Location
1	Noslab	Hughes-Cunningham	Production\Manufacturing\Zimbabwe	ZE - AVONDALE HARARE - FLAT NO 4 11 CERES RD 11
2	Tash	Bonnin	Accounting & Finance\Recruiting\Argentina	AR - Buenos Aires - Combatiente de Malvinas 3239
3	Chak-Hong	Jone	Accounting & Finance\Accounting\Australia	AU - Bayswater VIC - 5 - 7 Waldheim Rd.

Once again, this csv example could be a real-world example, but this type of export is just one type of exporting csv data and not the golden way to solve this type of problems. In this lab we like to introduce the Process engine on an easy-to-understand example.
To export csv data in detail you can use:
SQL Statement
Typical for data exported once, mainly unconverted and on an admin basis. This is for project developers, not only because project member shouldn't have plain SQL access to productive environments.
VB.NET script
Used if the data to export needs a lot of polish and must be converted. Expensive way, because you need to develop code first.
Export data in the Manager or Web Portal

Very easy and most user-friendly way to export csv data typically used by the business or operations.
Export using Processes
Fast way implementing simple (or complex) exports being recurrently needed. This way can as well be used to automate Export VB.NET scripts.
Exports using Synchronization Editor
A more expensive way to implement a recurring export often used if associated imports exist. An implementation takes more time as for example to create a process. Using this type of export, you can use the full power of the Synchronization engine.
Finally
This essay is the last chance to understand: “You are working with a solution Framework”! There are typically many ways to reach a goal. Which way you choose is based on a business case and your experience to solve a problem by considering technically and organizational facts. This means there is often not a golden way to do something. There is always a most suitable way for a specific situation instead. Therefore, you have always the same set of instruments:

- Process Engine
- Script Engine
- Synchronization Engine
- Direct Data Access (SQL)
- Front ends

Relax your eyes, now we start with lab again!

- Use **Launchpad** to open **Designer** and logon using your system user account.

NOTE:
It is not recommended to hardcode values for variable content such as server names, shares, and accounts in your scripts because you must update the process each time these variables change. Use configuration parameters instead of hardcoded content.
If you work together with your colleagues in the same environment, one person should create these configuration parameters for all to use. After this is done, everyone must restart **Designer**.

- Open the Configuration Parameters section in Designer
  - Create the following configuration parameter structure (be careful the root parameter Custom already exist): ***Custom -> Export -> Person -> FilePath***
    - Use a right click on the parent parameter to create a child parameter.
    - Ensure each node in the structure is checked as enabled.
    - For the FilePath parameter enter a value of ***\\IAMS10\training\Export\Person***
    - For all other (structuring) parameters in the structure enter a value of ***1***
  - In parallel to the Filepath parameter insert a parameter ExportCondition
    - For the ExportCondition parameter enter a value of ***isexternal=0***
  - Commit to database with a new change label [Prefix]_ExportEmployee
  - From the Database menu re-connect to the database

NOTE:
This is done so the system recognizes the newly created configuration parameters. It must also be performed on systems not used to create the parameters.

Developing the Process

NOTE:
In this lab you can select one of two options.
Lab-option 1: If you created a [Prefix]_Export_Person vb.net script in a lab before, we recommend automating this script. You can also take a template script from lab folder IM-BTS-02.
Lab-option 2: Use the standard csv export process step component to automate the export which is a bit more realistic but does not use results from an earlier lab.
Technically you learn the same, so the choice is up to you.

- Select **Process Orchestration** from main menu and **Custom process** from the navigation pane.
- Click on **Create a new process** (In Tasks may be minimized on right).
- Select the process (shape) and configure (**Process properties**):
  - >Name: ***[Prefix]_Export_Person 2 CSV***
  - Table: ***Dialogschedule***
  - Remarks: ***Your name, Actual Date***
  - Description: ***Exports identities to a CSV file.***
  - Add a Pre-script for generating to speed up process generation.
    Lab-option 1

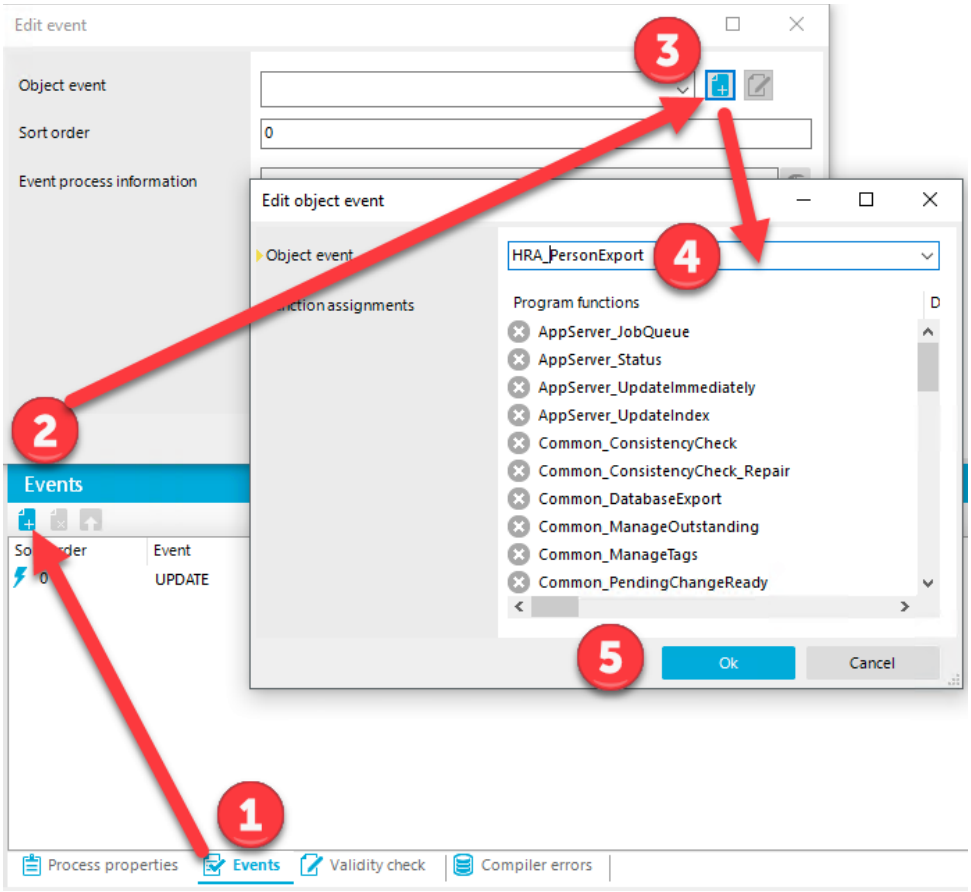
```
'--> For higher performance of the process, calculate or load values only once
 '    esp. configuration parameters or often used variables
Values("ExportPath") = connection.GetConfigParm("Custom\Export\Person\FilePath").ToString(
```

    Lab-option 2

```
'--> For higher performance of the process, calculate or load values only once ' esp. confi
```

NOTE:
It is helpful to use the editor which is displayed by clicking on the small icon in the lower right corner of the input box ( ).
→ Click on the save icon to close the form.
The Pre-script generates values needed in many places generating the process steps values to be developed next. The idea behind is, to perform a calculation, database access, etc. only once instead of for each process step or step parameter separately. In an example we are on the way using the created configuration parameter values in many process steps and process parameters which could be a database query/access for each usage.
With this Pre-script we will not query the same values again and again. Instead, we are querying the values in this Pre-script and assign the values to variables can be used in the following process steps and step.
You need two different Pre-Scripts because in Option 2 a time stamp variable is needed which is covered by your automated VB.NET script of Option 1.
For this purpose of this script, you may use any table as Base object. This is typical for all processes that don't depend on data events like UPDATE, INSERT and DELETE of a specific record. Also, you must use a self-defined event. Later, you will create a schedule to raise this event. We recommend always using the same table to make identifying the scheduled processes easier (for example **DialogSchedule**).
Next step is to create an event. Database record-based processes uses often Standard events like INSERT, UPDATE, DELETE. This means, a process will become generated on the basis of a changed record. In this case we like to run the process based on a schedule. Therefore, exist no associated data change and because of this we need to define a new event, could be called later by a schedule.

  - Add an Event. Select tab Events.
    - Click the blue Insert icon on left upper of the Events form
    - Click again the Insert icon of the sub-form, right beside **Object event**.
    - Object Event: ***[Prefix]_PersonExport***
    - Click **[OK]**
    - Click **[OK]**



- Insert 4 new process steps.

> **NOTE:**
> The fastest way to develop a process is to configure the same parameter for each process step starting with the first property form. This means starting over with the first step for each of the next configuration steps. This helps to ensure no parameter is missed and speeds up the process development significantly.

- Beginning with the first step, name your process steps:
  - [Step1]: ***[Prefix]_Export Person Data to CSV***
  - [Step2]: ***[Prefix]_Check if Archive Exists***
  - [Step3]: ***[Prefix]_Create Archive Folder***
  - [Step4]: ***[Prefix]_Move Export Result to Archive***
- Beginning with the first step, connect your process steps together (Click and hold a parent shape bottom icon () and move to the child element and release the mouse button):
  - [Step1]: ***connect to process header***
  - [Step2]: ***green connected from [Step1]***
  - [Step3]: ***red connected from [Step2]***
  - [Step4]: ***green connected from [Step3]***
  - [Step4]: ***green connected from [Step2]***
- To get a bit more structure in your process click the Folding rule ( ) icon in the top icon bar.
- Beginning with the first step, configure on tab General the Process task for each:
  - To follow Lab-option 1
    [Step1]: ***Script Component / ScriptExecSingle***
    To follow Lab-option 2
    [Step1]: Script Component / CSVExportSingle
  - [Step2]: File Component / Exists
  - [Step3]: File Component / CreatePath
  - [Step4]: File Component / Copy_Universal

NOTE:
The component gives each process step a functionality like creating a path or moving a file.

- Beginning with the first step, configure the Description for each:
  - [Step1]: ***Export of person data subset to csv file***
  - [Step2]: ***Check if archive sub-folder exists in folder export***
  - [Step3]: ***Create missing archive folder in folder export***
  - [Step4]: ***Move export- and log-file to archive folder***

NOTE:
Descriptions get displayed like process step names. To configure something helps understand what the process is doing later in the day.

- Select the Generation tab
- Beginning with the first step, configure for each process step:
  - Server function: ***SQL processing server***

NOTE:
The Identity Manager service is the executing instance of this specific step. AD operations for example should be done by the Active directory queue (in this environment IAMS01) and so on. In this specific case each service could execute a script or remotely access files. This means we can use every Job service in the system to execute our jobs. We decide to use the SQL processing server (IAMS02).

- Select the Error handling tab
- Beginning with the first step, configure the Error Handling:
  - [Step1]: ***check: Stop on errors***
  - [Step2]: ***check: Split processing***

NOTE:
During execution process steps can fail. In this case the red ending of the process step will be used to determine the next step to continue, and an error message is written into the associated Job service log. The Error handling tab allow to tweak this behavior a bit:
-> **In [Step1]** we stop the process where it fails and let the operator decide what's to do. Such process steps are known as FROZEN JOBS if they fail.
-> **In [Step2]** an error message appears in the Job service log if a folder did not exist. This is truly not an error, it is a decision and operators don't like to get a heart attack only because the process runs in another split.

- Select first Process Step and Parameters tab
- Select [Step1] and configure parameters:
  Lab-option 1:
  - ScriptName: ***Value = "[prefix]_Export_Person"***
    (if you use the from the lab folder imported script it's **HRA_Export_Person**)
  - Use a double click into the grey X icons to activate ParameterValue0 and ParameterValue1.
  - ParameterValue0: ***Value=Values("ExportPath").tostring()***
  - ParameterValue1: ***Value=Values("Condition").ToString()***

  Lab-option 2:
  - Double click on the grey X to enable the following parameters
    - Header
    - LineDefinition
    - OrderBy
    - WhereClause
  - Configure the following parameters:
    - FileName: ***Value = string.Format("{0}\Employees_{1}.csv",Values("ExportPath").tostring(),Values("TimeStamp").tostring())***

- ObjectType: ***Value="Person"***
- Header: ***Value="Firstname;Lastname;Department;Location"***
- LineDefinition:
  Value="$$Firstname$$;$$Lastname$$;$$FK(uid_department).fullpath$$;$$FK(uid_locality).fullpath$$"

NOTE:
For this parameter you may use the $ notation for the column references. Because the references are contained in a string (between the double quotes), each $ reference must be masked by a second $ (i.e. $$Firstname$$)

  - OrderBy: ***Value = "internalname"***
  - WhereClause: ***Value = Values("Condition").tostring()***

-> END of Lab Option 2

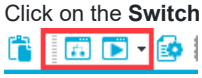
- Select **[Step2]** and configure Parameters:
  - FName: ***Value=string.Format("{0}\Archive",Values("ExportPath").ToString())***
- Select **[Step3]** and configure Parameters:
  - DirPath: ***Value=string.Format("{0}\Archive",Values("ExportPath").ToString())***
- Select **[Step4]** and configure Parameters:
  - Activate parameter FileList and Options.
  - DestDir: ***Value=string.Format("{0}\Archive",Values("ExportPath").ToString())***
  - SourceDir: ***Value=Values("ExportPath").ToString()***
  - FileList: ***Value="*.csv *.log"***
  - Options: ***Value="/mov"***

NOTE:
To configure the Parameters is an important part of each process design. Please have in mind that the list of parameters available is depending on the Process task you selected before. Changing this Process task will automatically drop all process step parameter configurations made before.
It is recommended to look into the shipped processes to get an idea how parameter values look like. Additionally, you can find help in Designer and in the Identity Manager manual.

- Check your process and correct errors if they appear.
  - Click **Examine process for errors**
  - Click **Compile process**

NOTE:
Both options are icons in the top icon bar.
If errors are displayed, double-click on the error message to highlight the associated process step in the editor. Check your process step and the process step parameters to resolve the problem and re-test.
The first check allows you to find all misconfigured parameters and options.
The second check validates the vb.net syntax.

- Click on the **Switch to simulation view** icon in the Designer toolbar



  - Click **[Next]** to begin stepping through the wizard.
  - Select the event (there should only be one displayed).
  - Click **[Next]**
  - Select one of the displayed objects (it doesn't matter which)
  - Click **[Next]**
  - Click **[Next]**
  - Click **[Next]**
  - Click **[Next]**

- Click **[Finish]**

> **NOTE:**
> The process is formatted in a lighter blue indicating it is in simulation mode. In simulation mode, the parameter list shows the calculated values rather than the script information we saw while in edit mode. Have a look at all the calculated values. Do they make sense? Calculations can be successful but the values they return will not automatically lead to a making sense result. This is often only something a project developer can decide. You can toggle between the two modes using the corresponding icons in the Designer toolbar.

- >Last step is to save changes. Click on Commit to Database and store the process to the database using a change label:
  - LabelName ***[Prefix]_PersonExport***
  - Description ***Person data export to csv***
- Now compile your Identity Manager database (use **Designer**).

Create a Schedule

- In **Designer** select **Process Orchestration/Process** automation from the navigation pane.
- Right click the main form and select **Add process plan**.
- Configure the process plan:
  - Name: ***[Prefix] Export Person to CSV***
  - Event: ***DialogSchedule/[Prefix]_PersonExport***
  - Description: ***Runs a Person sub-set export to a csv file on a half hourly schedule***
  - Condition: ***Name='[Prefix]_Export Person To CSV'***
- Hit the New icon next to “Activation schedule” and configure the schedule

  - Name: [Prefix] Export Person To CSV
  - Enabled: checked
  - Time zone: [Select your time zone]
  - Unlimited duration checked
  - Occurs Every Minute
  - Repeat every 30 Minute(s)
  - Click “Ok”.
- Commit changes to the database using your Change Label.
- Re-select your schedule and click on the Play icon in the top icon bar.
- Follow the process in Jobqueue Info and review the result in the File System.

Lab Exercise Complete

Lab IM-ASE-01 - HR Data Import Automation

Exercise Overview

In this lab you will create a recurring import using Synchronization Editor from the scratch without using any templates. This lab is mainly developed for students with a good basic understanding of Identity Manager.

NOTE:
To get this lab working several data prerequisites are needed.
They will be imported at the begin of this lab and need to depend on data was imported before. Especially for Greenfield environments (installation courses) several steps are necessary to generate import data. There is a bit voodoo behind, be careful.
Nevertheless, it is not necessary to understand all steps to go during the prerequisite section, but these are good examples and templates how to generate data based on other data as well.

What You Need To Know:

- You should have the images open and running for this lab.
- You need lab folder IM-ASE-01 on your T: drive open and ready to use

User credentials required for this lab:

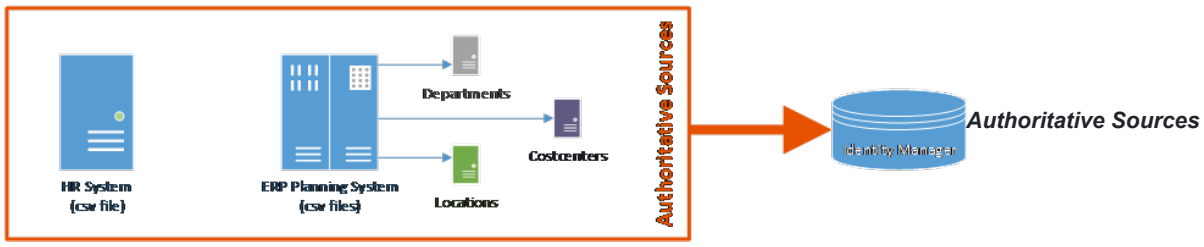
Affected Machines	IAMW01
AD login account	
Username	IAM\administrator
Password	I.4Madmin

Estimated Time To Complete This Lab: ***90 minutes***

Data model and interface planning

We like to import several data resources from external systems. To simulate these systems, we will use CSV (**C**omma **S**eparated **V**alues) files. It is only another system connector to configure in Identity Manager to access another system type. All other steps will be the same.

NOTE:
Any system connection an IGA project needs a proper and details interface and data flow planning. We can't go through all steps, meetings and all the research necessary. Please find in this section more a minimum summary as a real fine concept.



This import includes

- Locations (1)
- Cost centers (2)
- Departments (3), (5)
- Employees (4)

The import order is given in parentheses. In case of the departments, it is necessary in step (3) to import Departments and in step (5) to correct department managers depending on employees imported in step (4).

Further requirements

- This import resources are authoritative, there is no way back into the connected systems. The import will always correct Identity Manager data (authoritative source).
- Each import file holds the complete set of data. Missing records needs to be deleted in Identity Manager, except person records which will be deactivated.
- ERP-Data records can be deactivated if a flag is set in the import files.

Interface description

HR Import

IM Column	CSV Column	Notes
Person.DeactivationEnd	Temporary Leave End	
Person.DeactivationStart	Temporary Leave Start	
Person.EntryDate	Joining Date	
Person.ExitDate	Leaving Date	
Person.FirstName	First name	
Person.Initials	Initials	
Person.IsInActive	Deactivated	
Person.IsVIP	Important Manager	
Person.LastName	Last name	
Person.MiddleName	Other name	
Person.NameAddOn	Name addon	
Person.PersonalTitle	Working Title	
Person.PersonnelNumber	Employee ID	Primary Key (Unique)
Person.SubCompany	Unit	
Person.Title	Title	
Person.UID_Department	Department	
Person.UID_Locality	Location	
Person.UID_PersonHead	Manager	
Person.UID_ProfitCenter	Cost center	

Department Import

IM Column	CSV Column	Notes
Department.DepartmentName	Department	Primary Key (Unique)
Department.IsInActive	Deactivated	
Department.ShortName	Abbreviation	
Department.UID_Locality	Location	
Department.UID_ParentDepartment	Parent Department	
Department.UID_PersonHead	Department Manager	
Department.UID_PersonHeadSecond	Department Manager 2	
Department.UID_ProfitCenter	Costcenter	

Costcenter Import

IM Column	CSV Column	Notes
ProfitCenter.AccountNumber	Costcenter	Primary Key (Unique)
ProfitCenter.IsInActive	Deactivated	
ProfitCenter.ShortName	Abbreviation	
ProfitCenter.UID_Department	Department	
ProfitCenter.UID_Locality	Location	
ProfitCenter.UID_ParentProfitCenter	Parent Costcenter	
ProfitCenter.UID_PersonHead	Costcenter Manager	
ProfitCenter.UID_PersonHeadSecond	Costcenter Manager 2	

Location Import

IM Column	CSV Column	Notes
Locality.Building	Building	
Locality.City	City	
Locality.Ident_locality	Location	Primary Key (Unique)
Locality.IsInActive	Deactivated	
Locality.LongName	Location Name	
Locality.PostalAddress	Additional address	
Locality.Room	Room	
Locality.ShortName	Abbreviation	
Locality.Street	Street	
Locality.UID_Department	Department	
Locality.UID_ParentLocality	Parent Location	
Locality.UID_PersonHead	Location Manager	
Locality.UID_PersonHeadSecond	Location Manager 2	
Locality.UID_ProfitCenter	Costcenter	
Locality.ZipCode	Zip Code	

Lab Exercise

Data Prerequisites

- Until now, we used a simple view working with our Synchronization projects. Building such projects without templates (sync project from scratch) needs a more detailed view. Open **Synchronization Editor** and sign in with your system user.
- From the **Database** menu select **Settings**
  - General/Enable expert mode: ***activate***
  - Click **[OK]**

> **NOTE:**
> We like to import several data resources from an external system. To simulate the external system, we will use a CSV file resource. This import should become a combined import for identities (HR-Import), Departments, Cost centers and Locations (ERP-Import). Because of the nature of our foreign system (CSV) we can't use any template. We need to build anything from the scratch. This affects our data resources as well, especially in case to avoid deleting data which is in the current database. Additionally, we need to enrich the existing data first.
>
> In a first step we need to assume that there was an employee import before. As a primary key, personnel numbers are set (typical for an HR system). Let's generate as a prerequisite personnel number in Identity Manager NOT exist in a Greenfield environment (installation course).

> **WARNING:**
> **The following steps are only for Installation courses (Greenfield environments). Starting with a Full installed environment you can continue with step "FULL INSTALLED" (red message below).**

- From lab folder IM-ASE-01 open (double click) files:
  - **Calc_PersonnelNumbers_for_Greenfield.ods** → Libre Office - Calc
  - **IM-ASE-01_SQL-Snippets.sql** → SQL server Management Studio (SSMS)
  - **Temp_Import_SQL_SetPersonnelnumbers.sql** → SSMS
- In SSMS select tab **IM-ASE-01_SQL-Snippets.sql** and scroll down to Section: **Prepare data in Greenfield**.
  - Execute the following statement in SSMS, Result to Grid **[Ctrl]+[d]** mode (execute the statement using **[Ctrl]+[d]** followed by **[Ctrl]+[e]**

```
select uid_person, centralaccount, internalname, PersonnelNumber from person
where internalname not like '%Service%'
order by NewID()
go
```

    - Copy the first three columns.
- Switch to Libre Office - Calc
    - Paste the values into the first 3 columns of the spread sheet. Select cell **A1** and click **[Ctrl]+[v]**.
    - Have a look at the formula in column Update Statements and ensure it points to values in the same row.
    - Select and copy all values in column Update Statements.
- Open Microsoft Notepad.
  Paste the values into an empty document and copy the values again (in notepad **[Ctrl]+[v], [Ctrl]+[a], [Ctrl]+[c]**. This is needed to correct the line endings.
- Switch to SSMS
    - Select tab **Temp_Import_SQL_SetPersonnelnumbers.sql**.
        - Paste all values in (copied from notepad).
        - Ensure the query is targeting database **IAMDB**.
        - Execute the file **[Ctrl]+[e]**
    - Switch to document **IM-ASE-01_SQL-Snippets.sql**
        - In Section: **Prepare data in Greenfield** execute select statement:

```
select internalname, personnelnumber from person order by 2
```

        - Check the result list. Beside some service identities each person should have a personnel number now.

> **NOTE:**
> After having proper personnel numbers it is time to get some department managers assigned.

- From your lab folder open document Calc_Assign-Departmentmanager_2_Departments.sql.
    - Ensure the query is targeting database IAMDB.
    - Execute the file (Ctrl+e)
    - You can check your work using the following SQL command (part of the lab SQL snippets):

```
select
  d.departmentname,
  h1.internalname as Manager,
  h2.InternalName as Deputy
from department d
  join person h1 on d.uid_Personhead = h1.uid_person
  join person h2 on d.uid_personheadsecond = h2.uid_person
```

> **NOTE:**
> Now it's time to export our data source files.

- Close all Libre Office-Calc, notepad and SSMS and skip the next step "Before we can..." and it's subs. Continue with "Open Manager...".

> **WARNING:**
> **This is the starting point in a FULL INSTALLED training environment (non-installation courses)**

- Before we can start there might be some data clanking necessary. Please use Manager to correct the following values if necessary.
    - Costcenter: S&M - Retail Sales - AU → set value Costcenter to 30350060
    - Costcenter: R&D - IT Support - IL → set value Costcenter to 50220210
    - Costcenter: R&D - IT Support - DE → set value Costcenter to 50220150
    - Costcenter: R&D - IT Support - US → set value Costcenter to 50220050
- Open **Manager** and sign in with your **system user**.
    - Select Employees from main menu Employees.

- Click **Export Results** from the list menu icons  ***Manager Snapshot***
- In the open export form, there are two buttons allow to load and store a predefined export configuration. Click on the open configuration dialog ().
- Load configuration **Def_Employee_Export.xml** from your lab folder (T:\courses\IdentityManager\Labs\IM-ASE-01). This is a load from file action.
- Click the Preview button on top of the second half of the export form and have a look at the data browser ().
- Click the export button and export the data into a file named: **Data_Employee_Import.csv**. We recommend to store the data in a folder on your desktop.
- Repeat the same steps accordingly for Departments, Cost centers and Locations. You should end up with 4 exports:
  - Cost center: ***Data_Costcenter_Import.csv***
  - Department: ***Data_Department_Import.csv***
  - Employee: ***Data_Employee_Import.csv***
  - Location: ***Data_Location_Import.csv***
- With all files exported open file **Planning_Affected_Columns.ods** in Libre Office - Calc and all the above-mentioned csv files in Notepad++.
  - Take the file header line from the spread sheet **CSV-IM-Mapping** according to the export and replace the origin header line (4 files in total).
  - Save and close the csv documents
  - Close the spread sheet

NOTE:
Especially step h. seams to be a bit more nonsense as usual. The idea is the following:
We like to create a Synchronization project later on, as realistic as possible!
In real life your csv file header will never be similar to your database column names. Additionally, some of these exported header lines contains odd character complexing things. -> Because of this, we change the header lines!

- Copy these files into a folder T:\Import\Authoritative-Data. If this folder doesn't exist create the missing parts.

INFO:
If files already exist, please delete the complete old content first.

Create a CSV import connection using Synchronization Editor

NOTE:
All the prerequisites lead to the following situation. There are authoritative systems delivering data via csv files and these data is now available in T:\imports\Authoritative-Data. Let's assume they came from HR. In the next step we will create a Synchronization project using Synchronization Editor, which handles all these files at once.

- Open Synchronization Editor, for example using Launchpad (**Configure a new synchronization project**).
- Click **[Start a new synchronization project]** (the big green on your screen)
  - Click **[Next]**
  - Select CSV Connector from the list and click **[Next]**. Have also a look at the many connectors available (just for info).
  - For a CSV import we don't need a **Remote connection server**. Click **[Next]**.
  - Select **Create a new System connection** if prompted and click next.
  - Until now there is no CSV import. Let's create a new CSV system. Select Create new CSV system and click **[Next]**.
  - Select and open file: T:\Import\Authoritative-Data\Data_Employee_import.csv.
  - In the **Load CSV file** form, you can keep defaults and click **[Next]**.

NOTE:

A file encoding using utf-8 works in many cases. There are people around the world making the language **Invariant Language (invariant Country)** a good choice. **Read-only access** for importing an authoritative source makes sense.

- In form **File structure**
  - Increase the **Number of lines in header** to 1.
  - Keep **Columns identified by Delimiter**
  - Click **[Next]**
- In from **Line structure** keep defaults and klick **[Next]**
- In form Display information
  - Display pattern `%First_Name% %Last_Name% (%Employee_ID%)`

NOTE:
In a csv file all columns contain string values per default. This should not wonder; It is a text file. You can save a lot of time if convertible columns getting their right Datatype assigned in the connector. Nevertheless, if you can't be sure about the data quality you can as well convert this data later by creating the mappings. Of course, assigning the data types earlier will minimize the work later.

- Select column **Temporary_Leave_End** and select Data type: ***DateTime***
- Select column **Temporary_Leave_Start** and select Data type: ***DateTime***
- Select column **Joining_Date** and select Data type: ***DateTime***
- Select column **Leaving_Date** and select Data type: ***DateTime***
- Select column **Deactivated** and select Data type: ***Boolean***
- Select column **Important_Manager** and select Data type: ***Boolean***
- Select column **Employee_ID** and activate flag **Key column**
- Click **[Next]**
- In form Define CSV system file correct the file path to: T:\Import\Authoritative-Data\HR_ERP_Import.csvsys if needed and click **[Next]**

CAUTION:
You have not finished the CSV file system yet. Click on the tiny link on form **Create system connection…** named **Add another CSV file**. (If you missed this task, edit your connection and start with load CSV system file)

- Add your **Data_Location_Import.csv** like the first one and click on link **Add another CSV file**.
  - Remember and configure all forms similar to the person import down to **Display Information**.
  - Display pattern: ***%Location%***
  - Key column: ***Location***
  - Select column **Deactivated** and select Data type: ***Boolean***
  - Activate “Expert View”, select column **Parent_Location** and activate flag: **Hierarchical sort order**.
  - Click **[Next]** and select link **Add another CSV file** again.
- Take file **Data_Costcenter_Import.csv** This time we need to take care of a hierarchy.
  - Remember and configure all forms like the person import down to **Display Information**.
  - Display pattern: ***%Costcenter% - %Abbreviation%***
  - Select column **Costcenter** and activate flag **Key column**.
  - Select column **Deactivated** and select Data type: ***Boolean***
  - Select column **Parent_Costcenter** and activate flag **Hierarchical sort order**. Yes you need to activate Expert view first)
  - Click **[Next]** and select link **Add another CSV file** again.
- Take file **Data_Department_Import.csv** and configure similar until you reach form **Display information**.
  - Display pattern: ***%Abbreviation% - (%Department%)***
  - Select column Deactivated and select Data type: ***Boolean***
  - Select column Abbreviation and activate flag: **Key column**.
  - Select column **Parent_Department** and activate flag: **Hierarchical sort order**.
- Click **[Next]**
- Click **[Finish]**. Now the schema gets loaded.
- Click **[Next]**

- There will be no template available. Click **[Next]** having Create blank project selected.
- In form **Create synchronization project…**
  - Display name: ***HR and ERP Data - Authoritative source***
  - Scripting Language: ***Visual Basic .Net***
  - Description: ***Import of employees, departments, locations and cost centers***
  - Click **[Next]**
  - Click **[Finish]**
- Now let's test the data sources. In your synchronization project select **Target system**.
- Click button **[Browse…]**.
- Click on each entry in **Schema types** (this means as well the already selected first entry). There should be a list of objects displayed for each schema type in the **Result list**. You should not see any error message.
- If an entry returns with an error message, please read the message carefully. Typically, there is either data to correct or you need to upgrade your configuration. To upgrade your configuration, close the data browser and click on **[Edit Connection]**. After all is done, please don't forget to click **[Update schema]** to make your changes becoming true before you use the data browser again.
- Click **[Close]** to close your Schema browser.
- If all Schema types returns a list of entries. **[Commit to database]** using an appropriate change label (you have to create first, drop down the **[Commit to database]** box).
  - You like to save without data encryption ([Yes])
  - You don't want to compress your schema, because you need to configure the IM side and mappings. Take the default [No]

> **NOTE:**
> To create connection parameters can help you later to reuse Synchronization projects. Not very typical for a csv import of ERP and HR data but we like to show how to get variables. This task is formative but not really needed.

- Flip down the box **Connection parameters** and convert parameter SystemFile to a variable.
- Now we need to connect to the Identity Manager Database (second part of the connection). Select **One Identity Manager connection** and click on **[Edit connection….]**
  - Click **[Next]**
  - Use a **Direct database connection**.
  - Click **[Next]**
  - The connected SQL server gets pre-configured. Click the **[Test]** button and answer with **[OK]** on a success. Typically, there should not be an error message but use the following data if you need to correct an error:
    - Server: ***iams02.iam.corp***
    - Windows authentication: **unchecked**
    - User: ***svc_1im_sql***
    - Password: ***I.4Madmin***
    - Database: ***IAMDB***
  - Click **[Next]**
  - We currently don't use a **Private key**. Click **[Next]**.
  - No additional options to set. But click on the "?" icon and read the text carefully. This info is good to know. Keep the option unchecked and click **[Next]**.
  - Click **[Finish]** and if prompted click **[OK]**.
- Use **[Browse…]** to ensure you are properly connected to the database.
- Flip down the box **Connection parameters**.
  - Convert parameter Server password and Server user name to a variable.
  - **[Commit to database]** using an appropriated change label

Create data mapping and matching

> **NOTE:**
> We did the first steps and connected our target systems. Now it's time to create data mapping and data matching. This is what the wizard did before using standard target systems. And this is what typically eats the most amount of development time.

- In **Synchronization Editor** in the currently loaded **Synchronization project** select **Mappings**.
- Add a new mapping using the "+" icon underneath **Mappings**.
  - Mapping name: ***HR - Employees***
  - Mapping direction: ***One Identity Manager***
    This import is an import of authoritative data, and it is not allowed and necessary to correct data in the CSV files. Because of this we set a clear Mapping direction here.
  - One Identity Manager Schema class: ***Person (all)***
  - Target system schema class: ***Data_Employee_Import (all)***
  - Click **[OK]** and click **[Next]**

> **NOTE:**
> For many standard target systems exist a template which makes an import configuration easy. You saw this in previous labs. For a csv import or for a customer specific database such templates can't exist and because of this we need to build from scratch. Nevertheless, there exist a similarity wizard may help us selecting corresponding properties. Because we exported the csv data from Identity Manager previously, this wizard may reach 100% mapping accuracy which is very unrealistic, because of this we changed the header lines of our csv files (you may remember some voodoo above).

- Select **Create mapping rules dynamically based on similarity**. And click **[Next]**.
- The slider allows you tweak the level of similarity. High (full right) means the column names of both systems need to match to 100%. Low (full left) means there could be some equal character in both names available. As the description says **High** less mappings, less errors, **Low** many mappings but more errors.
  - Keep the default and click **[Next]**.
  - Open document **Planning_Affected_Columns.ods** from your lab folder IM-ASE-01 and select tab **CSV-IM-Mapping**. Something like this is typically part of your fine concept and it will help to double check selections.
  - Position the spread sheet and the wizard on your screen to allow you looking at both at the same time. This timetable **HR Import** is needed.
  - As you can see there are suggestions available for:
    - Firstname
    - Initials
    - NameAddOn
    - Title

      All other ideas or suggestions are not helpful. Ensure that checkmarks in column Selection are only set for the fields above and click **[Next]** and [Finish].
- Now we need to map all other not automatically mapped fields (in middle) from the target system (csv) on right with Identity Manager columns on left. Therefor we can get suggestions from our spread sheet (fine concept).
  - Drag **Cost_center** on right and drop it on **Primary cost center** on left. A **Property Mapping Rule Conflict Wizard** is getting started. The system knows that the values in column **Cost_center** are not fitting to the values in database column **Person.UID_Profitcenter** and tries to help us to find a solution.
  - Select the first choice and click **[OK]**.
  - Now we can select the column from **Profitcenter** need to be used (via column) in this case it is **Profitcenter.Accountnumber**.
    Click **[OK]** and accept the warning about uniqueness (this message tells us that we need to take care on data uniqueness in the data source or we will get error messages if the data is not correct).
  - As a result, of this selection the system is now creating a virtual property **Person.VRT_UID_ProfitCenter** which contains the **uid_profitcenter** based on the **accountnumber** we get from our import.
  - Have a look at the configured values and expand Filter
    System filter: ***1=1*** Click **[OK]**.

> **NOTE:**
> These columns are not marked as unique columns because of this it is necessary to set a system filter. In our example we know that values in these columns will be unique so we can set a condition which is always true.

  - Select field **Cost_center** on right and notice highlighted fields **Primary Costcenter** and Value resolution for **Primary cost center** on left.

NOTE:
As you have seen all property captions on the Identity Manager side are displayed using friendly names. For beginners this could be helpful but for people need to plan and develop with Identity Manager it is essential to know about the database schema. Because of this we will now switch to the technical display mode

- From the **database** menu select settings and enable switch **Enable the technical view** after program start.
- Press **[OK]** and have a look at the left side of the **Synchronization Editor**. All properties are named using the technical (column) names now.
- Continue the configuration we started above.
  - Map column **Deactivated** with column **isinactive**.
  - Map column **Department** with column using via column **Department.Shortname**. This works like the cost center column above. Don't forget to set the system filter as well.
  - Map column **Employee_ID** with column **PersonnelNumber**.
  - Map column **Important_Manager** with column **isVIP**.
  - Map column **Joining_Date** with column **EntryDate**.
  - Map column **Last_name** with column **lastname**.
  - Map column **Leaving_Date** with column **exitdate**.
  - Map column **Location** with column **uid_locality** using via column **Locality.Ident_Locality**.
  - Map column **Manager** with column **Manager** using via column **UID_PersonHead.personnelnumber**
  - Map column **Other_name** with column **MiddleName**.
  - Map column **Temporary_Leave_End** with column **DeactivationEnd**.
  - Map column **Temporary_Leave_Start** with column **DeactivationStart**.
  - Map column **Unit** with column **SubCompany**.
  - Map column **Working_Title** with column **PersonnelTitle**.
- The column to identify records (the unique key or primary key) in this import is the Personnelnumber (Employee_ID) of a record. This is what we use to match a csv record with an Identity Manager record. Select the line **PersonnelNumber ← Employee_ID** and click the **Convert selected property mapping rule into an object matching rule** icon ( ). Answer the question with **[yes]**. This is because we don't have uid columns gets filled by the system automatically. Remember we are mapping our objects using text columns. This means these values need to be mapped during the import and are used additionally as matching rules which is **NOT** the default option (of the question).

NOTE:
Now everybody will understand why Synchronization templates are such a great idea and building Synchronization projects from the scratch takes a lot of time. But hey, we need to configure database mappings and matchings for Location, Department and Cost centers. Before we can continue. Please have a closer look into the planning spreadsheet as well.

- Create another mapping for Department using the Navigation pane and configure like Employees. → Matching on Abbreviation/Shortname (Primary Key)
- Create another mapping for Cost center using the Navigation pane and configure like Employees. → Matching on Costcenter/Accountnumber (PK)
- Create another mapping for Location using the Navigation pane and configure like Employees. → Mapping on Location/Ident_Locality (PK)

Create Configuration Workflows

NOTE:
Right now, the system knows which systems to connect and which columns/properties to use and which data to map between those. In the last steps we configured rules to identify and match the same records on both sides of the synchronization project. Before we can start we need to define which steps the synchronization need to run through and in which order. This is what's called SYNCHRONIZATION workflows (please keep them separate from fulfillment workflows = processes and approval workflows).

- Switch to main menu **Workflows** and click the **Create a new empty workflow…** button ( ).
  - Display name: ***ERP Resource import***

- Description: ***Import of departments, costcenters, and locations***
- Click **[Ok]**
- Underneath **Workflow** click the **Add a new step…** button ( )
- Name: ***Location***
- Mapping: ***ERP - Locations***
- Synchronization direction: ***One Identity Manager***
  (Note: Remember there is only one way for authoritative resources)
- Exception handling: ***Continue on error***
  (Note: In a csv import there could be odd lines. Not a good idea to break the whole import if just one line shows bad data).
- Select tab Processing

NOTE:
The expert view, we configured above, allows us to see this extended view.

- Data set A1: Represent the set of unchanged data.
- Data set A2: Represent the set of property changes of existing records.
- Data set B: Represent the set of records only existing in the source
- Data set C: Represent the set of records only existing in the target

Now the behavior for each sub-set of records can be configured. Because there will no changes on the source side (authoritative resource) all changes needs to be configured on the side of Identity Manager (the left side of the form).

- For set A1 we need to configure nothing because existing records with the same properties needs not to be handled.
- For set A2 an update of changed source properties in Identity Manager needs to be initiated. Great, this is already pre-defined.
- For set B an insert of new records in Identity manager is needed and again pre-configured.
- For set C we don't want to delete records immediately. A better option is to mark them as outstanding and let the Synchronization admin decide what's to do.
- For set C, switch box Delete to **MarkAsOutstanding**
- Have a look at the other tabs (we don't need to configure), if you like.
  Click **[Ok]**

- Add a workflow step for cost centers like the one created above.
- Add a workflow step for departments like the one created above.
- Add a workflow step for identities like the one created above.

Configure Startup Configuration

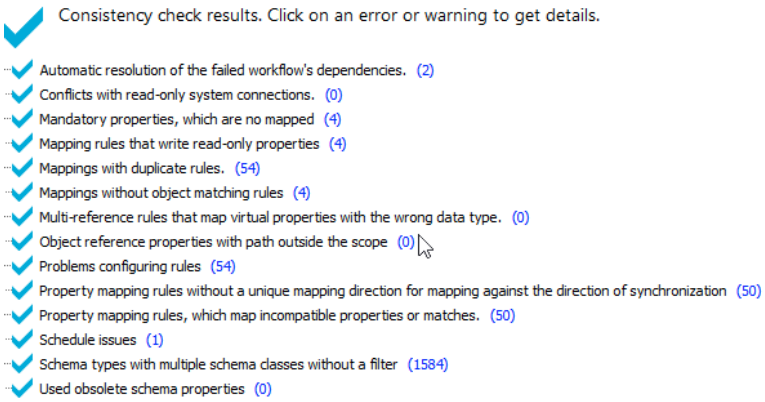
- Create a **Start up configuration**. Select the same named entry in main menu **Configuration** and click the add icon.
  - Display name: ***ERP and Identity Import***
  - Workflow: ***ERP resource import***
  - Variable set: ***default variable set***
  - Have a look at all other tabs but keep defaults
  - Click **[Ok]**
  - Click **[Create schedule…]** (may be you need to switch to form **Start up Configurations** first)
    - Name: ***ERP + Identity Synchronization***
    - Unlimited duration: ***set***
    - Occurs: ***Daily***
    - Start time: ***02:00***
    - Repeat every: ***1***
    - Click **[Ok]**
- Click **[Commit to database]** using your created Change label.

Test a new Synchronization Project

- To test and log all changes we will make during synchronization we need extended logging. Switch to **One Identity Manager connection** and click **Setup…** .
  - Activate **Create synchronization log**

- Activate all logging options.
  (This is not a great idea for a production environment - too many log messages creating performance loss - but for testing this is the right choice. We don't need to change logging on the side of our CSV connector. Nothing will happen there.)

- First, we will check the complete project. Switch to the tab **Start page**.
- On right, there is a **[Verify project]** button needs to be clicked.
- The result should look like in the picture below. If this is not the case, click on an error message and read all the message text carefully. Verry often you get es well hints to solve the problem.
- Change and verify the configuration until you reach the goal. Your trainer will help you if necessary.



- Now switch back to your **Workflow** (double-click). Here we will generate an execution plan first to test our workflow and steps ( ).
  - Ensure there is no error message.
  - Have a look at the report. Everything looks like expected.
  - Close the report
- Switch to your Startup Configuration and click **[Simulate…]** and confirm with [Yes].

> **NOTE:**
> Start with the first page of your Synchronization log. You should see:
> - Performance warning about extensive logging - great!
> - Messages about not executed phase 2 Synchronization steps. This means changes happens by assigning resources may be available after a first import run. These is not getting considered in simulations (to many spaces necessary or to complicated to handle during simulation). This means these changes are gitting dropped.
> - Executed synchronization steps for each type of objects (**Location, Department, Costcenter, Person**)
> - Executed synchronization post-processing step
> - About 9 or less Person objects to be marked as outstanding (should become deleted)
>   **- Why? -**
>   The marked as outstanding people are not part of the HR import file. Easy to verify. This is the reason to mark them as outstanding (which allows an IGA admin later to handle (delete, recreate) them later. To exclude these objects, we will create a filter to exclude them from the synchronization.

  - Because we don't want to deactivate all our identities with an empty value for Person.Exitdate and Person.DeactivationStart, we create a scope first to test this for one single record. To identify the record first, open your filed **Data_Employee_Import.csv** in folder T:\Import\Authoritative-Data.
  - Choose a record you like to test with and note the (record number = line number -1) to consider the header line
  - Switch to Synchronization Editor, main menu Configuration and select Target System.

> **NOTE:**
> As you can see there are two scopes available:
> - Reference Scope: This is the scope to be used to resolve object references.
> - Scope: This is the scope to limit objects to be handled.
>
> To get a better idea what's the difference here an example: In an Active Directory you like to synchronize just one AD container with all of its objects. Your scope will limit the FQDN to this AD container. This AD container may

contain AD groups referencing AD accounts outside this AD container. Because of this you can for example set a Reference scope to the whole domain.
→ **Result:**Only objects of this AD container will be handled during synchronization, but all references of these handled objects can be resolved or changed properly because the reference scope allow to resolve references cross the AD domain.

However in our csv example each of the scopes can be used because we talk about a flat file but we suggest to use the Scope.

- Click **[Edit scope]**.
  - Grep the form top frame above the word condition using a left mouse click and move the top border a bit to the top to get more space.

  - Select **Data_Employee_Import** in section Scope and select tab Object filter in section **Condition**.
  - Click **[Add condition]**
  - Click on **Variable** and select **RowID** from the list.
  - Click the tiny input box right beside **RowID** and select Text box and enter your Record number (noted above). In case the text box is already selected you can't see it in the selection list. If not, the text box should be the first entry.
  - Use icon Use text mode to see the condition in clear text ( ). The one or other might lice this input mode more as the graphical way.
- Switch back to Configuration/Start up configuration and run a simulation again.

NOTE:
Now your report shows 1 changed object and more as 1000 objects marked as outstanding. This is not too bad because there will be only changes on one object (the one you selected above) and all other objects will become added to the list of outstanding objects. This mark could easily be removed in Manager without further changes. In our lab we will implement some improvements first.

Final Test

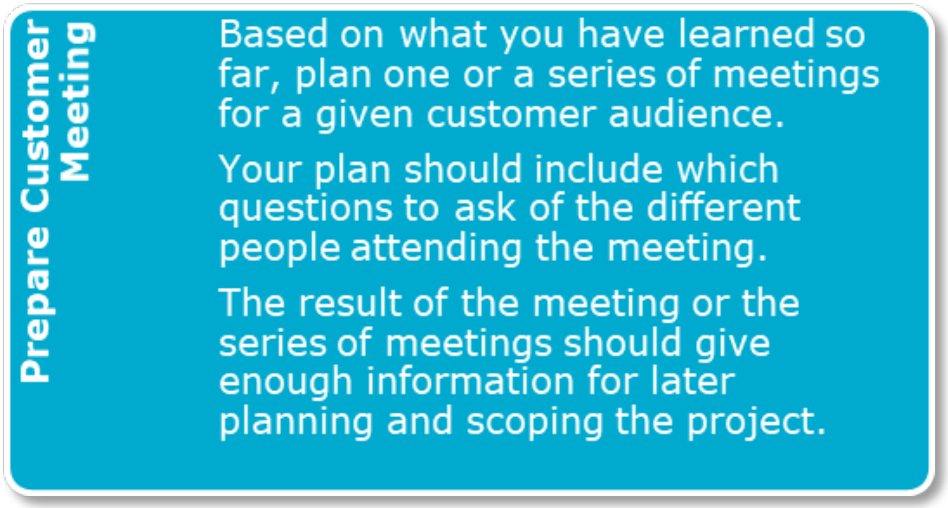
NOTE:
To run a final test you can remov scope and click **[Run]** instead of **[Simulate…]** on the **Start up configurations** page.
You will not learn something more, but you will see the system working. It is up to you if you like to perform this. However, have in mind depending on your current configuration you may generate several outstanding objects.

Be aware, even if you not run a synchronization now you schedule will do this like configured.

Lab Exercise Complete

Lab Exercise: Initial Project Meeting and Structure Planning

Exercise Overview



Interactive Group Exercise - Planning Identity Manager Deployments
In this lab you gain hands on experience planning Identity Manager deployments

What you need to know

- This is a group exercise.
- Work in a team of 3-4 students.
- Select a group leader to present your recommendations to the rest of the class.
- Use the provided flip charts and markers to document your plan.

Estimated Time To Complete This Lab: **30minutes**

Lab Exercise

Prepare Customer Meeting

You are the lead consultant on a Identity Manager deployment project for a company called Identity and Access Management Inc.

You are about to meet with company representatives to begin the planning of the deployment. The customer representatives include an IT Manager, the HR Manager and the Company Compliance and Security Officer (CISO).

- Identify all the potential issues and questions you need to discuss with the company reps to make recommendations for the way Identity Manager should be deployed and configured. Ensure you cover all aspects of the project planning and organize you preferred meeting structure.
- Chart your approach and have your group leader present your ideas to the rest of the class when it comes time to take up this lab.

Lab Exercise Complete

Lab Exercise: Hardware Sizing and Project Scoping (IM-DPL-02)

Exercise Overview

Interactive Group Exercise - Planning One Identity Manager Deployments
In this lab you gain hands on experience planning One Identity Manager deployments.

What you need to know

- This is a group exercise.
- Work in a team of 3-4 consultants.
- Select a group leader to present your recommendations to the rest of the class.
- Use the provided flip charts and markers to document your solution.
- Please read the exercise carefully to identify all important facts.

Estimated Time To Complete This Lab: **60 minutes**

Lab Exercise

Hardware Sizing / Project Planning and Scoping

After your meeting with the company representatives, you learn that the HR Manager was the initiator of the project, but also has sponsor funding from the Company Compliance Officer (CISO).

The primary goal of the HR Manager is to automate the management of contractor and employee resources. Responsible managers require an interface for requesting a contractor be added to the system. Once a new contractor is approved, they are to be added to the Contractor Management System and provisioned with an AD user account.

You also learn that the scope of the project has expanded to provide an Administration interface for all IT Administrators and Managers with appropriate delegated rights based on their job function. You also learn the project now has visibility by the corporate CEO who may consider adding their SAP systems to the project depending on the success of this initial phase of the implementation.

IAM Inc. is a company with 5000 employees and an equal number of contractors.

They run an Active Directory/Exchange network with approximately:

- 5300 Employee user accounts
- 5700 Contractor user accounts
- 320 Service accounts
- An unknown number of disabled accounts
- 1800 groups (security and distribution groups)

They have a single data center located at their head office where 2800 employees and 900 contractors work.

The Data Centre is also the location of the central Help Desk.

The remaining employees and contractors are split between 5 regional offices and several small one or two person sales offices throughout North America.

Employees work in their native local language which could be English, French, or Spanish.

The customer is also running LDAP (Open DS) and several database applications, including the primary HR System and Contractor Management System.

The customer wants to define roles within Identity Manager that provide a clear separation of duties between employees and contractors. They also want to automate the provisioning of AD User Accounts, Groups and Distribution List membership.

The Compliance Officer has joined the project and is providing funding to include compliance audit reporting and the implementation of attestation schedules to meet their internal and regulatory compliance requirements. Contractor attestation is to be performed by each responsible manager.

The HR Database application is considered the authoritative source of all employee data.

The Contractor Management System is used for tracking contractors in the IAM Inc. environment. This is a legacy application for IAM Inc. and requires updates when contractors join the company.

In your group, develop an architecture design for the company's Identity Manager deployment. Make sure you identify:

- Hardware Structure
  - The number and type of Servers required
  - The optimal location for each Server
  - High-level configuration information
- Develop a rough project plan for the implementation, ensuring you identify key activities and milestones. If you make any assumptions in your planning, make sure you include them in your solution. Divide your project into phases if necessary.
- Your group should be prepared to present your solution when the lab is taken up for review.

Lab Exercise Complete
