Microsoft Entra Connect

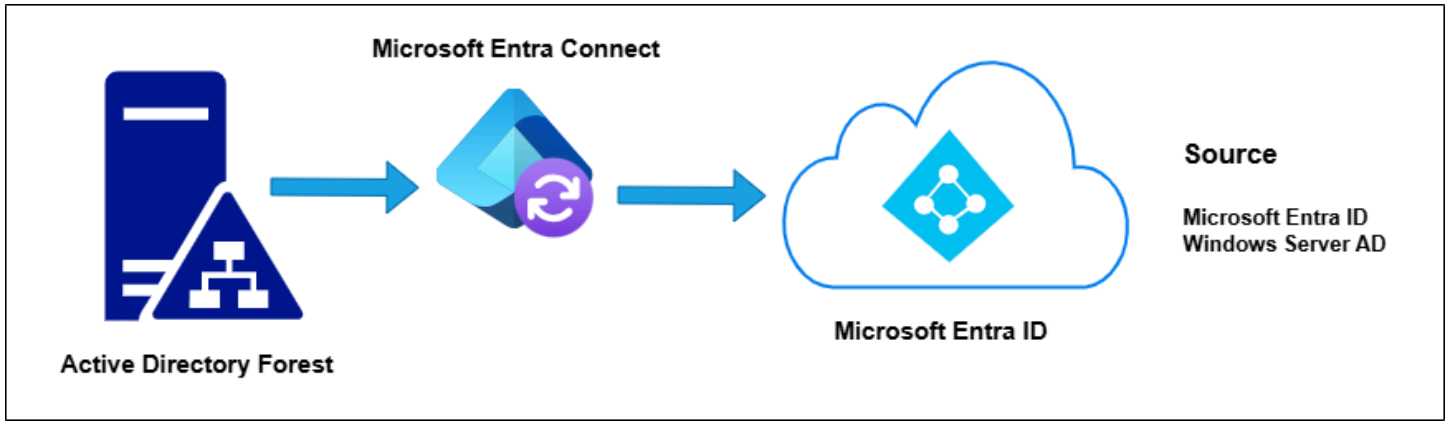
Topics:

- Entra Connect Architecture Fundamentals
- Sync Process Phases
- Types Of Filtering
- Synchronization Rule Editor
- Sync Rule hierarchy
- Connector Configuration & Attribute Flow Mapping

Entra Connect Architecture Fundamentals

Microsoft AAD Connect (Now Microsoft Entra Connect) is a hybrid identity bridge tool that synchronizes your on-premises Active Directory (AD) with Microsoft Entra ID (formerly Azure AD).

It enables a single identity for users across on-premises and cloud environments, allowing them to use the same credentials to access resources like Microsoft 365, Azure, and other cloud apps

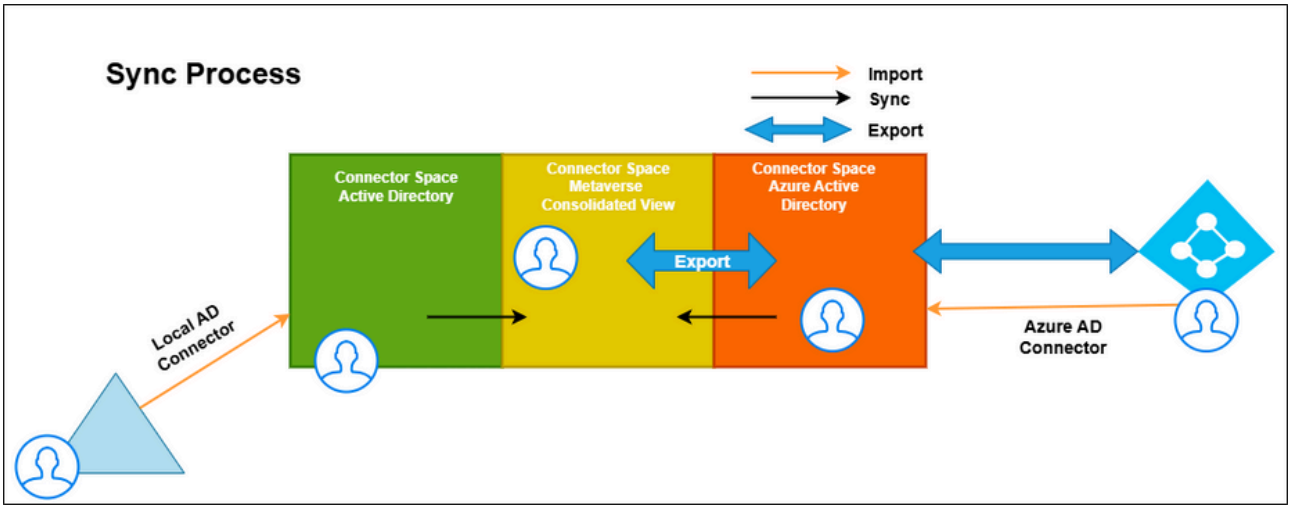


- The Users, groups & Devices on On-prem can be synced to Entra ID by using AAD Connect tool. The tool has its own inbuild logic and database on behalf of which, one consolidated data image is maintained all across the connected data sources.
- The connected data source here means either the local AD connector source or Entra ID connector source.
- There is a periodic communication that always happens between these connector sources and AAD Connect. The APIs that are responsible for this are called Connectors.
- With the help of Local AD connector, AAD Connect pulls information from On-prem AD and with the help of Entra ID connector, the same information is exported to Entra ID.
- Connectors are basically a medium on behalf of which AAD Connect, as an application tool communicates with the connector sources.
- The database of AAD Connect has three logical sub-divisions , which are called as connector space of Local Active Directory, Connector space of Azure Active Directory and Connector space of Metaverse; where you can see the consolidated view of an object that has to be synced to the cloud.
- There are two types of processes to sync an object: Delta Sync process and Full Sync process. In Delta sync process, only the attributes that are updated, deleted or removed i.e. only the changes that are done to the objects are queried. In Full sync process, the entire objects and the respective attributes are being queried.

Sync Process Phases:

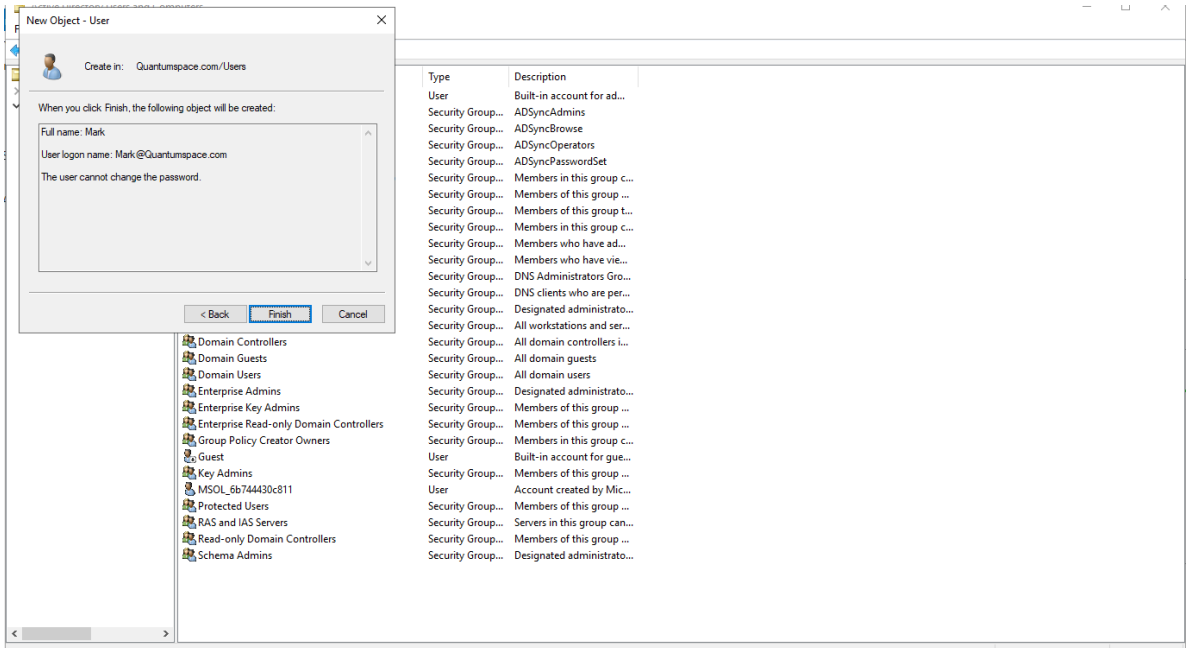
- Both Delta and Full sync process has three phases; Import, Sync and Export.
- The very first process which will be initiated will be the import on the local AD connector, so that the information from DC can be saved to the connector space of the local AD.

- Similarly, next process will be an import from Entra ID to the AAD connector space.
- Once the import is complete from On-prem as well as from Entra ID, a sync process will happen between the local AD connector space and Metaverse space. This will create an image or replica of the object in metaverse with a flag ‘Add’, this means there is a new user object created which needs to be exported to the cloud.
- The next process will be a sync from AAD connector space to metaverse; incase any new change in the objects of Entra ID reported, will be synced in the metaverse.
- The last process is the export which will be done on the AAD connector space. This will create an image of the object(to be synced to cloud) in connector space of AAD and will export it to Entra ID.
- When this whole process is completed, an acknowledgement flag of waiting export confirmation can be seen. This means that though information is being replicated AAD connector space to Entra ID, but the particular information is not yet acknowledged that it has been imported to Entra ID.
- In order to verify if the object is being successfully imported to Entra ID, an import can be run on the AAD connector that will remove the awaiting export confirmation flag from the particular object.



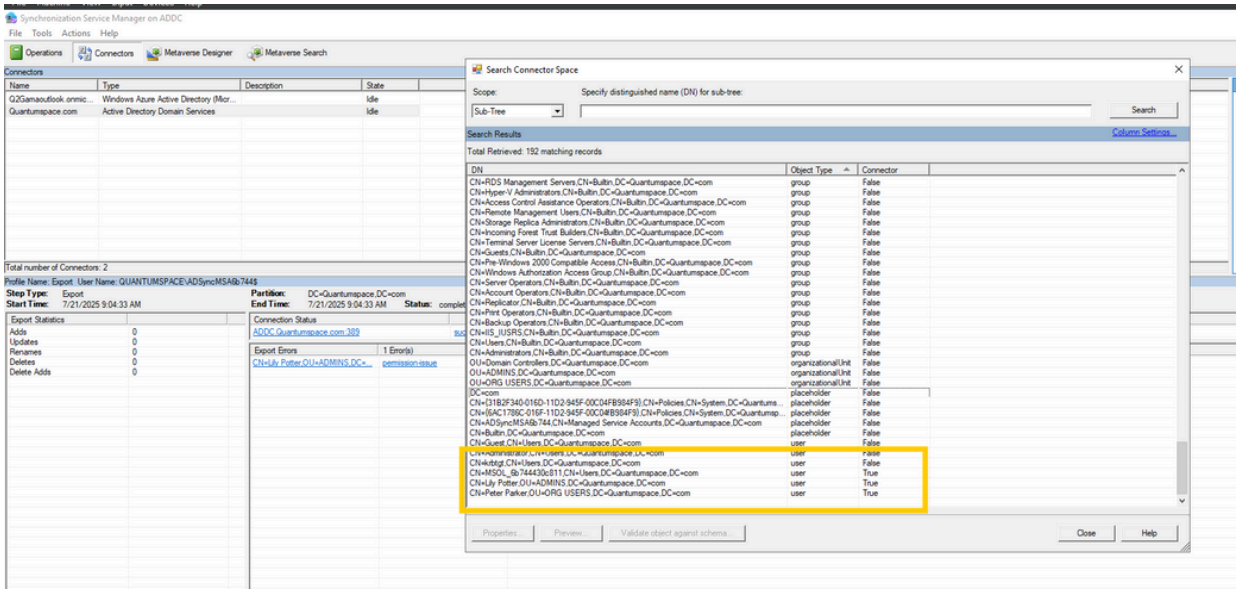
Example:

- Create a new object in local AD, go to AD users & Computers and create a new user: Mark. All the OUs in this demonstration are synced with Entra ID, there has been no filtering done here.

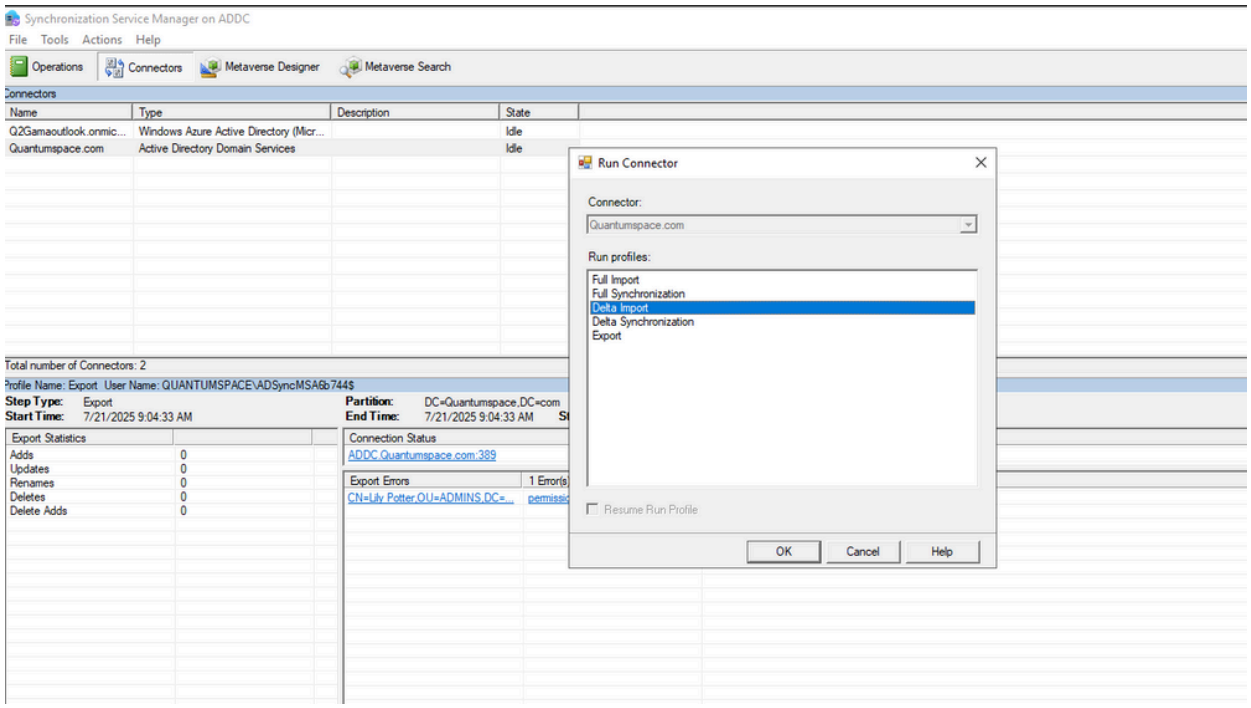


- Go to the Synchronization service manager > Connectors> right click on local domain connector> search connector space> Object type

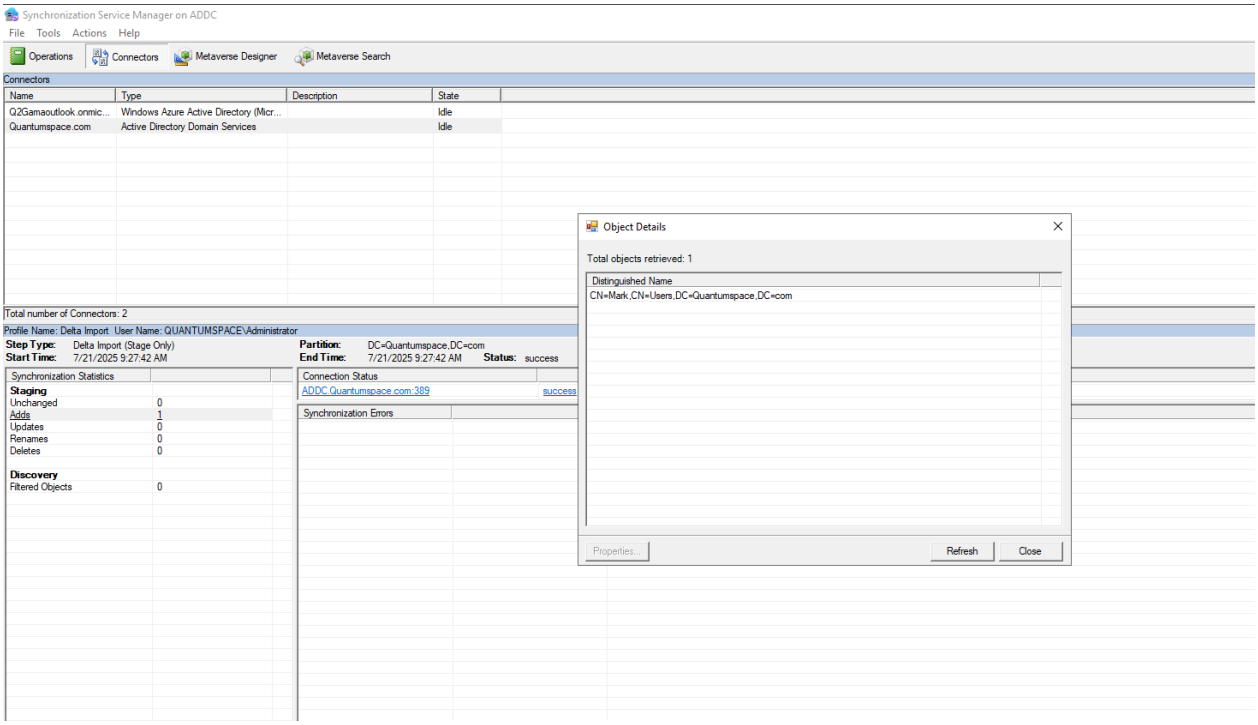
Here in the local AD connector space new user: Mark will not be visible yet.



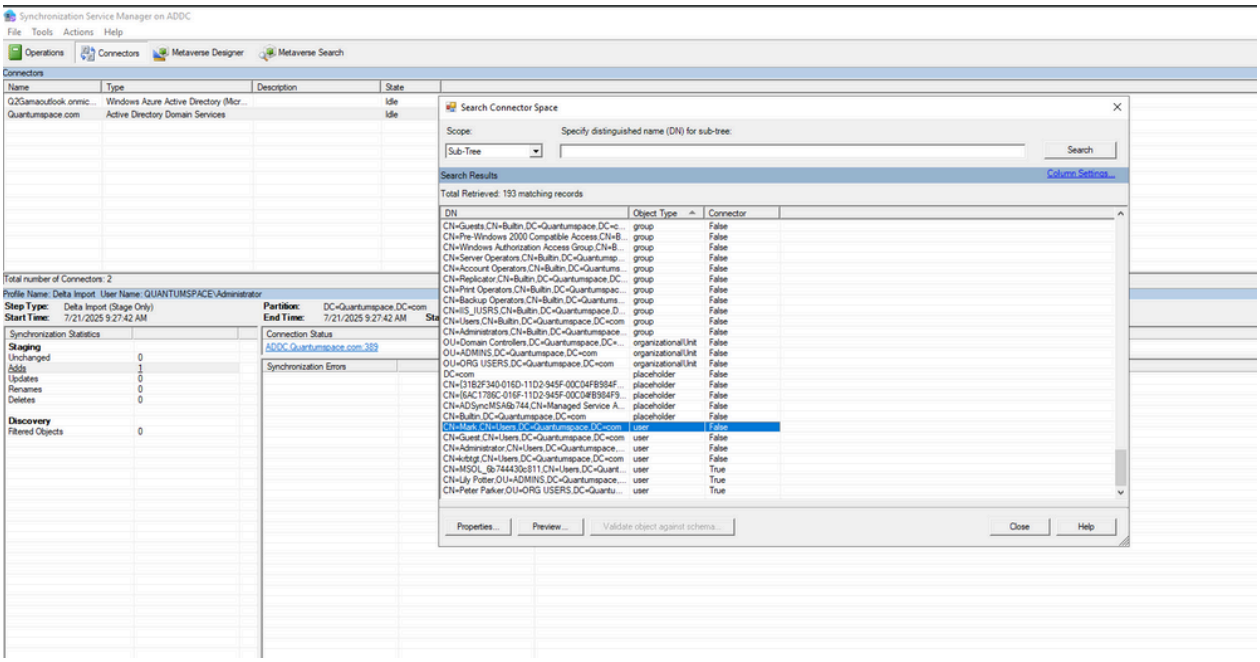
- Right click on local domain connector> Run> Delta Import. This will create a replica of the new object in local domain connector space.



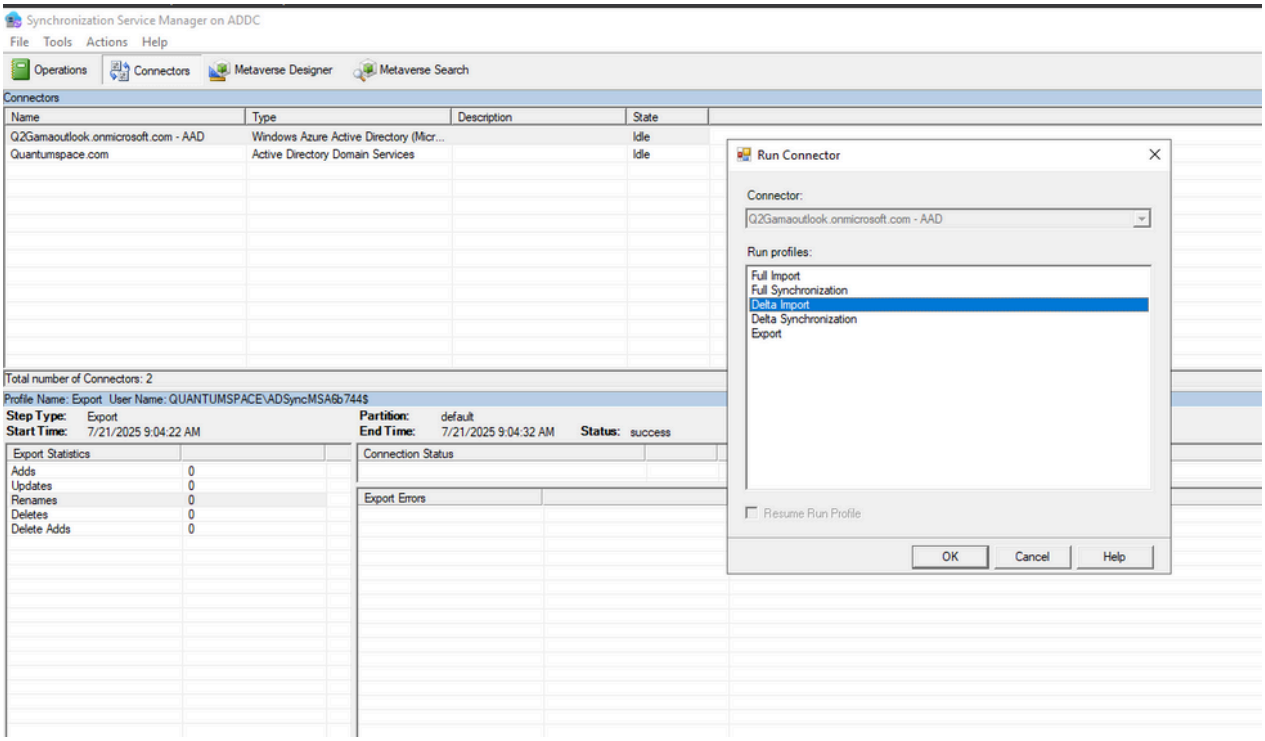
- An ‘Adds’ update will be visible after the import operation.



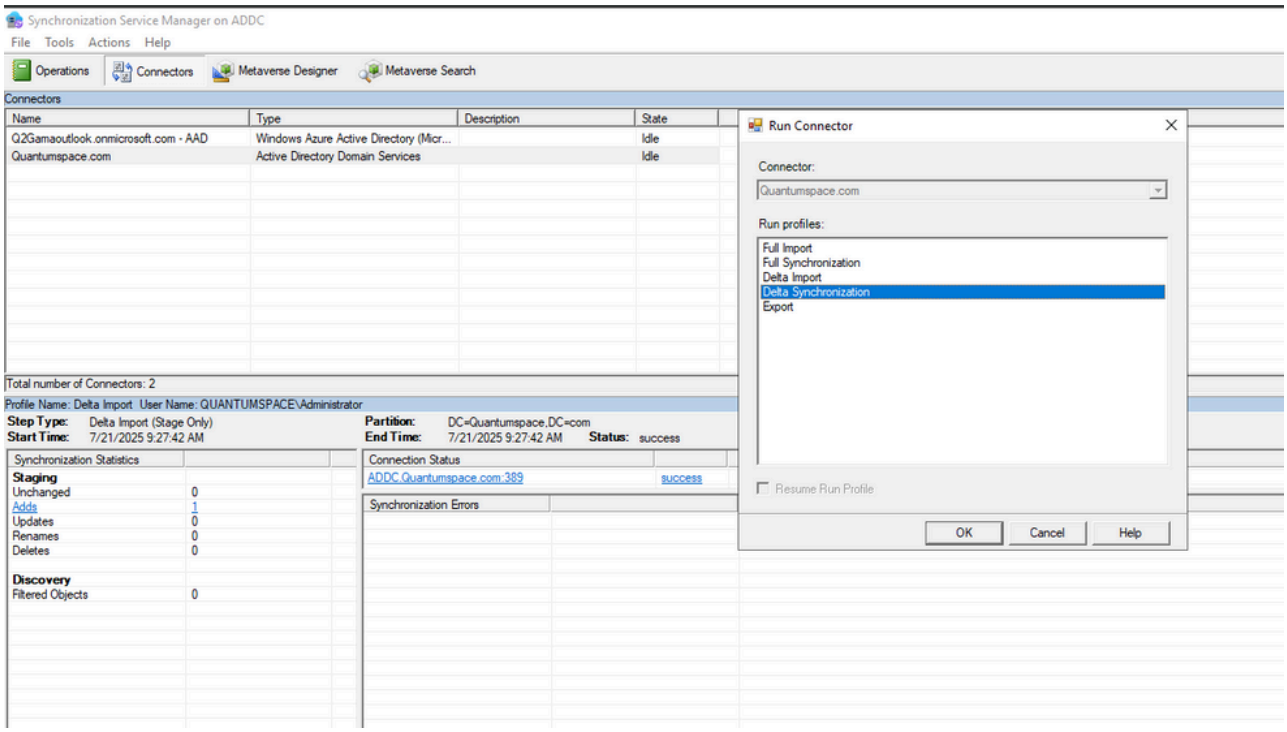
- The new user now will be visible in local AD connector space.

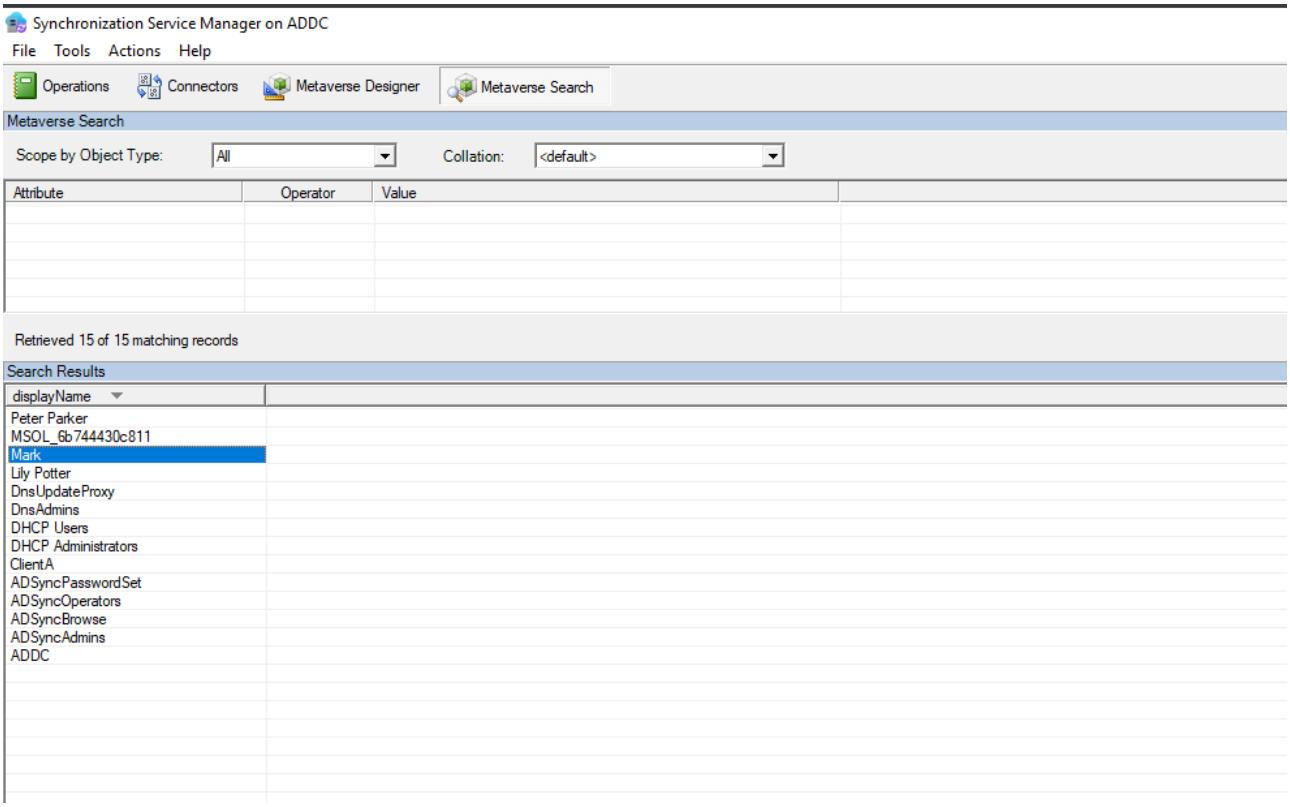


- To check for any object sync from Azure AD, run delta import on the AAD connector. Incase there is any object, it will be visible in the ‘Adds’.

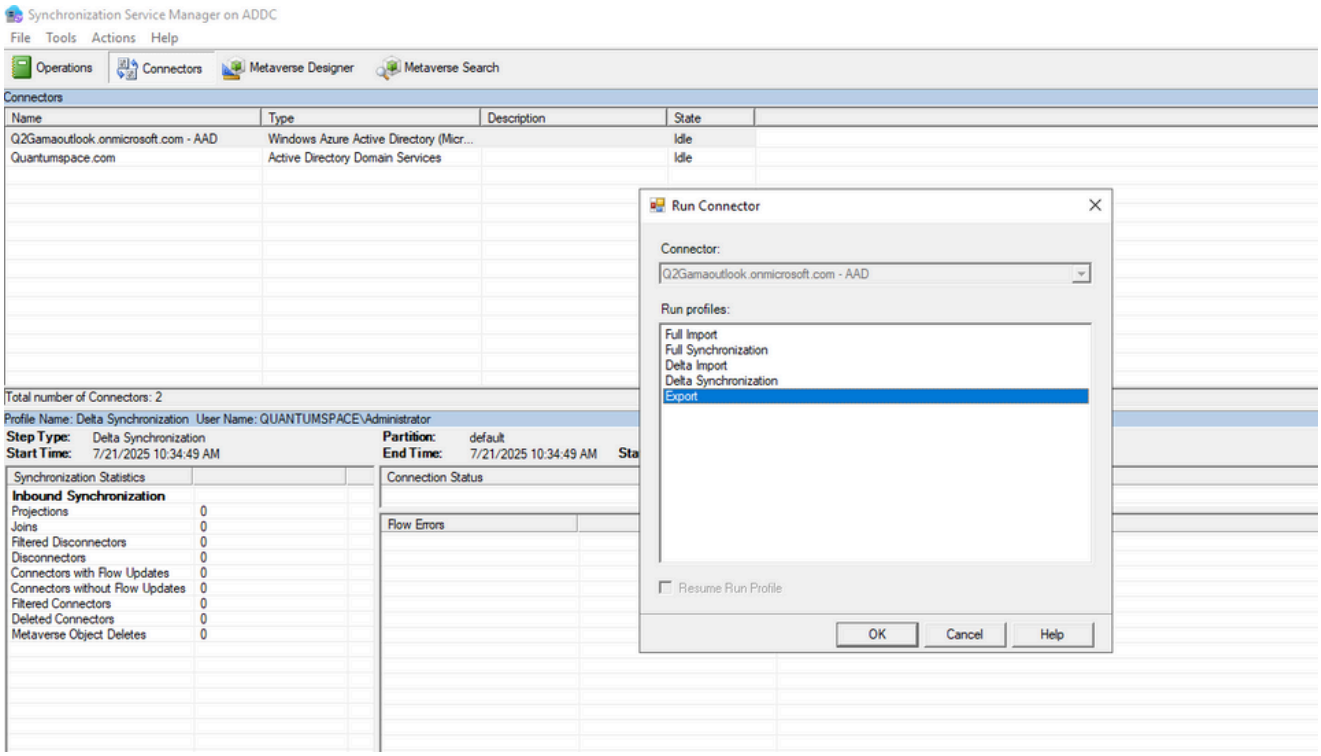


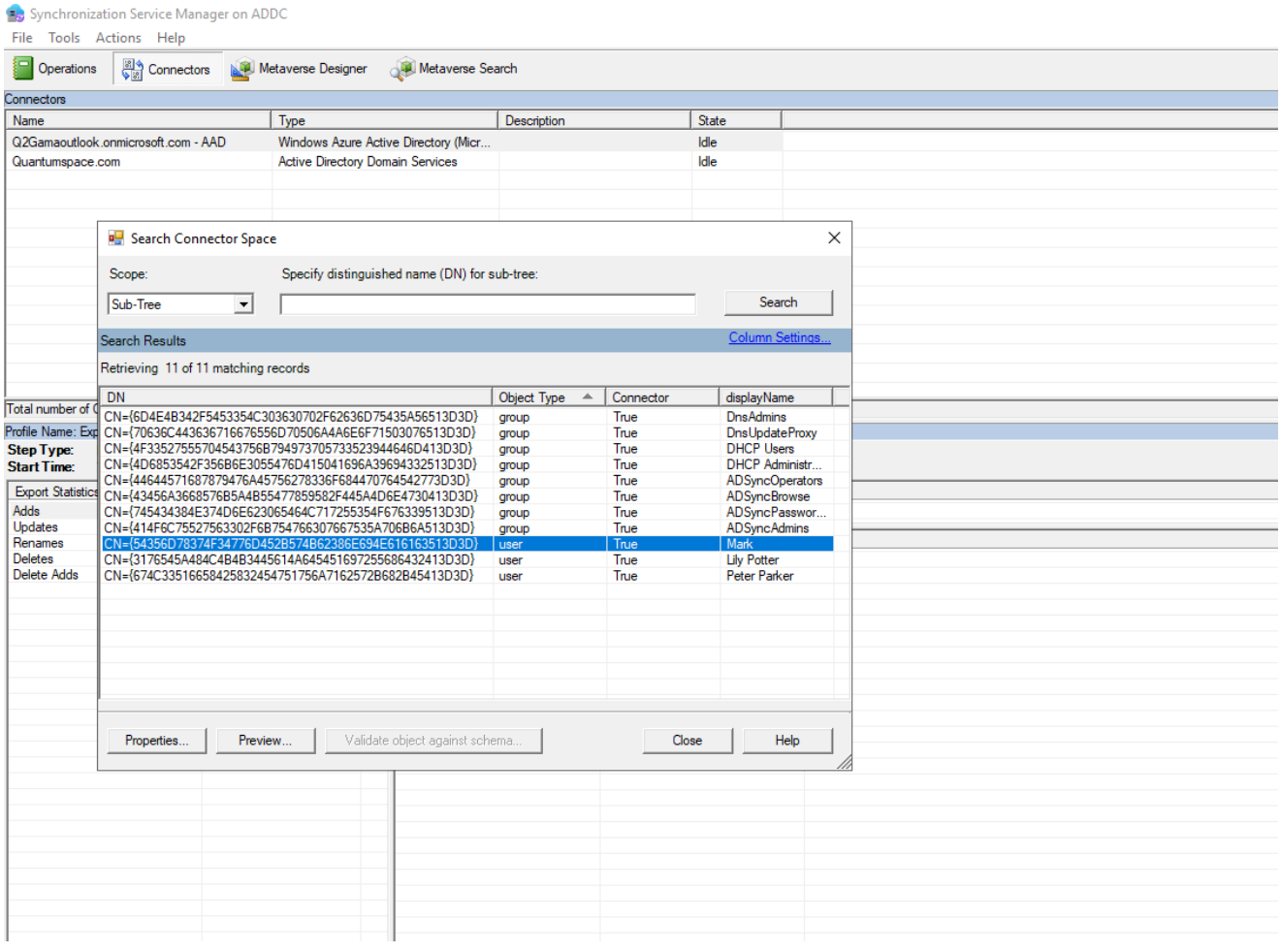
- Now run a delta sync on local AD connector to replicate the user: Mark into Metaverse connector space.





- Similarly, run delta sync on AAD connector space; this will bring changes from AAD connector space to metaverse space.
- For the final process, run an export on AAD connector to send the new change(user: Mark) to Entra ID. Once the export operation is complete, check search the connector space to see user object: Mark. If its showing then it means it has been successfully synced to Entra ID.

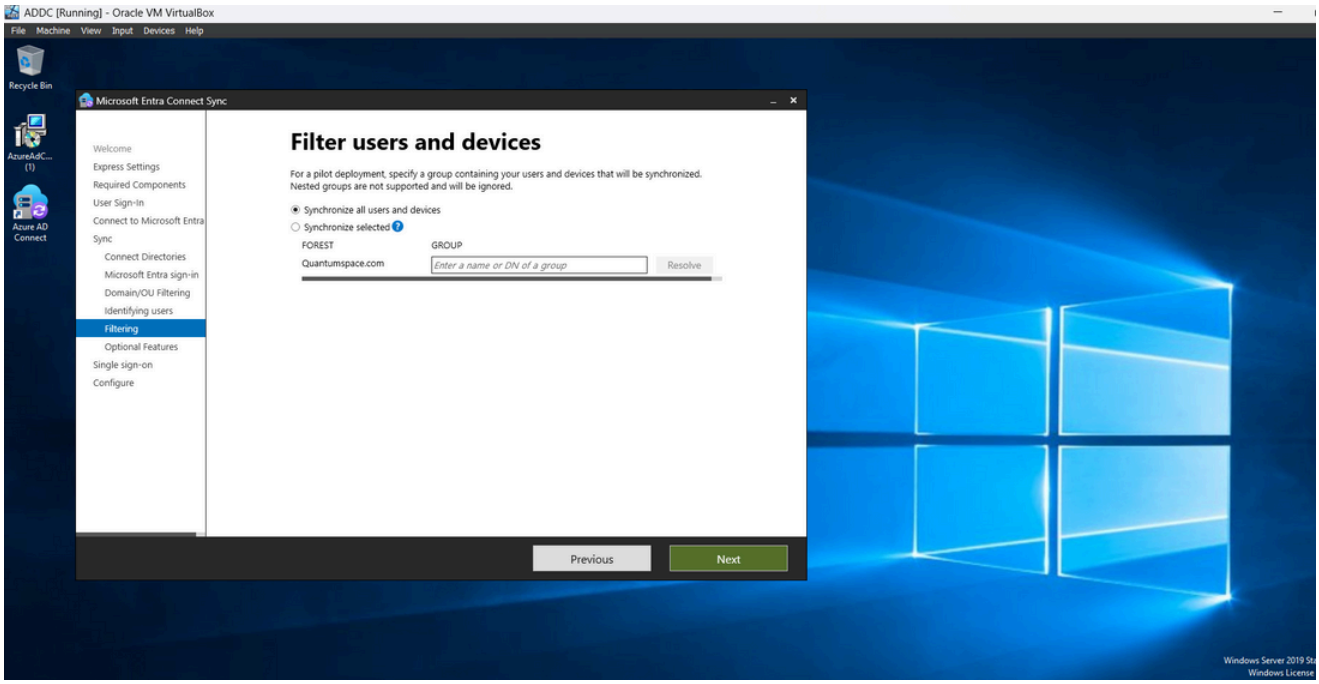




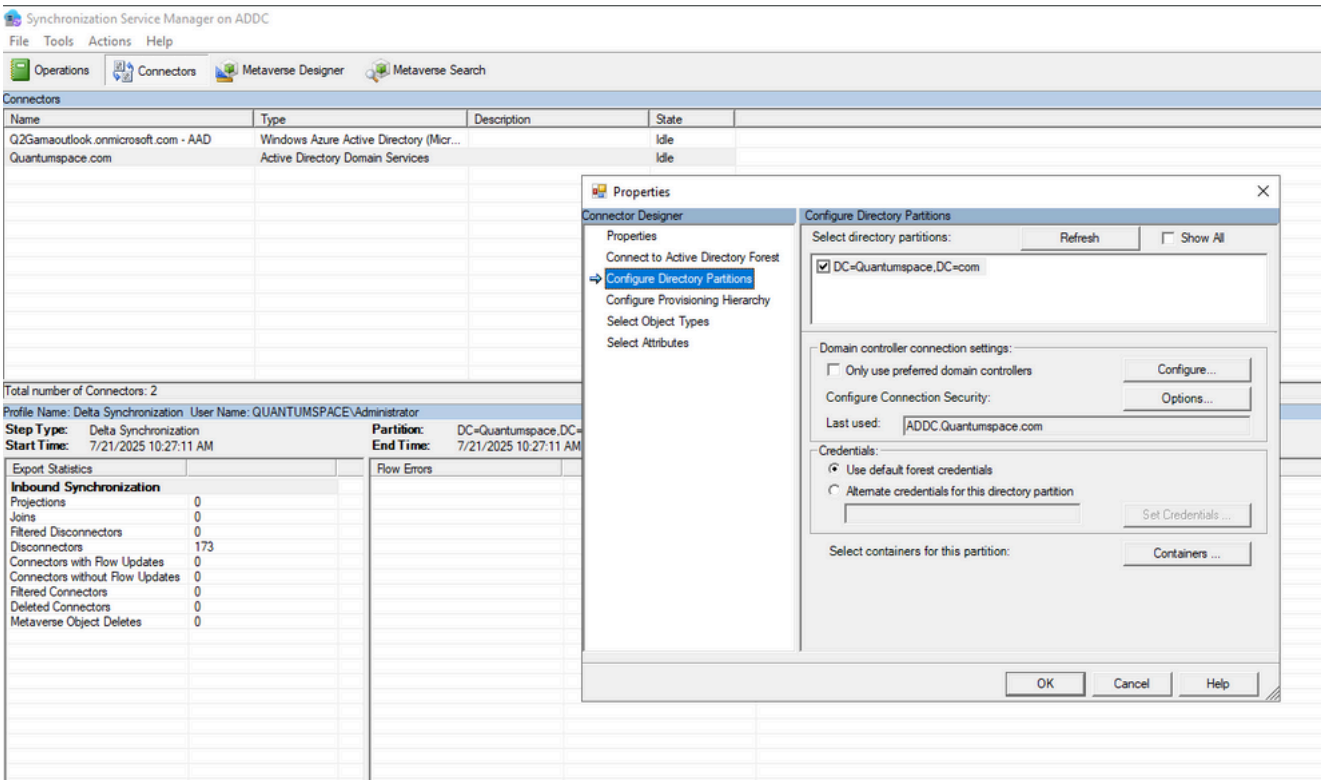
- If incase getting ‘waiting export confirmation’ on the new object in AAD connector space search, then run an import operation on AAD connector. This will successfully sync the new object to Entra ID.

Types Of Filtering:

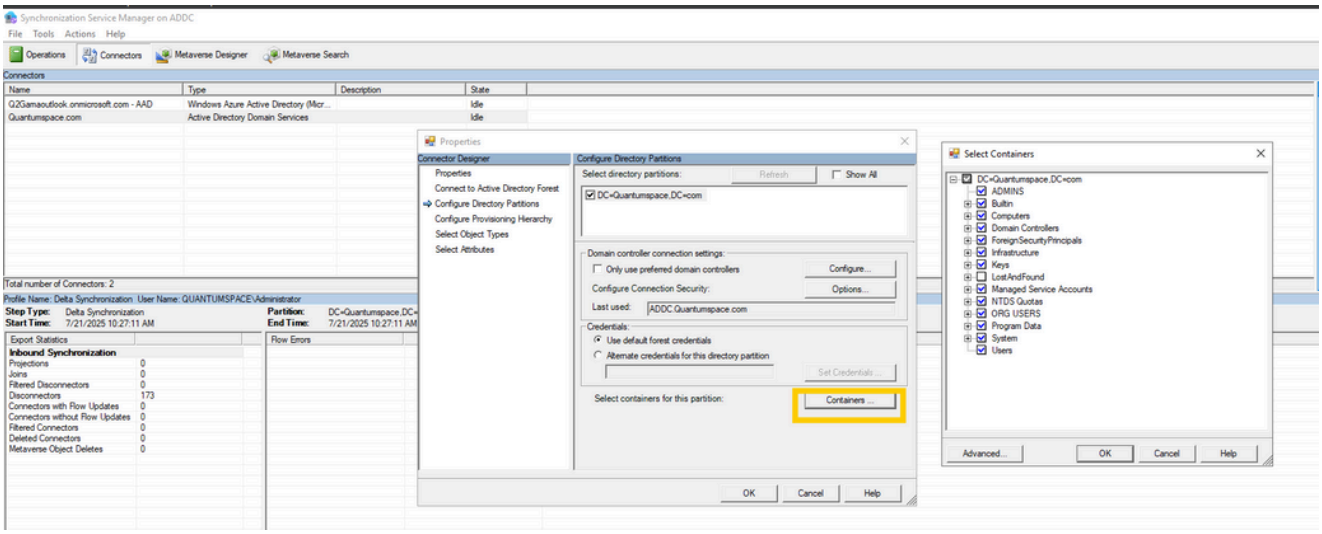
- **Group Based**: While installing the AAD connect setup, there comes an option to provide the DN of the group, that particular option is used to apply filtering to groups. This same can be achieved by sync rules, i.e. If a particular user belongs to a group then only sync to the cloud, or vise versa. Group based filtering are generally recommended during pilot phases or in testing environments, but for large enterprises attribute based filtering is always recommended.



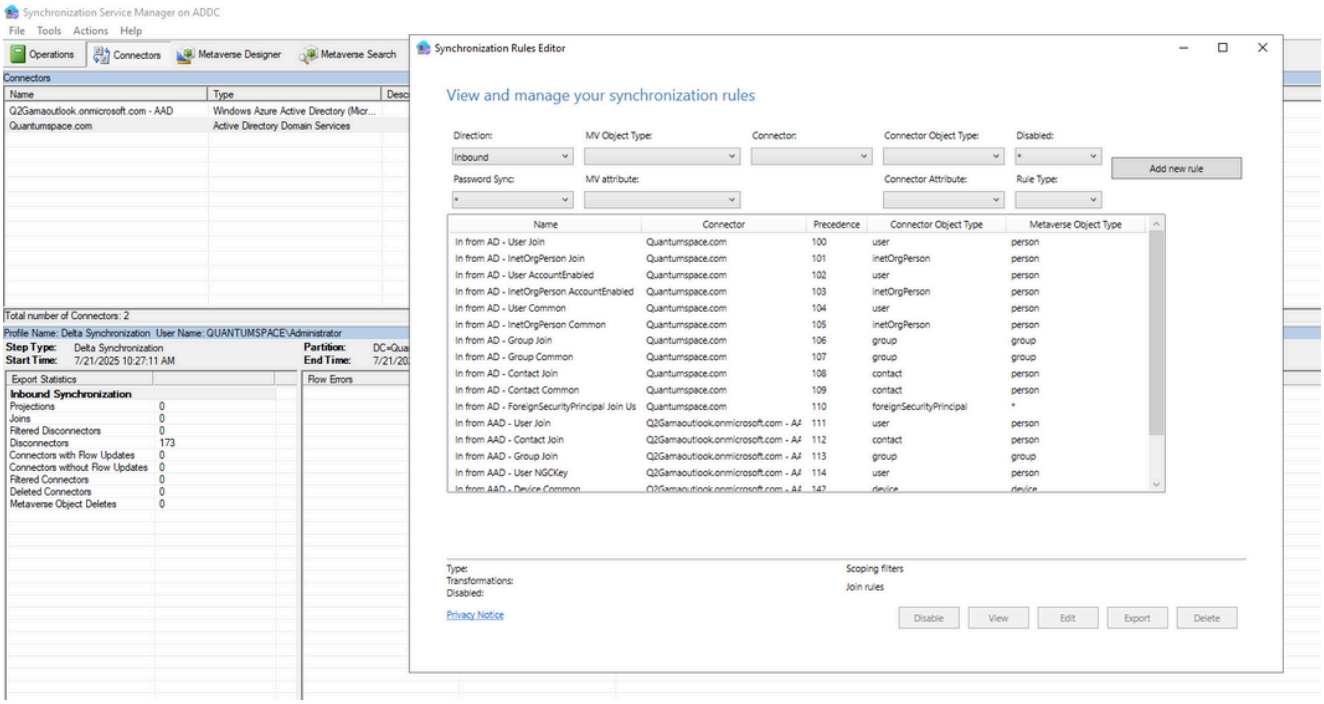
- **Domain Based:** This type of filtering prevents the entire domain to be synced with Entra ID. Incase any domain has several child domains, to not allow sync from any particular child domain, uncheck that particular domain from the console and the domain will not sync to the cloud. Go to local AD connector and right click to see the properties, in the configure directory partitions the domain will be listed. In below case only one domain is visible, but incase of multiple domains, uncheck the particular domain to not sync to Entra ID.



- **OU Based:** This type of filtering prevents the objects to be created in the connector space of local AD. At below, select the respective domain for OU filtering required, select the containers and give enterprise admin credentials to see the OUs listed. Here, check the OUs that are required to be synced.

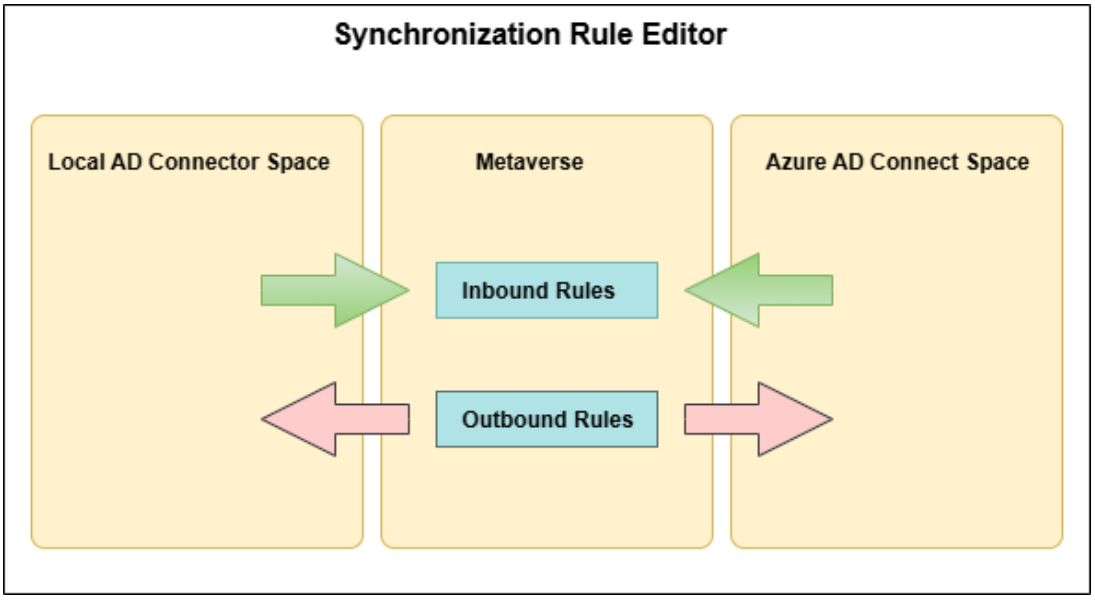


- **Sync Rules or Attribute Based:** For this type of filtering, synchronization rule editor is used. Filtering can be done on the basis of inbound and outbound rules. All the options visible below are for narrowing down the list of the rules that are associated with a particular object. Here different kind of values and attributes can be combined together to attach in a one single sync rule.



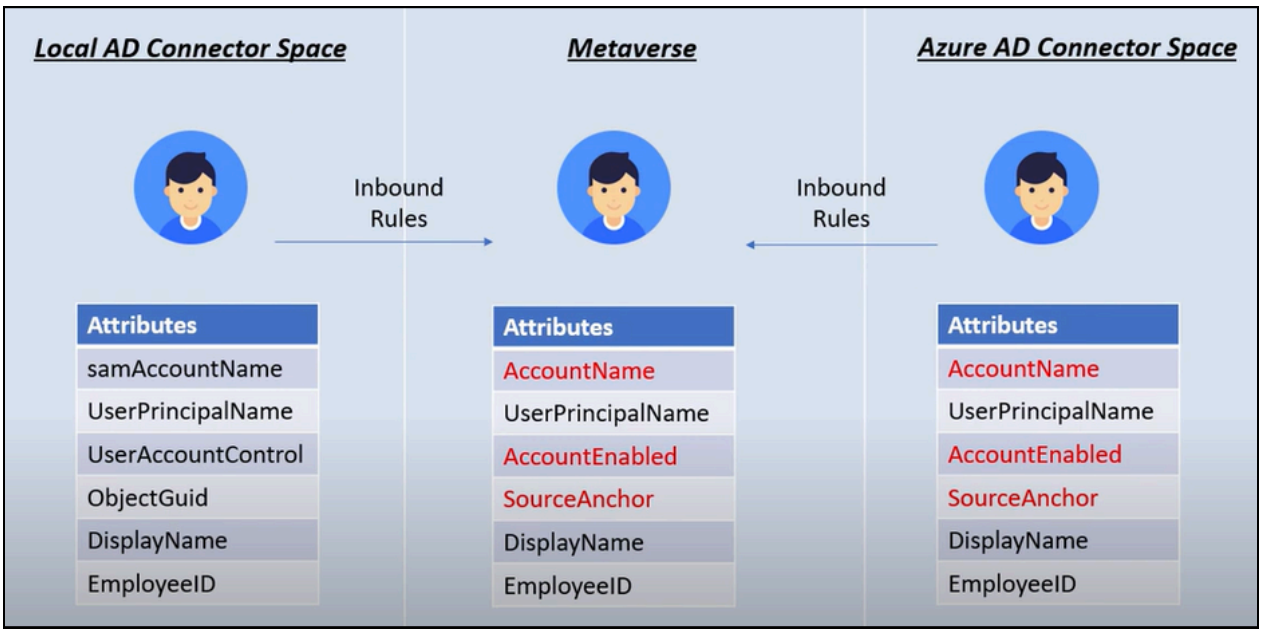
Synchronization Rule Editor:

Tool that lists all the sync rules. Through this, own custom sync rules can be created, basic fundamental of these rules is to define how attributes will be synced from On-prem to Entra ID(this is also called as attribute mapping).



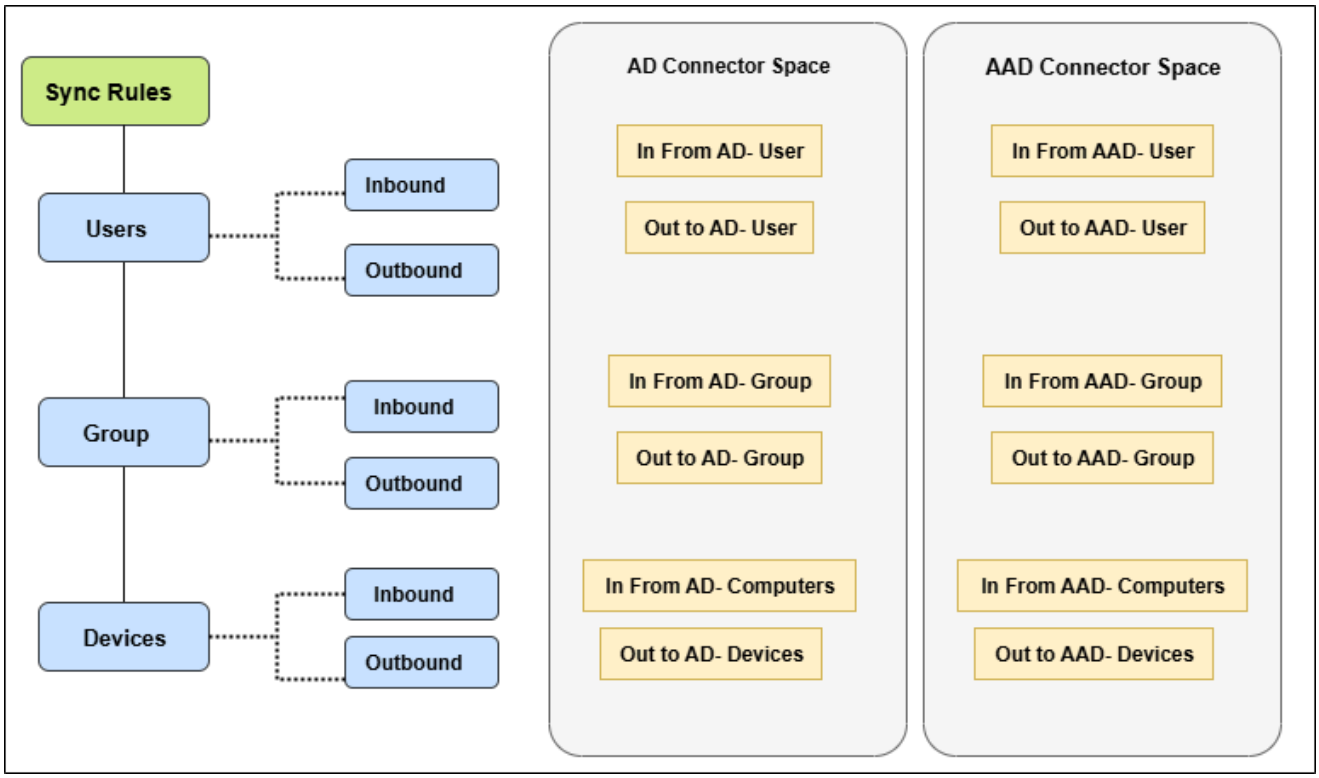
- When the information is being send from local AD connector space or AAD connector space to metaverse space, inbound rules are applied.
- When the information is being send from metaverse to both the connector spaces, then outbound rules are applied.

- All the attribute flow mapping, or getting the names of attributes changed as per the object type is defined in these rules itself.
- When an object is synced to Entra ID or when the replica of a particular object is created in the metaverse space from local AD connector, there are some changes in attribute names observed; like samAccountName is changed into AccountName. This means that attribute i.e. associated with user object type in metaverse is querying its corresponding attribute in local AD connector space.
- The same process happens for AAD connector space as well, when any attribute has to be written back to the local AD, there are inbound rules associated with AAD connector which write back the attributes from AAD connector space to metaverse, which then is synced with local AD.
- Likewise, same process goes for outbound rules, the attribute information will be write back from metaverse space to the connector spaces.



Sync Rule hierarchy:

- Sync rules are defined on the basis of object types, i.e. for every object type there will be a sync rule.
- User, Group and Device; these three object types can have same as well as different attributes. In order to define the attribute flow mapping for all the three object types, two different kinds of rules are created i.e. Inbound and Outbound rules.
- If there is a change that is updated in local AD connector space that has to be send to metaverse, then the inbound rule will be named as 'In from AD-object type'. The same will be followed for the AAD connector space.
- Hence, for each object type, there will be two categories of inbound and outbound rules created; first will be related to local AD connector space and the second for AAD connector space.
- Depending upon the direction of the attribute flow, the rules are named accordingly.

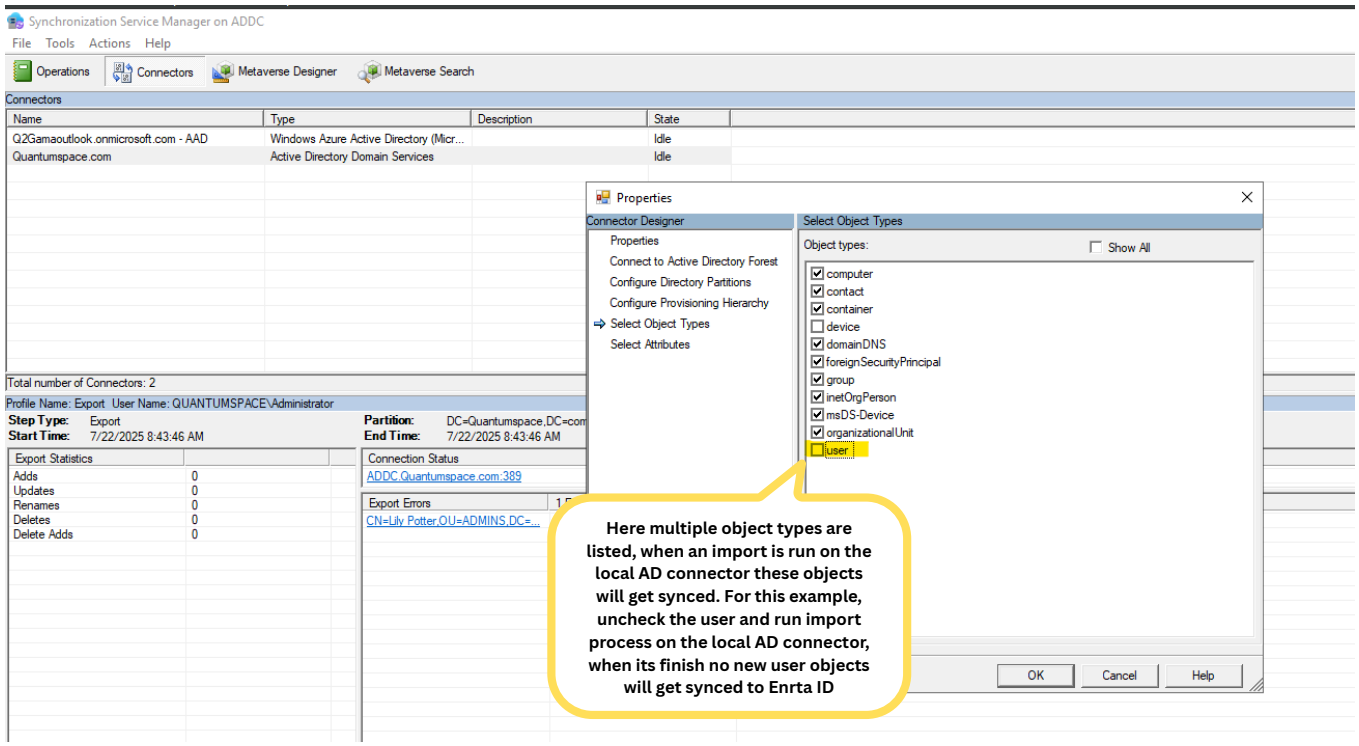


Connector Configuration & Attribute Flow Mapping:

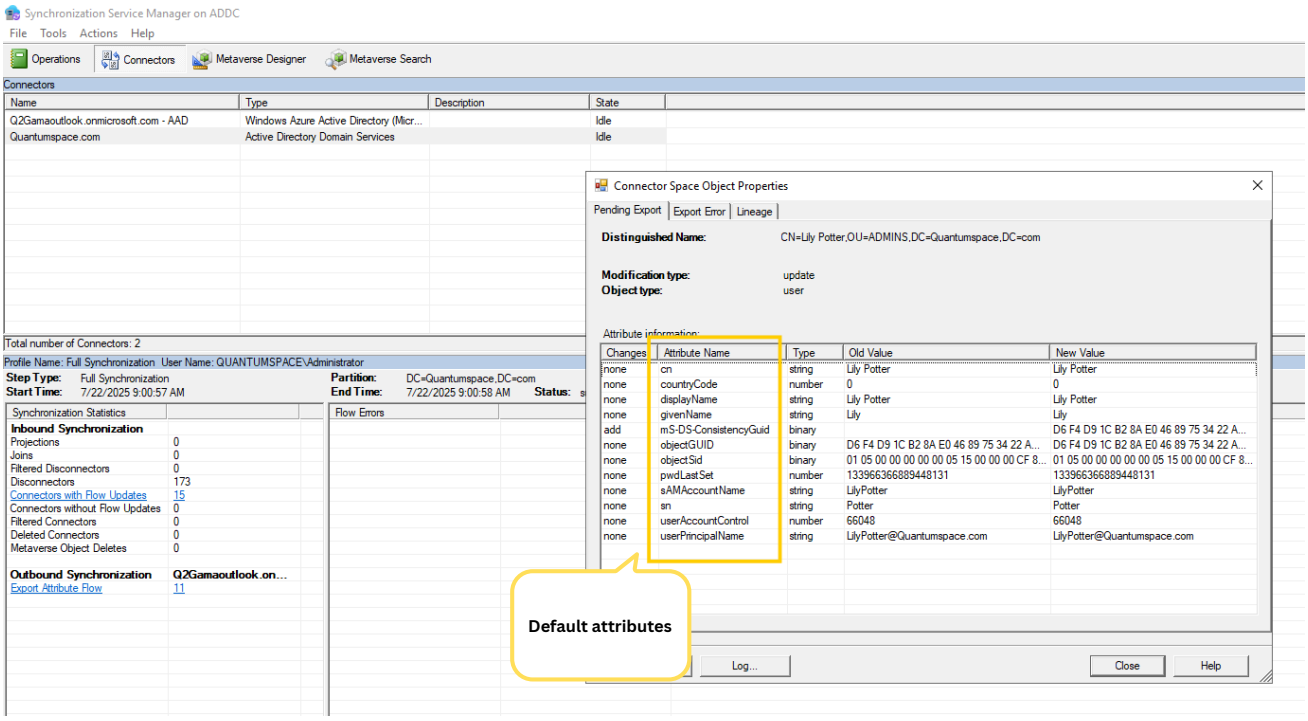
Respective connector spaces are customizable by configuring each connectors as per requirements.

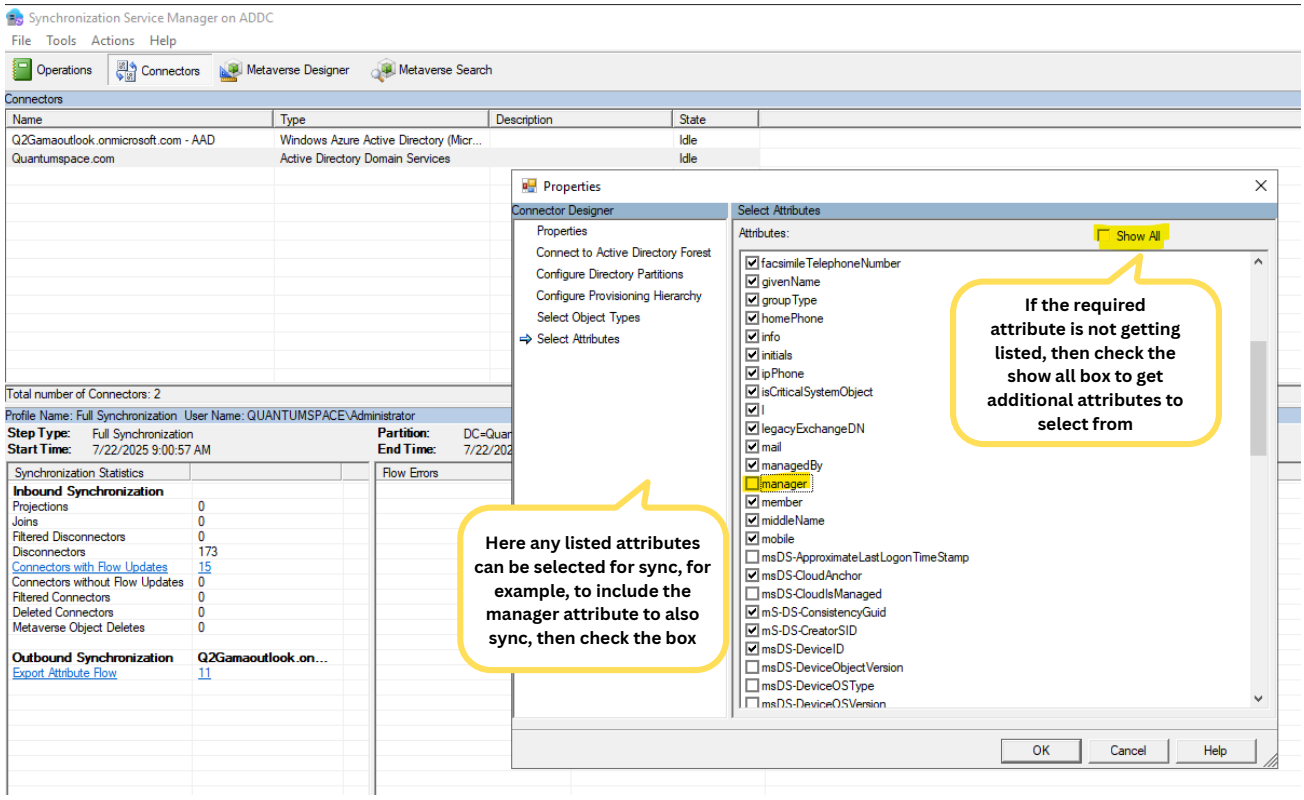
Example:

- Right click on the local AD connector> properties> Select object types

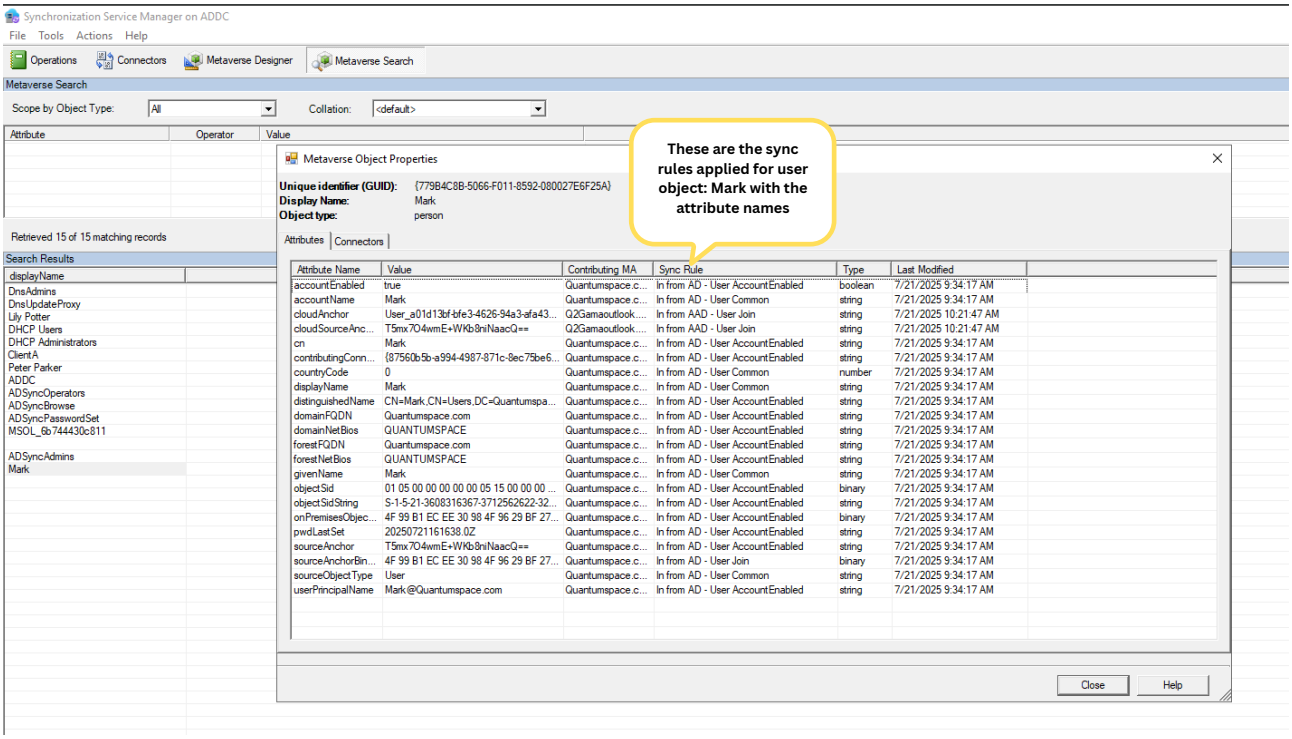


- Select attributes: Every object has multiple types of attributes associated with it. When a user object is created, there are certain default attributes that get populated automatically and are called mandatory attributes. There are also attributes that can be used as per sync requirements. Right click on the local AD connector> properties> Select attributes.

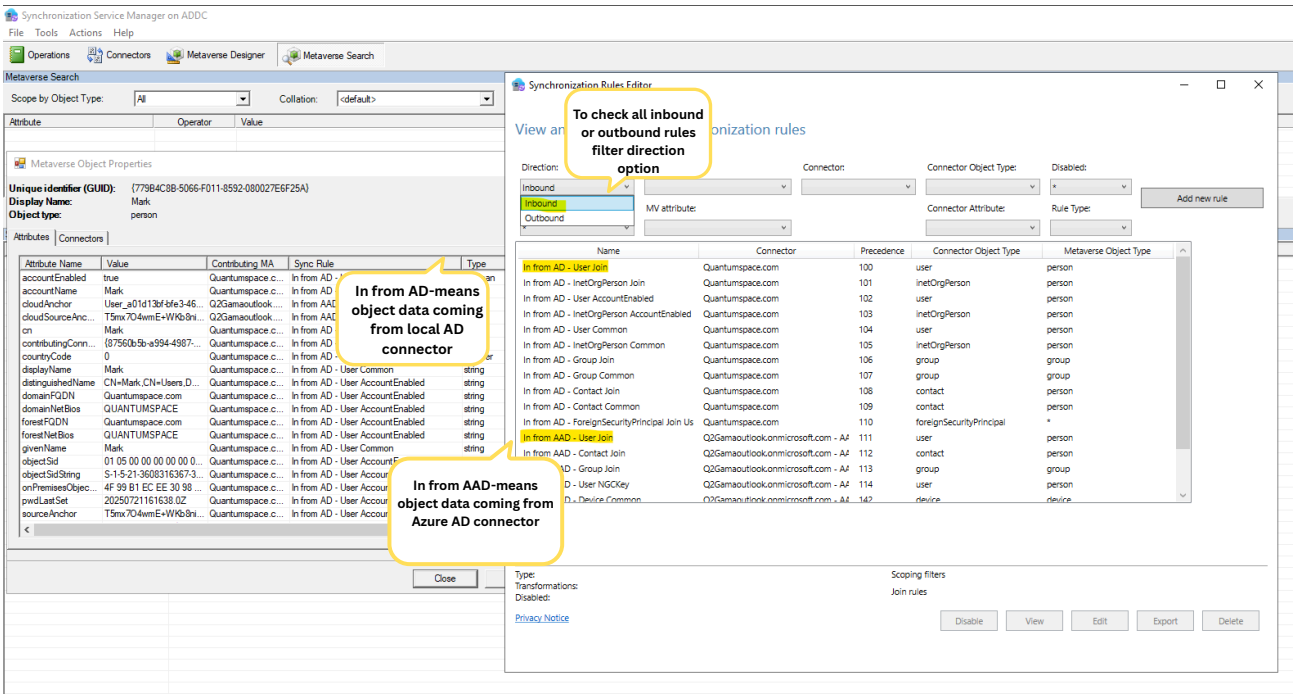


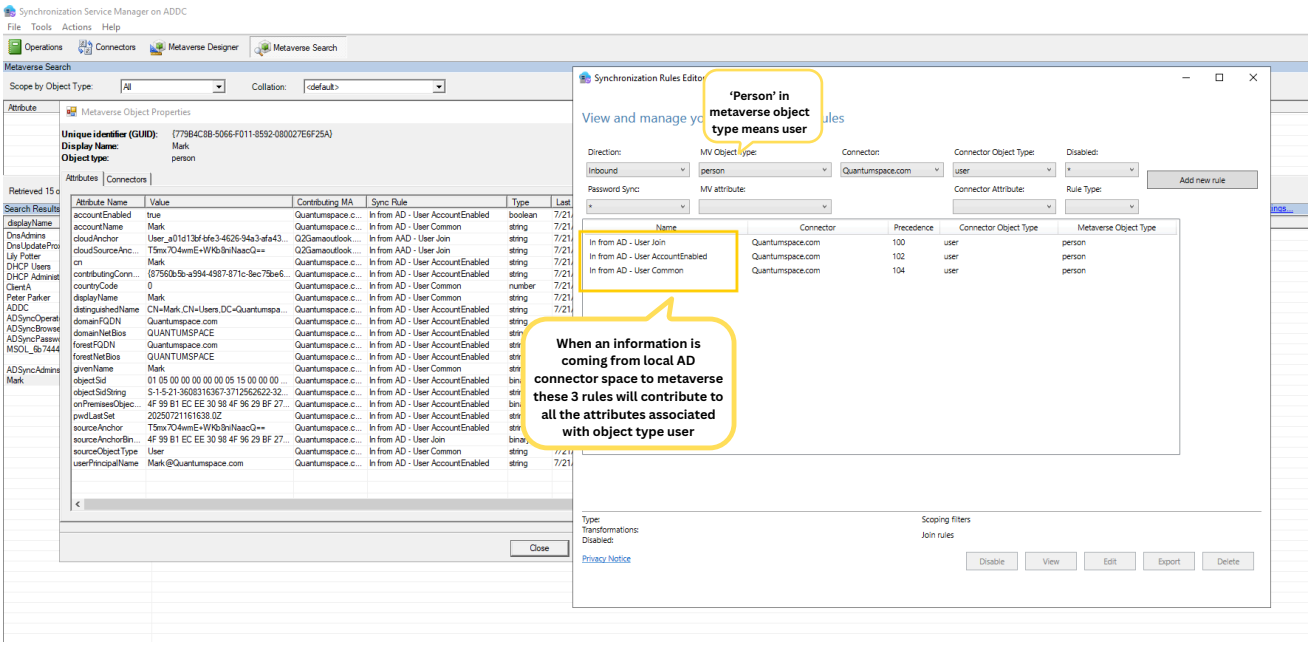


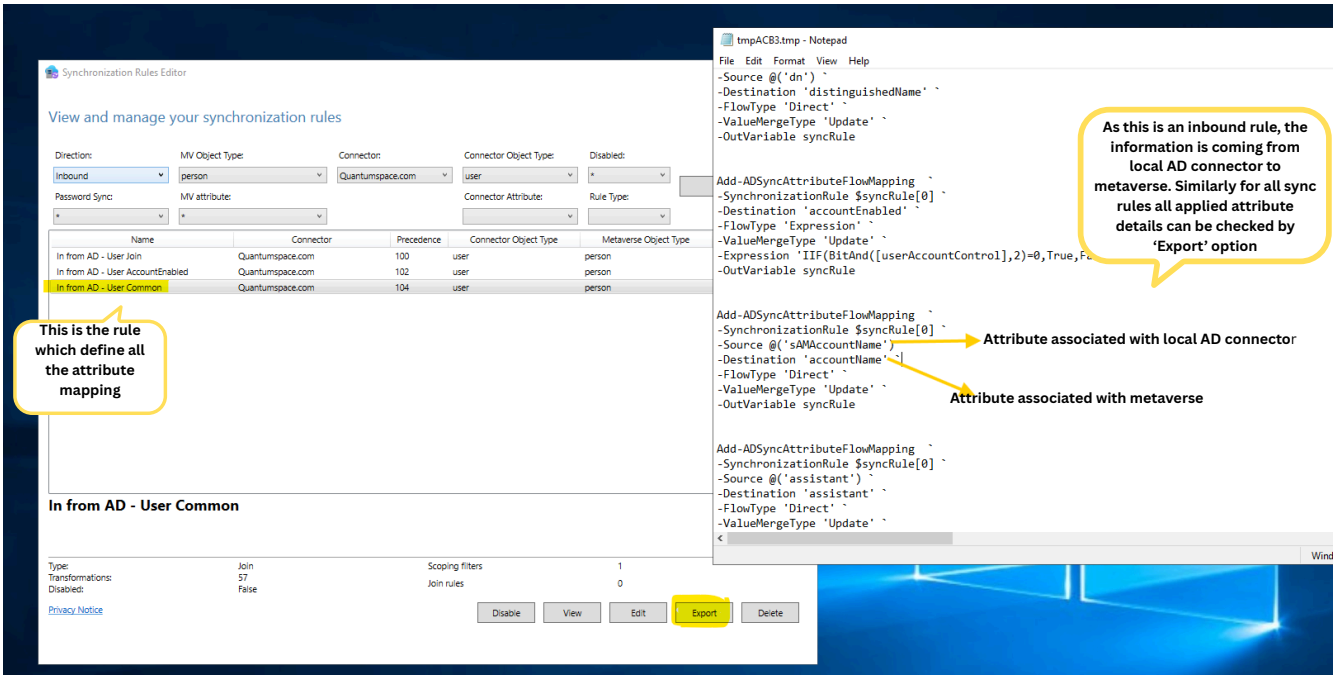
- To check the sync rules applied for an object; in metaverse search> double click on the object to see properties.

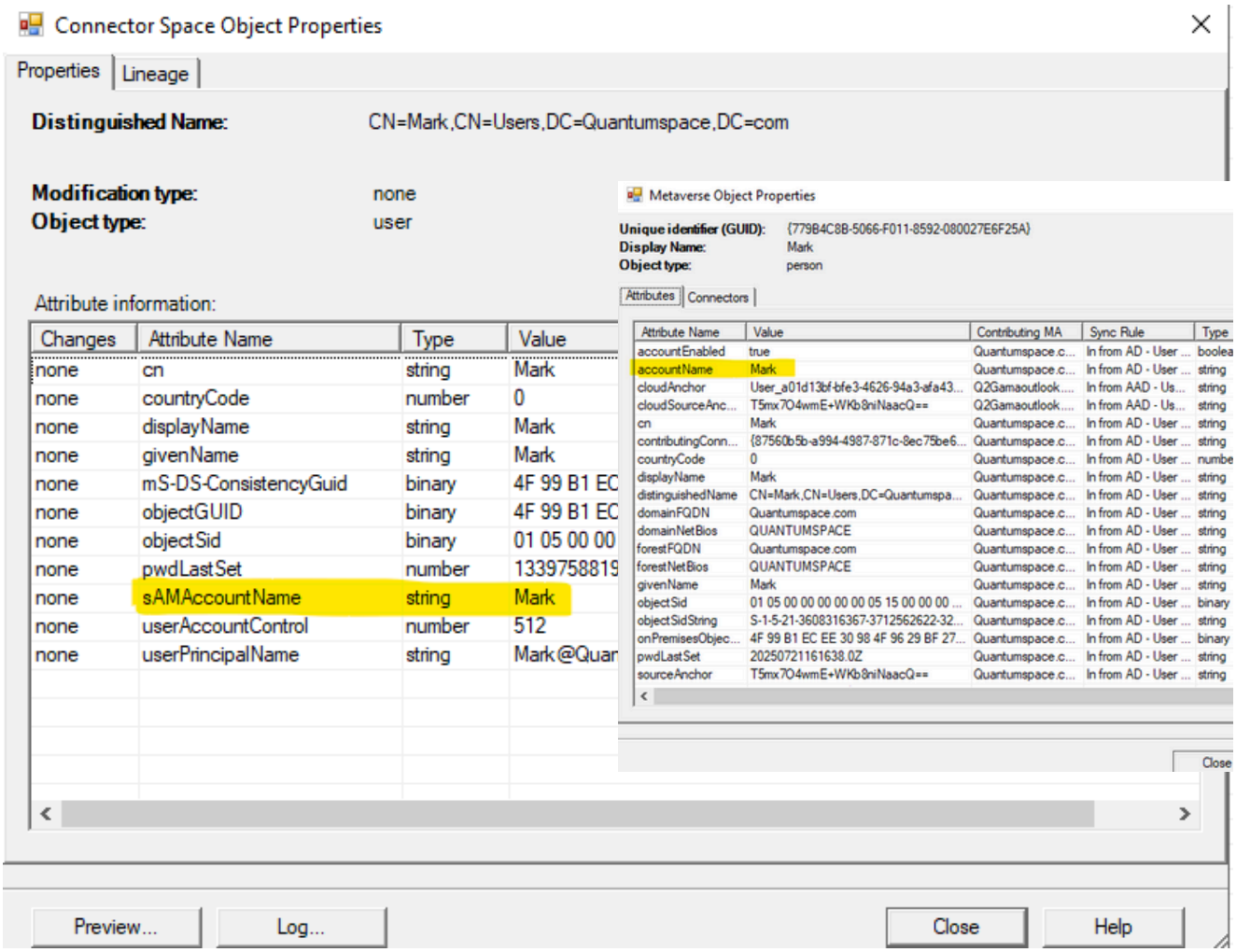


- To check all the inbuild connector rules, launch synchronization tool editor. It is not recommended to edit the inbuild rules rather create custom rules as per requirements.




'Person' in metaverse object type means user
When an information is coming from local AD connector space to metaverse these 3 rules will contribute to all the attributes associated with object type user


This is the rule which define all the attribute mapping
In from AD - User Common
As this is an inbound rule, the information is coming from local AD connector to metaverse. Similarly for all sync rules all applied attribute details can be checked by 'Export' option
Attribute associated with local AD connector
Attribute associated with metaverse


Connector Space Object Properties
Properties
Lineage
Distinguished Name:
CN=Mark,CN=Users,DC=Quantumspace,DC=com
Modification type:
none
Object type:
user
Attribute information:
Changes
Attribute Name
Type
Value
none cn string Mark
none countryCode number 0
none displayName string Mark
none givenName string Mark
none mS-DS-ConsistencyGuid binary 4F 99 B1 EC
none objectGUID binary 4F 99 B1 EC
none objectSid binary 01 05 00 00
none pwdLastSet number 1339758819
none sAMAccountName string Mark
none userAccountControl number 512
none userPrincipalName string Mark@Quar
Metaverse Object Properties
Unique identifier (GUID):
{779B4C8B-5066-F011-8592-080027E6F25A}
Display Name:
Mark
Object type:
person
Attributes
Connectors
Attribute Name
Value
Contributing MA
Sync Rule
Type
accountEnabled true Quantumspace.c... In from AD - User ... boolea
accountName Mark Quantumspace.c... In from AD - User ... string
cloudAnchor User_a01d13bf-bfe3-4626-94a3-afa43... Q2Gamaoutlook.... In from AAD - Us... string
cloudSourceAnc... T5mx7O4wmE+WKb8niNaacQ== Q2Gamaoutlook.... In from AAD - Us... string
cn Mark Quantumspace.c... In from AD - User ... string
contributingConn... {87560b5b-a994-4987-871c-8ec75be6... Quantumspace.c... In from AD - User ... string
countryCode 0 Quantumspace.c... In from AD - User ... numbe
displayName Mark Quantumspace.c... In from AD - User ... string
distinguishedName CN=Mark,CN=Users,DC=Quantumspa... Quantumspace.c... In from AD - User ... string
domainFQDN Quantumspace.com Quantumspace.c... In from AD - User ... string
domainNetBios QUANTUMSPACE Quantumspace.c... In from AD - User ... string
forestFQDN Quantumspace.com Quantumspace.c... In from AD - User ... string
forestNetBios QUANTUMSPACE Quantumspace.c... In from AD - User ... string
givenName Mark Quantumspace.c... In from AD - User ... string
objectSid 01 05 00 00 00 00 00 05 15 00 00 00 ... Quantumspace.c... In from AD - User ... binary
objectSidString S-1-5-21-3608316367-3712562622-32... Quantumspace.c... In from AD - User ... string
onPremisesObjec... 4F 99 B1 EC EE 30 98 4F 96 29 BF 27... Quantumspace.c... In from AD - User ... binary
pwdLastSet 20250721161638.0Z Quantumspace.c... In from AD - User ... string
sourceAnchor T5mx7O4wmE+WKb8niNaacQ== Quantumspace.c... In from AD - User ... string
Close
Preview...
Log...
Close
Help