Quest

Directory Sync Pro for Active Directory 20.11.2

User Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

20 Enterprise, Suite 100

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

Directory Sync Pro for Active Directory User Guide
Updated - May 2024

Contents

Project Overview

Synchronization

The first step in the Directory Sync process is to create a profile. If you don't have any profiles listed on the Project Overview page, click on **Add Profile**, and follow the steps. You can edit the settings of any profile listed by selecting it, and choosing **Manage**.

The status column is a live status display of all sync cycles. You can also trigger a manual synchronization of any profile at any time by selecting it and choosing **Run Sync**. You can then choose the type of synchronization that you need.

Logs and Reports

Select any log or report for more information. If you choose to run a simulated sync, the results will be viewed as a sync report. The level of detail for the log files is determined by the profile settings.

Creating Profiles

Profile Security Delegation

The Profile Security Delegation feature allows you to control and delegate access to Synchronization Profiles by entering a list of users to grant access. For example, you may want to restrict access to a synchronization profile to a business unit or national team. Only profiles which users have access to will be available to them in Directory Sync Pro for Active Directory and Migrator Pro for Active Directory.

To control access to a Synchronization Profile:

1. Check **Enable Profile Security Delegation** in the Profile wizard or on the Manage Settings General Profile Info page.
2. Enter the list of users that can access the profile in DOMAIN\Username format. Users must be separated by comma. Note that users added to the list must be in the BTDirSyncPro group of the local machine.

Note: The profile creator will always have access to the profile.

Organizational Units

Add your organization units. Click on select OU and browse to your desired OUs. You can add multiple OUs to a single profile, or create a new profile for each, if you want to customized the settings for each OU individually.

Click on an OU to select it. Be sure a check mark appears after each selection. Click again to de-select that OU.

By default, all sub-OUs of any selected OU are also included in the profile. If that's not what you want, then uncheck the box next to it. Then, pick and choose each OU manually.

Notice the number of OUs specifically selected is reflected in the ADD button at the bottom. If you want to start over completely, choose the **Refresh** button. Click the **Add** button when you have made all selections.

You can filter the objects included in the profile by double-clicking on the profile. You can select or deselect types of objects by checking or unchecking the boxes. For more granular control, you can edit the filter boxes.

Mail-Enabled and Non-Mail Enabled Users

This page is where you control the characteristics of the objects as they are created in the target.

Options for AD Inter-forest and Intra-Forest Profiles

AS-IS means the objects will be created just as they currently exist in the source. If the account was disabled in Active Directory in the source, it will be disabled in Active Directory when created in the target. If the account was enabled in Active Directory in the source, it will be created as enabled in Active Directory in the target.

You can also choose to Active Directory enable all objects when they are created in the target, no matter their Active Directory account status in the source. Or, just the opposite, you can choose to have all objects created in an account disabled state in the target, no matter their status in the source.

For mail-enabled objects only, there is also the option is to convert all mail-enabled objects into contacts when they are created in the target.

Options for Exchange Inter-forest Profiles

AS-IS means the objects will be created just as they currently exist in the source. If the account was disabled in Active Directory in the source, it will be disabled in Active Directory when created in the target. If the account was enabled in Active Directory in the source, it will be created as enabled in Active Directory in the target.

You can also choose to enable all objects when they are created in the target, no matter their status in the source. Or, just the opposite, you can choose to have all objects created in an account disabled state in the target, no matter their status in the source.

You may also choose to convert all the mail-enabled objects into contacts when they are created in the target.

You would use this profile in conjunction with our Exchange Pro mailbox migration product.

Options for Exchange IntRA-forest Profiles

AS-IS means the objects will be created just as they currently exist in the source. If the account was disabled in Active Directory in the source, it will be disabled in Active Directory when created in the target. If the account was enabled in Active Directory in the source, it will be created as enabled in Active Directory in the target.

Note that All objects created will be Mail-Disabled, no matter what their Active Directory account status.

You can also choose to enable all objects when they are created in the target, no matter their status in the source. Or, just the opposite, you can choose to have all objects created in an account disabled state in the target, no matter their status in the source.

You may also choose to convert all the mail-enabled objects into contacts when they are created in the target.

User Conflicts

How do you want to handle any users conflicts? That is what should happen if (based on your matching criteria) that Directory Sync Pro for Active Directory finds a matching user already in the target? If you choose skip, Directory Sync Pro for Active Directory will not make an association between those objects, and an error will be noted in the log file.

With Update, Directory Sync Pro for Active Directory will consider those items the same. This means that any changes made to the source will update that matched item in the target, if you have set updates to occur. No new object will be created.

With Rename, a new object will be created in the target. You will need to distinguish this from the matched target object by giving it a new name. You can manually add a prefix or suffix of your choice, or, you choose any existing AD attribute to be prepended or appended to the name. Remember that if you choose rename, when you update the object in the source, it will be the Renamed object in the target that gets updated during a synchronization.

User SID History

You have the option to include an object's SID history during the migration. This will help prevent issues with some software, and network shared printers. We suggest this option. Consider however, that in a large enterprise, this might cause the Kerberos token to exceed the max token size for users that belong to many groups. You could mitigate that issue with a GPO that is set to accept larger tokens.

If you do choose to migrate SID History, all Domain Controllers that you have listed in the Target DC's tab will need access to the Domain Controller that holds the PDC Emulator FSMO role in the source.

Groups

Options for AD Profiles

By default, groups will retain their current group scope when they are migrated. You have the option to change that here, so that you can transform a group's scope as it is migrated. For example, if the new target does not have multiple domains, you may choose to convert your Universal Groups into Domain Local groups. Or you can choose not to migrate a particular group scope at all. There are some limitations on changing the scope of nested groups, so you may want to refer to the following TechNet link.

https://technet.microsoft.com/en-us/library/cc755692(v=ws.10).aspx

Options for Exchange Profiles

By default, your mail-enabled groups will retain their current group scope when they are migrated. You have the option to change that here, so that you can transform a group's scope as it is migrated. You can also change the group to a contact, or you can choose not to migrate a particular group scope at all.

Group Conflicts

How do you want to handle any group conflicts? That is, what should happen if (based on your matching criteria) that Directory Sync Pro for Active Directory finds a matching group already in the target?

Options for AD and Exchange to AD Profiles

If you choose skip, Directory Sync Pro for Active Directory will not make an association between those objects, and an error will be noted in the log file.

If you choose Merge, Directory Sync Pro for Active Directory will consider those items the same. This means that any members of the source group will be added to the membership list of the target group, if you have set updates to occur. No new object will be created.

With Rename, a new Active Directory group object will be created in the target. You will need to distinguish this from the matched target object by giving it a new name. You can manually add a prefix or suffix of your choice, or, you choose any existing AD attribute to be prepended or appended to the name. Remember that if you choose rename, when you update the object in the source such as adding another member, it will be the Renamed group object in the target that gets updated during a synchronization.

User Groups

When you migrate a user, you can also have Directory Sync Pro for Active Directory migrate any groups in which they are a directly a member. Just check the Synchronize Accompanying Groups box. If they are member of a group, that is itself a member of another group, you can choose to include the entire nested chain of groups by checking the Include Parent Groups box also.

However, the group objects themselves must also be included within the scope of this profile, or another profile, or this setting will have no immediate effect. If you later fixed the issue by including those particular groups within a profile, the user's membership would then be included automatically at that time.

To avoid this issue, if you plan to use this option, you may want to first make a profile that includes all the groups, and only groups, in the entire domain. You would then run only a push synchronization, to get these items into the SQL database without pulling them into the target. Then this option would always behave as expected.

Devices

By default, the Active Directory account status of device is maintained when the object is created in the target. If a device was Active Directory enabled in the source, it will be enabled in the target, and vice-versa. Or, choose enabled, to make all migrated devices immediately Active Directory enabled, no matter what their status was in the source.

Maybe you want to ensure that these devices should not be available until a later time even after the device has been cutover. In that case, you can choose disabled, which will cause all migrated devices to be Active Directory disabled, no matter what the status in the source.

Device Conflicts

How do you want to handle any device conflicts? That is, what should happen if (based on your matching criteria) that Directory Sync Pro for Active Directory finds a matching device already in the target? If you choose skip, Directory Sync Pro for Active Directory will not make an association between those devices, and an error will be noted in the log file.

If you choose Update, Directory Sync Pro for Active Directory will consider those items the same. This means that any changes to the source device object attributes will be made to the target device, if you have allowed updates to occur. No new object will be created.

With Rename, a new Active Directory device object will be created in the target. You will need to distinguish this from the matched target object by giving it a new name. You can manually add a prefix or suffix of your choice, as long as it does not exceed 20 characters, or, you choose any existing AD attribute to be prepended or appended to the name. Remember that if you choose rename, when you update the device object's attributes in the source, it will be the Renamed device object in the target that gets updated during a synchronization.

Exchange Migration

Target Proxy Address Overwrite Behavior

If you check this box, source proxy addresses will always overwrite the proxy addresses in the target, replacing whatever values are there, if any. If this box is left unchecked, the source proxy address will only be added to those target objects where this attribute is currently empty.

Promote Target User Contacts

If you check this box, any TARGET contacts will be converted into mail-enabled users.

For the scope of this feature a Microsoft Exchange Mail Enabled Contact is defined as an Active Directory contact where the LegacyExchangeDN attribute is not null. A contact will be promoted to a user if the primary SMTP address on the a source object matches the external or target email address of the contact. Once the attributes have been stored on the newly created Microsoft Exchange User on the target, the Contact object will be removed from the target. The source User must have a LegacyExchangeDN. The contacts in the source, that will be converted, must be in a different OU than the Target OU selected on the AD Target tab.

This option may not be selected if the setting Create Mail Enabled Users As on the AD Target Options Users tab is set to Contact, or if the source object is already a contact.

Promote Target Group Contacts

If you check this box, any TARGET groups will be converted into mail-enabled users.

Update Mailbox-Enabled Objects only

Checking this box will cause Directory Sync Pro for Active Directory to only update those objects that are mail-enabled.

Inter Forest Exchange Migration

Configure Contacts for Delegation

Choose how to configure contacts for delegation.

Add x500 Proxy to Source

If you need to migrate mailbox permissions, check the box that adds the x500 proxy to the source. Note that this is one of the only times that Directory Sync Pro for Active Directory makes any changes to a SOURCE object.

Enable Resource Forest

If you are migrating your mailboxes into a resource forest, check the Enable Resource Forest box. This will set the Master Account SID on all synchronized mailboxes in the target environment.

Email Address Policies

You have the option to create your own scripts using PowerShell that can be run against after a sync is completed. The script will run using the target credentials that you entered when creating this profile.

Matching Options

Directory Sync Pro for Active Directory looks for selected object attributes that you have chosen to match objects between the source and target. This screen allows you to control several Directory Sync Pro for Active Directory parameters for this process.

Matching Level Method

Choose the scope in which Directory Sync Pro for Active Directory should search for matching objects. If you choose Forest, Directory Sync Pro for Active Directory will examine the entire AD forest to match objects. If you choose domain, Directory Sync Pro for Active Directory will only check for matching objects at the domain level for those domains within the scope of this profile.

Matching Action

This is perhaps the most important parameter on this page. What do you want Directory Sync Pro for Active Directory to do if it finds a match based on your chosen mapping parameters? The default is Create or Update. This means that if Directory Sync Pro for Active Directory does not find a match, it will create a new object in the target. If a match is found, Directory Sync Pro for Active Directory will update the attribute values on the target object using the values from the attributes of the source object.

If you choose Create Only, then Directory Sync Pro for Active Directory will create a new object in the target for any unmatched objects. It will not update any attributes for those objects that have been matched.

Choose Update Only to update the attributes from source objects to matched target objects. No new objects will be created if a match is not found. A scenario in which you might choose this would be when the users have been pre-created in the target manually, and you just want to keep changes synchronized.

And finally, Match Only, No update (option not available for Exchange Intra-Forest Profiles) will make no changes to any objects. This is only chosen when you are using another product other than Migrator Pro for Active Directory for AD synchronization. It will import the values that are needed when Migrator Pro for Active Directory performs the ReACL and Cutover actions.

Matching Object Types

There may be the rare occasion where an object of one type in the source has a matching value for an object of another type in the target. Since these are not the same type, you may want Directory Sync Pro for Active Directory

to be more precise in deciding if an object is a match. Check this box to require the type of object to be a final matching criterion.

For example, suppose CN or Common name is one of your matching criterion. And in the source we have a user with a Common Name of Cheryl in the source. In the target, we have a contact with the Common name of Cheryl. Directory Sync Pro for Active Directory would normally match these objects because they have the same Common name. If you check this box, it will consider that the object class is not the same, and therefore these objects do not match after all.

Relink Objects

The relink option only comes in to play in the rare occasion that you have reset a profile thereby removing the objects created by this profile from the SQL database. But you did not delete the actual target objects created by Directory Sync Pro for Active Directory. Without the relink option, when this profile is synced again, Directory Sync Pro for Active Directory would not recognize the objects that it may have already migrated to the target as created by itself. This could cause unwanted behavior, depending on your Matching Action choices. This may also cause problems if you had chosen the rename option for collisions, as the rename could be appended or prepended twice due to an already existing renamed target object. We suggest that you leave this box checked. This will allow Directory Sync Pro for Active Directory to look for a special attribute that is populated by Directory Sync Pro for Active Directory in the target so that it knows that this object was created by Directory Sync Pro for Active Directory.

Restore Ready-to-Sync

This option works in conjunction with the relink option. If Directory Sync Pro for Active Directory finds an target object that it had previously created based on the special relink attribute, it will mark the matching source object as Ready to Sync. This means the object will be included and updated during the next sync cycle, as long as Update is part of one of your Matching Action choices. We suggest that you leave this box checked.

Attribute Mapping

The mappings page controls where and how the values of a source attribute should be placed in the target attribute. By default this is a one-to-one mapping, but you can change it. For example, whatever the value is for company name for all objects in the source that have that value will be used to the fill the company name value for all objects that have that attribute in the target. However, you can edit and customize the mappings to fit any special needs.

As an example, suppose that you are doing an inter-forest migration where the target company has acquired the source company. The source company uses the Employee Number field as a unique identifier. However, the target company uses the Employee ID for this same purpose. We can modify the mappings to make this adjustment. First, we will make sure that the Employee ID field in the source does NOT get mapped to the EmployeeID field in the target as we plan to have a different source field mapping to that. we can just empty it out, or we could remove the entire mapping.

Now we will map the Employee Number source field to the employee ID target field. If you need to get more granular, you can specify the source and target object types that this should only occur with. Such as just user target objects. In my example, there is no need because this attribute is only found on user objects anyway.

You can control the number of items included in the window here. You can search for a particular mapping with the search box. You can filter the attributes by object type to narrow your listing.

Click on the advanced button for more options, including the ability to reset everything.

Reset Mappings

Choose default mappings to return all mappings to the default. All standard AD attributes will be mapped, any manually added mappings or attributes discovered as part of the AutoMap process will be deleted.

Choose Discover Custom Attributes if you are using software that has extended the schema. Directory Sync Pro for Active Directory will populate the source and target field column with any newly-discovered attributes. You can then manually choose the ones that you want to map.

Or, choose Auto Map, and Directory Sync Pro for Active Directory will map these extended attributes wherever it find a match between the source and target fields.

As a final option, you can import a CSV file that contains only the mappings that you would like to use. If you import mappings, be sure that the file contain all of the mappings that you intend to use, as importing this file will completely overwrite all existing mappings.

Sync Types

Synchronization is the process of making changes to the SQL database. You can run synchronization on a regular schedule as part of your profile settings, or you can manually run a synchronization here at any time.

Before we examine these choices, let's look at the terminology used for synchronization. Extracting information from the source and putting it into the SQL database is called a PUSH. Extracting information from SQL to create objects in the TARGET is call a PULL.

The most common action is a Push Pull. This will update or PUSH, the SQL database with any changes to the source, and then the target will pull those changes from SQL into itself. This will cause any new objects to be created in the target, and updates to existing source objects to be updated in the matching target object, depending on your matching action choices. If you are using our Migrator Pro for Active Directory product, a Push Pull sync is what happens when you press the Sync button in that console.

Another common action is to run a simulation. This will do a PUSH into the SQL database, but no changes will be made in the target. This will result in a sync report appearing in the logs and reports page. It's a good idea to run a simulation before you actually do a real Push/Pull. This will allow you to look for any errors or issues and fix them before the real thing.

Rarely, you may choose to perform only a PUSH or only a Pull action if need to made some corrections to help SQL match the actual environment without a complete sync ,or as instructed by Support.

A profile must be in the Active state before you can perform any type of synchronization.

Profile Actions

Once you have configured and saved a profile, you can optionally export it for reuse later. You can then import again and make only the needed changes for your next profile, instead of starting from scratch.

Resetting a profile will remove all objects from SQL that were "pushed" into SQL by the profile. If this includes devices, you will be prompted to confirm that you want to remove devices also, as this is not typical. Resetting a profile is not common. If you reset a profile without removing the objects "pulled" into the target by that profile, consider the relink and "Mark as ready to sync" options on the Matching Options settings page.

Removing a profile is the most extreme profile action. It resets the profile as just mentioned, and then, removes the profile entirely.

You can Validate a profile to run a pre-check on your profile connectivity settings.

Nodes

The Nodes feature allows two or more Directory Sync Pro for Active Directory services to be installed and configured to point to the same SQL database, and ensures that only one instance is active and syncing objects. This feature is designed for basic disaster recovery purposes. This feature only applies to the AD service (BinaryTree.DirSync.Exhange.exe).

Each instance of the Directory Sync Pro for Active Directory service is referred to as a Node. Only one node can be active at any moment and is the only node that will sync profiles. Nodes can be switched between active and passive on the Nodes screen.

Nodes must be started and stopped manually from the server on which they are installed. Only the state of the Node (active or passive) can be changed on the Nodes screen.

Directory Sync Pro for Active Directory Nodes

The Nodes list has the following columns:

- **Name:** The name of the server on which the Node is running.
- **Status**: The status of the server, whether it is Online or Offline.
- **State:** The state of the server, whether it is the Active Node or a Passive node.
- **Last Contact:** The last time the Node checked in with SQL.

The Nodes screen has the following buttons:

- **Deactivate:** Makes an Active Node into a Passive Node. This button is only available when the Active Node is selected in the list. Any running sync jobs will be canceled.
- **Activate:** Makes a Passive Node into the Active Node. Only one Node can be active at a time, so this button is only available when all Nodes are Passive Nodes.
- **Remove:** Removes a Node from the list. The Active Node cannot be removed, so this button is only available for Passive Nodes.
- **Refresh:** Refreshes the Nodes list. The list does not automatically refresh.

Click the Node to view additional details, such as the Node's unique GUID.

Node Running

Periodically (every 30 seconds), a node will check in with SQL to determine if it should switch state to Active or Passive. Any node state switches will be written to the Windows Event Log.

If the node is Active and it is switched to Passive, any running syncs will continue to run to completion. This will allow the node to cancel any running profiles.

Removing a node from the list on the Nodes screen does not terminate or uninstall the node. Nodes must be manually stopped and uninstalled.

The Last Contact time will be updated every time the node checks in. If a node shows as online but there have not been any updates to the Last Contact time within the last 30 seconds, the node may have terminated unexpectedly.

Node Shutdown - Normal Termination

When a node is shutdown (the service is stopped) it will notify SQL that it is shutting down. This will change the status of the node to Offline. The Last Contact time will also be updated. The state of the node will not change.

Node Shutdown - Unexpected Termination

If a node terminates unexpectedly, then SQL will not be notified of the shutdown. In this case, the node will still be shown in the Nodes screen as Online, but the Last Contact time will no longer be updated.

If a passive node terminates unexpectedly, the service can be manually restarted.

If the active node terminates unexpectedly, it will still be displayed on the Nodes screen as the active node. There are two options in this case:

- The node may be manually restarted, and will resume processing as the active node.
- The node may be deactivated on the Nodes screen. Running profiles will be marked for cancellation and the currently active node will be made a passive node. Once this is done, a different node can be made the active node.

If the crashed node will no longer be used, it can be removed from the Nodes screen.

General Settings

If your migration project includes Exchange as a source or target, you can modify your options on this screen.

Exchange Options

Promote Target User Contacts

If you check this box, any TARGET contacts will be converted into mail-enabled users.

For the scope of this feature a Microsoft Exchange Mail Enabled Contact is defined as an Active Directory contact where the LegacyExchangeDN attribute is not null. A contact will be promoted to a user if the primary SMTP address on the a source object matches the external or target email address of the contact. Once the attributes have been stored on the newly created Microsoft Exchange User on the target, the Contact object will be removed from the target. The source User must have a LegacyExchangeDN. The contacts in the source, that will be converted, must be in a different OU than the Target OU selected on the AD Target tab.

This option may not be selected if the setting Create Mail Enabled Users As on the AD Target Options Users tab is set to Contact, or if the source object is already a contact.

Promote Target Group Contacts

If you check this box, any TARGET groups will be converted into mail-enabled users.

Update Mailbox-Enabled Objects only

Checking this box will cause Directory Sync Pro for Active Directory to only update those objects that are mail-enabled.

Configure Contacts for Delegation

Choose how to configure contacts for delegation.

Add x500 Proxy to Source

If you need to migrate mailbox permissions, check the box that adds the x500 proxy to the source. Note that this is one of the only times that Directory Sync Pro for Active Directory makes any changes to a SOURCE object.

Enable Resource Forest

If you are migrating your mailboxes into a resource forest, check the Enable Resource Forest box. This will set the Master Account SID on all synchronized mailboxes in the target environment.

PowerShell Script

You have the option to create your own scripts using PowerShell that can be run against after a sync is completed. The script will run using the target credentials that you entered when creating this profile.

General Object Settings

Target Proxy Address Overwrite Behavior

If you check this box, source proxy addresses will always overwrite the proxy addresses in the target, replacing whatever values are there, if any. If this box is left unchecked, the source proxy address will only be added to those target objects where this attribute is currently empty.

User Object Settings

Options for AD Inter-forest and Intra-Forest Profiles

AS-IS means the objects will be created just as they currently exist in the source. If the account was disabled in Active Directory in the source, it will be disabled in Active Directory when created in the target. If the account was enabled in Active Directory in the source, it will be created as enabled in Active Directory in the target.

You can also choose to Active Directory enable all objects when they are created in the target, no matter their Active Directory account status in the source. Or, just the opposite, you can choose to have all objects created in an account disabled state in the target, no matter their status in the source.

For mail-enabled objects only, there is also the option is to convert all mail-enabled objects into contacts when they are created in the target.

Options for Exchange Inter-forest Profiles

AS-IS means the objects will be created just as they currently exist in the source. If the account was disabled in Active Directory in the source, it will be disabled in Active Directory when created in the target. If the account was enabled in Active Directory in the source, it will be created as enabled in Active Directory in the target.

You can also choose to enable all objects when they are created in the target, no matter their status in the source. Or, just the opposite, you can choose to have all objects created in an account disabled state in the target, no matter their status in the source.

You may also choose to convert all the mail-enabled objects into contacts when they are created in the target.

You would use this profile in conjunction with our Exchange Pro mailbox migration product.

Options for Exchange IntRA-forest Profiles

AS-IS means the objects will be created just as they currently exist in the source. If the account was disabled in Active Directory in the source, it will be disabled in Active Directory when created in the target. If the account was enabled in Active Directory in the source, it will be created as enabled in Active Directory in the target.

Note that All objects created will be Mail-Disabled, no matter what their Active Directory account status.

You can also choose to enable all objects when they are created in the target, no matter their status in the source. Or, just the opposite, you can choose to have all objects created in an account disabled state in the target, no matter their status in the source.

You may also choose to convert all the mail-enabled objects into contacts when they are created in the target.

User Conflicts

How do you want to handle any users conflicts? That is what should happen if (based on your matching criteria) that Directory Sync Pro for Active Directory finds a matching user already in the target? If you choose skip, Directory Sync Pro for Active Directory will not make an association between those objects, and an error will be noted in the log file.

With Update, Directory Sync Pro for Active Directory will consider those items the same. This means that any changes made to the source will update that matched item in the target, if you have set updates to occur. No new object will be created.

With Rename, a new object will be created in the target. You will need to distinguish this from the matched target object by giving it a new name. You can manually add a prefix or suffix of your choice, or, you choose any existing AD attribute to be prepended or appended to the name. Remember that if you choose rename, when you update the object in the source, it will be the Renamed object in the target that gets updated during a synchronization.

User SID History

You have the option to include an object's SID history during the migration. This will help prevent issues with some software, and network shared printers. We suggest this option. Consider however, that in a large enterprise, this might cause the Kerberos token to exceed the max token size for users that belong to many groups. You could mitigate that issue with a GPO that is set to accept larger tokens.

If you do choose to migrate SID History, all Domain Controllers that you have listed in the Target DC's tab will need access to the Domain Controller that holds the PDC Emulator FSMO role in the source.

Group Object Settings

Options for AD Profiles

By default, groups will retain their current group scope when they are migrated. You have the option to change that here, so that you can transform a group's scope as it is migrated. For example, if the new target does not have multiple domains, you may choose to convert your Universal Groups into Domain Local groups. Or you can choose not to migrate a particular group scope at all. There are some limitations on changing the scope of nested groups, so you may want to refer to the following TechNet link.

https://technet.microsoft.com/en-us/library/cc755692(v=ws.10).aspx

Options for Exchange Profiles

By default, your mail-enabled groups will retain their current group scope when they are migrated. You have the option to change that here, so that you can transform a group's scope as it is migrated. You can also change the group to a contact, or you can choose not to migrate a particular group scope at all.

Group Conflicts

Options for AD and Exchange to AD Profiles

If you choose skip, Directory Sync Pro for Active Directory will not make an association between those objects, and an error will be noted in the log file.

If you choose Merge, Directory Sync Pro for Active Directory will consider those items the same. This means that any members of the source group will be added to the membership list of the target group, if you have set updates to occur. No new object will be created.

With Rename, a new Active Directory group object will be created in the target. You will need to distinguish this from the matched target object by giving it a new name. You can manually add a prefix or suffix of your choice, or, you choose any existing AD attribute to be prepended or appended to the name. Remember that if you choose rename, when you update the object in the source such as adding another member, it will be the Renamed group object in the target that gets updated during a synchronization.

Do Not Sync Group Members

If the "Do Not Sync Group Members" option is enabled, only the Group object and associated mapped fields will be synced and Group members will be skipped.

Synchronize Members as Foreign Security Principals

If "Synchronize Members as Foreign Security Principals" is enabled, group members that cannot be matched in the target will be synchronized as Foreign Security Principals if trust relationships allow it and the target group is a Domain Local Security Group.

Device Object Settings

By default, the Active Directory account status of device is maintained when the object is created in the target. If a device was Active Directory enabled in the source, it will be enabled in the target, and vice-versa. Or, choose enabled, to make all migrated devices immediately Active Directory enabled, no matter what their status was in the source.

Maybe you want to ensure that these devices should not be available until a later time even after the device has been cutover. In that case, you can choose disabled, which will cause all migrated devices to be Active Directory disabled, no matter what the status in the source.

Device Conflicts

By default, the Active Directory account status of device is maintained when the object is created in the target. If a device was Active Directory enabled in the source, it will be enabled in the target, and vice-versa. Or, choose enabled, to make all migrated devices immediately Active Directory enabled, no matter what their status was in the source.

Maybe you want to ensure that these devices should not be available until a later time even after the device has been cutover. In that case, you can choose disabled, which will cause all migrated devices to be Active Directory disabled, no matter what the status in the source.

Advanced Settings

Matching Advanced Settings

Directory Sync Pro for Active Directory looks for selected object attributes that you have chosen to match objects between the source and target. This screen allows you to control several Directory Sync Pro for Active Directory parameters for this process.

Matching Level Method

Choose the scope in which Directory Sync Pro for Active Directory should search for matching objects. If you choose Forest, Directory Sync Pro for Active Directory will examine the entire AD forest to match objects. If you choose domain, Directory Sync Pro for Active Directory will only check for matching objects at the domain level for those domains within the scope of this profile.

Matching Action

This is perhaps the most important parameter on this page. What do you want Directory Sync Pro for Active Directory to do if it finds a match based on your chosen mapping parameters? The default is Create or Update. This means that if Directory Sync Pro for Active Directory does not find a match, it will create a new object in the target. If a match is found, Directory Sync Pro for Active Directory will update the attribute values on the target object using the values from the attributes of the source object.

If you choose Create Only, then Directory Sync Pro for Active Directory will create a new object in the target for any unmatched objects. It will not update any attributes for those objects that have been matched.

Choose Update Only to update the attributes from source objects to matched target objects. No new objects will be created if a match is not found. A scenario in which you might choose this would be when the users have been pre-created in the target manually, and you just want to keep changes synchronized.

And finally, Match Only, No update (option not available for Exchange Intra-Forest Profiles) will make no changes to any objects. This is only chosen when you are using another product other than Migrator Pro for Active Directory for AD synchronization. It will import the values that are needed when Migrator Pro for Active Directory performs the ReACL and Cutover actions.

Matching Object Types

There may be the rare occasion where an object of one type in the source has a matching value for an object of another type in the target. Since these are not the same type, you may want Directory Sync Pro for Active Directory to be more precise in deciding if an object is a match. Check this box to require the type of object to be a final matching criterion.

For example, suppose CN or Common name is one of your matching criterion. And in the source we have a user with a Common Name of Cheryl in the source. In the target, we have a contact with the Common name of Cheryl. Directory Sync Pro for Active Directory would normally match these objects because they have the same Common name. If you check this box, it will consider that the object class is not the same, and therefore these objects do not match after all.

Relink Objects

The relink option only comes in to play in the rare occasion that you have reset a profile thereby removing the objects created by this profile from the SQL database. But you did not delete the actual target objects created by Directory Sync Pro for Active Directory. Without the relink option, when this profile is synced again, Directory Sync Pro for Active Directory would not recognize the objects that it may have already migrated to the target as created by itself. This could cause unwanted behavior, depending on your Matching Action choices. This may also cause problems if you had chosen the rename option for collisions, as the rename could be appended or prepended twice due to an already existing renamed target object. We suggest that you leave this box checked. This will allow Directory Sync Pro for Active Directory to look for a special attribute that is populated by Directory Sync Pro for Active Directory in the target so that it knows that this object was created by Directory Sync Pro for Active Directory.

Restore Ready-to-Sync

This option works in conjunction with the relink option. If Directory Sync Pro for Active Directory finds an target object that it had previously created based on the special relink attribute, it will mark the matching source object as Ready to Sync. This means the object will be included and updated during the next sync cycle, as long as Update is part of one of your Matching Action choices. We suggest that you leave this box checked.

Mapped Fields Advanced Settings

The mappings page controls where and how the values of a source attribute should be placed in the target attribute. By default this is a one-to-one mapping, but you can change it. For example, whatever the value is for company name for all objects in the source that have that value will be used to the fill the company name value for all objects that have that attribute in the target. However, you can edit and customize the mappings to fit any special needs.

As an example, suppose that you are doing an inter-forest migration where the target company has acquired the source company. The source company uses the Employee Number field as a unique identifier. However, the target company uses the Employee ID for this same purpose. We can modify the mappings to make this adjustment. First, we will make sure that the Employee ID field in the source does NOT get mapped to the EmployeeID field in the target as we plan to have a different source field mapping to that. We can just empty it out, or we could remove the entire mapping.

Now we will map the Employee Number source field to the employee ID target field. If you need to get more granular, you can specify the source and target object types that this should only occur with. Such as just user target objects. In my example, there is no need because this attribute is only found on user objects anyway.

You can control the number of items included in the window here. You can search for a particular mapping with the search box. You can filter the attributes by object type to narrow your listing.

Click on the advanced button for more options, including the ability to reset everything.

Exceptions Advanced Settings

The exceptions screen allow you make exceptions to guide Directory Sync Pro for Active Directory in matching and or mapping particular attributes when you know there is an exception to normal behavior. For example, suppose that a company had pre-created some users in their target Active Directory environment whose attributes are not an exact match for one of Directory Sync Pro for Active Directory Matching attributes. In the source, we have a user whose sAMAccountName is Fred. They have already made an account in the target for Fred, but the sAMAccountName is Frederick in the target. Directory Sync Pro for Active Directory would not find a match, and

would consider Fred and Frederick to be different users. Directory Sync Pro for Active Directory would create a new account called Fred in the target, not knowing they were supposed to be the same. You can let Directory Sync Pro for Active Directory become aware of this by making a manual exception.

Choose the source field, in this case sAMAccountName, and the source value of Fred, the target field will be the same, only the value will be Frederick. Next,choose the exception type, Map Only, Match Only, or Map and Match. In this example, you would choose Match Only, because you want Directory Sync Pro for Active Directory to consider these mismatched attributes as a match for matching purposes. Choose Map only if you just want to change the value of a particular target attribute based on the specific value of a source attribute. For example, the source company has a department call Information Technology, but they have been acquired by a target company that calls that department Business Technology. Just enter the appropriate values , and choose Map only. You can also do both by choosing Map and Match.

If you have a lot of exceptions, you can create a CSV file and import it on this screen. A sample template file is provided for download.

Overrides Advanced Settings

An override is used to transform data as it is migrated from source to target. If it can be done with a SQL statement, you can make an override to perform the task. A full SQL Select statement is not required as Directory Sync Pro for Active Directory generates portions of the statement for you. For example, if the target company requires a five digit employee number and the source company has no requirements, you could create an override to add those leading zeros

Click **Add Override** and then tell Directory Sync Pro for Active Directory if this override affects people or groups. Choose a valid internal field name that will be transformed by this override. You can see a list on the mapping screen.

For Field value, this is where you would enter a correctly formatted SQL statement.

We recommend that you add a comment to describe this override.

Double click on an override if you need to edit it. You cannot change the View or Field Name of an existing override.

Please use caution as Overrides are global. Once you create an override in a profile, it affects all profiles in Directory Sync Pro for Active Directory. You can import and export your Overrides, or choose reset overrides to return DirSync to the default profile settings.

See the help topic called Customizing Overrides for more details and more examples.

Logs and Reports

Logs

Select any log for more information. The level of detail for the log files is determined by the profile settings.

Reports

Select any report for more information. If you choose to run a simulated sync, the results will be viewed here as a sync report.

Additional Topics

Command-line Sync

A synchronization or sync report of a profile cannot be started if a synchronization or sync report of the profile is already running.

To manually start a synchronization process from a command line:

1. Open a Command Prompt window.
2. Navigate to %Program Files%\Binary Tree\Dirsync
3. Enter the command *BinaryTree.DirSync.Exchange.exe*, followed by the desired switch, *ProfileID* (if required), and the “Quit” option if desired.

Command switches:

/validate - Validates profile settings.

/settings - Write settings to console.

/reset - Clears all data from database.

/sync - Sync all profiles in parallel.

/resync - Clears all data from database and sync all profiles in parallel.

The following switches accept a DirSync Profile ID or will prompt you to select a profile:

/push - Scans source OUs for changes and stores in database.

/pull - Writes changes to target objects.

/pushpull - Scans source OUs for changes and writes changes to target objects.

/repush - Clears profile specific objects from database and run push operation.

/repull - Marks profile specific objects for resync and writes changes to target.

/repushpull - Clears profile specific objects from database and runs full sync operation.

Option:

/quit - Quits after a command executes, otherwise will prompt for user input.

Renames and moves fail to work if you are using a manual /repushpull or /resync command. Before running the /repushpull /repush /repull and /resync commands, administrators should clear the target OU of any previously created Directory Sync Pro for Active Directory objects.

If you do not include a Profile ID in the command, you will be prompted to choose one.

Supporting a Mixed Exchange 2003, 2007, 2010, 2013, 2016 Environment

Synchronizing Rooms from Exchange 2003 to Exchange 2010

Due to the differences in the management of Rooms between Exchange 2003 and Exchange 2010, a custom mapping is required for Rooms from an Exchange 2003 source to appear as a Room object in a target Exchange 2010 environment. The following fields must appear in the target Room objects for them to display as Rooms.

Attribute	Value
MSExchResourceDisplay	Room
MSExchResourceMetaData	Resource Type: Room
MSExchResourceSearchProperties	Room
MSExchResourceDisplayType	7
MSExchResourceRecipientTypeDetails	16

The Room must be a mailbox –enabled object in the source AD and cannot be a Public Folder

Quest does not recommend manually editing any attributes from the target directory. All updates should be from the authoritative source directory or via custom mapping

There must be an identifying attribute in the source object that is used to distinguish these objects as Exchange 2003 Rooms. For this example, we have set the extension Attribute1 to “btroom”.

To customize the mapping so that Exchange 2003 rooms appear as rooms in Exchange 2010:

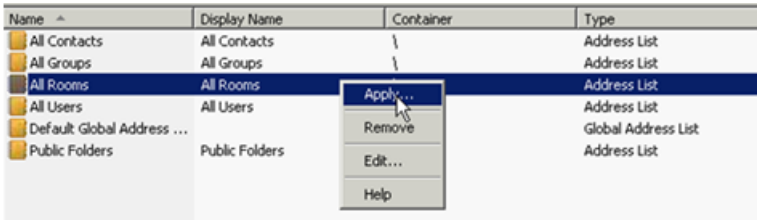
1. From the project overview, choose your profile and click **Manage**.
2. From the summary screen choose **Settings**, then **Advanced**, then **Overrides**.
3. Click **Add Override**. The Override dialog box appears.
4. Select a **Person** or **Groups** from the **View** drop-down list.

5. Enter the following values:
    - **FieldName**: Enter the name of the field from the view that you want to override (TargetAddress, BTCustom001, and so on)
    - **FieldValue**: Enter the SQL statement that is used to calculate the value for the field.

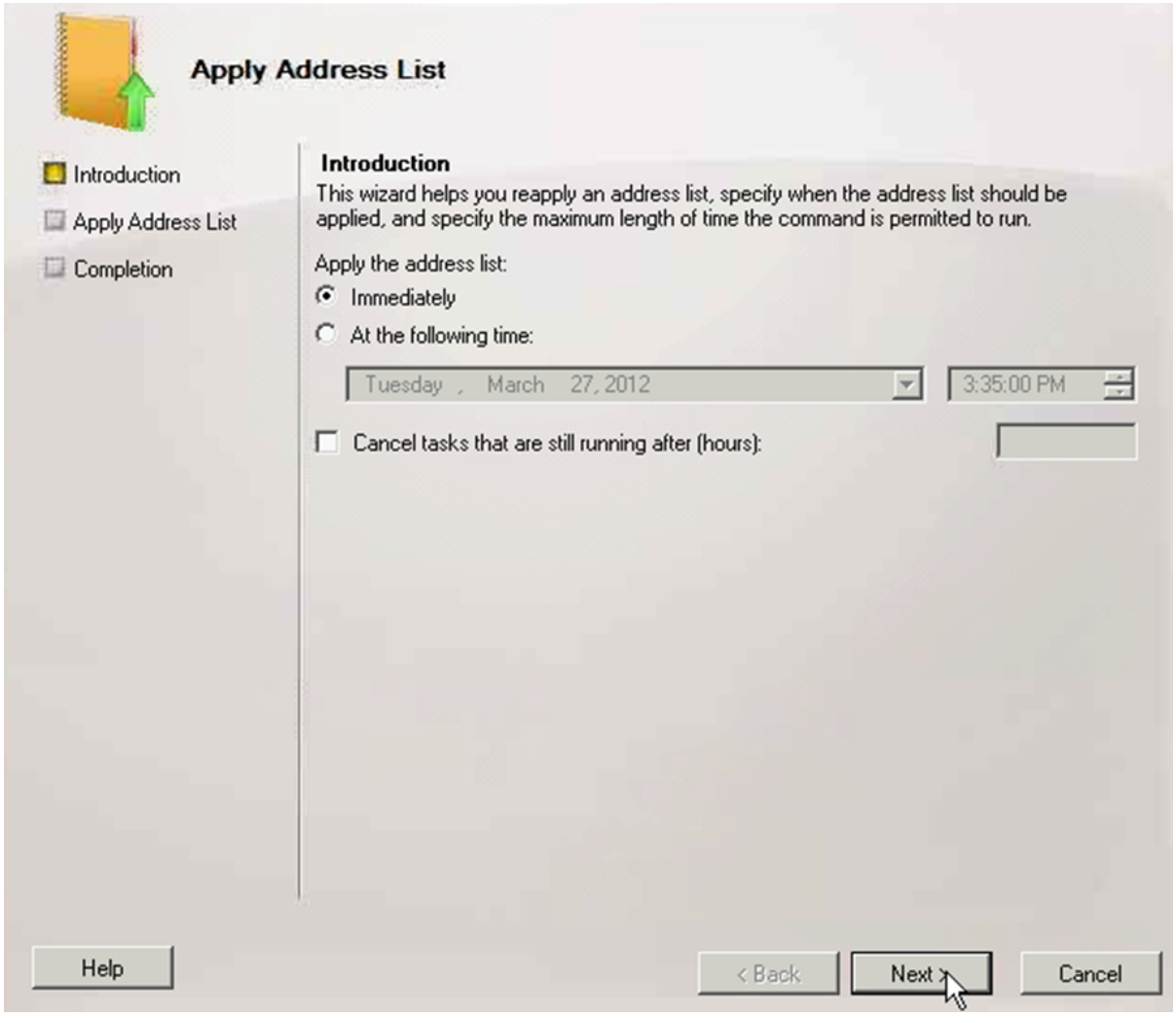
View	Field Name	Field Value
Person	msExchResourceDisplay	CASE WHEN P.msExchResourceDisplay IS NOT NULL THEN P.msExchResourceDisplay ELSE (CASE P.Extension1 WHEN 'btroom' THEN 'Room' ELSE NULL END) END
Person	msExchResourceMetaData	CASE WHEN P.msExchResourceMetaData IS NOT NULL THEN P.msExchResourceMetaData ELSE (CASE P.Extension1 WHEN 'btroom' THEN 'ResourceType:Room' ELSE NULL END) END
Person	msExchResourceSearchProperties	CASE WHEN P.msExchResourceSearchProperties IS NOT NULL THEN P.msExchResourceSearchProperties ELSE (CASE P.Extension1 WHEN 'btroom' THEN 'Room' ELSE NULL END) END
Person	msExchRecipientDisplayType	CASE WHEN P.msExchRecipientDisplayType IS NOT NULL THEN P.msExchRecipientDisplayType ELSE (CASE P.Extension1 WHEN 'btroom' THEN '7' ELSE NULL END) END
Person	msExchRecipientTypeDetails	CASE WHEN P.msExchRecipientTypeDetails IS NOT NULL THEN P.msExchRecipientTypeDetails ELSE (CASE P.Extension1 WHEN 'btroom' THEN '16' ELSE NULL END) END

6. You can now synchronize Rooms from Exchange 2003 to Exchange 2010.
7. Once these rooms are in the target directory, go to the Exchange Management Console (EMC) in the target 2010 environment.
8. Expand the Organization Configuration folder, select **Mailbox**, and then select **All Rooms**.

9. Right click on **All Rooms** and then select **Apply**.



10. Click **Next** and then **Finish** to reapply the address list.



Additional Configuration Options

Changing the attribute used for "Created by Dirsync" or "Updated by Dirsync"

By default, the adminDescription attribute is stamped on objects on the Target that are created or updated by Directory Sync Pro for Active Directory with "Created by Dirsync" or "Updated by Dirsync" to define which objects can be safely deleted from the Target. An app setting is available in the config file to allow you to define a different attribute/field for this purpose.

To use an attribute other than adminDescription or $BTAction, define a new DirSyncAttribute setting in the <appSettings> section of the config file. For example, the below setting will use adminDisplayName instead of adminDescription:

Warning: This must be configured before the initial sync.

```
<appSettings>
<add key="DirSyncAttribute" value="adminDisplayName"/>
</appSettings>
```

Setting msExchRecipientDisplayType and msExchRecipientTypeDetails Exchange attributes

A configuration option to allow you to set msExchRecipientDisplayType and msExchRecipientTypeDetails Exchange attributes based on the value of a configurable attribute is available. This option is only applied to target objects not created by Directory Sync Pro for Active Directory.

The configuration option must defined in the <appSettings> section of the config file, as shown below. “Value=” should be contain the attribute to be used. (proxyAddresses shown below). If the value of the target attribute is null, msExchRecipientDisplayType and msExchRecipientTypeDetails will be populated. See the list below for the values that will be populated.

```
<appSettings>
<add key="RecipientType_MailEnabledAttribute" value="proxyAddresses"/>
</appSettings>
```

Mail Enabled Users in the source:

- msExchRecipientDisplayType = 6
- msExchRecipientTypeDetails = 128

Room Mailbox in the source:

- msExchRecipientDisplayType = 7
- msExchRecipientTypeDetails = 16

Resource Mailbox in the source:

- msExchRecipientDisplayType = 8
- msExchRecipientTypeDetails = 32

Shared Mailbox in the source:

- msExchRecipientDisplayType = 0
- msExchRecipientTypeDetails = 4

Allow objects with remote mailboxes to be treated as mailbox-enabled objects

A setting that allows objects with connected O365 remote mailboxes to be treated as mailbox-enabled objects is available. To enable this feature, add the RemoteMailboxAsMailboxEnabled option to the <appSettings> section of the BinaryTree.DirSync.Exchange.exe.config file as displayed below.

```
<appSettings>
<add key="RemoteMailboxAsMailboxEnabled" value="True"/>
</appSettings>
```

If this setting is set to any value other than True or if omitted from the file, objects with remote mailboxes will be treated as non-mailbox-enabled. If set to True, objects with remote mailboxes will be treated as mailbox-enabled.

Specify a timeout for password sync

A configuration option in the appSettings section of the config file to specify a timeout for password sync is available. In large environments, it may take longer than the default 300 second timeout to complete the password sync process and may need to be lengthened.

This setting should be added to the BinaryTree.DirSync.Exchange.exe.config file.

```
<appSettings>
<add key="PasswordSyncTimeoutSeconds" value="300"/>
</appSettings>
```

Set the value to configure the timeout to a specific number of seconds. If this setting is omitted, or set to an invalid value, the timeout will be set to 300 seconds (5 minutes). To disable the timeout functionality, set to -1 (or any negative value).

Disable the caching of group members

A configuration option can be used in the appSettings section of the config file to disable the caching of group members.

This setting should be added to the BinaryTree.DirSync.Exchange.exe.config file.

```
<appSettings>
<add key="OptimizeGroupSyncMemoryUsage" value="true"/>
</appSettings>
```

Valid values are true and false. If this setting is omitted, or set to an invalid value, the value defaults to false. If set to false, group members will be cached during push and pull. If set to true, group members will not be cached during push and pull.

Disable the initialization of the sync report

A configuration option can be used in the appSettings section of the config file to disable the initialization of the sync report. If disabled, a sync report will still be recorded, but it will not be initialized between syncs. The result will be that an object will show data from the last time it was processed by Directory Sync Pro for Active Directory, rather than just the most recent time it was processed. In other words, if an object is inserted during a sync, it will show in the sync report as Inserted. Assuming a second sync does not touch this object, then if the sync report is initialized, a second sync will show this object as No Change, but if the sync report is not initialized, the object will still show as Inserted.

This setting should be added to the BinaryTree.DirSync.Exchange.exe.config file.

```
<appSettings>
<add key="DisableSyncReportInitialization" value="true"/>
</appSettings>
```

Valid values are true and false. If this setting is omitted, or set to an invalid value, the value defaults to false. If set to false, the sync report will be initialized. If set to true, the sync report will not be initialized.

Set the maximum number of users and groups synced simultaneously

During pull processing, Directory Sync Pro for Active Directory will sync multiple Active Directory user and group objects simultaneously into the target AD. The maximum number of users and groups synced simultaneously can be changed using the ThreadCount setting in the config file. If this configuration option is not specified, the ThreadCount will be set to the same number of logical processor cores of the server on which Directory Sync Pro for Active Directory is running.

The configuration option is not included by default. To add, modify the BinaryTree.DirSync.Exchange.exe.config file located at C:\Program Files\Binary Tree\DirSync and add a new key to the <appSettings> section as follows:

```
<appSettings>
<add key="ThreadCount" value="4"/>
</appSettings>
```

This option should never be set to a number greater than the number of processor cores on the server. However, you may need to specify a lower number if other applications also running on the server require a specific number of cores set aside for processing. Best practice is to leave the setting at the default value and lower it only if additional processing power is needed for other applications on the server.

Multiple passes will be needed to make sure all data is synchronized to the target when multi-threading is used. An example scenario is:

- User B is the Manager of User A.
- User A is synchronized first.
- Then, User B is synchronized.
- Another sync is needed for User B to be the Manager on User A.

Passwords are copied if a prior sync failed

A configuration option can be used in the appSettings section of the config file to ensure passwords are copied even if a prior sync failed.

This setting should be added to the BinaryTree.DirSync.Exchange.exe.config file.

```
<appSettings>
<add key="RepushAllPasswords" value="true"/>
</appSettings>
```

Valid values are true and false. If set to true, Directory Sync Pro for Active Directory will process passwords for all users during the push. Any users with changed passwords will be processed on the pull. Using this option will increase the sync time, but ensure that all passwords are made current. If set to false or the setting is omitted, this option is disabled.

Set the number of objects selected when the user selects all (Ctrl+A)

A configuration option can be added to control how many objects are selected when the user selects all (Ctrl+A):

```
<appSettings>
<add key="SelectAllLimit" value="1000"/>
</appSettings>
```

If this configuration option is omitted, the default value is 1000. Setting this option to a high number may cause performance issues when selecting and marking objects.

Setting select all limit when marking objects as Ready to Sync

Selecting objects to mark as Ready to Sync can be done from the Objects tab within the Sync Report, which contains all object types.

A configuration option can be used in the appSettings section of the config file to control how many objects are selected when the user selects all (Ctrl+A):

This setting should be added to the BinaryTree.DirSync.Exchange.exe.config file.

```
<appSettings>
<add key="SelectAllLimit" value="1000"/>
</appSettings>
```

If this configuration option is omitted, the default value is 1000. Setting this to a high number may cause performance issues when selecting and marking objects.

This option does not apply to Windows Server Migration profiles.

Set the attribute used for the linking function

A configuration option can be added to change the attribute used for the linking functionality.

This setting should be added to the BinaryTree.DirSync.Exchange.exe.config file.

```
<appSettings>
<add key="LinkedIDAttribute" value="adminDisplayName"/>
</appSettings>
```

If this configuration option is omitted, adminDisplayName is used.

Set the delay period before running a post sync PowerShell script

A configuration option can be added to change the delay length prior to running the post sync PowerShell script. By default, the delay is 300 seconds (5 minutes).

This setting should be added to the BinaryTree.DirSync.Exchange.exe.config file.

```
<appSettings>
<add key="PostScriptDelaySeconds" value="300"/>
</appSettings>
```

Define attributes to treat as multi-value attributes

A configuration option can be added to include a comma separated list of user defined attributes to treat as multi-value attributes:

```
<appSettings>
<add key="MultiValuedAttributes" value=""/>
</appSettings>
```

To enable this specialized handling, provide one or more multi-value attributes to write to in the list.

Example:

<add key="MultiValuedAttributes"
value="accountNameHistory,msExchExtensionCustomAttribute1,msExchExtensionCustomAttribute2"/>

Then, specify the mapping that targets this attribute.

Mapping can be:

- SingleValue to MultiValue - Supports Overrides
- MultiValue to MultiValue - Does not support Overrides

When the attribute is defined in MultiValuedAttributes, the source values are merged with any existing target value.

Using the User, Group, and Device LDAP filters

Active Directory provides a powerful way of retrieving data through the use LDAP filters. Directory Synchronization exposes three filters during the creation of a synchronization profile: **User OU Filter**, **Group OU Filter**, and **Device OU Filter** whose defaults are:

- Users: (&(!(adminDescription=Created By DirSync))(|(objectClass=Person)(objectClass=room))(!(objectClass=computer)))
- Groups: (&(!(adminDescription=Created By DirSync))(objectClass=Group))

- Devices: (&(!(adminDescription=Created By DirSync))(objectClass=computer)(!(primaryGroupID=516)))

These filters are per organizational unit and apply to sub-OUs when the **Sync Sub-OUs** option is selected.

Modifying these filters requires a basic understanding of the attributes, their value representations, and their data types. LDAP filters support any number of options including filtering by date ranges, wildcards, and the use of bitmasks as in the userAccountControl property.

The use of the objectClass and objectCategory properties can greatly reduce the number of records retrieved resulting in improved performance. You may use other attributes to further restrict your results.

The following are common examples of queries and their LDAP query syntax.

- Selecting users that are part of the 'Accounting' department:
  - (&(objectClass=User)(objectCategory=Person)(department=Accounting))
- Selecting mailbox-enabled users:
  - (&(objectClass=User)(objectCategory=Person)(homeMDB=*))
- Selecting mail-enabled users and contacts:
  - (|(&(objectClass=User)(objectCategory=Person)(!homeMDB=*))(objectClass=Contact))
- Selecting users created after January 1, 2011:
  - (&(objectClass=User)(objectCategory=Person)(whenCreated>=20110101000000.0Z))
- Selecting distribution lists:
  - (&(objectClass=Group)(groupType=2))

Quest recommends that you use the Active Directory Users and Computers management console to test your filters to prevent Directory Synchronization from failing due to an invalid filter.

Using the User and Group LDAP Filters

Active Directory provides a powerful way of retrieving data through the use LDAP filters. Directory Synchronization exposes two filters during the creation of a synchronization profile: User OU Filter and Group OU Filter whose defaults are:

- Users: (&(!(adminDescription=Created By DirSync))(|(objectClass=Person)(objectClass=room))(!(objectClass=computer)))
- Groups: (&(!(adminDescription=Created By DirSync))(objectClass=Group))

These filters are per organizational unit and apply to sub-OUs when the Sync Sub-OUs option is selected.

Modifying these filters requires a basic understanding of the attributes, their value representations, and their data types. LDAP filters support any number of options including filtering by date ranges, wildcards, and the use of bitmasks as in the userAccountControl property.

The use of the objectClass and objectCategory properties can greatly reduce the number of records retrieved resulting in improved performance. You may use other attributes to further restrict your results.

- Selecting users that are part of the ‘Accounting’ department:
  - (&(objectClass=User)(objectCategory=Person)(department=Accounting))
- Selecting mailbox-enabled users:
  - (&(objectClass=User)(objectCategory=Person)(homeMDB=*))
- Selecting mail-enabled users and contacts:
  - (|(&(objectClass=User)(objectCategory=Person)(!homeMDB=*))(objectClass=Contact))
- Selecting users created after January 1, 2011:
  - (&(objectClass=User)(objectCategory=Person)(whenCreated>=20110101000000.0Z))
- Selecting distribution lists:
  - (&(objectClass=Group)(groupType=2))

The following are common examples of queries and their LDAP query syntax.

Quest recommends that you use the Active Directory Users and Computers management console to test your filters to prevent Directory Synchronization from failing due to an invalid filter.

Default Mappings

AD Source – AD Target Default Mapping

The below table displays the default values of the AD Source to AD Target mapping table.

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
accountExpires	AccountExpires	accountExpires	any	any		
altRecipient	ForwardingAddress	altRecipient	any	any		
assistant	Assistant		any	any		
authOrig	AuthOrig	authOrig	any	any		
C	CountryAbbreviation	C	an	an		

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
			y	y		
cn	CommonName	cn	any	any		
Co	CountryName	Co	any	any		
codePage	CodePage	codePage	any	any		
Comment	Comment	Comment	any	any		
company	Company	company	any	any		
countryCode	CountryCode	countryCode	any	any		
deletedItemFlags	DeletedItemFlags	deletedItemFlags	any	any		
delivContLength	DelivContLength	delivContLength	any	any		
department	Department	department	any	any		
departmentNumber	DepartmentNumber	departmentNumber	any	any		
description	Description	description	any	any		
displayName	DisplayName	displayName	any	any		
division	Division	division	any	any		
dLMemSubmitPerms	DLMemSubmitPerms	dLMemSubmitPerms	any	any		
dLMemRejectPerms	DLMemRejectPerms	dLMemRejectPerms	an	an		

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
			y	y		
employeeID	EmployeeID	employeeID	any	any		
employeeNumber	EmployeeNumber	employeeNumber	any	any		
employeeType	EmployeeType	employeeType	any	any		
expirationTime	ExpirationTime	expirationTime	any	any		
extensionAttribute1	Extension1	extensionAttribute1	any	any		These are Exchange defined custom attributes.
extensionAttribute10	Extension10	extensionAttribute10	any	any		These are Exchange defined custom attributes.
extensionAttribute11	Extension11	extensionAttribute11	any	any		These are Exchange defined custom attributes.
extensionAttribute12	Extension12	extensionAttribute12	any	any		These are Exchange defined custom attributes.
extensionAttribute13	Extension13	extensionAttribute13	any	any		These are Exchange defined custom attributes.

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
extensionAttribute14	Extension14	extensionAttribute14	any	any		These are Exchange defined custom attributes.
extensionAttribute15	Extension15	extensionAttribute15	any	any		These are Exchange defined custom attributes.
extensionAttribute2	Extension2	extensionAttribute2	any	any		These are Exchange defined custom attributes.
extensionAttribute3	Extension3	extensionAttribute3	any	any		These are Exchange defined custom attributes.
extensionAttribute4	Extension4	extensionAttribute4	any	any		These are Exchange defined custom attributes.
extensionAttribute5	Extension5	extensionAttribute5	any	any		These are Exchange defined custom attributes.
extensionAttribute6	Extension6	extensionAttribute6	any	any		These are Exchange defined custom attributes.
extensionAttribute7	Extension7	extensionAttribute7	any	any		These are Exchange

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
						defined custom attributes.
extensionAttribute8	Extension8	extensionAttribute8	any	any		These are Exchange defined custom attributes.
extensionAttribute9	Extension9	extensionAttribute9	any	any		These are Exchange defined custom attributes.
facsimileTelephoneNumber	OfficeFAXNumber	facsimileTelephoneNumber	any	any		
generationQualifier	Suffix	generationQualifier	any	any		
givenName	FirstName	givenName	any	any		
homePhone	HomePhoneNumber	homePhone	any	any		
HomePostalAddress	HomePostalAddress	HomePostalAddress	any	any		
Info	Info	Info	any	any		
initials	Initials	initials	any	any		
internationalISDNNumber	InternationalISDNNumber	internationalISDNNumber	any	any		
internetEncoding	internetEncoding	internetEncoding	any	any		
ipPhone	IPPhone	ipPhone	any	any		

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
jpegPhoto	JPEGPhoto	jpegPhoto	any	any		
l	OfficeCity	l	any	any		
language	Language	language	any	any		
legacyExchangeDN	LegacyExchangeDN	legacyExchangeDN	any	any		Created using the source object's GUID as the CN.
localeID	LocaleID	localeID	any	any		
mail	InternetAddress	mail	any	any		
mailNickname	PrimaryAlias	mailNickname	any	any		
manager	Manager		any	any		
mAPIRecipient	MAPIRecipient	mAPIRecipient	any	any		
middleName	MiddleName	middleName	any	any		
mobile	CellPhoneNumber	mobile	any	any		
msDS-PhoneticCompanyName	msDSPhoneticCompanyName	msDS-PhoneticCompanyName	any	any		
msDS-PhoneticDepartment	msDSPhoneticDepartment	msDS-PhoneticDepartment	any	any		
msDS-PhoneticDisplayName	msDSPhoneticDisplayName	msDS-PhoneticDisplayName	any	any		

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
msDS-PhoneticFirstName	msDSPhoneticFirstName	msDS-PhoneticFirstName	any	any		
msDS-PhoneticLastName	msDSPhoneticLastName	msDS-PhoneticLastName	any	any		
msExchAddressBookFlags	msExchAddressBookFlags	msExchAddressBookFlags	any	any		
msExchALObjectVersion	msExchALObjectVersion	msExchALObjectVersion	any	any		
msExchArchiveGuid	msExchArchiveGuid	msExchArchiveGuid	any	any		
msExchArchivename	msExchArchivename	msExchArchivename	any	any		
msExchAssistantName	msExchAssistantName	msExchAssistantName	any	any		
msExchBlockedSendersHash	msExchBlockedSendersHash	msExchBlockedSendersHash	any	any		
msExchBypassAudit	msExchBypassAudit	msExchBypassAudit	any	any		
msExchELCExpirySuspensionEnd	msExchELCExpirySuspensionEnd	msExchELCExpirySuspensionEnd	any	any		
msExchELCExpirySuspensionStart	msExchELCExpirySuspensionStart	msExchELCExpirySuspensionStart	any	any		
msExchELCMailboxFlags	msExchELCMailboxFlags	msExchELCMailboxFlags	any	any		
msExchExternalOOFOptions	msExchExternalOOFOptions	msExchExternalOOFOptions	any	any		
msExchHideFromAddressLists	msExchHideFromAddressLists	msExchHideFromAddressLists	any	any		
msExchMailboxAuditEnable	msExchMailboxAuditEnable	msExchMailboxAuditEnable	any	any		

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
msExchMailboxAuditLogAgeLimit	msExchMailboxAuditLogAgeLimit	msExchMailboxAuditLogAgeLimit	any	any		
msExchMailboxGuid	msExchMailboxGUID	msExchMailboxGuid	any	any		
msExchMDBRulesQuota	msExchMDBRulesQuota	msExchMDBRulesQuota	any	any		
msExchMessageHygieneFlags	msExchMessageHygieneFlags	msExchMessageHygieneFlags	any	any		
msExchMessageHygieneSCLDeleteThreshold	msExchMessageHygieneSCLDeleteThreshold	msExchMessageHygieneSCLDeleteThreshold	any	any		
msExchMessageHygieneSCLJunkThreshold	msExchMessageHygieneSCLJunkThreshold	msExchMessageHygieneSCLJunkThreshold	any	any		
msExchMessageHygieneSCLQuarantineThreshold	msExchMessageHygieneSCLQuarantineThreshold	msExchMessageHygieneSCLQuarantineThreshold	any	any		
msExchMessageHygieneSCLRejectThreshold	msExchMessageHygieneSCLRejectThreshold	msExchMessageHygieneSCLRejectThreshold	any	any		
msExchModerationFlags	msExchModerationFlags	msExchModerationFlags	any	any		
msExchPoliciesExcluded	msExchPoliciesExcluded	msExchPoliciesExcluded	any	any		
msExchPoliciesIncluded	msExchPoliciesIncluded	msExchPoliciesIncluded	any	any		
msExchProvisioningFlags	msExchProvisioningFlags	msExchProvisioningFlags	any	any		
msExchRecipientDisplayType	msExchRecipientDisplayType	msExchRecipientDisplayType	any	any		This mapping is ignored and msExchRecipientDisplayType is set to 6 when the profile is set to

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
						sync users as Mail-Enabled Users or Disabled Mail-Enabled Users, or the profile is set to sync users “As-Is” and the object in the source is Mailbox-Enabled.
msExchRecipientTypeDetails	msExchRecipientTypeDetails	msExchRecipientTypeDetails	any	any		This mapping is ignored and msExchRecipientTypeDetails is set to 128 when the profile is set to sync users as Mail-Enabled Users or Disabled Mail-Enabled Users, or the profile is set to sync users “As-Is” and the object in the source is Mailbox-Enabled.
msExchRequireAuthToSendTo	msExchRequireAuthToSendTo	msExchRequireAuthToSendTo	any	any		
msExchResourceCapacity	msExchResourceCapacity	msExchResourceCapacity	any	any		
msExchResourceDisplay	msExchResourceDisplay	msExchResourceDisplay	any	any		

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
msExchResourceMetaData	msExchResourceMetaData	msExchResourceMetaData	any	any		
msExchResourceSearchProperties	msExchResourceSearchProperties	msExchResourceSearchProperties	any	any		
msExchSafeRecipientsHash	msExchSafeRecipientsHash	msExchSafeRecipientsHash	any	any		
msExchSafeSendersHash	msExchSafeSendersHash	msExchSafeSendersHash	any	any		
msExchTransportRecipientSettingsFlags	msExchTransportRecipientSettingsFlags	msExchTransportRecipientSettingsFlags	any	any		
msExchUMDtmfMap	msExchUMDtmfMap	msExchUMDtmfMap	any	any		
msExchUMSpokenName	msExchUMSpokenName	msExchUMSpokenName	any	any		
msExchUserCulture	msExchUserCulture	msExchUserCulture	any	any		
msExchVersion	msExchVersion	msExchVersion	any	any		
name	Name	name	any	any		
O	O	O	any	any		
objectGUID	AdminDisplayName	adminDisplayName	any	any		
otherFacsimileTelephoneNumber	OtherFacsimileTelephoneNumber	otherFacsimileTelephoneNumber	any	any		
otherHomePhone	OtherHomePhone	otherHomePhone	any	any		
otherIpPhone	OtherIpPhone	otherIpPhone	any	any		

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
otherMobile	OtherMobile	otherMobile	any	any		
otherPager	OtherPager	otherPager	any	any		
otherTelephone	OtherTelephone	otherTelephone	any	any		
pager	PagerNumber	pager	any	any		
personalPager	PersonalPager	personalPager	any	any		
personalTitle	PersonalTitle	personalTitle	any	any		
Photo	Photo	Photo	any	any		
physicalDeliveryOfficeName	Location	physicalDeliveryOfficeName	any	any		Important, particularly for printers.
pOPCharacterSet	POPCharacterSet	pOPCharacterSet	any	any		
pOPContentFormat	POPContentFormat	pOPContentFormat	any	any		
postalAddress	PostalAddress	postalAddress	any	any		
postalCode	OfficeZip	postalCode	any	any		
postOfficeBox	PostOfficeBox	postOfficeBox	any	any		
preferredDeliveryMethod	PreferredDeliveryMethod	preferredDeliveryMethod	any	any		
primaryInternationalISDNNumber	PrimaryInternationalISDNNumber	primaryInternationalISDNNumber	any	any		

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
primaryTelexNumber	PrimaryTelexNumber	primaryTelexNumber	any	any		
proxyAddresses	ProxyAddresses		any	any		ProxyAddresses contains the InternetAddress as the primary SMTP, the legacyExchangeDN of both the source and target as X500 addresses, and any email policies from the target (if enabled).
pwdLastSet	PwdLastSet					
roomNumber	RoomNumber	roomNumber	any	any		
sAMAccountName	SAMAccountName	sAMAccountName	any	any		The following restricted chars will be replaced with underscores: , + " < > ; = / [ ] : | * ? \
showInAdvancedViewOnly	ShowInAdvancedViewOnly	showInAdvancedViewOnly	any	any		
sn	LastName	sn	any	any		Sometimes used as surname.
st	OfficeState	st	any	any		

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
street	Street	street	any	any		
streetAddress	OfficeStreetAddress	streetAddress	any	any		
	TargetAddress	targetAddress	any	any		
telephoneAssistant	TelephoneAssistant	telephoneAssistant	any	any		
telephoneNumber	OfficePhoneNumber	telephoneNumber	any	any		
terminalServer	TerminalServer	terminalServer	any	any		
textEncodedORAddress	TextEncodedORAddress	textEncodedORAddress	any	any		
thumbnailLogo	ThumbnailLogo	thumbnailLogo	any	any		
thumbnailPhoto *	ThumbnailPhoto *	thumbnailPhoto *	any	any		
title	JobTitle	title	any	any		
unauthOrig	UnauthOrig	unauthOrig	any	any		
url	WebSite	url	any	any		
userCert	UserCert	userCert	any	any		
userCertificate	UserCertificate	userCertificate	any	any		
userPrincipalName	UserPrincipalName	userPrincipalName	any	any		

Source Field	Internal Field	Target Field	Source Type	Target Type 1	Target Type 2	Comments
userSMIMECertificate	UserSMIMECertificate	userSMIMECertificate	any	any		
wWWHomePage	WWWHomePage	wWWHomePage	any	any		
managedBy	ManagedBy		group	group	contact	
groupType	GroupType	groupType	group	group		

* thumbnailPhoto values are synced directly from the Source to the Target.

Customizing Overrides

In Directory Sync Pro for Active Directory, an override is used to transform values in the target directory based upon a formula.

The formula language used is T-SQL, used in Microsoft's SQL Server product line. A valid select statement in T-SQL would be ***Select (FirstName + LastName) from BT_Person***. When adding an override you do not need to include a full SQL select statement as portions of the SQL statement are generated for you. Specifically, you are not required to use the select or from commands in the override. It is only required to enter the columns that should be selected. To continue the example above, a valid override would only need to contain the value of **FirstName + LastName**.

To add an Override:

1. From the project overview, select your profile and choose **Manage**.
2. From the summary page, choose **Settings**, then **Advanced**, then **Overrides**.
3. Click **Add Override**. The Override dialog appears.
4. Select a **Person** or **Groups** from the **View** drop-down list.
5. Enter a **Field Name** for the new override. This must be a valid internal field name in SQL.
6. Enter a **Field Value** for the new override. This must be a correctly formatted SQL statement.
7. Enter optional **Comments** for the new override.
8. Click **Save**.

When you save an override, Directory Sync Pro for Active Directory re-generates the Person or Groups view. It does this by dynamically generating a single SQL statement using the snippet of SQL code that is part of all overrides. The max size for this SQL statement is 8000 total characters. If many new overrides are added, this limit could be

exceeded and an error when adding the overrides will occur. In addition to the default overrides, approximately 15-20 more Person and 20-25 Group overrides can be added before hitting the size limit.

To edit an override:

1. From the project overview, select your profile and choose **Manage**.
2. From the summary page, choose **Settings**, then **Advanced**, then **Overrides**.
3. Select the desired override and double-click on it.
4. The dialog box for the selected override opens.
5. Make any desired edits to the Field Value and or Comments. (The **View** type and **Field Name** cannot be modified.)
6. Click **Save**.

To delete an override:

1. From the project overview, select your profile and choose **Manage**.
2. From the summary page, choose **Settings**, then **Advanced**, then **Overrides.**
3. Select one or more overrides and click **Remove Override(s)**.
4. Choose **Yes** in the confirmation box.

To export overrides:

1. From the project overview, select your profile and choose **Manage**.
2. From the summary page, choose **Settings**, then **Advanced**, then **Overrides**.
3. Select one or more overrides using Ctrl-click.
4. Choose **Export**.
5. In the export dialog box, choose a file format, and enter a file location.
6. Click **Export**.

You can reset all overrides to the “factory defaults” by clicking the **Reset Overrides** button. Caution: This will remove any custom overrides or any edits to existing overrides. If you have made changes, you may want to export those changed overrides before a reset. You can import them later if you wish.

Controlling actions with Overrides

Directory Sync Pro for Active Directory uses the TypeOfTransaction column from the BT_Person table, or the Operation column from the BT_Groups table to determine what action to perform on the target object. These may have overrides applied to them, to control what actions Directory Sync Pro for Active Directory will take for an object. The below image shows an example of this kind of override.

Matching user accounts with Overrides

The values used for matching can have overrides applied to them. This is accomplished by setting up a new override using the field names MatchValue1, MatchValue2, MatchValue3 and MatchValue4. Each MatchValue1-4 corresponds the respective Source and Target pair on the matching tab.

These values are used for matching only. Values that get written to the target are based on the mappings, not the matching.

When updating an existing object, the attributes UserPrincipalName and SAMAccountName will only be written in response to a change after the initial sync. To always update these attributes, change the Internal Field mapping to an unused CustomXXX field.

Internal field must be entirely blank/NULL or source written to a different Custom value.

Make your override for Custom001 and map Custom001 to UserPrincipalName…then un-map userPrincipalName.

Make your override for Custom002 and map Custom002 to sAMAccountName…then un-map sAMAccountName

Example Overrides - For informational purposes only. Please create and test overrides for each project.

Field Name	Field Value	Description
TargetAddress	CASE EntryType WHEN 'user' THEN 'SMTP:' + P.Custom20 + '@exchange.contoso.com' ELSE 'SMTP:' + dbo.ReplaceDomain (InternetAddress,'exchange.contoso.com') END	This formula will dynamically set the targetaddress value based on the EntryType.
TargetAddress	'SMTP:' + dbo.UpdateInternetAddress (InternetAddress,'exchange.')	This formula will set the TargetAddress value based on the InternetAddress and prefix the domain with the value specified, in this case "exchange.".
TargetAddress	' 'SMTP:' + dbo.ReplaceDomain (InternetAddress,'exchange.contoso.com')	This formula will set the TargetAddress value based on the InternetAddress and replace the domain with the value specified, in this case "exchange.contoso.com".
TargetAddress	CASE WHEN InternetAddress LIKE '%@example.com' THEN 'smtp:' + dbo.UpdateInternetAddress (P.InternetAddress, 'exchange.') WHEN InternetAddress LIKE '%@knotes.contoso.com' THEN 'smtp:' + dbo.ReplaceDomain(P.InternetAddress, 'exchange.contoso.com') ELSE P.InternetAddress END	This formula will dynamically set the targetaddress value based on the existing InternetAddress domain name value. If the first domain is found then the TargetAddress will be set to one value, if the second domain is found another value will be used and if neither domain is found then the TargetAddress will be set the same as the current InternetAddress value.
CommonName	CASE EntryType WHEN 'user' THEN 'do$$' + SourceDirectoryID WHEN 'sharedmail' THEN 'do$$' + SourceDirectoryID ELSE CommonName END	This formula will dynamically set the CommonName value based on the EntryType.
CommonName	CASE WHEN LEN(CommonName) > 64 THEN LTRIM (RTRIM(LEFT(CommonName,64))) ELSE CommonName END	This formula will limit the CommonName value to 64 characters if it exceeds that

Field Name	Field Value	Description
		limit.
ProxyAddresses	CASE ProxyAddresses WHEN '' THEN 'smtp:' + dbo.ReplaceDomain (InternetAddress,'@contoso.mail.onmicrosoft.com;smtp:') + dbo.UpdateInternetAddress(InternetAddress,'exchange.') ELSE ProxyAddresses + ';smtp:' + dbo.ReplaceDomain (InternetAddress,'@contoso.mail.onmicrosoft.com;smtp:') + dbo.UpdateInternetAddress(InternetAddress,'exchange.') END	This formula will set or append to the list of ProxyAddresses values the coexistence routing addresses. This example specifically is designed for Office 365.
Company	LTRIM(RTRIM(LEFT(company, 50)))	This formula will Trim, then limit the string value by 50 characters.
Custom001	'this is a string'	This formula will set any string value to the any SQL field.
Custom001	REPLACE(InternetAddress,'@','.')	This formula will replace the '@' symbol with a period '.' to create a string like so. (i.e. first.last.contoso.com)
Custom001	LEFT(InternetAddress,CHARINDEX('@',InternetAddress)-1)	This formula will extract the localpart of InternetAddress.

Directory Sync Pro for Active Directory Fields with Special Processing

AD Directory Sync Pro for Active Directory Fields with Special Processing

The below tables include AD fields with some kind of special processing in Directory Sync Pro for Active Directory. Fields can have the following characteristics:

- Cannot be mapped
- Can be mapped and have an override
- May be explicitly ignored or changed by Directory Sync Pro for Active Directory if object meets certain conditions, even if mapping and override exists
- Actual attribute may be set via config file

Additional notes are available below for field marked with a *.

Writing Users to AD

Attributes that may be set by Directory Sync Pro for Active Directory regardless of mapping:

Field	Cannot be mapped	Can be mapped / have override	May be explicitly ignored	May be set with config file
distinguishedName	•			
objectClass	•			
userPassword		•		
unicodePwd		•		
userAccountControl		•		
msExchRecipientDisplayType		•	•	
msExchRecipientTypeDetails		•	•	
msExchResourceDisplay		•		
msExchResourceSearchProperties		•		
msExchResourceMetaData		•		
showInAddressBook*	•		•	
msExchMasterAccountSid		•	•	
msExchPoliciesExcluded	•		•	
msExchPoliciesIncluded		•	•	
userAccountControl	•		•	
pwdLastSet	•			
adminDescription	•			•

Special processing if mapped:

Field	Cannot be mapped	Can be mapped / have override	May be explicitly ignored	May be set with config file
mail		•	•	
assistant*		•		
manager*		•		
managedBy*		•		
altRecipient*		•		
authoring		•		
unauthOrig		•		
dLMemSubmitPerms		•		

Field	Cannot be mapped	Can be mapped / have override	May be explicitly ignored	May be set with config file
dLMemRejectPerms		•		
sAMAccountName*		•	•	
legacyExchangeDN*		•	•	
mailNickname		•	•	

Never set:

Field	Cannot be mapped	Can be mapped / have override	May be explicitly ignored	May be set with config file
objectGUID	•			
objectSid	•			
whenCreated	•			
whenChanged	•			
uSNChanged	•			
name	•			
cn	•			

Writing Groups to AD

Attributes that may be set by Directory Sync Pro for Active Directory regardless of mapping:

Field	Cannot be mapped	Can be mapped / have override	May be explicitly ignored	May be set with config file
objectClass	•			
msExchRecipientDisplayType		•	•	
msExchVersion		•		
showInAddressBook*	•		•	
msExchPoliciesExcluded	•		•	
msExchPoliciesIncluded			•	
adminDescription	•			•

Special processing if mapped:

Field	Cannot be mapped	Can be mapped / have override	May be explicitly ignored	May be set with config file
mail		•	•	
assistant*		•		
manager*		•		
managedBy*		•		
altRecipient*		•		
authOring		•		
unauthOrig		•		
dLMemSubmitPerms		•		
dLMemRejectPerms		•		
sAMAccountName*		•	•	
legacyExchangeDN*		•		
groupType		•	•	
mailNickname		•	•	

Never set:

Field	Cannot be mapped	Can be mapped / have override	May be explicitly ignored	May be set with config file
objectGUID	•			
objectSid	•			
whenCreated	•			
whenChanged	•			
uSNChanged	•			
name	•			
cn	•			

Special processing by Internal Field Name:

Field	Cannot be mapped	Can be mapped / have override	May be explicitly ignored	May be set with config file	If this internal field name is mapped and value is empty, actual value comes from different internal field
DisplayName		•			•
PrimaryAlias		•			•

Field	Cannot be mapped	Can be mapped / have override	May be explicitly ignored	May be set with config file	If this internal field name is mapped and value is empty, actual value comes from different internal field
SAMAccountName*		•			•
InternetAddress		•			•
Name		•			•
CommonName		•			•

Additional Notes

1. TargetDN – this column contains the distinguishedName of the target object to be created or the existing distinguishedName of a matched target object. If the object is created, the following values are used:
    a. Non-group objects from AD sources use the DN column (or override value if specified) to compute a target object DN. This preserves the sub-OU hierarchy the object may be in from the source.
    b. Groups from AD sources, use the OU column (or override value if specified) to compute a target object DN. This preserves the sub-OU hierarchy the object may be in from the source.
2. LegacyExchangeDN – the legacyExchangeDN of the target object is computed by constructing a value relative to the target Exchange organization.
3. ShowInAddressBook – unless hiding from GAL is enabled. No override column is available for this field. To prevent overwriting object values in the target, GAL visibility for the ShowInAddressBook attribute should be set to Hidden.
    a. Rooms are added to the All Rooms address book, except for Exchange 2003 which doesn't have rooms or the All Rooms address book.
    b. Users are added to the All Users address book.
    c. Groups are added to the All Groups address book.
    d. All objects are added to the All Global Address Lists (GAL) address book.
4. Manager – all objects except Groups
    a. Uses the Manager column (or override value if specified) for the source object.
    b. Locates the referenced Manager in the target.
    c. If the referenced Manager is a reference to itself, the Manager on the target object will be set on the next sync.
5. ManagedBy – group objects only
    a. Uses the ManagedBy column (or override value if specified) for the source object.
    b. Follows the same process as Manager above.

6. Assistant – all objects
    a. Uses the Assistant column (or override value if specified) for the source object.
    b. Follows the same process as Manager above.
7. AltRecipient – all objects
    a. Uses the AltRecipient column (or override value if specified) for the source object.
    b. Follows the same process as Manager above.
8. sAMAccountName – The sAMAccountName may be calculated under special circumstances, such as when a collision occurs. For this reason, during a sync following a reset, repush, or repushpull, the existing sAMAccountName in the target will be assumed to be current and therefore will be used in any mappings involving the sAMAccountName internal field.

AD Built-in Groups Handling

Directory Sync Pro for Active Directory automatically ignores certain AD built-in groups during sync. The definition of which built-in groups to ignore is held in the database table `DirSync_GroupsToIgnore_PK`. This table is created and populated during the install process of Directory Sync Pro for Active Directory and is not configurable from the product UI. This list of groups can be modified only with direct access and permissions to SQL. When Directory Sync Pro for Active Directory performs a sync, any group encountered that matches with a group named in the `DirSync_GroupsToIgnore_PK` table is skipped and not entered into the database. This built-in group handling functionality is separate from the blacklisting functionality for groups which can be configured by an operator through the product UI, so when ignored these built-in groups are not considered to be 'blacklisted'.

How to Process GDPR Requests

What is a GDPR Request?

The General Data Protection Regulations (GDPR) is the new European Union (EU) data protection regulations which go into effect May 25th, 2018. Under the GDPR individuals have certain rights to their personal data. They can make requests to exercise those rights to the data controller, and the controller must respond within 1 month. It is expected that the controller will verify the identity of the requestor.

There are four primary types of GDPR requests:

1. **Export** – Request for a copy of all personal data about an individual held by this controller and any related processors. Must be in a commonly accepted portable data format.
2. **Update** – Request to rectify inaccurate personal data.
3. **Delete** – Request to remove all personal data about an individual from our systems. Can be initiated by an individual or by a revocation of consent process. Includes burden of proof. (Ideally follow a delete with an export to show no remaining data)

4. **Hold** – Request to halt processing of personal data but not delete that data.

How to handle GDPR Requests for Directory Sync Pro for Active Directory

When Directory Sync Pro for Active Directory is installed, the data associated with the application is hosted locally within the client's environment. The client has full control over this data. By default, the user and configuration data is stored in the SQL database called, "DirectorySyncPro_<*date*>". It is assumed the operator has the proper administrative SQL Permissions to execute the following methods outlined.

SQL Tables containing User data:

- [DirectorySyncPro_<Date>].[dbo].[BT_Person]
  Unique Key Look-up Columns:
  [SAMAccountName]
  [TargetSAMAccountName]
  [TargetUserPrincipalName]
  [OriginalSAMAccountName]
  [OriginalUserPrincipalName]
  [UserPrincipalName]
  If user data is used for matching (e.g. SAMAccountName, UserPrincipalName, etc.) then those values will also appear in one of the following columns:
  [MatchValue1]
  [MatchValue2]
  [MatchValue3]
  [MatchValue4]

- [DirectorySyncPro_<Date>].[dbo].[BT_Groups]
  Unique Key Look-up Columns:
  [MatchValue1]
  [MatchValue2]
  [MatchValue3]
  [MatchValue4]

Be aware that data can be mapped to different Internal Fields (table columns) depending on customer specific configuration, so just about any SQL column could theoretically contain user data if so configured. For example, if SAMAccountName has been mapped to Custom001 or to any other Internal Field selectable in the mappings. Therefore this process should be undertaken by someone knowledgeable about the schema and attribute mappings in use. It may also be helpful to work with Support when completing these requests if you are not comfortable with the database.

Where does the Directory Sync Pro for Active Directory get its user data?

All user data within Directory Sync Pro for Active Directory is derived from the source Active Directory Forest configured in the product. Therefore, the authoritative source of any user related data stored in Directory Sync Pro for Active Directory is Active Directory. Any remediation required from a GDPR request should first be remediated in Active Directory or the source feeding Active Directory. Once that user data is updated in the source directory, running a new discovery within the product will update those values as well.

The following sections will provide guidance on fulfilling the 4 primary GDPR request types.

1. **Exports** – Request for a copy of all personal data about an individual held by this controller and any related processors. Must be in a commonly accepted portable data format.

For the purposes of this document, using PowerShell with the SQLPS Module is the recommended method to refine the results of the output. One may export any SQL Query result to a CSV file. Below is an example script to do so. Replace the variables to conform to your environment.

```
Import-Module sqlps
$SQLquery='SELECT * FROM [DirectorySyncPro_<Date>].[dbo].[BT_Person]'
$result=invoke-sqlcmd -query $SQLquery -serverinstance <servername> -database <dbname>
$result |export-csv c:\temp\ExportQueryResults.csv -notypeinformation
```

2. **Updates** – Request to rectify inaccurate personal data.

As previously stated, all user data within Directory Sync Pro for Active Directory is derived from the source Active Directory Forest configured in the product. Therefore, the authoritative source of user data is Active Directory. Any remediation required from a GDPR request should first be remediated in Active Directory or the source feeding Active Directory.

If editing the user data within SQL is still required, using any SQL editor such as SQL Server Management Studio, run an update command against one or more columns for one or more records. Below are examples to accomplish this. Note however, that any new discovery will update the values based on the source Active Directory.

Update multiple columns for a single record:

```
UPDATE [DirectorySyncPro_<Date>].[dbo].[BT_Person]
SET <Column1 Name> = <New Value1>, <Column2 Name> = <New Value2>
WHERE userPrincipalName='<Unique ID>'
```

```
UPDATE [DirectorySyncPro_<Date>].[dbo].[BT_Person]
SET <Column1 Name> = <New Value1>, <Column2 Name> = <New Value2>
WHERE userPrincipalName='<Unique ID>'
```

Update multiple columns for multiple records:

UPDATE [DirectorySyncPro_<*Date*>].[dbo].[CMTEUP_Person]
SET <*Column1 Name*> = <*New Value1*>, <*Column2 Name*> = <*New Value2*>
WHERE DistinguishedName='<Unique ID>' OR DistinguishedName='<Unique ID>'

UPDATE [DirectorySyncPro_<*Date*>].[dbo].[CMTEUP_PersonADData]
SET <*Column1 Name*> = <*New Value1*>, <*Column2 Name*> = <*New Value2*>
WHERE userPrincipalName='<Unique ID>' OR userPrincipalName='<Unique ID>'

Update multiple columns for multiple records using a list:
UPDATE [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
SET <*Column1 Name*> = <*New Value1*>, <*Column2 Name*> = <*New Value2*>
WHERE DistinguishedName IN ('<*Unique ID1*>', '<*Unique ID2*>', '<*Unique ID3*>')

UPDATE [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
SET <*Column1 Name*> = <*New Value1*>, <*Column2 Name*> = <*New Value2*>
WHERE userPrincipalName IN ('<*Unique ID1*>', '<*Unique ID2*>', '<*Unique ID3*>')

3. **Deletes** – Request to remove all personal data about an individual from our systems. Can be initiated by an individual or by a revocation of consent process. Includes burden of proof. (Ideally follow a delete with an export to show no remaining data.)

Using any SQL editor such as SQL Server Management Studio, run a Delete command against one or more records. Below are examples to accomplish this. However, as previously stated, if the user is not deleted in the source Active Directory during any subsequent new discovery the user will be re-populated into SQL. The only way to truly remove the data is to delete the source user or delete the entire SQL database when it is no longer required.

Delete a single record then verify:
DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName='<*Unique ID1*>'

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName='<*Unique ID1*>'

DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE userPrincipalName='<*Unique ID1*>'

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE userPrincipalName='<*Unique ID1*>'

Delete multiple records then verify:
DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName='<*Unique ID1*>' OR SAMAccountName='<*Unique ID2*>'

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName='<*Unique ID1*>' OR SAMAccountName='<*Unique ID2*>'

DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE userPrincipalName='<*Unique ID1*>' OR userPrincipalName='<*Unique ID2*>'

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE userPrincipalName='<*Unique ID1*>' OR userPrincipalName='<*Unique ID2*>'

Delete multiple records then verify:
DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName IN ('<*Unique ID1*>', '<*Unique ID2*>', '<*Unique ID3*>')

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE SAMAccountName IN ('<*Unique ID1*>', '<*Unique ID2*>', '<*Unique ID3*>')

DELETE FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE userPrincipalName IN ('<*Unique ID1*>', '<*Unique ID2*>', '<*Unique ID3*>')

SELECT * FROM [DirectorySyncPro_<*Date*>].[dbo].[BT_Person]
WHERE userPrincipalName IN ('<*Unique ID1*>', '<*Unique ID2*>', '<*Unique ID3*>')

4. **Holds** – Request to halt processing of personal data but not delete that data.

This can also be accomplished using the product interface. Halting a user from processing can be achieved using the Exclusion List feature.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product