User Management Tool for Policy-Based Administration

Contents

What’s new 3

System requirements 4

About ShareFile User Management Tool 5

Install 6

Upgrade 8

Configure 9

Provision user accounts and distribution groups 11

Migrate users between StorageZones 15

Re-linking users in your ShareFile account 15

What's new

March 20, 2019

> **Important**
>
> Version 1.9 and later of the ShareFile User Management Tool is designed specifically for customers utilizing the ShareFile Policy Based Administration feature and will differ from typical UMT setup instructions. More information about that feature can be found here. For customers utilizing the UMT without the policy administration feature, please refer to the current version of UMT documentation.

What's new in User Management Tool 1.13

- Improved performance when loading & working with large numbers of Rules
- Logging enhancements

What's new in User Management Tool 1.12

- The User Management Tool 1.12+ (for Policy Based Administration accounts) now defaults to the TLS 1.2 Security Protocol. As part of this change, the Proxy Configuration Tool has also been updated to support TLS 1.2 and .NET 4.5.

What's new in User Management Tool 1.11

- Log Archiving
- Added the ability to re-link users in your ShareFile account. More details on how this flow works can be found here: Re-linking users in your ShareFile account.
- Removed the contact information for ShareFile Support under the UMT help menu and instead replaced with information for Citrix Support.

What's new in User Management Tool 1.10

- Consolidated the User and Groups tab into one tab as well as modified the Rule created flow to improve ease of use.
- The User and Groups tab was consolidated into a 'Search' tab.

- When creating a rule, you now have the option to specify whether the rule is a User Rule, Group Rule or Both.
- An 'Export Actions' button was added to the 'Rules' tab which runs a simulation of the rules and creates a .sim file in the logs.
- The help text guide on the right of the User Rule creation page was updated to reflect Policy Based Administration.
- Link to Proxy Configuration Tool was added to the login page for easy access.

What's new in User Management Tool 1.9

- User Management Tool 1.9 is designed for customers utilizing ShareFile's Policy-Based Administration feature. The PBA feature allows ShareFile Enterprise Administrators to apply policies to groups of users for more efficient assignment and management of user permissions. Policy creation is done via the Web Application and Policy assignment can be performed through the User Management Tool (UMT) or the ShareFile API.

System requirements

October 4, 2018

The following is a list of operating system requirements for the ShareFile User Management Tool for Policy-Based Administration.

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows 8
- Windows 7

.NET Requirements

- .NET Framework 4.5
- For best performance, install .NET Framework on a domain-joined machine or VM.

IMPORTANT: Users on the following machines must **manually** enable .NET 3.5 in order to run the ShareFileProxyConfig.exe file.

- Windows Server 2012 R2
- Windows 8 or later

Information on manually enabling .NET 3.5 can be found within the following Microsoft article: https://msdn.microsoft.com/en-us/library/windows/desktop/hh848079%28v=vs.85%29.aspx

ShareFile requirements

You ShareFile account must have:

- Policy Based Administration enabled
- Available employee licensees in ShareFile for each user who is to be added

A ShareFile admin user with the following permissions:

- Create and Manage Policies
- Create Employees
- Create Shared Distribution Groups
- Edit Shared Distribution Groups

Active Directory Requirements

An admin or service account with full read permissions to the domain to run the User Management Tool

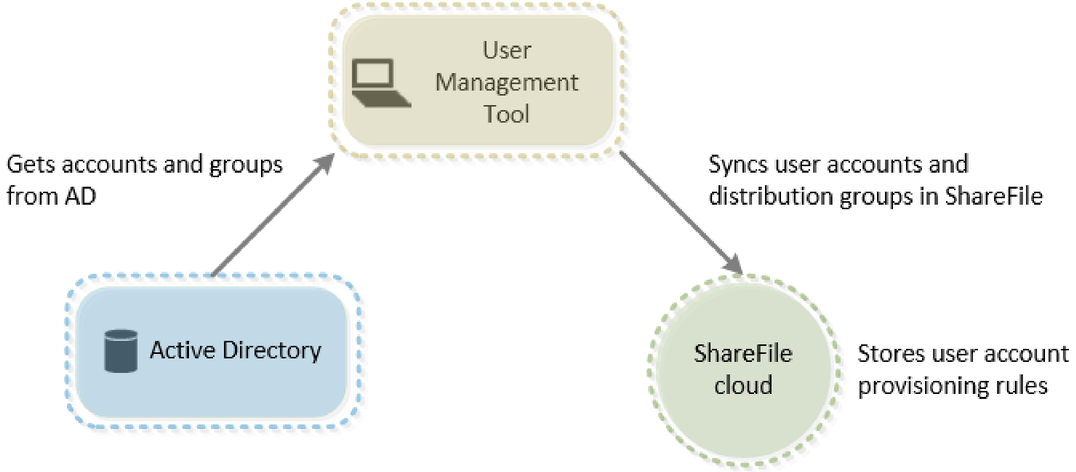
User accounts to be mirrored in AD must have the following attributes:

CN	LDAP-Display-Name
E-mail Addresses	mail
ms-DS-Phonetic-First-Name	msDS-PhoneticFirstName
ms-DS-Phonetic-Last-Name	msDS-PhoneticLastName
Object-Guid	objectGUID

About ShareFile User Management Tool

October 4, 2018

The User Management Tool enables you to provision employee user accounts and ShareFile distribution groups from Active Directory (AD).


User Management Tool
Gets accounts and groups from AD
Syncs user accounts and distribution groups in ShareFile
Active Directory
ShareFile cloud
Stores user account provisioning rules

The ShareFile User Management Tool(UMT) enables you to match ShareFile accounts to AD based on email address and will provision and update user information in ShareFile. This tool allows you to specify policies a user should be a part of, as well as distribution group membership. Through this application you can create multiple, named synchronization jobs which can be run repeatedly through windows scheduler through the Windows user context that is active when creating the job.

> **Note:**
>
> When deploying ShareFile along with XenMobile Enterprise, user provisioning may also be accomplished through roles established in the XenMobile console which is out of scope for this documentation. For accounts with Policy Based Administration enabled, it is best practice to disable the provisioningof ShareFile users through XenMobile.

Install

October 4, 2018

Best Practices

The UMT will allow you to connect into a selected domain but for best speed and results the tool should be installed on a domain joined server. It is recommended to install this tool on a server or box that is rarely taken offline.

The windows scheduler integration allows the User Management Tool rules to be run recurrently, keeping ShareFile up to date with changes in Active directory. These tasks cannot run if the machine is offline or shut down as often happens with personal machines. Tasks will be run using the windows user context that created the scheduled task and will require the correct permissions (listed above) to complete.

Additionally, an admin or service account in ShareFile may be used with the UMT and all user and group creation will be logged in ShareFile as an action of the admin or service account user. If segregating the logging of user creation by the UMT for tracking purposes is needed then it is recommended to create a service account to use with this tool. Use of a service account will allow for detailed reporting on the users and groups creating on the accounts name.

First Steps

Once the requirements are in place and all appropriate user accounts have been acquired, you can install the application.

Before installation, make sure that any prior UMT instance that is version 1.8 or older has been uninstalled and the Scheduled Tasks have been disabled or deleted. This is important because the UMT rules on a Policy Based Administration account are vastly different and you cannot upgrade an old-style UMT rule to a new PBA-style rule.

Once you have made sure all previous versions of the UMT have been removed, navigate to **www.citrix.com/downloads** and log in. If you do not have a user account you can easily register for one on the page. Once logged in, hover over the downloads link at the top of the page and then select **ShareFile** from the product drop down. On this page,you should see a link to download the latest ShareFile User Management Tool installer. Run the installer and follow the prompts to complete the installation. When finished a shortcut for the application will be placed on your desktop and in the start menu.

First-time setup

Upon first starting the tool you will be brought to a ShareFile login page. You will need to fill in which account you want to connect to as well as the ShareFile administrative or service account credentials listed in the requirements to run the application. This tool is designed to be run by an administrator and therefore does not support SAML authentication even if it is configured on the connected ShareFile account.

After logging into the correct ShareFile account with administrative credentials you will proceed to a domain log in. Here you will need to enter the domain and the credentials of a user with full read permissions to allow the UMT to read necessary properties from AD. If you are running this tool on a domain joined machine and logged in with a user account with the necessary permissions you can leave the form blank and click connect to use the local domain and user.

For best load times and speed, it is recommended to run this tool on a domain joined machine. Once authenticated you can choose to always use this domain in the future. Additionally, the tool should only be kept open when updating and managing rules. The log in token will expire if the tool is kept open and cause error messages upon next load.

Proxy Setup

If you need to configure a proxy server, click the Settings icon and then select Configure Proxy.

If you are unable to log in to configure these settings you can open this page manually by navigating to

Program Files>Citrix>ShareFile>User Management Tool

and opening the "ShareFileProxyConfig.exe"

Dashboard

Once logged in you will be navigated to the Dashboard page. This page displays quick links to see your existing rules, to create user rules or great group rules. Midway on the dashboard you will see a description of which ShareFile account and user as well as the domain and user you are logged in as for this session. Finally, you will see a history section, which displays status updates and logs for recently run rules and tasks.

Rule Creation

Information on Rule Creation and scheduling can be found under provision accounts and distritbution groups.

Upgrade

October 4, 2018

> **Important**
>
> Before installation, make sure that any prior instance of the User Management Tool that is version 1.8 or earlier has been uninstalled and the associated Scheduled Tasks have been disabled or deleted. This is required because the UMT rules on a Policy Based Administration account are vastly different and you cannot upgrade an old-style UMT rule to a new PBA-style rule.

> Once you have made sure all previous versions of the UMT have been removed, navigate to www.citrix.com/downloads and log in. If you do not have a user account you can easily register for one on the page. Once logged in, hover over the downloads link at the top of the page and then select **ShareFile** from the product drop down. On this page, you should see a link to download the latest ShareFile User Management Tool installer. Run the installer and follow the prompts to complete the installation. When finished a shortcut for the application will be placed on your desktop and in the start menu.

1. From the ShareFile download page at MyCitrix.com, download the latest User Management Tool installer to a server that is in the AD domain.
2. Follow the prompts to complete the installation.

   A shortcut for the tool is placed on the Start menu and your desktop.
3. Start the User Management Tool. The User Management Tool log on page appears.
4. Enter the ShareFile account information and then click Log on.

   Account URL is your ShareFile account URL, in the form `https://mysubdomain.sharefile.com` or, in Europe, `https://mysubdomain.sharefile.eu`.

   The User Management Tool window appears.
5. If you need to configure a proxy server, click the options icon and then click Configure Proxy.

Configure

October 4, 2018

To reach the settings section click the gear icon in the upper right hand side of the UMT. The UMT has two sets of options which can be set on the tool.

One is a set of global options which will applyacross all UMT installations for your account and the other is a set of local options specific to the current installation.

Global Options

Global options affect the way rules are run through UMT and will be changed across all installations for your account. Options will come preset with the most common settings seen.

Automatically disable users not part of domain rules: This option should only be used in extremely rare cases where all membership in ShareFile is very strictly managed by a single set of all-encompassing rules.If you currently or will eventually have more than one domain in your organization, it is best practice to leave this rule unchecked. When enabled the user management tool will find any users in ShareFile who are not part of the active rules(per domain)being run and will disable them. For security, the master admin will not be disabled even when this is selected. Best practice is to keep this item unchecked.

What should UMT do if an error occurs process a Rule in a scheduled job?: Occasionally errors are encountered when running tasks and this setting determines how the tool should react to those errors when performing unattended scheduled tasks. Options are to abort the entire scheduled job or to continue working on the job and process other rules after the failed one. Either option will create errors in the dashboard logs and mark the rule as failed.

Local Options

These options will only apply to a single UMT installation and will not be carried over to other installs connected to your account.

Log details of rules processing & API calls: This feature provides more in-depth logging of actions including the API communication the tool performs to communicate with the ShareFile SaaS application.

Enable detailed logging of Active Directory Operations: This feature will store more in-depth logging information over AD operations and features such as ID's, groups, and users. The path for storing this data is also typically C:\ProgramData\Citrix\ShareFile\User Management Tool \Umt_AD_Diagnostic.log

Proxy: Information for configuring and exporting proxy settings is also stored under local configuration. Since proper traffic flow is needed to log in with this tool if you are unable to authenticate to the UMT you can also manually set up proxy using the settings in the proxy section above.

Help and Information

You can locate the help and information section by clicking the question mark icon in the top right hand corner of the User Management Tool. A pop up help window will appear providing contact information for the ShareFile support team as well as web resources for more information.

Additionally, this page will indicate the UMT version and legal information as well as provide links to the logs, data folder, and install location.

If you encounter an error which needs additional troubleshooting support please reach out to the ShareFile support team with the email address or phone number listed here and be prepared to provide the version number and logs for review.

Provision user accounts and distribution groups

October 4, 2018

Rule Creation

The User Management Tool provisions users and groups to ShareFile through the creation of rules which correspond to Active Directory OUs and security groups. Once rules are created they can be run once or set to run on a schedule keeping ShareFile users and groups in sync with changes in AD. Customers can choose to create users and groups based on existing AD organization or may choose to create a designation for ShareFile in Active Directory so that users can be managed centrally through AD but stay synced with the ShareFile application.

If you are testing this tool or running a POC of ShareFile it is recommended that you create a ShareFile group in active directory to test with that contains all your POC users. This will allow you to test adding and removing users from the group.

Creating User Provisioning Rules

To create a rule which will provision user accounts in ShareFile navigate to the Users tab. The left-hand panel will display your Active Directory forest where you can browse to find the correct user group. When a valid user group is selected,you will see users displayed in the right-hand panel.

For a user to be provisioned into ShareFile that user must have a first name, last name and email address displayed in the right-hand column. If any of these fields are missing that user will not be added and an error will show when you attempt to run the rule.

Once the desired Active Directory user group is selected click add rule in the bottom left hand corner. The Edit Users Rule options will appear where you can determine how you would like these users created in ShareFile. Once the correct settings are selected click save and then click close.

Edit User Rule Options

After choosing to run a rule on a specific AD user group you must choose settings for how that rule will run. The Edit Users Rule pop up will appear allowing you to choose the appropriate settings for this rule.

Please note that clicking close on this screen will close the editing with current settings and does not cancel the creation of the rule. If you have created the rule in error it will need to be deleted from the rules tab. The question mark icon in the upper right hand corner will open a pop out that gives additional information about some settings available. Setting details are also listed below.

Policies, User Access: Choose which User Access Policy you want to assign the group by selecting the Policy from the drop-down list.

Policies, File and Folder Management: Choose which File and Folder Management Policy you want to assign the group by selecting the Policy from the drop-down list.

Policies, Storage Location: Choose which Storage Location Policy you want to assign the group by selecting the Policy from the drop-down list.

Update ShareFile employee information based on selected AD object (will disable user if disabled in AD): When using the UMT for long term user management it is recommended to keep this box selected. When this item is selected the rule is able to both provision users and update existing ShareFile users based on changes in AD. This will only update users email, first name, last name, and status. When rules are run on a recurring schedule this will mean that users who are disabled in AD will become disabled in ShareFile as well which is useful when centralizing user management to active directory.

Create ShareFile employees based on the selected AD object: This checkbox allows you to provision users into ShareFile and will enable all the below options as well.

Default Company Name: Typically this is the company name listed on your account and is only used for display and organizational purposes. If you work with multiple companies this field can be changed to label employees in ShareFile appropriately.

Notify Employees with email: When checked this will send a system generated welcome to ShareFile email to any newly created users.

Creating Distribution Group Provisioning Rules

ShareFile distribution groups allow you to easily send files and manage folder permissions for groups of users in a single instance. If you would like to use Active Directory security groups to create and provision group membership in ShareFile you will need to click on the groups tab in the top navigation bar of the UMT. On the groups page, you must search for the group you desire to use. You can search by what the group name contains or what it starts with based on a setting on the right.

Please note that ShareFile Distribution Groups can only support up to 2000 users per group. Once this limit is hit no additional users will be added and errors will be shown in the logs.

Once you have found the correct group click Add Rule in the bottom left corner. The edit groups rule pop up will appear where you can choose if this rule should be for one time use to create the group and populate existing members or if you would like it to update the group membership as well when running the rule on a schedule. Best practice is to leave both options selected so that rules can keep ShareFile groups synced with AD groups for centralized management.

> **Note:**
>
> Clicking close on this screen will close the editing with current settings and does not cancel the creation of the rule. If you have created the rule in error, it will need to be deleted from the rules tab.

The Groups tab is designed specifically to create distribution groups and populate them with existing ShareFile users but not to provision users initially in ShareFile. If you select a rule which contains users who are not already covered by a user provisioning rule a pop up asking if you would like to create a corresponding user provisioning rule will appear. If you do not create the corresponding user provisioning role then only users who already have ShareFile accounts will be added to the group membership.

Schedule and Manage Rules

Rules can be run on manual; single instance use or can be scheduled to run recurring to keep ShareFile synced with changes in Active Directory.

Understanding the Rules tab

The Rules tab will display all the rules you have currently configured with the UMT. This information is stored long term as a part of your account in the SaaS application so previously created rules will show up for all administrators on any machine. Rules are listed in the left-handpane and will be named first off, the AD attribute selected and then will say if the rule is to sync users or sync groups.

Rules are split between two tabs:

The first tab is the **User Rules** tab. This will house all your User rules in a hierarchy order. Beside each rule, you will see a number to the left of the rule's name. On the right, you will see up/down arrows which can be used to move the rule up or down in the hierarchy. It is important to make sure your rules are in the correct order because **if a user is part of more than one rule, the rule which runs first (highest in the hierarchy order) will be the policies that the user is assigned to.**

The second tab is the **Group Rules** tab. This tab houses all Group rules.The middle pane will display users and groups which will be affected by running rules. Finally,the far-right hand pane will show all actions to be completed ifthe rules are run. This will show the users and groups affected as well as if they need to be created or simply updated based on a change in AD. This pane can help you determine the impact of committing active rules based on the current state of your active directory.

Commit a Rule

If you would like to immediately apply the rules you can click the Commit Now button. This will perform all the actions listed in the right-hand actions pane. If you see no actions listed it is recommended that a refresh is done first so that you can review the effects of committing the rule.

Commit now should be used for running fules for one time or manual use or for immediately applying changes which may be needed outside an existing schedule.

Schedule a Rule

Rulescan be set to run as a scheduled activity through integration with Windows Scheduler. This is the most common configuration of the User Management Tool as it allows centralized user and group management for IT in active directory where most user management is performed by IT. This way if a user changes job roles, changes email or personal information, or is deactivated in AD a corresponding action will be performed in ShareFile automatically.

Clicking schedule will allow you to create a scheduled task with Windows Scheduler. Scheduled tasks can be run weekly, daily, continuously, once, or on a manually configured schedule. You can also configure the start date and time for the schedule task to initiate.

Updates to a rule or rules being added or removed will not change an existing scheduled task. If necessary you can update existing scheduled tasks through the schedule option as well.

Edit Existing Rules

To edit the settings of an existing rule, first highlight the rule in question and then click the Edit button. This will open the same options screen used when initially creating the rule where policies and settings can be changed. This will only update the settings forthe single highlighted rule at a time.

When saving edits to a rule, a pop-up will appear to remind you to update any scheduled tasks before the changes will apply.

Note: Unlike earlier versions of the UMT, editing a rules list of policies will affect how new users are provisioned in ShareFile and any existing user that is in the rule that has already been provisioned in ShareFile.

Deleting Rules

To delete a single rule you will want to highlight that rule and then click the delete button near the bottom of the rules screen. This should be used when a rule is created in error or the wrong AD item was used.

Please note that deleting a rule will not affect previously schedule tasks. If you wish to make this change you will also need to update the scheduled task.

Rules can also be cleared entirely by using the delete all option. Keep in mind that since rules are stored in the cloud for the account you will removing all of this configuration data which could be from other installations or administrators. Note, the delete all option only deletes the rules within the tab you are under. If you wish to delete every rule in the UMT, you need to select 'Delete All' under both the 'User Rules' tab and the 'Group Rules' tab.

Logs

A quick view of logged actions performed by the UMT can be seen on the dashboard. This will list all users and groups created or updated as well as list any errors that occurred in the process of running rules.

Migrate users between StorageZones

October 4, 2018

> **Note**
>
> As of version 1.9, zone migration is no longer a supported function of the UMT.

Re-linking users in your ShareFile account

November 27, 2018

When creating a user in ShareFile via the User Management Tool (UMT), we are adding a specific AD GUID to the ShareFile users and ShareFile Distribution Groups which "links" that user/group to Active Directory (AD). This GUID is used as the anchor so that if a user's information, such as their name or email address, is changed in AD, then we update it in ShareFile. However, in a few scenarios, such as changing domains where your existing "AD linked" ShareFile user/group is created as a new user/-group in the new domain, you would need to re-link the user/group via the UMT. Only UMT versions 1.8.1+ and 1.11+ support re-linking users in your ShareFile account.

AD Link Reset Mode

AD Link Reset Mode is a special operating mode in the UMT which allows the UMT to update the AD GUID in ShareFile that maps a ShareFile User or Distribution Group to the corresponding AD User or Group. (When in "normal" operating mode, UMT does not update this field once it has been set.) This GUID-based link is normally set by UMT when a ShareFile User/Group is either initially created from AD or when an existing ShareFile user is associated with an AD user via email matching.

AD Link Reset Mode is only available in the UMT UI application. Scheduled jobs will not run while UMT is in AD Link Reset Mode - they will exit, with an appropriate exit code & log message - before processing any rules. Additionally, any other UMT UI instances will be prevented from executing (on machines / Windows users other than the one on which the mode was enabled - see below for details).

Once UMT has been placed in AD Link Reset Mode (see below), it will not exit AD Link Reset Mode until Rules have been refreshed (on the Rules tab), and any re-link actions have committed successfully.

UMT will reset AD links based on existing user & group rules, and will only update links of existing ShareFile Users and Groups that already have the AD GUID field set. While in AD Link Reset Mode, UMT will not make any other changes to ShareFile users or groups - it will only update the AD GUID / link in ShareFile.

UMT will also prevent any other changes to Rules or configuration changes while in AD Link Reset Mode; unavailable functionality will be disabled & greyed in the UI. Unavailable functionality includes, but is not limited to the following:

All Versions:

- Creating new Rules
- Editing Existing Rules
- Scheduling Jobs via the **Schedule** button on the Rules tab

v 1.11:

- Re-ordering Rule Priority
- Search Tab

v 1.8.1:

- Users Tab
- Groups Tab
- Zones Tab

How to perform the AD Link Reset via the UMT

1. Disable any scheduled UMT jobs in Windows Task Scheduler.

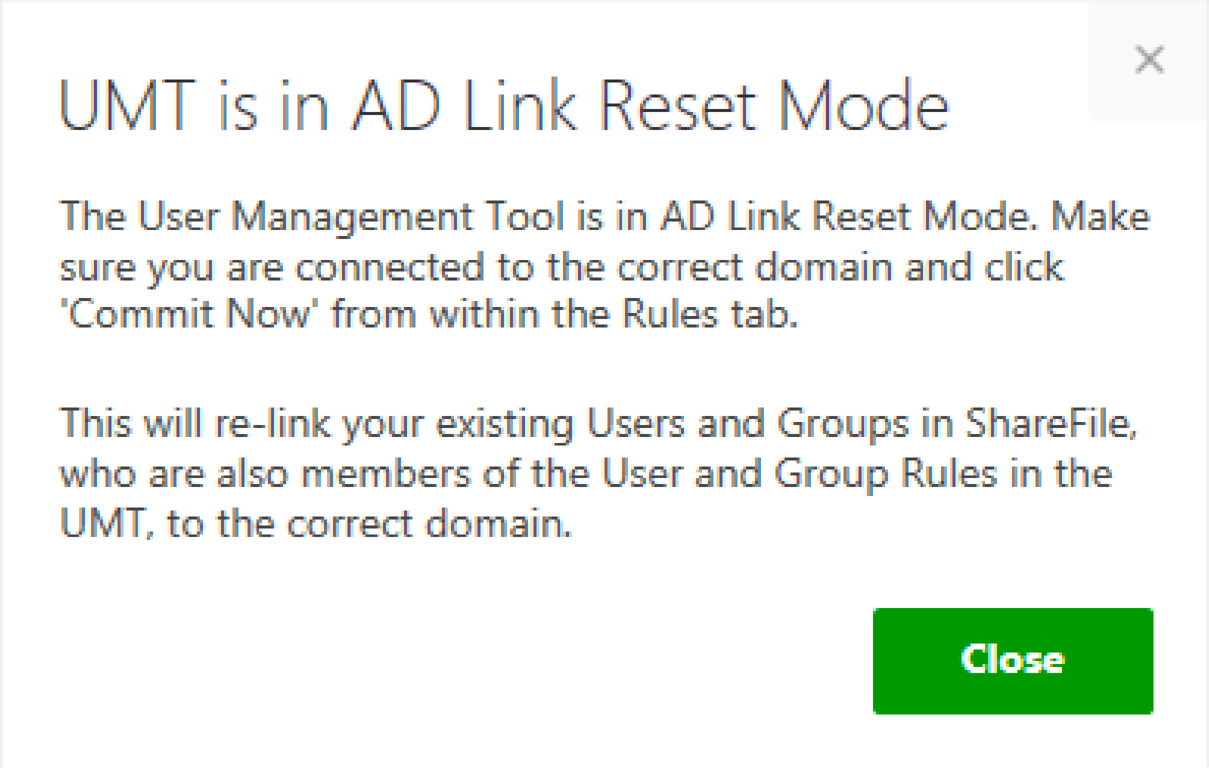
2. Launch the UMT, log into the new domain and create the correct User and Group Rules, however, DO NOT commit those Rules at this point.
3. Close the UMT.
4. Add the following AD Link Reset Mode Registry Key.

> **Note:**
>
> If you are using more than one UMTs in your environment, you only need to add the Registry Key to one machine and run the AD re-linking from that machine.

```
HKEY\_CURRENT\_USER\\SOFTWARE\\Citrix\\ShareFile\\UMT
String Value
Name: EnableADLinkReset
Data: you can leave this blank
```

5. Launch the UMT and log into the new domain

You will see a message letting you know that your UMT is in AD Link Reset Mode. If another user logs into a different machine and launches the UMT, they will receive a message letting them know that the account / UMT is in AD Link Reset Mode and which machine (via Machine Name) is the one performing the AD Link Reset.



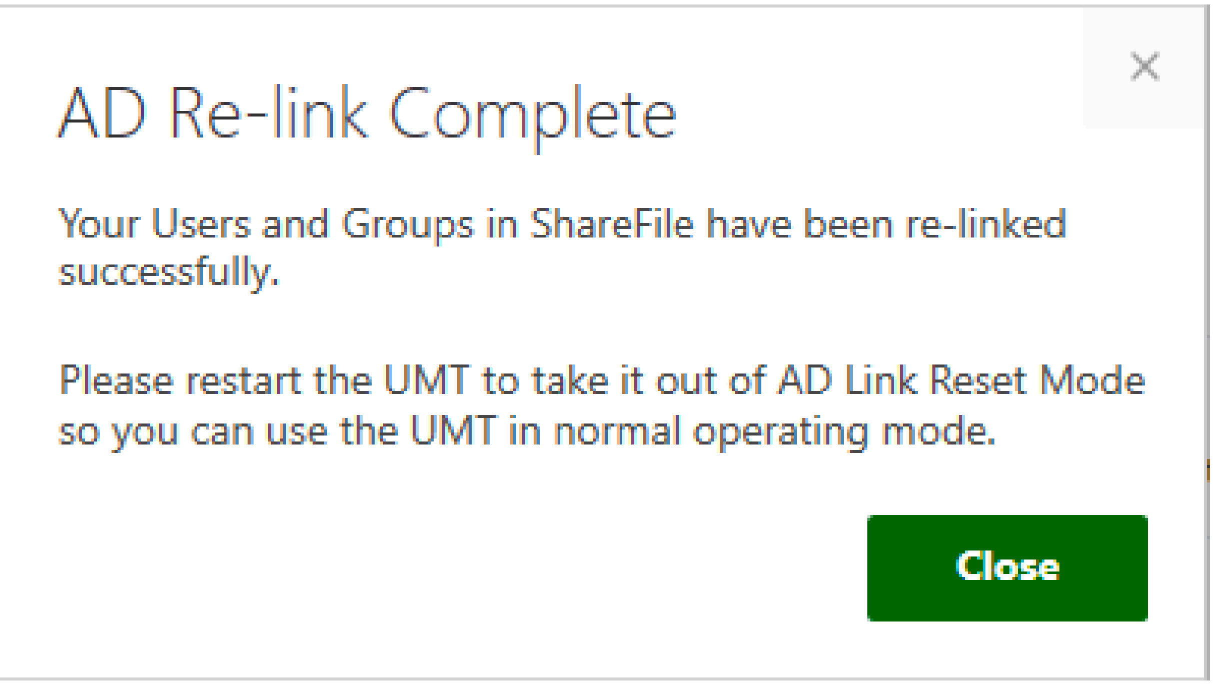
UMT is in AD Link Reset Mode

The User Management Tool is in AD Link Reset Mode. Make sure you are connected to the correct domain and click 'Commit Now' from within the Rules tab.

This will re-link your existing Users and Groups in ShareFile, who are also members of the User and Group Rules in the UMT, to the correct domain.

6. Navigate to the Rules tab, click 'refresh' followed by 'commit now.' The users who will be re-linked will have the words 'Reset User Link' next to their email address in the actions column.

7. If the re-link was successful you will get a success message, at which point you can exit the UMT (note, upon exiting, the EnableADLinkReset key will be removed if the re-linking was successful)



AD Re-link Complete

Your Users and Groups in ShareFile have been re-linked successfully.

Please restart the UMT to take it out of AD Link Reset Mode so you can use the UMT in normal operating mode.

8. Launch the UMT again, log into the new domain and begin using the UMT in normal operating mode.

At this point, you will want to reconfigure any Scheduled Tasks to point to the new Rules.

If you encounter any errors during the re-linking process and you need to make a change to the UMT Rules to correct the error, such as a User Rule points to a non-existing AD group, etc, follow the below steps to remove the specific machine from being in AD Link Reset Mode:

1. Close the UMT
2. Navigate to the AD Link Reset Mode Registry Key.
   - In the data field add the word: False
     - This will remove this specific UMT machine, under the current logged in user, from being in AD Link Reset Mode
3. Re-launch the UMT and continue with fixing the miss-configured Rules.
4. Close the UMT.
5. Navigate to the AD Link Reset Mode Registry Key
   - Delete the world False from the data field
6. Re-launch the UMT and continue forward with the AD Link Reset Mode process.

Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States