ShareFile

User Management Tool for Policy-Based Administration

Contents

About

July 26, 2024

> **Important**
>
> This version of the User Management Tool (UMT) is designed specifically for customers utilizing the Policy Based Administration feature and differs from typical UMT setup instructions. For customers utilizing the UMT without the policy administration feature, see the current version of UMT documentation.

About User Management Tool

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

The User Management Tool enables you to match ShareFile accounts to AD based on email address. It provisions and updates user information in ShareFile. In addition to distribution group membership, the tool allows you to specify policies a user is a part of, and to create multiple, named synchronization jobs that you can run repeatedly.

What's new

What's new in 1.17.2

- This release addresses connection timeouts related to slow proxy configurations.

What's new in 1.16.4

- This release addresses a number of issues that include:
  - Logging enhancements
  - Proxy file handling

What's new in 1.15

- This release addresses a number of issues that help to improve overall performance and stability.

What's new in 1.14

- Improved performance when loading and working with large numbers of rules and large numbers of ShareFile/Citrix Content Collaboration employees
- Logging enhancements

What's new in 1.13

- Improved performance when loading and working with large number of Rules
- Logging enhancements

What's new in 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 1.11

- Log Archiving
- Added the ability to relink users in your ShareFile account. More details on how this flow works can be found here: Relinking 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 1.10

- Consolidated the User and Groups tab into one tab and 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 can 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 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 2, 2023

The following is a list of operating system requirements for the 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 to run the ShareFileProxyConfig.exe file.

- Windows Server 2012 R2
- Windows 8 or later

Information on manually enabling .NET 3.5 can be found at this Microsoft article.

ShareFile/Citrix Content Collaboration requirements

Your account must have:

- Policy Based Administration enabled.
- Available employee licensees in ShareFile/Citrix Content Collaboration for each user who is added.

A ShareFile/Citrix Content Collaboration administrator user with the following permissions:

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

Active Directory requirements

An administrator 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
Email Addresses	mail
ms-DS-Phonetic-First-Name	msDS-PhoneticFirstName
ms-DS-Phonetic-Last-Name	msDS-PhoneticLastName
Object-Guid	objectGUID

Install

March 7, 2024

Introduction

The User Management Tool (UMT) allows you to connect into a selected domain, but for best speed and results the tool must be installed on a domain joined server. 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 (AD). These tasks cannot run if the ma-

chine is offline or shut down. Tasks are run using the Windows user context that created the scheduled task and require the correct permissions to complete.

Also, an administrator or service account in ShareFile can be used with the UMT and all user and group creation is logged in ShareFile as an action of the administrator or service account user. If segregating the logging of user creation by the UMT for tracking purposes is needed, it is recommended to create a service account to use with this tool. Using a service account allows for detailed reporting on the users and groups creating on the account's 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 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 different, and you cannot upgrade an old UMT rule to a new PBA rule.

1. Choose whether you need a x86 version or x64 version of the ShareFile User Management Tool with Policy Based Administration and down the latest version below:
   - ShareFile User Management Tool x64
   - ShareFile User Management Tool x86
2. Follow the prompts to complete the installation. A shortcut for the tool is placed on the **Start** menu and on your desktop.
3. Start the User Management Tool. The User Management Tool sign in page appears.
4. Enter the account information and then select **Log on**.

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

First-time setup

Upon first starting the tool, you are brought to a sign in page. Fill in which account you want to connect to in addition to the ShareFile administrative or service account credentials listed in the requirements to run the application. This tool is run by an administrator and therefore does not support SAML authentication even if it is configured on the connected account.

If your ShareFile account requires ShareFile Two-Factor Authentication when logging in with ShareFile credentials, you will need to set up an application specific password for the user. For more information about setting up this application specific password within your ShareFile account see, Create an application specific password.

After signing into the correct ShareFile account with administrative credentials, you proceed to a domain sign in. Here you 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 signed in with a user account with the necessary permissions, you can leave the form blank and select 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. Also, the tool must be kept open only 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, select the **Settings** icon and then select **Configure Proxy**.

If you are unable to sign in to configure these settings, you can open this page manually by navigating to `Program Files\>Citrix\>ShareFile\>User Management Tool` and opening `ShareFileProxyConfig.exe`.

Dashboard

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

Rule creation

Information on rule creation and scheduling can be found under provision accounts and distribution groups.

Configure

July 9, 2019

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

One is a set of global options which applies across all UMT installations for your account. 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 are changed across all installations for your account. The most common settings are set by default.

Automatically disable users not part of domain rules: This option should only be used in extremely rare cases where all membership in ShareFile/Citrix Content Collaboration is very strictly managed by a single set of all-encompassing rules. If there is more than one domain in your organization, it is considered best practice to leave this rule unchecked. When enabled, the User Management Tool finds users who are not part of the active rules (per domain) being run and disables them. For security, the master admin is not be disabled even when this is selected. Best practice is to leave this rule unchecked.

What should UMT do if an error occurs processing 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. The 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 creates errors in the dashboard logs and marks the rule as failed.

Local options

These options apply only to a single UMT installation and are 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/Citrix Files SaaS application.

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

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

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 appears, providing contact information for the Citrix support team, as well as web resources for more information.

Additionally, this page indicates the UMT version and legal information, as well as providing links to logs, data folders, and the install location.

If you encounter an error which needs additional troubleshooting support, reach out to Citrix support 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

December 8, 2021

Rule creation

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

If you are testing this tool or running a POC, it is recommended that you create a ShareFile/Citrix Content Collaboration group in Active Directory to test with that contains all your POC users. This allows you to test adding and removing users from the group.

Creating user provisioning rules

To create a rule which provisions user accounts in ShareFile/Citrix Content Collaboration, navigate to the **Users** tab. The left-hand panel displays your Active Directory forest where you can browse to find the correct user group. When a valid user group is selected, the users display in the right-hand panel.

For a user to be provisioned, the 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 is not added and an error displays when you attempt to run the rule.

Once the desired Active Directory user group is selected, select **Add rule** in the bottom left-hand corner. The **Edit Users Rule** options appears where you can determine how you would like these users created in ShareFile/Citrix Content Collaboration. Once the correct settings are chosen, select **Save** and then select **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 runs. The **Edit Users Rule** pop up appears, allowing you to choose the appropriate settings for this rule.

The question mark icon in the upper right hand corner opens 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, keep this box selected. When this item is selected, the rule is able to both provision users and update existing users based on changes in AD. This only updates user's email, first name, last name, and status. When rules are run on a recurring schedule, users who are disabled or deleted in AD are disabled in ShareFile/Citrix Content Collaboration 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/Citrix Content Collaboration and enables all the below options.
- **Default Company Name**: 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/Citrix Content Collaboration appropriately.
- **Notify Employees with email**: When checked, this sends a system generated welcome email to any newly created users.

Creating distribution group provisioning rules

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/Citrix Content Collaboration, select the **Groups** tab in the top navigation bar of the UMT. On the **Groups** page, you must search for the group you want to use. You can search by what the group name contains or what it starts with based on the settings on the right.

Distribution groups can support up to 2,000 users per group. Once this limit is hit, no additional users can be added and errors are shown in the logs.

Once you have found the correct group, select **Add Rule** in the bottom left corner. The **Edit Groups Rule** pop up appears where you can choose if this rule is 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. We recommend leaving both options selected so that rules can keep ShareFile/Citrix Content Collaboration groups synced with AD groups for centralized management.

> **Note:**
>
> Selecting **Close** on this screen closes the editing with current settings and does not cancel the creation of the rule. If you have created the rule in error, it must be deleted from the **Rules** tab.

The Groups tab is designed specifically to create distribution groups and populate them with existing ShareFile/Citrix Content Collaboration users but not to provision users initially. 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 appears. If you do not create the corresponding user provisioning role, then only users who already have ShareFile/Citrix Content Collaboration accounts are 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/Citrix Content Collaboration synced with changes in Active Directory.

Understanding the Rules tab

The **Rules** tab displays 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 show up for all administrators on any machine. Rules are listed in the left-hand pane and are named first, then by the AD attribute selected and then say if the rule is to sync users or sync groups.

The first tab is the **User Rules** tab. This houses all your user rules in a hierarchy order. Beside each rule, a number to the left of the rule's name is shown. On the right, up/down arrows are shown 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 displays users and groups which are affected by running rules. The far-right hand pane shows all actions to be completed when the rules are run. This shows the users and groups affected as well as if they need to be created or updated based on changes 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

To immediately apply the rules, select **Commit Now**. This performs 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 rules for one time or manual use or for immediately applying changes which might be needed outside an existing schedule.

Schedule a rule

Rules can 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. If a user changes job roles, email, or personal information or is deactivated in AD, a corresponding action is performed in ShareFile/Citrix Content Collaboration automatically.

Selecting **Schedule** allows 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 do 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, highlight the rule and then click **Edit**. This opens the same options screen used when initially creating the rule where policies and settings can be changed. This only updates the settings for the single highlighted rule at a time.

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

Editing a rules list of policies affects how new users are provisioned and any existing user that is in the rule that has already been provisioned.

Deleting rules

To delete a single rule, highlight that rule and then select **Delete** near the bottom of the **Rules** screen. This is used when a rule is created in error or the wrong AD item was used.

Deleting a rule does not affect previously schedule tasks. If you want to make this change, update the scheduled task also.

Rules can also be cleared entirely by using the **Delete All** option. Since rules are stored in the cloud for the account, all of this configuration data is removed which could be from other installations or administrators. The **Delete All** option only deletes the rules within the tab you are under. If you want to delete every rule in the UMT, 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 lists all users and groups created or updated, in addition to listing any errors that occurred in the process of running rules.

Relinking users

July 9, 2019

When creating a user in ShareFile/Citrix Content Collaboration using the User Management Tool (UMT), a GUID is added to the users and distribution groups which "links"that user or group to Active Directory (AD). This GUID is used as an anchor so that if a user's information, such as their name or email address, is changed in AD, then it is also updated in ShareFile/Citrix Content Collaboration. However, in a few scenarios, such as changing domains where your existing AD linked user or group is created as a new user or group in the new domain, you must relink the user or group using the UMT.

Only UMT versions 1.8.1 and later and UMT for PBA versions 1.11 and later support relinking users.

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 that maps a 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 user or group is either initially created from AD or when an existing ShareFile/Citrix Content Collaboration user is associated with an AD user using email matching.

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

Once UMT has been placed in AD Link Reset Mode, it does not exit AD Link Reset Mode until the rules have been refreshed on the **Rules** tab and any relink actions have committed successfully.

UMT resets AD links based on existing user and group rules, and only updates links of existing users and groups that already have the AD GUID field set. While in AD Link Reset Mode, UMT does not make any other changes to ShareFile/Citrix Content Collaboration users or groups, it only updates the AD GUID link.

UMT also prevents any other changes to rules or configuration changes while in AD Link Reset Mode. Unavailable functionality is disabled and grayed in the UI. Unavailable functionality includes but is not limited to the following:

All Versions:

- Creating rules
- Editing existing rules
- Scheduling jobs using the **Schedule** button on the **Rules** tab

v 1.11:

- Reordering rule priority
- **Search** tab

v 1.8.1:

- **Users** tab
- **Groups** tab
- **Zones** tab

Perform the AD Link Reset

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

2. Launch the UMT, sign in to the new domain and create the correct user and group rules. Do **not** commit the rules yet.
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 relinking 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.

A message displays 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 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.

6. Navigate to the **Rules** tab, click Refresh, and then **Commit now**. The users who are relinked have the words **Reset User Link** next to their email address in the **Actions** column.

7. If the relink was successful, a success message appears. You can exit the UMT (upon exiting, the EnableADLinkReset key is removed if the relinking was successful).

8. Launch the UMT again and sign in to the new domain and begin using the UMT in normal operating mode.

At this point, you might want to reconfigure any scheduled tasks to point to the new rules.

Fixing errors

If you encounter any errors during the relinking process and you need to make a change to the UMT rules to correct the error, 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.
3. In the data field, add the word False. This removes the specific UMT machine under the current logged in user from being in AD Link Reset Mode.
4. Relaunch the UMT and continue fixing the misconfigured rules.

5. Close the UMT.
6. Navigate to the AD Link Reset Mode registry key.
7. Delete the world False from the data field.
8. Relaunch the UMT and continue forward with the AD Link Reset Mode process.