CITRIX

User Management Tool

Contents

What's new 3

System requirements 6

About ShareFile User Management Tool 8

Install 9

Upgrade 12

Configure 12

Provision user accounts and distribution groups 14

Migrate users between StorageZones 16

What's new

October 4, 2018

What's new in User Management Tool 1.8.1

- Support for TLS 1.2 Security Protocol
- AD Link Reset Mode - Added the ability to re-link users in your ShareFile account. More details on how this flow works can be found at Re-linking users in your ShareFile account.
- Added an additional check when 'linking' a user via the UMT. We are now checking to see if the email address matches in AD compared to the user in ShareFile, as well as whether or not the AD GUID in AD matches the user in ShareFile.

What's new in User Management Tool 1.8

User Management Tool 1.8 includes performance enhancements and quality improvements.

What's new in User Management Tool 1.7.6

User Management Tool 1.7.6 includes these improvements and fixes:

- If the UMT cannot read the user's disabled state, we leave the user as "unknown" and populate a message requesting the UMT to be run in elevated mode.
- Fixed an odd bug where if a Group rule is added to the UMT and a user in that group is not in ShareFile (or going to be in ShareFile via User rule) then that user was being created as a client.
- If the user adds a ShareFile secondary email address through the ShareFile web application, the UMT is now aware of such actions.
- Fixed a bug where after a rule has been created and successfully run, the Refresh button fails to show any newly added members of the group in the Actions column unless UMT is restarted.

What's new in User Management Tool 1.7.5

User Management Tool 1.7.5 includes performance enhancements.

What's new in User Management Tool 1.7.4

User Management Tool 1.7.4 includes these enhancements:

- Update to the Groups tab. Groups no longer load automatically. Users must search for them individually. Note: if you do not add any text in the search field and click “search” it will attempt to load all the companies groups.
  - There are two settings for how you can search for Groups in the Groups tab:
    * Contains: Returns all groups with names containing the specified search term(s)
    * Starts With: Returns all groups with names starting with the specified search term
- Returned Groups are now reordered alphabetically
- Email notifications are sent when a client is prompted to an employee

What’s new in User Management Tool 1.7.3

User Management Tool 1.7.3 includes these enhancements:

- The User Management Tool now supports provisioning user accounts into restricted zones.
- When you update a rule that is part of scheduled jobs, the User Management Tool displays a message to remind you to update the jobs.

What’s new in User Management Tool 1.7.1

- A new global option lets you choose whether to continue scheduled jobs when the User Management Tool cannot process a rule due to a problem such as a missing last name or email address in an Active Directory record. Previously, the tool always stopped jobs when it encountered an error. By default, the User Management Tool now continues to the next rule after an error occurs.

  The tool also skips subsequent rules that are based on the same AD object as a rule that resulted in an error. For example, if the action to create users for a particular AD group fails, the tool also skips an action to create a distribution group for the same AD group. This prevents the creation of a distribution group with members that are not yet created as ShareFile users.
- The Options page includes a Save or Close button so you know whether your changes have been saved.
- Scheduled jobs can now use the proxy settings configured for the User Management Tool even if those jobs are run under a different account, such as a Windows service account. This feature requires configuration, as described in the “Configure a proxy server” section of Configure the User Management Tool.

What’s new in User Management Tool 1.7

- Support for migrating a group of AD users to a different StorageZone, including Citrix-managed and on-premises zones.

To get started, click the new Zones tab in the User Management Tool.

- Per-user storage quota for ShareFile files and folders. Specify the quota when provisioning accounts with the User Management Tool.

  In the Edit Users Rule dialog box, you can choose to use the default storage quota specified in the ShareFile account-wide preferences or you can specify a storage quota to override the default value.

  A user who is in multiple AD groups is allowed the largest quota specified in the groups.

Fixed issues

Issues fixed in User Management Tool 1.7.5:

- Added rule that prevents a user from entering more than 50 characters in the company field within a rule [SFUMT-53]
- Corrected issue where UMT may fail to import users in a group if users are in a particular named OU [SFUMT-51]

Issues fixed in User Management Tool 1.7.4:

- Fixed layout issues and registry errors [SFUMIT-40]

Issues fixed in User Management Tool 1.7.3:

- The User Management Tool does not support provisioning user accounts into restricted StorageZones. [SFUMT-42]
- For some accounts, scheduled tasks assign all new users to the wrong zone. [SFUMT-34]

Issues fixed in User Management Tool 1.7:

- The User Management Tool installer prompts you to install .NET Framework 4.0 instead of the required .NET Framework 4.5. [17846]
- The User Management Tool does not indicate that a distribution group was not created because it contains more than the maximum of 2000 users allowed by ShareFile. [127822 and 91356]
- A scheduled job will not run if you save the job with the default Start On date. To work around this issue, type a different Start On date and then change the date back to the current date. [87453]
- The Update existing job setting is active in the Save Job dialog box even if there are no scheduled jobs. [88609]
- The User Management Tool allows invalid values for custom storage quotas. [89554]
- The User Management Tool cannot run a job that includes a space in the job name. To work around this issue, do not use spaces in job names. [17230]

Known issues

- If your site uses ShareFile Two-Step Verification, you must use a password that is specific to the User Management Tool to log on to it.
- The User Management Tool will create a new distribution group if it finds a distribution group name in ShareFile that matches an AD group name. The tool will not combine the AD group with the existing distribution group.

System requirements

October 4, 2018

The following is a list of operating system requirements for the ShareFile User Management Tool version 1.8:

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

General requirements

- .NET Framework 4.5
- Minimum monitor resolution of 1024 x 768

ShareFile requirements

- Available employee licensees in ShareFile for each user who is to be added.
- A ShareFile admin account with permissions to configure single sign on, manage employee users, edit shared distribution groups, and select storage zone for root level folders.

Active Directory Requirements

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

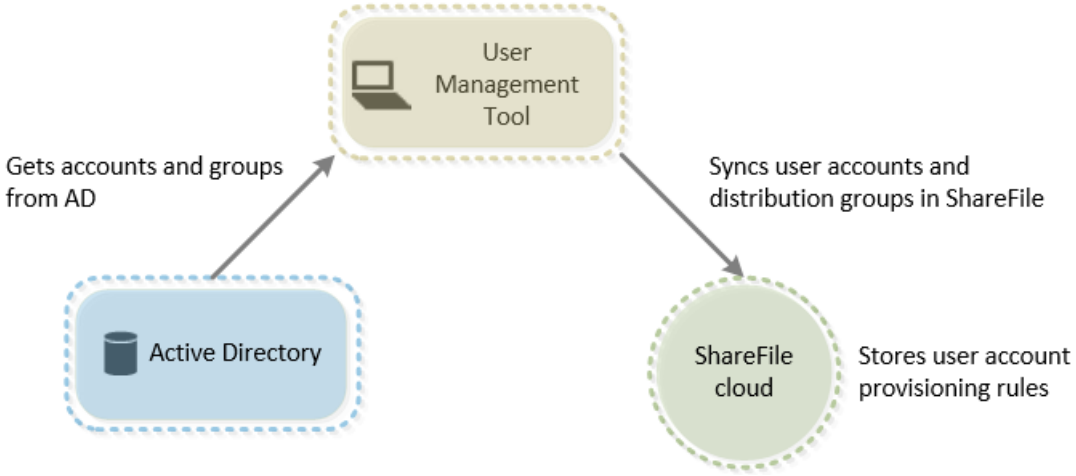
User accounts to be mirrored in Active Directory must have the following attributes:

CN	LDAP-Display-Name
Email Addresses	mail
ms-DS-Phonetic-First-Name	msDS-PhoneticFirstName
Ms-DS-Phonetic-Last-Name	msDS-PhoneticLastNAme
Object-Guid	objectGUID
SAM-Account-Name	sAMAccountName (used before Windows 2000)
User-Principal-Name	userPrincipalName

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).



The User Management Tool:

- Enables provisioned users to log in to ShareFile using their AD credentials.
- Stores user account provisioning rules with your account information in the ShareFile cloud. You can install the tool on any machine and access your rules by logging in to your ShareFile account.
- Matches ShareFile accounts to AD based on email address, links your existing ShareFile employee accounts to AD, and updates employee account information in ShareFile.
- Enables you to specify options, including the authentication method and default StorageZone, for each provisioning rule.

- Enables you to use distribution groups to manage folders and easily share documents with a group.
- Keeps ShareFile in sync with AD changes based on the schedule you specify. You can create multiple, named synchronization jobs in the User Management Tool. To run a job, the User Management Tool uses the same Windows user context that was active when the job was scheduled.
- Supports a proxy server connection between the User Management Tool and ShareFile.
- Includes a log file to help with troubleshooting ShareFile API-related issues.

Install

October 4, 2018

The User Management Tool stores account provisioning rules with your account information in the ShareFile cloud. You can install the tool on any machine and access your rules by logging in to your ShareFile account.

The ShareFile account information needed to log on to the User Management Tool are saved on your local machine in the configuration file for each job and secured with DPAPI encryption. When you open the User Management Tool, your ShareFile account URL and user name are pre-filled and you must enter your password.

Verify that your environment meets the system requirements before installing the tool.

> **Tip**
>
> If you encounter an error referencing "Try enabling AD Diagnostic Logging" or "Try running UMT elevated", you should:
>
> 1. Run the UMT tool as an Administrator by right-clicking the UMT Program Icon and selecting Run As…Administrator, or editing the shortcut properties to always Run as Admin within the Advanced Tab.
> 2. When working with scheduled tasks - select "Run with highest privileges" when creating a Task.

First Steps

In AD, create a test group containing a few users that already have ShareFile employee accounts. If that is not possible, identify an AD Organizational Unit (OU) that you can use for testing.

From the ShareFile download page at MyCitrix.com, download the User Management Tool installer to a server that is in the AD domain.

If you do not plan to schedule synchronization, you can install the tool on a workstation instead.

Run the installer, following the prompts to complete the installation.

A shortcut for the tool is placed on the Start menu and your desktop.

Start the User Management Tool. The User Management Tool log on page appears.

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`.

Specify an email address that is associated with an administrative or service user on the ShareFile account.

The User Management Tool window appears.

Connect to the AD domain to be used to create users and distribution groups in ShareFile.

Specify an AD user account that has full read permission on the AD domain.

Proxy

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

- 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 2012R2
- 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

Next Steps

Based on the test group or OU that you identified in step 1, click either the **Groups** tab or the **Users** tab, click the test group or OU, and then click **Add Rule**.

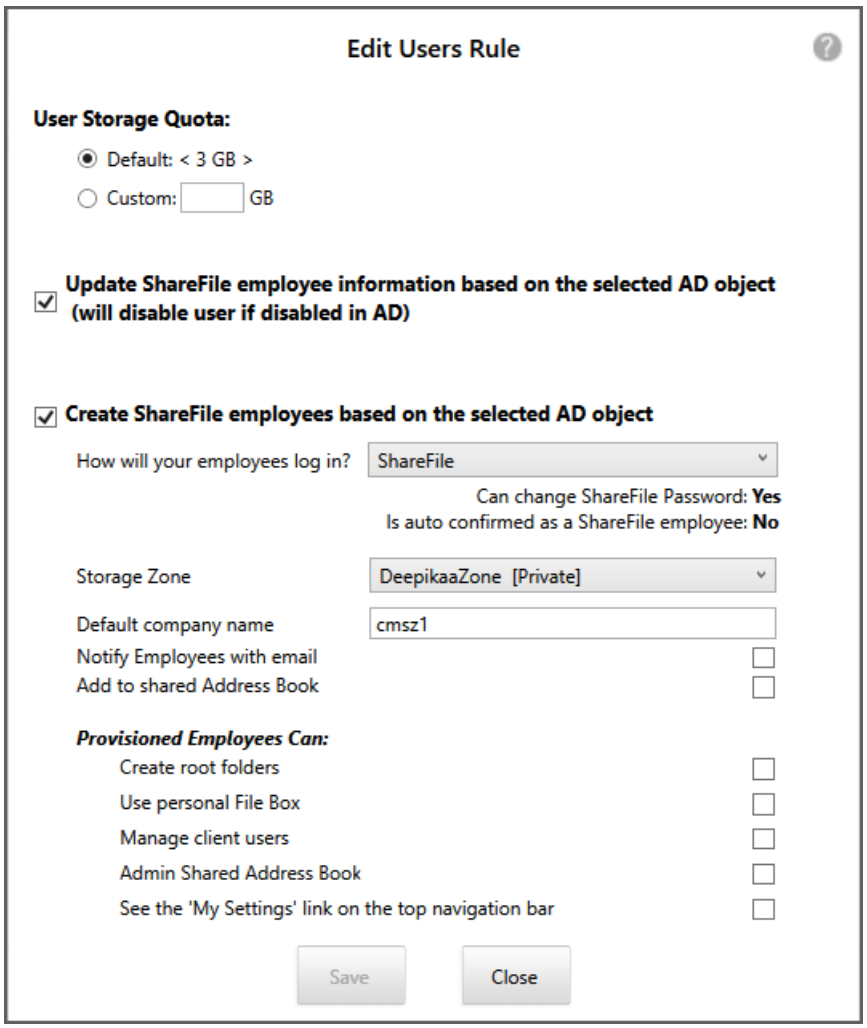
Click the **Rules** tab and then click **Refresh**. The changes that will occur when the rules are run appear in the **Actions** area. If no changes are listed, the rules you applied did not result in new or changed user accounts or groups.

Schedule the AD synchronization: Click **Schedule** and then use the **Save Job** dialog box to create a named job and specify a synchronization schedule.

After the scheduled synchronization, log on to the ShareFile interface and verify that the accounts are created.

If you clicked the Groups tab: In the Edit Groups Rule dialog box, select the check boxes for Create a ShareFile distribution group… and Update the ShareFile distribution group… to create and update new employee accounts and distribution groups. If the AD group includes users that do not have ShareFile accounts, you have the option to create the employee accounts too. Review and update the user options that appear, as needed. The options apply to each user created.

If you clicked the Users tab: In the Edit Users Rule dialog box, review and update the options as needed. The options apply to each user created.



The Windows user context in effect when you create a job is also used to run the job.

> **Note:**
>
> To create a job that uses advanced configuration such as triggers, actions, or conditions, specify a Schedule of Manual and then use the Windows Task Scheduler.

Upgrade

October 4, 2018

> **Note:**
>
> When you upgrade from a version of the User Management Tool that is earlier than release 1.5, existing rules are moved to the ShareFile cloud.

Verify that your environment meets the system requirements before upgrading the tool.

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 change the options described in this topic, click the cog icon.

Disable users in ShareFile

By default, the User Management Tool retains ShareFile user accounts that would not be created by the current rules. This prevents the automatic deletion of ShareFile user accounts that were created outside of the User Management Tool. Select the Automatically disable users not part of domain Rules option only if you want to remove ShareFile user accounts that do not meet the current rules for account creation.

Continue or stop scheduled jobs after an error

You can choose whether to continue scheduled jobs when the User Management Tool cannot process a rule due to a problem such as a missing last name or email address in an Active Directory record. By default, scheduled jobs continue to the next rule after an error occurs.

After the User Management Tool skips a rule due to an error, it also skips any subsequent rules that are based on the same AD object. For example, if the action to create users for a particular AD group fails, the tool also skips an action to create a distribution group for the same AD group. This avoids creating a distribution group with members that are not yet created as ShareFile users.

For rules that are run directly from the User Management Tool Rules tab, the User Management Tool always skips a rule that causes an error and continues to the next rule.

Log Active Directory operations

Automatically disable users not part of domain rules: This option should only be used in extremely rare cases in which the following is true.

- All membership in ShareFile is very strictly managed by a single set of all-encompassing rules.
- All of the groups and users in those rules are members of the same domain.

When enabled, the User Management Tool finds any users in ShareFile who are not part of the active rules being run and disables the users. For security, the master admin is not disabled even when you select this option. A best practice is to keep this item unchecked.

Configure a proxy server

To specify a proxy server for the User Management Tool, you must be logged on as an administrative user. As a result, scheduled jobs that are run under a Windows service account cannot use the proxy server until you configure the job to use the proxy settings. The following steps describe how to specify a proxy server, export the settings, and then configure a scheduled job to use those settings.

1. Log on to Windows as an administrative user.
2. Click the cog icon to open the **Options** page, click **Configure Proxy**, and then specify the proxy settings.

   If you will run scheduled jobs as administrator, you have completed the proxy setup.
3. If scheduled jobs will be run as another user, such as a Windows service account, export the proxy settings: In the **Options** page, click **Export Proxy Settings**.

   The proxy settings are exported to C:\ProgramData\Citrix\ShareFile\User Management Tool\proxy.config. The file is encrypted using Windows Data Protect API (DPAPI) machine-level

encryption, plus a key that is unique to your User Management Tool installation. Use this file for all of the jobs scheduled from the computer where you are logged on.

4. Configure each scheduled job to use the exported proxy settings.

   a) Open the Windows Scheduled Tasks management console, right-click the job you need to configure with the proxy settings, and then select **Properties**.

   b) Click the **Actions** tab, select the **Start a program** action, and then click **Edit**.

   c) Add the following to the end of the **Add arguments** entry: A space followed by /import-proxy.

      Make sure that you enter the argument after the existing entry and a space.

   d) After you click **OK**, the Task Scheduler might ask you if you want it to run C:\Program with some arguments. Click **No**.

   After the scheduled job successfully uses the proxy settings, the umt.log file will include the following entries:

```
ImportedProxy_Get
    Found exported proxy settings at:  C:\ProgramData\Citrix\
       ShareFile\User Management Tool\proxy.config
    Retrieved proxy settings from file.
```

Provision user accounts and distribution groups

October 4, 2018

You provision user accounts by choosing AD Organizational Units (OUs). The User Management Tool matches accounts based on email address and adds or updates employee account information in ShareFile.

When you add a distribution group and choose to create employee accounts, users accounts are linked to AD only if those users already have a ShareFile employee account. If an employee user is not in ShareFile, they do not appear in the distribution group created using the User Management Tool.

When ShareFile synchronizes with AD, ShareFile uses logon names and email addresses to validate employee accounts against AD. AD groups synced with ShareFile through the User Management Tool will sync as a distribution group in ShareFile.

ShareFile has a limit of 2000 users per distribution group.

1. Log on to the User Management Tool.

A shortcut for the tool is on the Windows Start menu. The tool is installed in C:\Program Files\ShareFile\umt.exe.

The connected subdomain appears on the Dashboard. To connect to a different subdomain, click the  icon.

2. To add users from AD:

   1. Click the Users tab.

   ```
   Your AD Organizational Units (OUs) appear.
   ```

   2. Click one or more objects and then click Add Rule.

   3. In the Edit Users Rule dialog box, review and update the options as needed.

   ```
   You can specify storage quotas, whether to use values from AD for
       ShareFile employee information, and settings for new accounts,
       such as a StorageZone and user permissions. For more
       information, click the question mark icon in the dialog box.

   The settings are applied when a new account is created.
   ```

3. To add distribution groups from AD:

   1. Click the Groups tab.

   2. Click one or more groups and then click Add Rule.

   ```
   The Edit Groups Rule dialog box opens.
   ```

   3. To create and update new employee accounts and distribution groups, select the check boxes for Create a ShareFile distribution group… and Update the ShareFile distribution group….

   ```
   If you choose to create employee accounts and a user in an AD
       group already has a ShareFile employee account, the account is
       linked to AD.
   ```

   4. In the Edit Users Rule dialog box, review and update those options as needed.

4. To apply the added rules:

   1. Click the Rules tab.

   ```
   - The Rules area lists all added rules.
   - The Desired Users or Desired Groups area lists the users or
       groups to be added by the selected rule.
   - The Actions area shows the results of the applied rules.
   ```


2. To manage rules:

```
- To make a rule active or inactive, click a calendar icon. The
  calendar icon for an inactive rule is dimmed.
- To delete a rule, select it and click Delete.
- To view the user accounts or groups to be added by a rule,
  select the rule. The information to be added appears in the
  Desired Users or Desired Groups area.
```

3. To preview the results of all active rules, click Refresh.

```
The changes that will occur when the rules are run appear in the
   Actions area. If no changes are listed, the rules you applied
   did not result in new or changed user accounts or groups. Click
    a user to view details provided from AD.
```

4. To immediately apply the active rules, click Commit Now.

```
To ensure that ShareFile is kept up-to-date with AD changes,
   specify a synchronization schedule.
```

5. To schedule AD synchronization for all active rules, click Schedule and use the Save Job dialog box to create a named job and specify a synchronization schedule. You can also update a job.

   Jobs are stored in %ProgramData%\Citrix\ShareFile\UserManagementTool\Jobs.

   The Windows user context in effect when you create a job is also used to run the job.

   Note: To specify advanced scheduling features such as triggers and conditions, specify a Schedule of
   Manual and then use Windows Task Scheduler.

   If you will run the scheduled job as a non-administrative user, you must configure it to use the proxy settings as described in the “Configure a proxy server” section of Configure the User Management Tool.

6. To view recent activity and synchronization results, click the Dashboard tab.

Migrate users between StorageZones

October 4, 2018

ShareFile offers a variety of storage options, including Citrix-managed cloud storage in multiple worldwide locations as well as storage that you manage with ShareFile StorageZones Controller. The User

Management Tool enables you to migrate ShareFile users, based on their membership in AD groups or Organizational Units (OUs), between StorageZones.

1. In the User Management Tool, click the Zones tab.
2. In the Active Directory listing, select the group or OU containing the users you want to migrate.

   The group or OU that you select does not need to correspond to an existing rule. You will have the option to remove individual users from the selection.

   A list of AD users who already have ShareFile accounts appears.
3. Choose a StorageZone from the drop-down menu above the list of users.

   The User Management Tool selects each user who is not already in the zone you chose.
4. As needed, change the user selection by selecting or clearing individual check boxes. To clear all check boxes, click Clear All.
5. To start the migration, click Apply.

   The User Management Tool schedules the data migration and lets you know that the zone has been changed for the user accounts. The data migration is transparent to users and can take days or weeks to complete, depending on the amount of data.

