Progress | ShareFile

# User Management Tool

# Contents



# About

September 3, 2024

## 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 provisioned users to sign in to ShareFile/Citrix Files using their AD credentials.
- Stores user account provisioning rules with your account information in the Citrix cloud. You can install the tool on any machine and access your rules by logging in to your account.
- Matches ShareFile accounts to AD based on email address, links your existing employee accounts to AD, and updates employee account information in ShareFile.
- Enables you to specify options, including the authentication method and default storage zone 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 Citrix API-related issues.

For information about new features, see What's new.

## What's new

### User Management Tool 1.8.6

This release addresses issues that help to improve overall performance.

### User Management Tool 1.8.5

- This release addresses issues that help to improve overall performance and include the enhancement:
  - **RightSignature permissions** - updated permission options for accounts with RightSignature and electronic signature functionality.

#### User Management Tool 1.8.4

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

## Fixed issues

#### Fixed issues 1.8.6

- Attempts to authenticate might fail for some users. [SFUMT-417]

#### Fixed issues 1.8.5

This release addresses issues that help to improve overall performance.

#### Fixed issues 1.8.4

User Management Tool 1.8.4 includes performance enhancements.

#### Fixed issues 1.8.3

User Management Tool 1.8.3 includes performance enhancements.

#### Fixed issues 1.8.2

User Management Tool 1.8.2 includes performance enhancements.

#### Fixed issues in 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 might fail to import users in a group if users are in a particular named OU. [SFUMT-51]

#### Fixed issues in 1.7.4

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

### Fixed issues in 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]

### Known issues

- Azure Active Directory is not directly supported in the User Management Tool. To work around this issue, set up a local active directory on the same server as the User Management Tool. The local active directory will then connect to Azure Active Directory. For more information, see Deploy.
- 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 creates a new distribution group if it finds a distribution group name in ShareFile that matches an AD group name. The tool does not combine the AD group with the existing distribution group.

## System requirements

September 3, 2024

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

- 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 and higher
- Minimum monitor resolution of 1024 x 768

### ShareFile requirements

- Available employee licensees in ShareFile for each user who is to be added.
- An administrator 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 |

## Install

September 3, 2024

The User Management Tool (UMT) 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 account information needed to log on to the User Management Tool is 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 username are pre-filled and you must enter your password.

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 informa-

tion about setting up this application specific password within your ShareFile account see, Create an application specific password.

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

If you encounter an error referencing *Try enabling AD Diagnostic Logging* or *Try running UMT elevated*:

- 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.
- When working with scheduled tasks, select **Run with highest privileges** when creating a task.

### First steps

1. In Active Directory (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.
2. 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
3. Run the installer, following the prompts to complete the installation. A shortcut for the tool is placed on the Start menu and your desktop.
4. Start the User Management Tool.

    The User Management Tool sign in page displays.
5. Enter the ShareFile account information and then select **Log on**. The account URL is your ShareFile account URL, in the form `https://mysubdomain.sharefile.com` or, in Europe, `https://mysubdomain.sharefile.eu`.
6. Specify an email address that is associated with an administrative or service user on the ShareFile.

    The User Management Tool window displays.
7. Connect to the AD domain used to create users and distribution groups in ShareFile.
8. Specify an AD user account that has full read permission on the AD domain.

> **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 Citrix cloud.

### Proxy

If you need to configure a proxy server, select the **Options** icon and then select **Configure Proxy**. For best performance, install .NET Framework on a domain-joined machine or VM.

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.

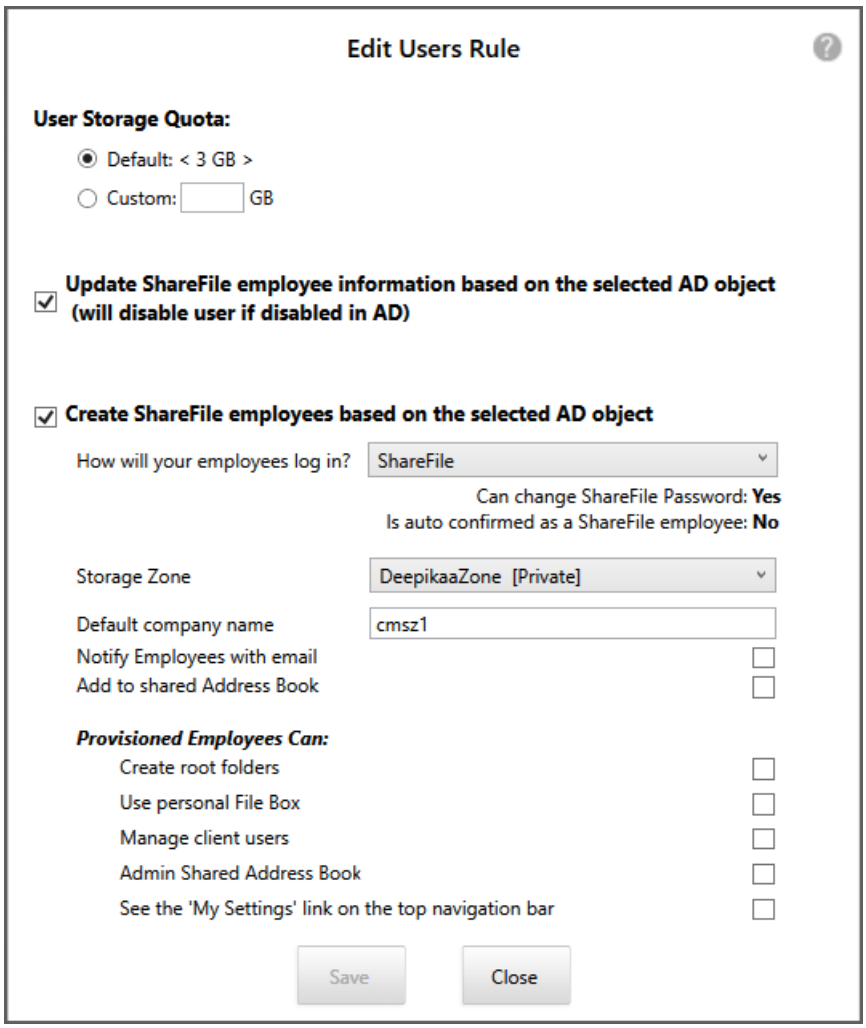
### Next steps

1. Based on the test group or OU that you identified, select either the **Groups** tab or the **Users** tab, select the test group or OU, and then select **Add Rule**.
2. Select the **Rules** tab and then select **Refresh**. The changes that 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.
3. Schedule the AD synchronization by selecting **Schedule** and then use the **Save Job** dialog box to create a named job and specify a synchronization schedule.
4. After the scheduled synchronization, sign in 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 accounts, you have the option to create the employee accounts too. Review and update the user options that appear. 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.




> **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.

## Configure

September 3, 2024

To change the options described in this topic, select the cog icon.

### Disable users

By default, the User Management Tool retains ShareFile user accounts that are not created by the current rules. This prevents the automatic deletion of 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 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 (AD) 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 is only used in rare cases in which the following are true.

- All membership in ShareFile is 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 who are not part of the active rules being run and disables the users. For security, the master administrator is not disabled even when you select this option. A best practice is to keep this item cleared.

### Configure a proxy server

To specify a proxy server for the User Management Tool, you must be signed in 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 run scheduled jobs as administrator, you have completed the proxy setup.

3. If scheduled jobs are 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.

Configure each scheduled job to use the exported proxy settings.

1. Open the Windows Scheduled Tasks management console, right-click the job you need to configure with the proxy settings, and then select **Properties**.
2. Click the **Actions** tab, select the **Start a program** action, and then click **Edit**.
3. Add the following to the end of the **Add arguments** entry: A space followed by /importproxy.

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

September 3, 2024

You can provision user accounts by choosing Active Directory (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 create employee accounts, users accounts are linked to AD only if those users already have a ShareFile employee user account. If an employee user is not in the account, they do not appear in the distribution group created using the User Management Tool.

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

ShareFile has a limit of 2,000 users per distribution group.

### Provision accounts and groups

To provision accounts and groups:

1. Sign in to the User Management Tool. The connected subdomain appears on the Dashboard. To connect to a different subdomain, select the subdomain icon.
2. To add users from AD:
   1. Select the **Users** tab. Your AD Organizational Units (OUs) displays.
   2. Select one or more objects as needed and then select **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 employee information, and settings for new accounts, such as a storage zone and user permissions. For more information, select the question mark icon in the dialog box.

The settings are applied when a new account is created.

### Distribution groups

To add distribution groups from AD:

1. Select the **Groups** tab.
2. Select one or more groups as needed and then select **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 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.

### Rules

To apply the added rules, select the **Rules** tab.

- The **Rules** area lists all added rules.

- The **Desired Users** or **Desired Groups** area lists the users or groups added by the selected rule.
- The **Actions** area shows the results of the applied rules.

To manage rules:

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

To preview the results of all active rules, select **Refresh**.

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

To immediately apply the active rules, select **Commit Now**.

### Scheduling

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

To schedule AD synchronization for all active rules, select **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`.

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

If you 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.

To view recent activity and synchronization results, select the **Dashboard** tab.

## Migrate users between storage zones

September 3, 2024

ShareFile offers a variety of storage options, including Citrix-managed cloud storage in multiple worldwide locations in addition to storage that you manage with storage zones controller. The User Management Tool enables you to migrate users, based on their membership in Active Directory (AD) groups or Organizational Units (OUs), between storage zones.

1. In the User Management Tool, select the **Zones** tab.
2. In the Active Directory listing, select the group or OU containing the users you want to migrate. A list of AD users who already have accounts appears.

   The group or OU that you select does not need to correspond to an existing rule. You have the option to remove individual users from the selection.
3. Choose a storage zone from the 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, select **Clear All**.
5. To start the migration, select **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.