



Triofox Administration Guide

Triofox Server Version 13.5.9497.54016

JUNE 8, 2022

COPYRIGHT © 2022 GLADINET, INC

Contents

Getting Started	2
Introduction.....	2
Administration Scope	3
Partner Portal.....	3
Self-Hosted Triofox.....	3
Cluster Administrator	4
Cluster Administration	5
The Basics.....	5
Login and Manage.....	6
Published Shares	7
File Servers.....	15
Devices.....	17
Users	19
Reports.....	24
Settings.....	29
Client Downloads	38
Cluster System Info	39
Cluster Info.....	39
Server Farm.....	40
Client Versions.....	49
Administrators.....	51
Cluster Branding.....	52
Cluster Settings	61
Application Manager	67
Languages.....	68
Anti-Virus.....	68
Cloud Backup	69
Cloud Backup.....	69
Enabling Cloud Backup	71
Cloud Backup Settings	72

Getting Started

Introduction

Welcome to the **Triofox Server** Administration Guide. This guide describes administration tasks for Triofox, the mobile access and secure file sharing solution that focuses on local file server cloud-enablement.

Triofox includes the Triofox server running on the Microsoft Windows server platform, and client agent applications for web browsers, Microsoft Windows, macOS, and for mobile platforms such as the Android and Apple iOS operating systems.

Important

Triofox includes a client application for Windows File Server called "Server Agent". This document is about Triofox itself, not about the "Server Agent".

Attention

This admin guide has been updated for Triofox version 13.4.9785.53973.

Administration Scope

Partner Portal

You can register a Triofox cluster in the Triofox Partner Portal.

The Partner Portal is located at <https://www.triofox.com>, and you can log in here: <https://www.triofox.com/management/partnerloginpage.aspx>. Through the Partner Portal you can download the Triofox software as well as manage the licensing of your servers.

Tip

Typically, you download the Triofox software, set it up, and use the built-in 30-day trial period to complete the setup. Towards the end of the trial period, you assign licenses to your server via the partner portal and activate it in a production environment.

Self-Hosted Triofox

In the user interface, the Self-Hosted Triofox instance is referred to as a Cluster or a Server Farm. A Cluster can be as small as a single server or scaled out to include multiple servers in a Server farm.

Users, Devices, File Server Shares

The objects you manage in the cluster include Users and Devices as well as File Server Network Shares for Team Folder collaboration (Team Shares).

This document focuses on the management scope for a Self-Hosted Triofox. In the server management interface, the administration scopes is called Cluster Administrator.

Cluster Administrator

The Cluster Administrator can manage cluster-wide functionalities, such as email SMTP server setup and worker node properties etc.

Cluster Administrator is often referred to as the Master Admin, Root Admin, or simply the Server Administrator. Although the Cluster Server Farm may have multiple servers, in most cases a server-farm with one single server is sufficient for your use case and user base.

Note

1. All administration work is done through the web portal in a web browser. Recommended browsers include Google Chrome first, followed by Firefox, Internet Explorer, Safari, and Opera (Internet Explorer requires version 9 and above and includes Microsoft Edge browser).
2. The very first user who installed the Cluster Server is also the Cluster Admin.
3. You can start the administration work at any time by pointing your web browser to the Cluster Server IP address or DNS name. If you are on the Cluster Server console, you can even use `http://localhost` to get started.

Cluster Administration

The Basics

To access your Cluster Administration features, log in to the Web Portal on the server. The description in this guide assumes that you are logged in as the Master Administrator (aka., Cluster Administrator). Some of the options listed may not be available if you are logged in with other privileges. In this document, the Triofox is also referred to simply as Cluster Server.

Tip

The Web Portal URL is the DNS name of the server, the IP address, or the local host (<http://localhost>) when you are in the server console.



Note

At the bottom of the login screen, you will find version information that tells you which version you have installed.

Login and Manage

After you log in to the web portal as a Cluster Administrator, you are in the dashboard.

The screenshot shows the Triofox Dashboard with the following sections:

- Published Shares:** You have 1 file share published. Add a share. Browse file servers.
- My Website URL:** You and your users can access the published shares (and/or management console) from the following web site URL:
 - Web File: <https://win-bp9o9l6epkq.triofox.io/portal/files>
 - Browser: <https://win-bp9o9l6epkq.triofox.io/portal/files>
 - Admin: <https://win-bp9o9l6epkq.triofox.io/management/clustermgrconsole>
 - Console: [bp9o9l6epkq.triofox.io/management/clustermgrconsole](https://win-bp9o9l6epkq.triofox.io/management/clustermgrconsole)
- System Info:** 30 trial day(s) left.
- Charts:**
 - File uploads in last 60 minutes: A line chart showing zero activity.
 - File uploads in last 24 hours: A line chart showing zero activity.
 - Bandwidth usage in last 60 minutes (Upload): A line chart showing zero activity.

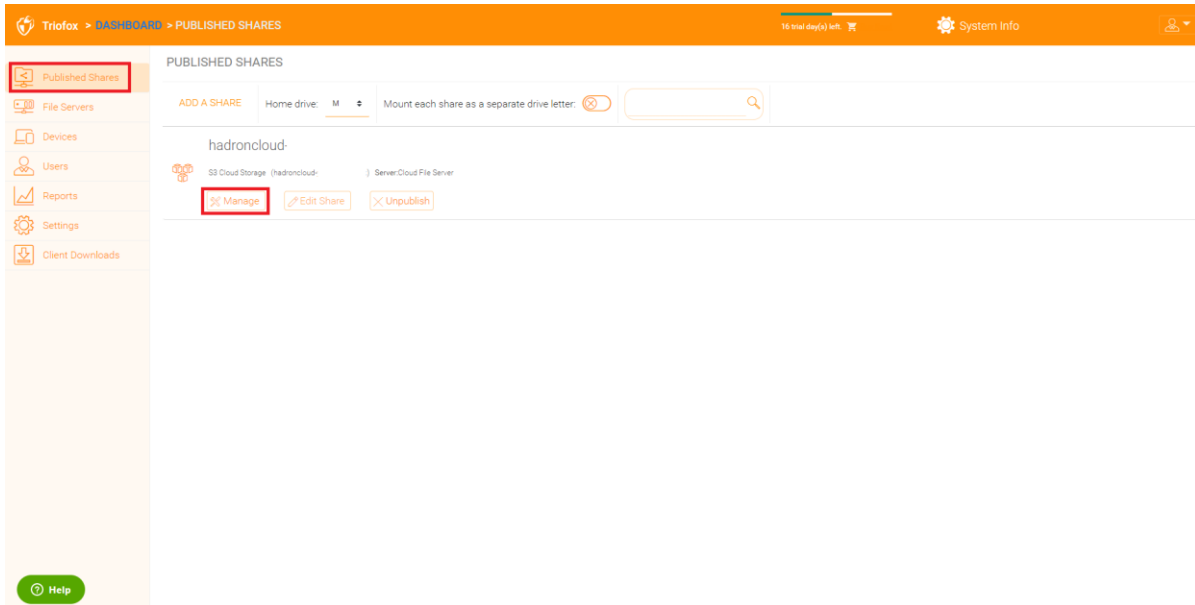
As a Cluster Administrator, you can also see the total number of normal users in the system, the total number of guest users, the number of groups, assigned licenses, devices, and created roles.

Statistics

Normal Users	2	>	Assigned License	Trial	>
Guest Users	0	>	Devices	0	>
Groups	0	>	Roles	0	>

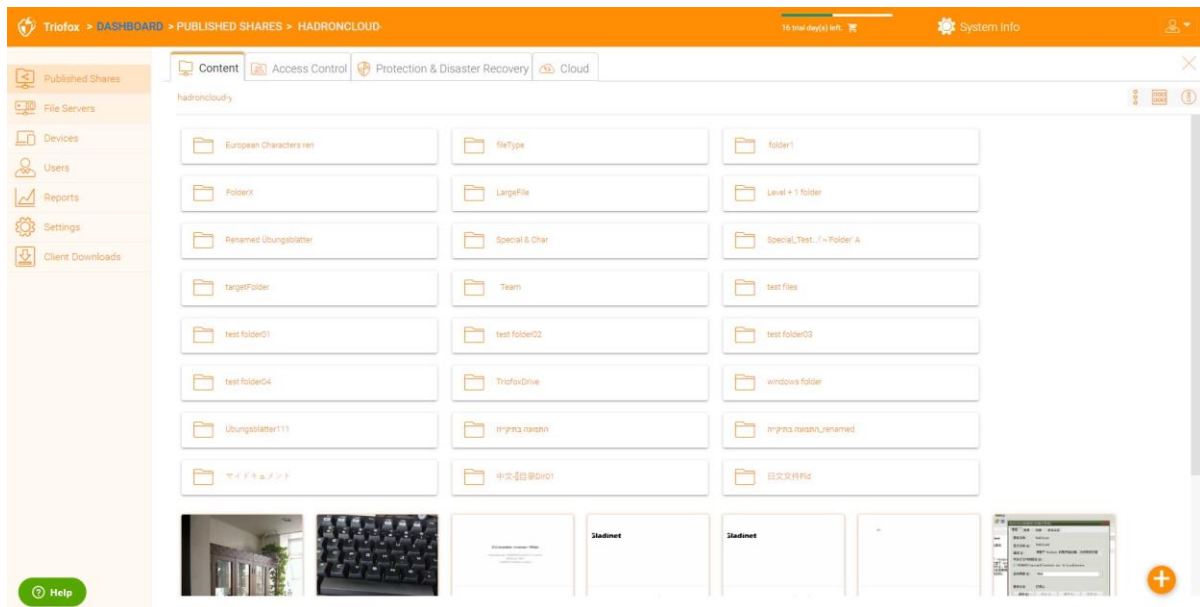
Published Shares

In this section you can browse your published shares. Click **Manage** to view details of published shares.



Content

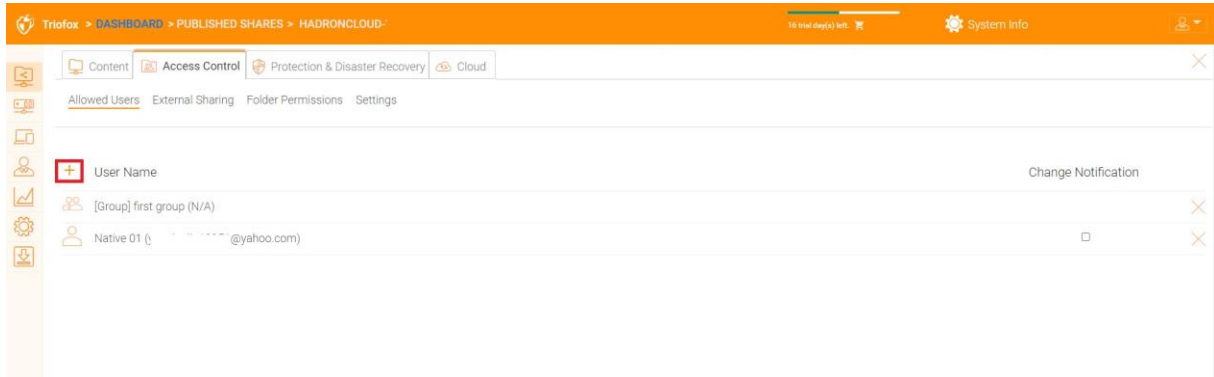
Here you can find files and folders within the published shares.



Access Control

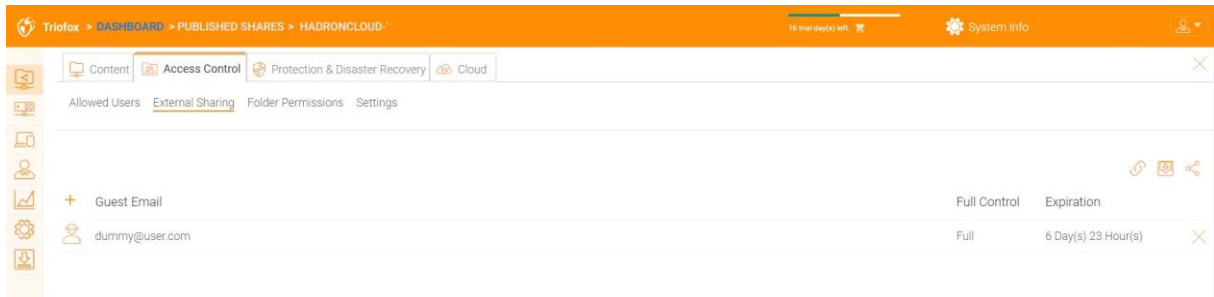
Allowed Users

You can add users and groups in the Allowed Users section.



External Sharing

With this setting you can see which folders and files have been shared and control access to them.



Folder Permission

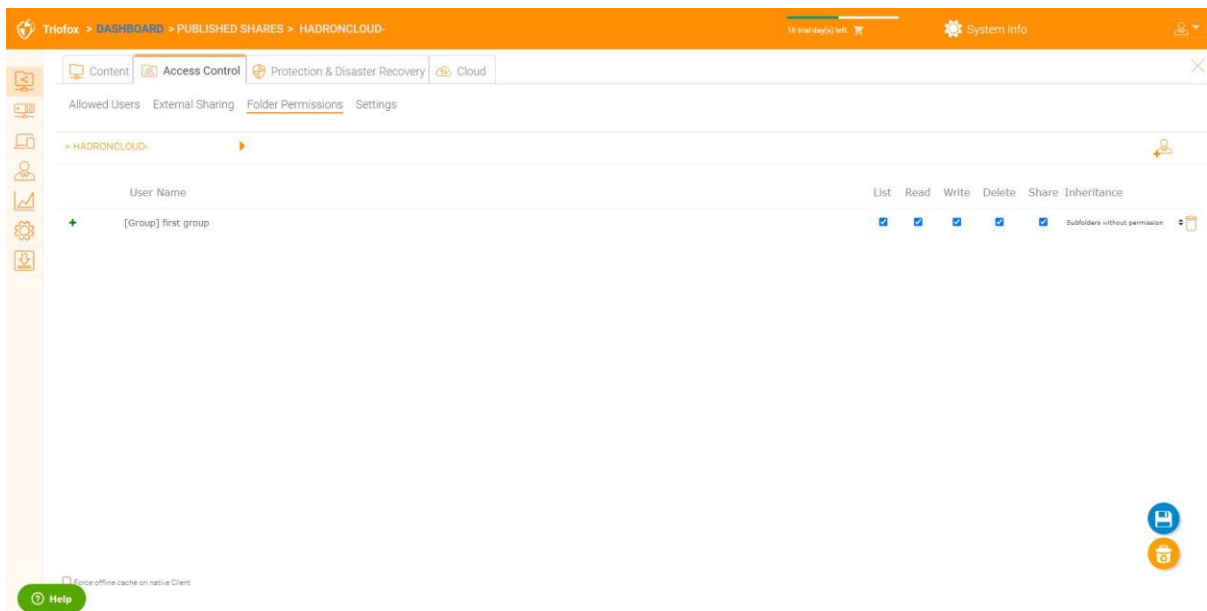
You can browse to different subfolders and set the folder permission. The folder permissions defined here represent the Cluster Server side of the permission.

If you are using the native Active Directory/NTFS permission of a file server, you do not need to define permissions here.

Note

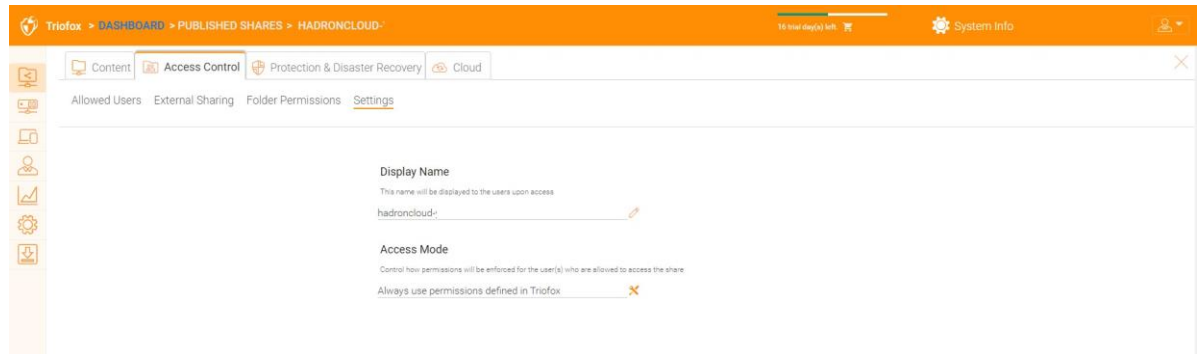
You can think of the permissions as two different gates that control access to files and folders. The first gate is defined here as "Cluster Server Folder Permission". After this permission check, there is another check at the file server level (the NTFS permission).

In practice, this is usually done one way or another. If you have chosen to use NTFS natively, you can leave the permission settings here blank and undefined.

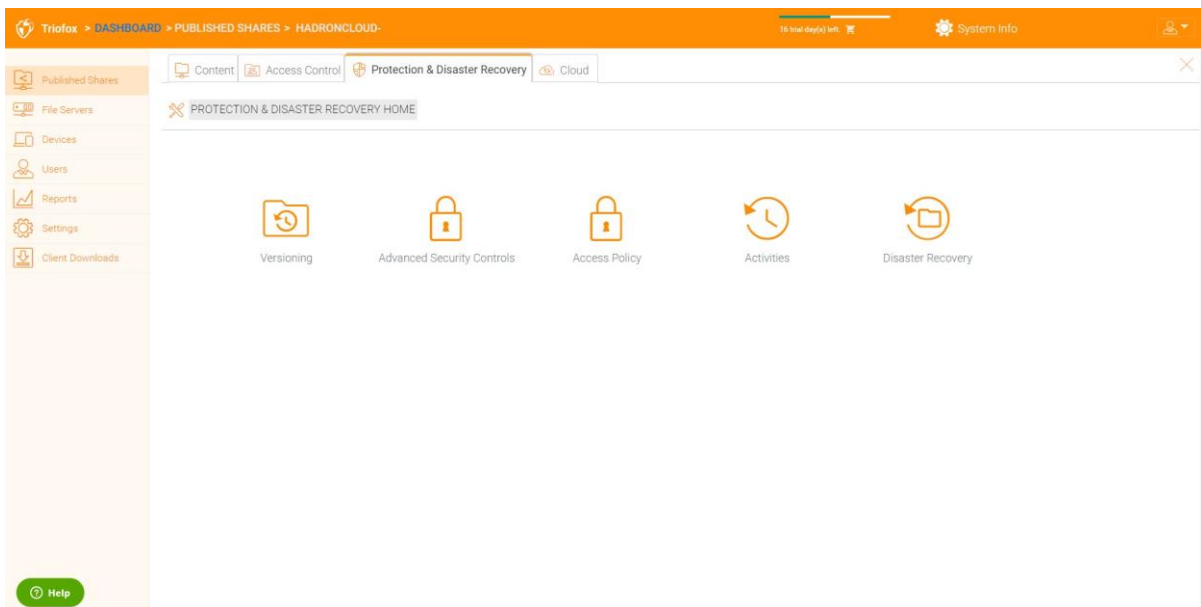


Settings

Here you can change the settings for your published shares.

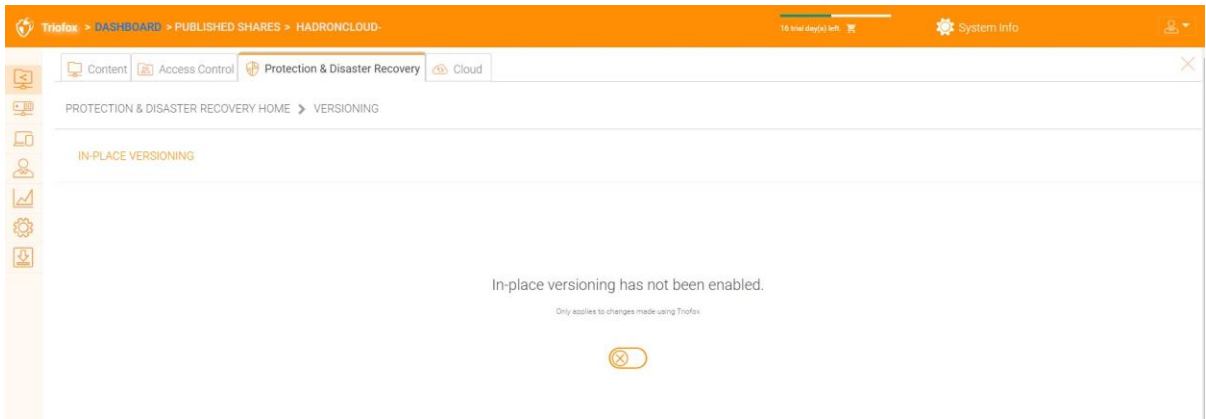


Protection & Disaster Recovery



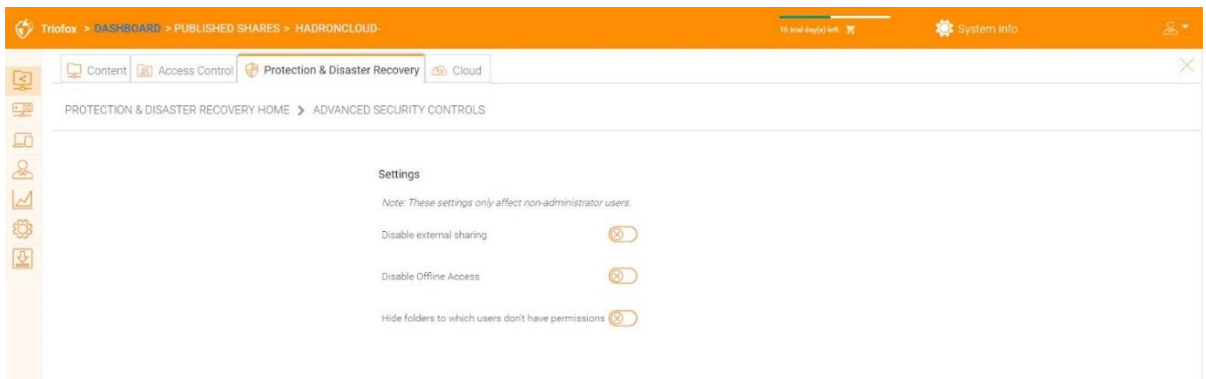
Versioning

In-place versioning can be enabled here.



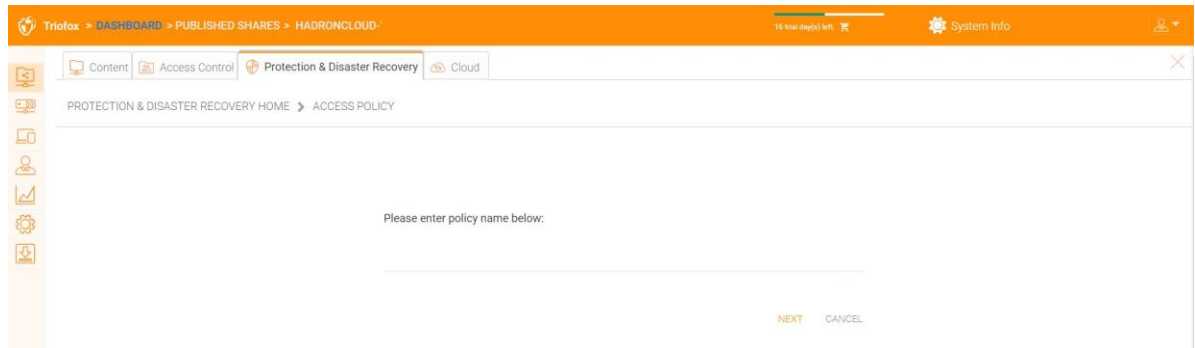
Advanced Security Controls

Here you can find some settings for advanced security controls. You can disable external sharing, disable offline access, or hide folders for which users do not have permission.



Access Policy

On this tab you can enable an access policy.



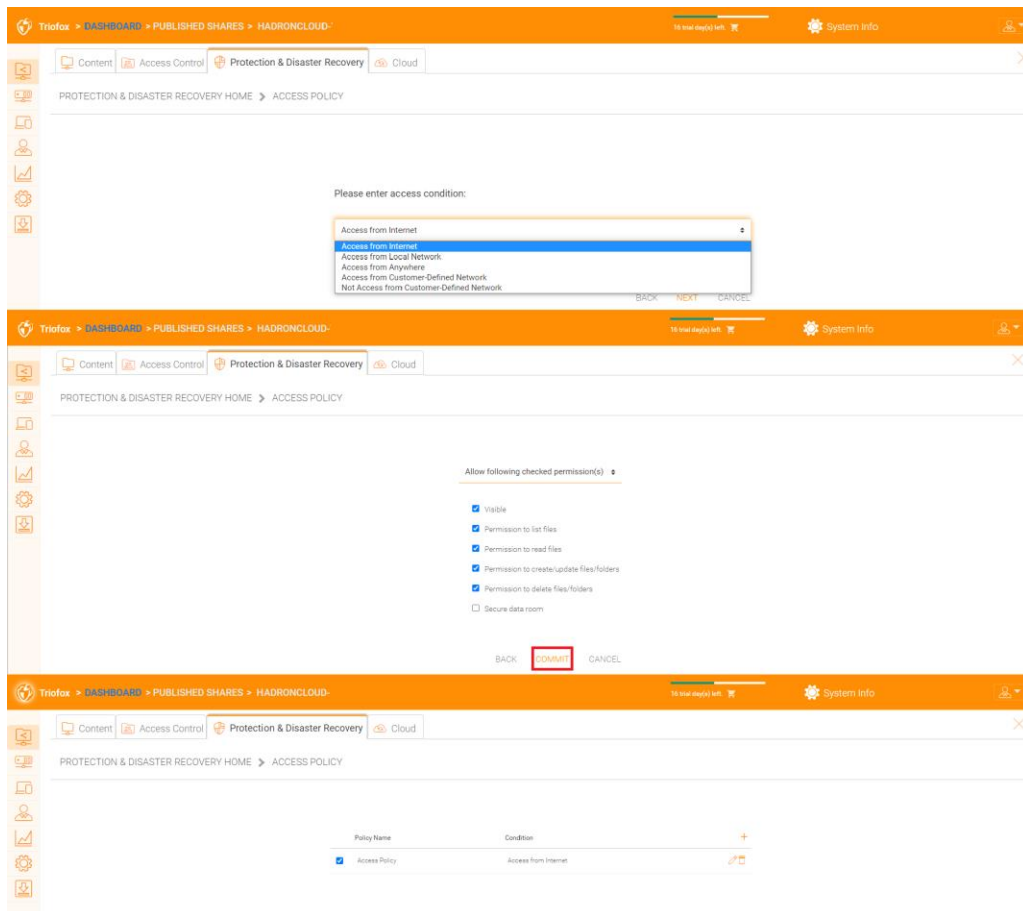
Client Access Policies:

Define custom access policies to restrict or allow access based on the location of the device. For example, a company may want to allow access from the Internet only for Windows clients and Web clients. IT can configure policies to allow or deny client access from the following locations:

- Access from the Internet
- Access from Local network
- Access from Anywhere
- Access from Customer-Defined Network
- Deny access from Customer-Defined network

The above policies for allowing and denying client access can be configured for the following clients:

web client, web management, windows client, mac client, mobile client.



Share Access Policy:

IT can also prevent data loss and data leakage of important company confidential shares by configuring “Share Access Policies” for external users who are not employees of the company. Again, IT can configure access policies to approve or deny shares from the following locations:

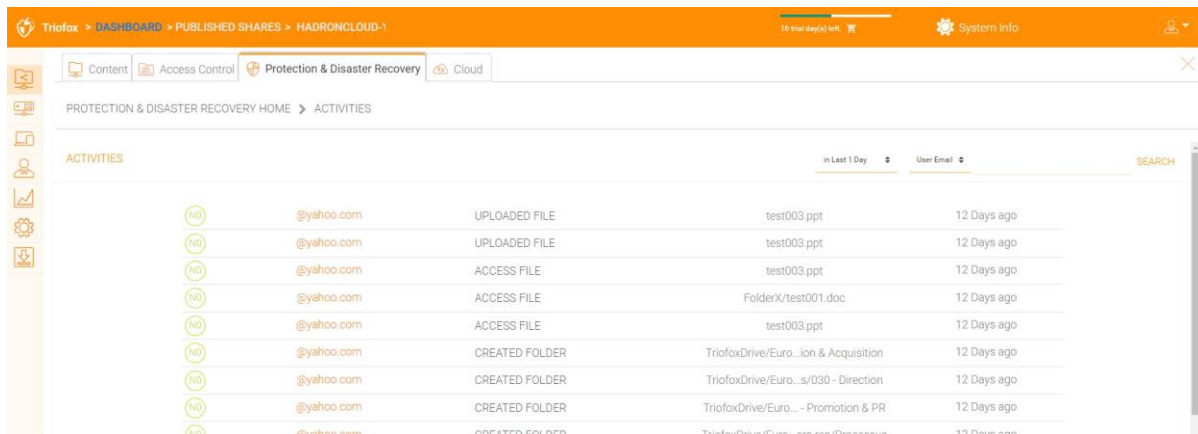
- Access from the Internet
- Access from Local network
- Access from Anywhere
- Access from Customer-Defined Network
- Deny access from Customer-Defined network

The above allow and deny share access policies can be configured with the following conditions:

- Visible
- Permissions to list files
- Permissions to read files
- Permissions to create or update files and folders
- Permissions to delete files and folders
- Secure data room.

Activities:

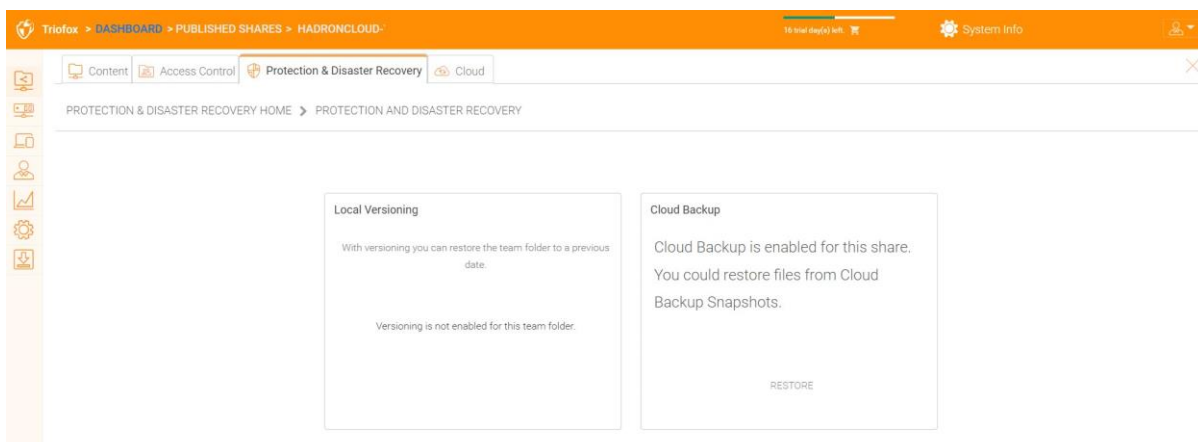
Here you can see activities for shares.



Activity	User	Action	File/Folder Name	Time
UPLOADED FILE	@yahoo.com	test003.ppt	12 Days ago	
UPLOADED FILE	@yahoo.com	test003.ppt	12 Days ago	
ACCESS FILE	@yahoo.com	test003.ppt	12 Days ago	
ACCESS FILE	@yahoo.com	FolderX/test001.doc	12 Days ago	
ACCESS FILE	@yahoo.com	test003.ppt	12 Days ago	
CREATED FOLDER	@yahoo.com	TriofoxDrive/Euro...ion & Acquisition	12 Days ago	
CREATED FOLDER	@yahoo.com	TriofoxDrive/Euro...s/030 - Direction	12 Days ago	
CREATED FOLDER	@yahoo.com	TriofoxDrive/Euro... - Promotion & PR	12 Days ago	
PDFATTN FOR DFP	@yahoo.com	TriofoxDrive/Euro...ere ran/Dronep...	12 Days ago	

Disaster Recovery:

You can restore the team folder to a previous date by "Local Versioning", or restore files from a "Cloud Backup".



Local Versioning

With versioning you can restore the team folder to a previous date.

Versioning is not enabled for this team folder.

Cloud Backup

Cloud Backup is enabled for this share. You could restore files from Cloud Backup Snapshots.

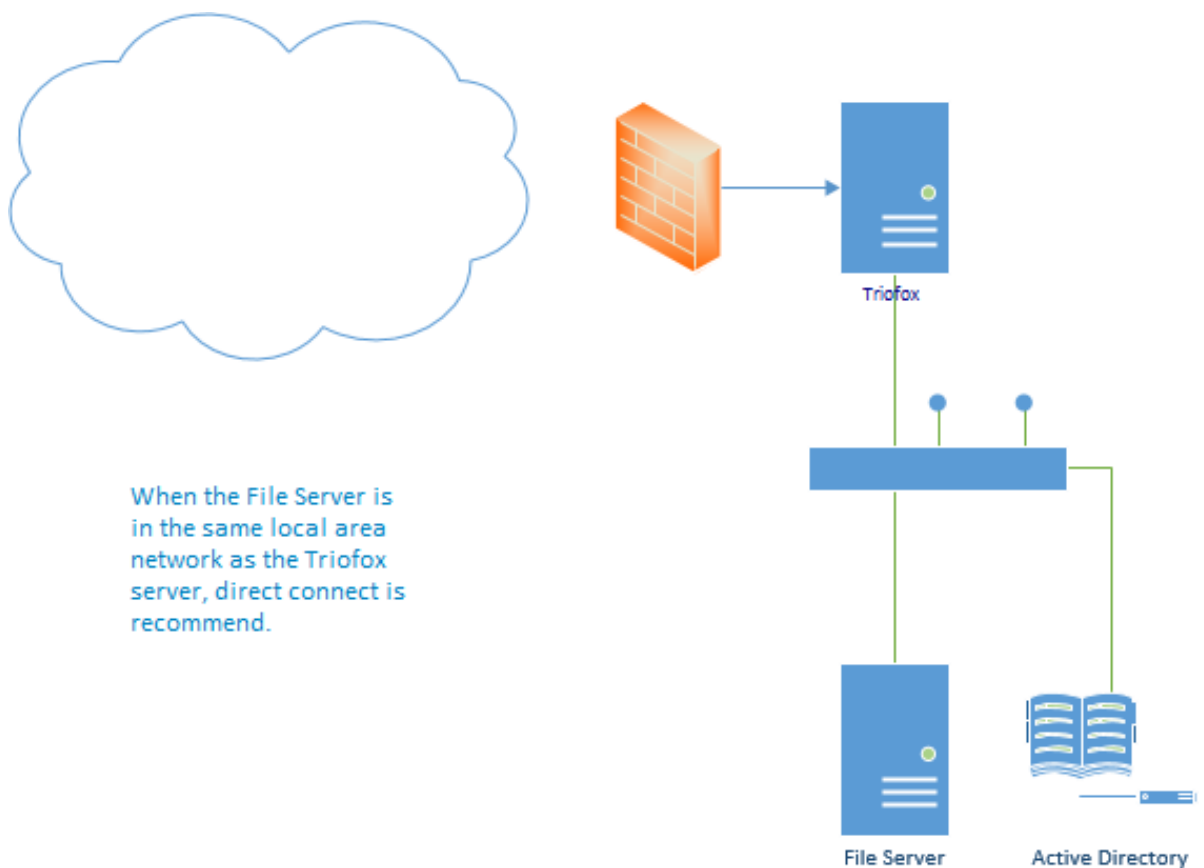
RESTORE

File Servers

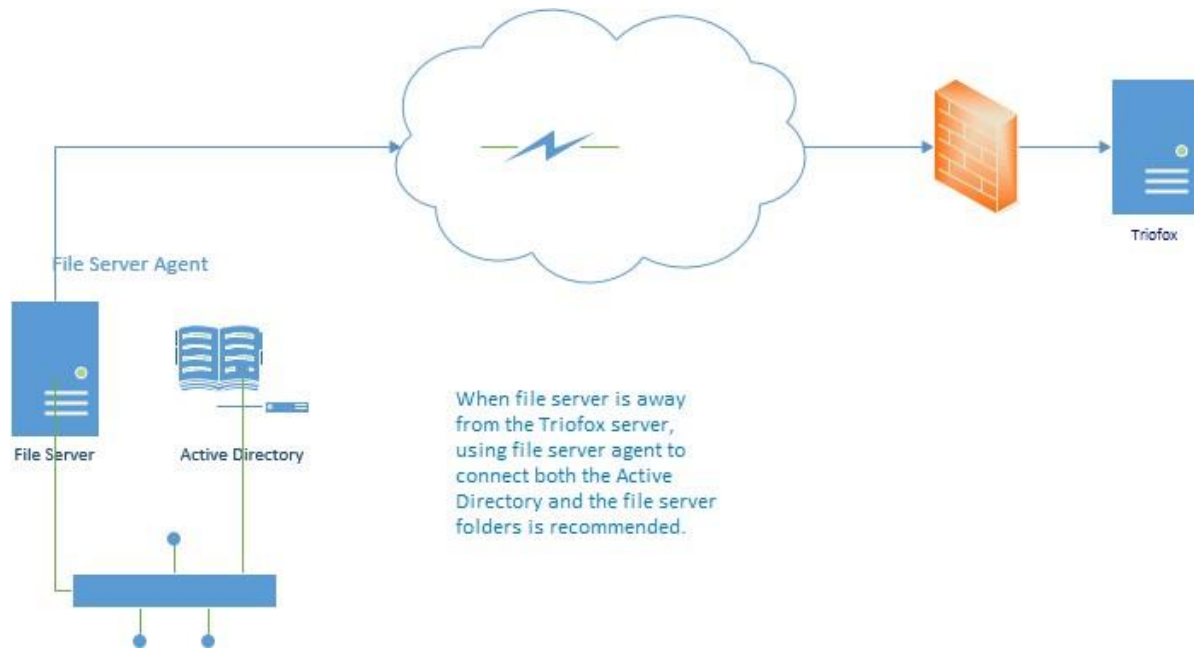
Connect Your File Server

Depending on where your file server is located, there are several ways to connect it.

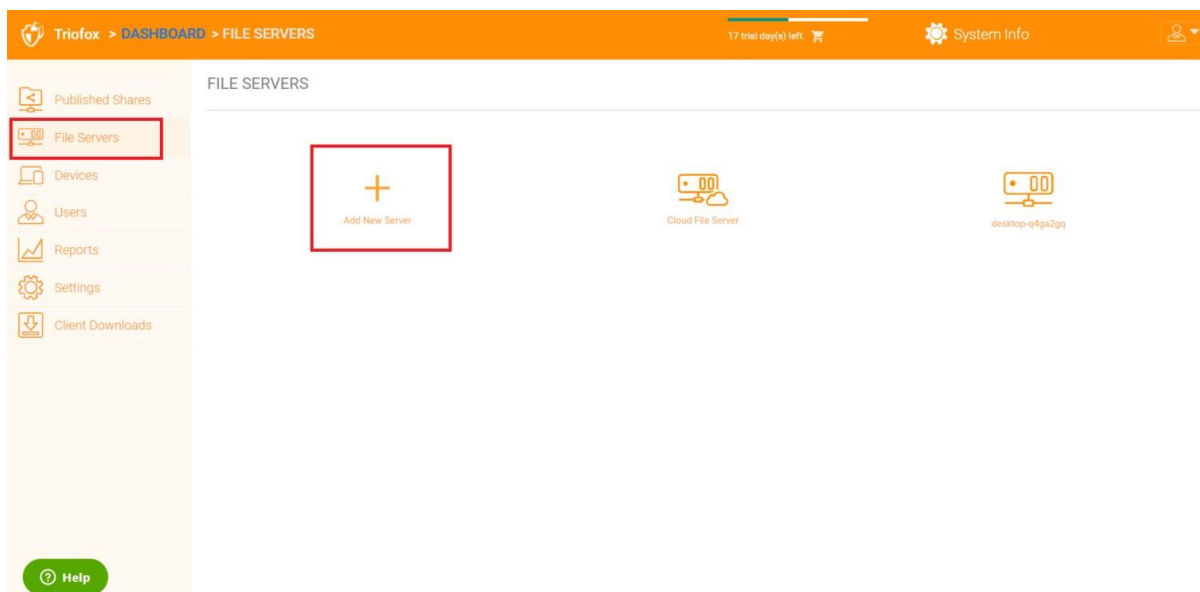
The file server may be on the same local area network (LAN) as the Triofox server. In this case, the direct network share connection is the best. This is usually combined with setting up a direct LDAP connection to Active Directory.



The file server can also be remote, away from the Triofox server and at the customer's premise. In this case, it is recommended to use a file server agent. The file server agent is installed on the file server and is able to connect to the customer's Active Directory and synchronize both folder contents and Active Directory over HTTPS. In this case, the user interface displays "Proxied AD User" to indicate that the Active Directory user or group originated from the file server agent.



The best way to start using a file server agent is to add a file server via the web portal.



Devices

The cluster administrator can look at the devices that have the client agent software installed and connected in the specific user.

The screenshot shows the Triofox Dashboard > DEVICE MANAGER interface. The left sidebar contains navigation options: Published Shares, File Servers, Devices (highlighted with a red box), Users, Reports, Settings, and Client Downloads. The main content area displays a list of 3 devices found. Each device card shows the following information:

Device Name	Login Email	Type	OS Version	Client Version	Last Login Time	Sync Status	Status Report Time	Actions
s-MacBook-Pro.local	@yahoo.com	Mac Client	MacOS 11.0.0	64bit13.4.311.3028	2022-05-11 16:07:08Z	?	2022-05-19 15:53:42Z	MANAGE WIPE DELETE
MacBook Pro	@yahoo.com	iPad	iPadOS 15.2	2022.4.13	2022-05-24 14:35:44Z	?		MANAGE WIPE DELETE
DESKTOP-7IE03RC	@yahoo.com	Windows Client	Windows 10 64bit	13.4.9785.53973	2022-05-22 21:01:04Z	✓	2022-05-24 14:35:06Z	MANAGE WIPE DELETE

Here you can find the settings for the device management.

The screenshot shows the Triofox Dashboard > DEVICE MANAGER Settings page. The settings are as follows:

- Require approval for device access:** When a user attempts to log in from a new device via native client applications, the connection will be rejected until the cluster admin approves the new device.
- Require approval for device access from external network:** When a user attempts to log in from a new device via native client applications, the connection will be rejected until the cluster admin approves the new device.
- Enable auto-installation of the Outlook Plugin:**
- Create shortcut in documents library:** When enabled, the windows client will create a shortcut to the mapped drive in the documents library.
- Create shortcut on Desktop:** When enabled, the windows client will create a shortcut to the mapped drive in the documents library.

CLOSE

Requiring approval for device access

Disabled by default. When a user attempts to log in from a new device via native client applications, the connection will be rejected until the cluster admin approves the new device. Approval can be done via the "Client Device Manager".

Enable auto-install of Outlook Plugin

Disabled by default. The Cluster Server Windows desktop client comes with an Outlook plug-in. If this option is enabled, the Outlook plugin will be enabled upon client startup.

Create a shortcut in the documents library

Enabled by default. This is a convenient feature to add a link to documents library to the cloud drive.

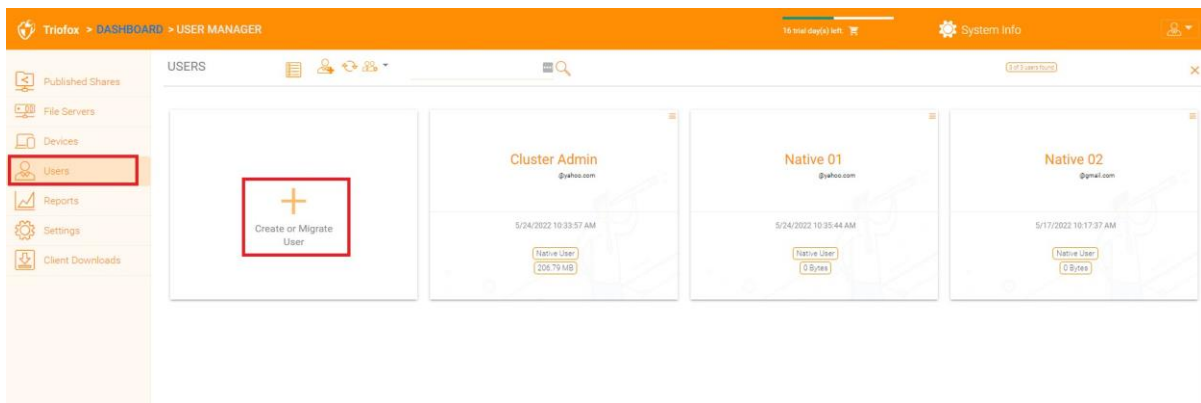
Create shortcut on desktop

Enabled by default. Same as above but the shortcut is on the desktop.

Users

Normal User

Normal users can be added here:



If you have Active Directory, these are normally the users in Active Directory.

Native User

- These are the users that are manually created with an email.

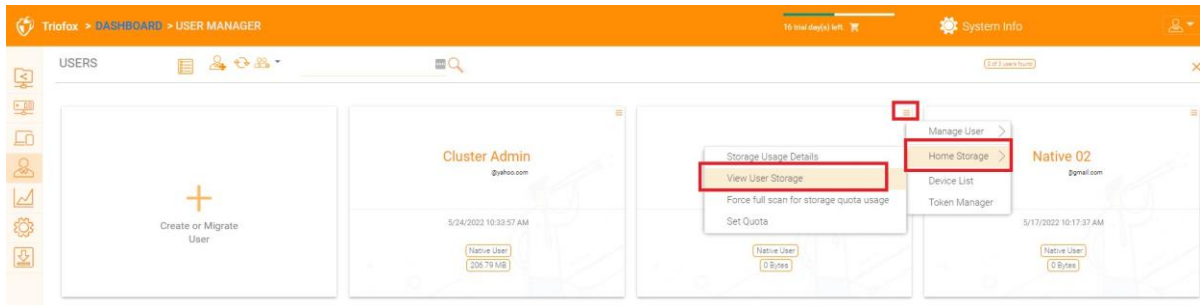
AD User

- These are the users that are imported from Active Directory via LDAP.

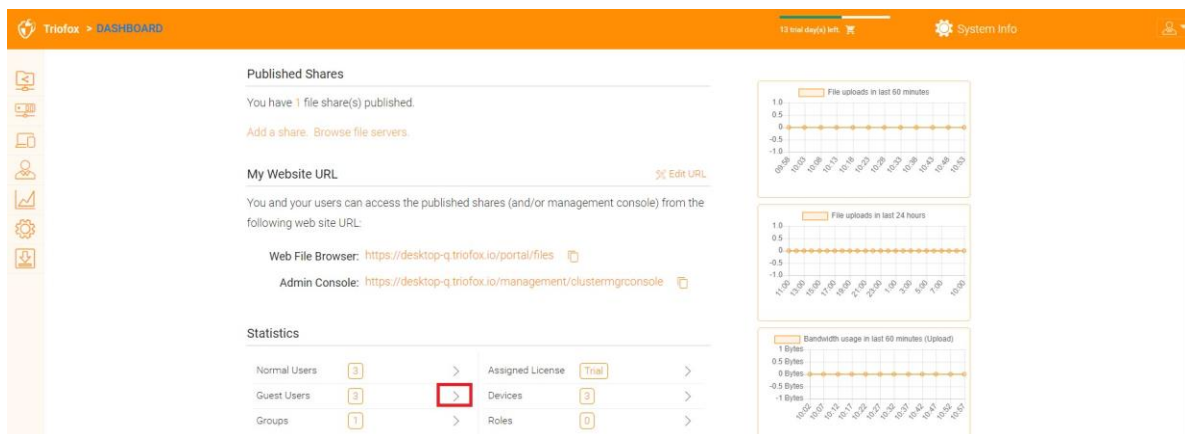
Proxied AD User

- These are the users that are imported from Server Agent, where the file server agent is remote and away from the Cluster Server at the customer's site. The customer's Active Directory domain is also remote, and the file server itself (where server agent is installed) is in the remote Active Directory.

An admin can view a user's file and folder list.



Guest Users



Guest users are users who do not have a home directory. The only folder they have is "Files Shared with Me". So, they rely on other "Normal User" to share files and folders with them before they can do anything. If no one shares anything with a guest user, the guest user will not have any read/write permissions to any folder.

The main reason for the existence of guest users is to provide a secure way for external users to collaborate and edit documents.

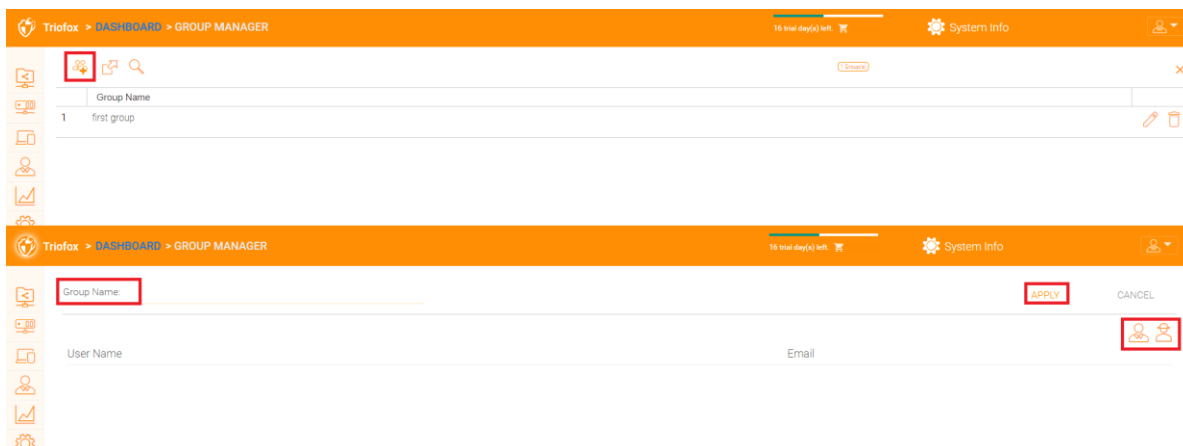
Group Manager

If you have Active Directory integration, you will use the Active Directory group instead of using Group Manager here. This group manager allows you to easily create a group of users. It's not as complicated as Active Directory (such as supporting nested groups), but it makes it easy for non-Active Directory users. This is native Cluster group. In the product, you can also see the AD group in the user selection interface and the Proxied AD group in the user-related interface. The AD group and the Proxied AD group are not the same as the group mentioned here.

You can add new groups by clicking the Groups tab.

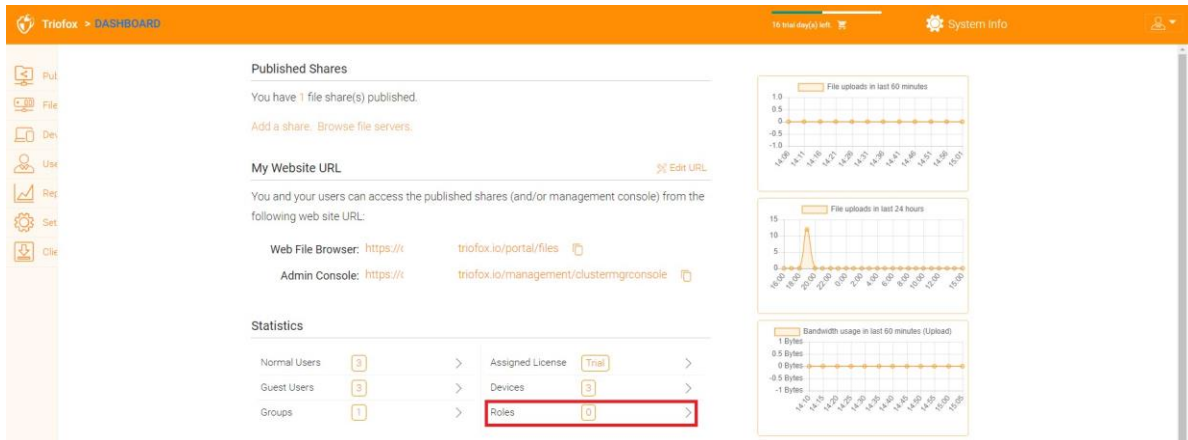
Statistics			
Normal Users	2	>	Assigned License
Guest Users	0	>	Devices
Groups	0	>	Roles

Click "Create New Group" icon at the top to create a new group, then set the "Group Name", click the icons at the top right to add users, and then click "Apply" to finish.



Role Manager

The Role Manager is used for role-based management. For example, you can assign read-only permissions to some users. You can also set specific group policies for certain groups of users. More and more policy elements are added to the Role Manager, so that the Role Manager can be used not only to manage user roles, but also to define policy elements for users.

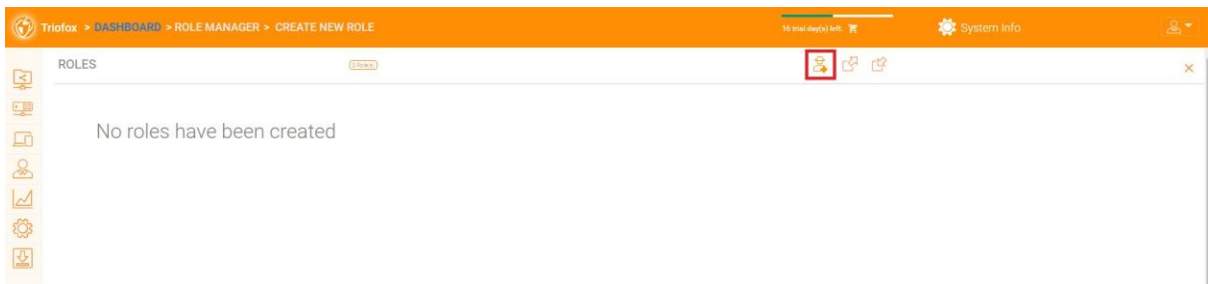


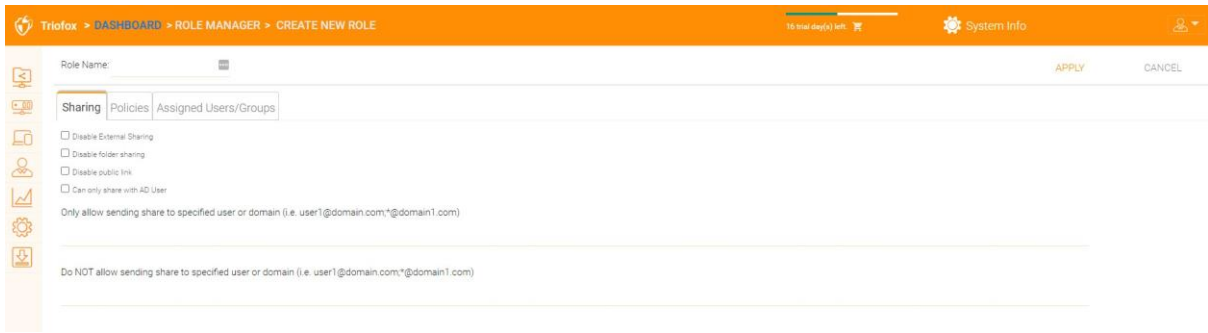
There are 3 different sections when creating a roll:

- Sharing
- Policies
- Assigned Users/Groups

Create New Role

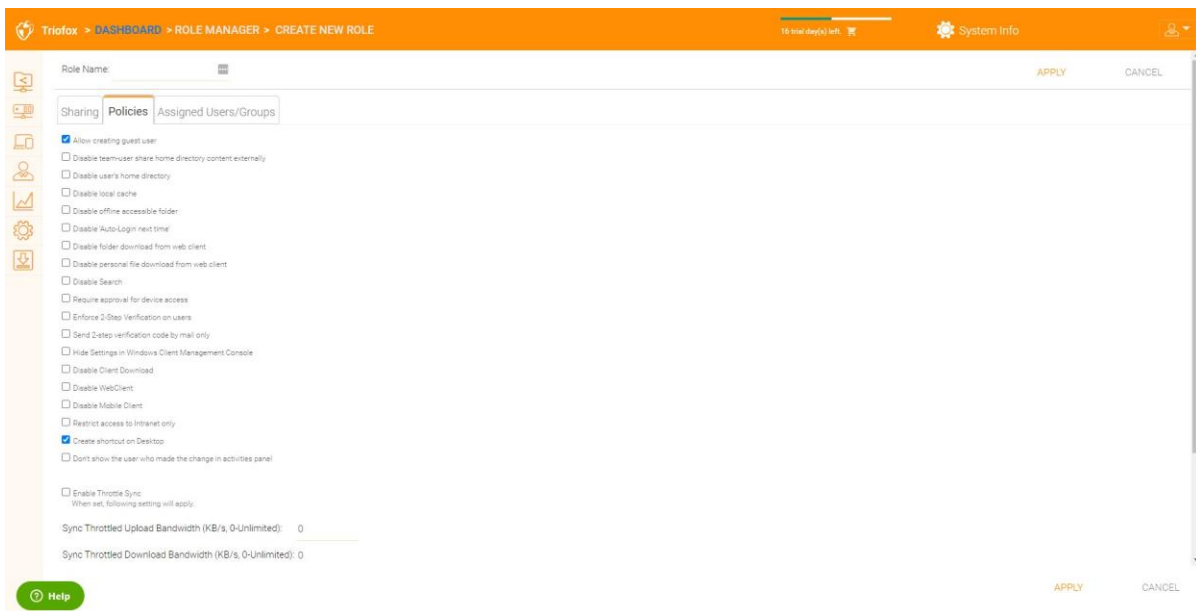
You can define areas in the Role Manager and assign them to a role.





Policies

Additional policies for the role.



Assigned Users/Groups

After the content of the role is all set, users and groups can be assigned to a role.



Reports

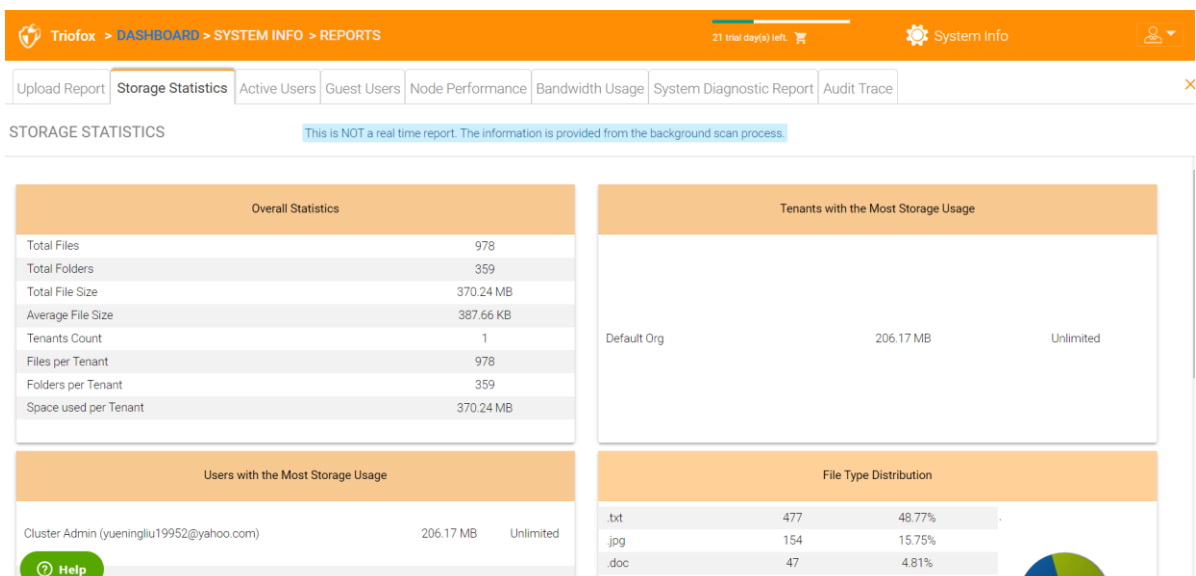
Upload Report

The Upload Report tab shows you graphs for all uploads that have occurred in the last sixty minutes, 24 hours, 30 days, and a full week.



Storage Statistics

Storage Statistics gives you a quick overview of the overall storage statistics, the file type distribution pie charts, and the users who have used the most storage so far.



Active Users

Active Users show the activity of users on the web portal. The Active Users report does not include users from the Windows client or other native clients, as these users are more persistent (always there). To access this report, click the Active Users section in the panel near the top of the screen.

The screenshot shows the Triofox dashboard navigation bar with the path: Triofox > DASHBOARD > SYSTEM INFO > REPORTS. The 'Active Users' report is selected in the top menu. Below the menu, a status bar indicates '0 users(s) found'. A table with the following columns is visible: Name, Email, Last Access, Session Create, and Worker Node.

Guest Users

Other reports are also available, such as Guest Users, which are users who do not have their own directory but are invited to participate in some shared folders and files.

Node Performance

You can use the Node Performance to check out the worker node health and the database health.

The screenshot shows the Triofox dashboard with the path: Triofox > DASHBOARD > SYSTEM INFO > REPORTS. The 'Node Performance' report is selected. It displays two main sections: 'Database' and 'desktop-q4ga2gq'.

Database Section:

- Total Configuration Records: 219
- Total File Change Records: 3.58 K
- Total File Index Records: 978
- Total Audit Trace Records: 73

desktop-q4ga2gq Section:

- Last Reported: 2 seconds ago
- Total Requests Processed: 273
- Request Executing: 0
- Last Request Time: 414
- Pending Change Notifications: 0
- Active Node Request: 0
- Pending Changes Polling: 0
- Active Clients: 0
- Pending Dir Request (+): 0
- Pending Dir Request (L): 0

A 'PURGE' button is visible in the Database section, and a 'Help' button is at the bottom left.

Last Reported

You should see that this field contains small numbers like 6 seconds or 10 seconds. If you see a number like "3 hours ago", it means that the node is not reporting the health.

Total Requests Processed

This number should be as large as possible. This number is a cumulative number since the last restart of the service. The larger the number, the more stable the service is. If you have multiple worker nodes, you should see the total number of requests evenly distributed among the worker nodes.

Request Executing

You want to keep this number as small as possible. This refers to the number of requests that are concurrently executing on the server. In general, a number less than 100 is normal. Greater than 100 is abnormal. Anything greater than 20 needs to be investigated.

Last Request Time

You should keep this number as small as possible. It is the number of milliseconds for the last request. In general, numbers smaller than 3000 or 5000 are normal, i.e. less than 3-5 seconds.

Pending Change Notification

For files and folders that are changed, a change notification is written to the database. In general, the queue for pending changes should be kept as short as possible.

Active Node Request

These are the clients that contact the server. Normally they are for reporting purposes only.

Pending Change Polling

These are the clients out there polling to see whether there are files and folders that have been changed. As a rule, the smaller the better.

Active Clients

For reporting purpose.

Pending Dir Request(H)

The pending directory listing calls from the remote clients to the Cluster Server. This is the high priority queue.

Pending Dir Request(L)

The pending directory listing calls from the remote clients to the Cluster Server. This is the low priority queue.

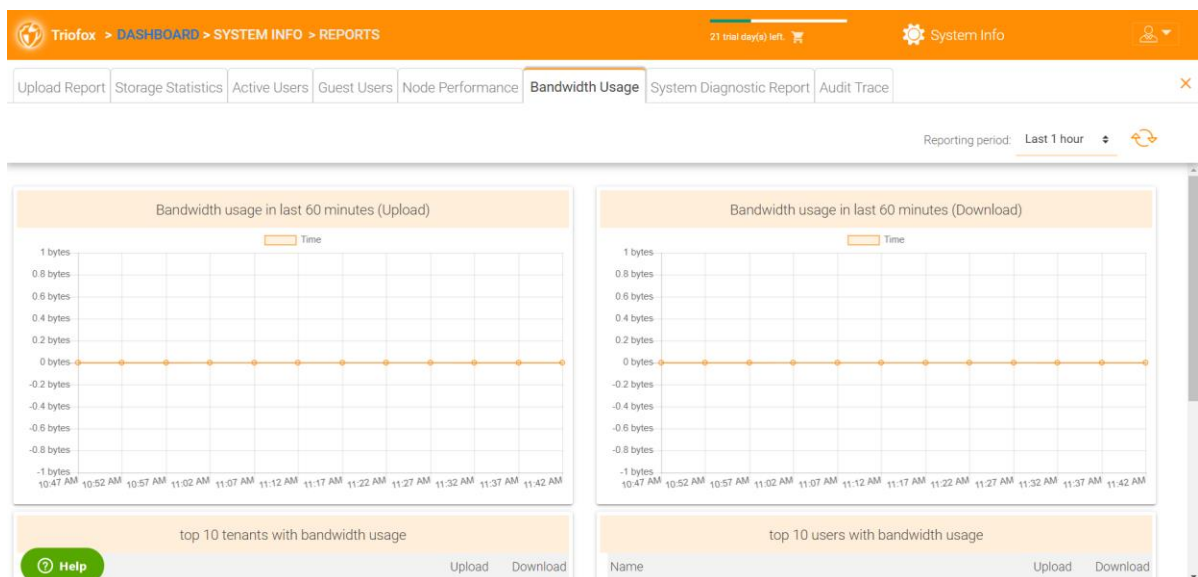
Note

If you do not see the Node Performance report, check the **Internal URL** setting of each worker node.

Under Reports, you can view the upload graphs and storage statistics.

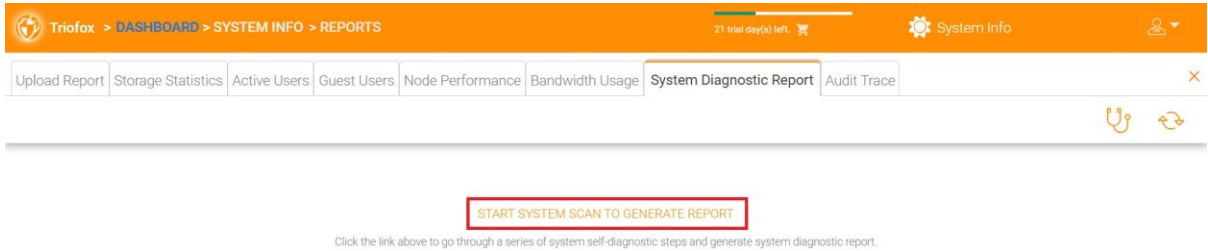
Bandwidth Usage

This shows the overall bandwidth usage statistics as well as more granular tenant and user level statistics.



System Diagnostic Report

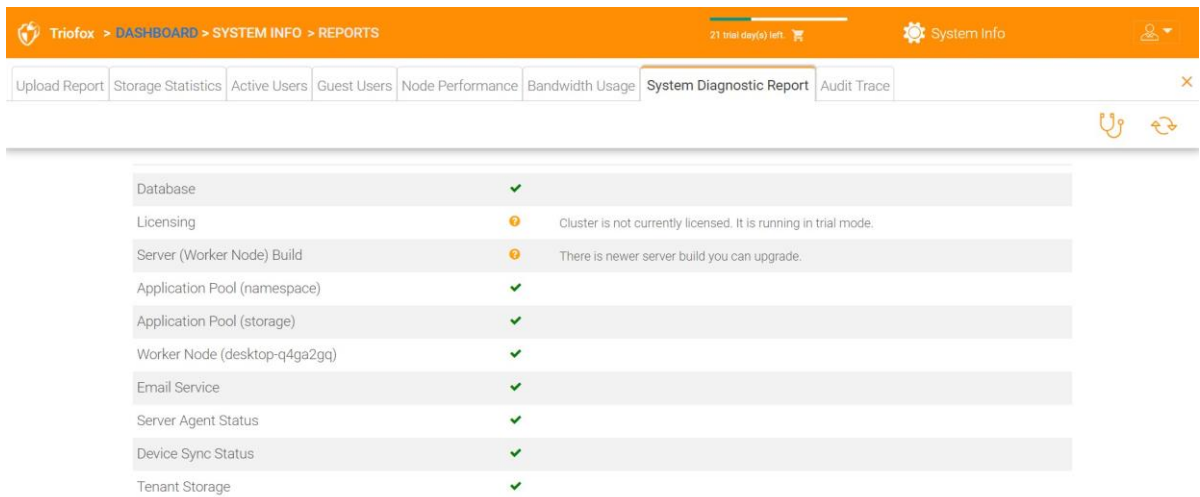
Click the "Start System Scan To Generate Report" button to generate system diagnostic report.



The screenshot shows the Triofox dashboard navigation bar with the path: Triofox > DASHBOARD > SYSTEM INFO > REPORTS. The 'System Diagnostic Report' tab is active. Below the navigation bar, a red box highlights the button labeled 'START SYSTEM SCAN TO GENERATE REPORT'. Below this button, a text instruction reads: 'Click the link above to go through a series of system self-diagnostic steps and generate system diagnostic report.'

[Help](#)

An example of a system diagnostic report is shown below.



The screenshot shows the Triofox dashboard navigation bar with the path: Triofox > DASHBOARD > SYSTEM INFO > REPORTS. The 'System Diagnostic Report' tab is active. Below the navigation bar, the report content is displayed as follows:

Database	✓	
Licensing	⚠	Cluster is not currently licensed. It is running in trial mode.
Server (Worker Node) Build	⚠	There is newer server build you can upgrade.
Application Pool (namespace)	✓	
Application Pool (storage)	✓	
Worker Node (desktop-q4ga2gq)	✓	
Email Service	✓	
Server Agent Status	✓	
Device Sync Status	✓	
Tenant Storage	✓	

[Help](#)

Audit Trace

This is an example of an audit trace.

	Action	Trace	Time	Server Time	User Email	Full Name
1	Login_Success	,50.221.11.194,	2022-05-19 14:04:14Z	5/19/2022 10:04:14 ...	@ya...	Cluster Admin
2	used_4521	388226623	2022-05-19 13:44:44Z	5/19/2022 9:44:44 AM	cloudmon	cloudmon
3	used_4521	388226623	2022-05-19 13:44:44Z	5/19/2022 9:44:44 AM	cloudmon	cloudmon
4	used_4521	0	2022-05-19 13:44:00Z	5/19/2022 9:44:00 AM	cloudmon	cloudmon
5	used_4521	0	2022-05-19 13:43:59Z	5/19/2022 9:43:59 AM	cloudmon	cloudmon
6	Login_Success	,50.221.11.194,	2022-05-18 14:25:44Z	5/18/2022 10:25:44 ...	@ya...	Cluster Admin
7	Add_Group	first group	2022-05-18 14:03:33Z	5/18/2022 10:03:33 ...	@ya...	Cluster Admin
8	Login_Success	,50.221.11.194,	2022-05-18 13:19:56Z	5/18/2022 9:19:56 AM	@ya...	Cluster Admin
9	used_4520	388226623	2022-05-18 13:11:11Z	5/18/2022 9:11:11 AM	cloudmon	cloudmon

Settings

In the Settings, the administrator can enable/disable some features, such as Active Directory, 2-Step Verification (MFA), Single Sign-On, Ransomware Protection. And there are also many other options that can be configured.

Setting Name	Toggle	Expandable
Active Directory	<input type="checkbox"/>	>
2-Step Verification (MFA)	<input type="checkbox"/>	>
Single Sign on (SAML Integration)	<input type="checkbox"/>	>
Ransomware Protection	<input type="checkbox"/>	>
File Locking	>	>
Data Leak Protection	>	>
Notifications	>	>
Personal Home Drive	>	>
Sharepoint Online Integration	>	>
Clients & Applications	>	>
User Account & Security	>	>
Folder & Storage	>	>

Active Directory

If the Active Directory is in the local area network (LAN), LDAP can be used to connect to the Active Directory. There are several cases here,

- Sometimes you want the user account to be automatically provisioned so that it is easy for the administrator.
- Sometimes you want the user account to be limited to a specific AD group, but still automatically provision the user's account when the users are in the AD group.
- Sometimes you want the user account to be limited to a specific Organization Unit.

AD account auto provision

This option can be found in Settings - > Active Directory.

The image shows two screenshots of the Triofox web interface. The top screenshot displays the 'SETTINGS' page with a grid of configuration options. The 'Active Directory' option is highlighted with a red box. The bottom screenshot shows the 'ENABLE ACTIVE DIRECTORY INTEGRATION' page, which prompts the user to enter LDAP information. The 'APPLY' button is highlighted with a red box.

Settings Page:

- Active Directory (highlighted)
- 2-Step Verification (MFA)
- Single Sign on (SAML Integration)
- Ransomware Protection
- File Locking
- Data Leak Protection
- Notifications
- Personal Home Drive
- Sharepoint Online Integration
- Clients & Applications
- User Account & Security
- Folder & Storage

Enable Active Directory Integration Page:

Please enter your AD (LDAP) information below:

Domain Controller or LDAP Server Address (myhost.389) [Required]

User name (used to connect to your Active Directory Service) [Required]

Password [Required]

APPLY CANCEL

As long as the “Don't allow user auto-creation” is unchecked, Active Directory users will be allowed to go to the web portal and log in. The first time the user logs in, the Triofox account will be automatically provisioned.

The screenshot shows the 'ADD USER' page in the Triofox User Manager interface. The 'Advanced Settings' tab is active. The 'Don't allow user auto-creation' checkbox is highlighted with a red box. The page includes a sidebar with navigation icons and a top navigation bar with the path 'Triofox > DASHBOARD > USER MANAGER > ADD USER'.

APPLY AD Server Advanced Settings

Friendly Domain Name (i.e. mydomain.com, the domain name you see in Active Directory tools)

Enable LDAPS for secure access

Only include users and groups from the following Organizational Units (e.g. OU+ou1,OU+ou2. Leave this blank to include all OUs)

Allow Switching to Global Catalog if needed

Disable Nested Groups (Enabling it may slow down your access to cloud)

This is the root of the AD Forest and contains multiple sub-domains

Discover domain controller IP at runtime

Don't allow user auto-creation

Publish user's home drive

When unchecked, the user home drive space will be allocated from enterprise storage. When checked, existing user home drives will be automatically published from Active Directory.

Help

AD account auto provision, limiting to Organization Unit

The organization unit field can be used to further restrict the Active Directory user account to be provisioned automatically.

The screenshot shows the 'ADD USER' page in the Triofox User Manager interface. The 'Advanced Settings' tab is active. The 'Only include users and groups from the following Organizational Units' field is highlighted with a red box. The page includes a sidebar with navigation icons and a top navigation bar with the path 'Triofox > DASHBOARD > USER MANAGER > ADD USER'.

APPLY AD Server Advanced Settings

Friendly Domain Name (i.e. mydomain.com, the domain name you see in Active Directory tools)

Enable LDAPS for secure access

Only include users and groups from the following Organizational Units (e.g. OU+ou1,OU+ou2. Leave this blank to include all OUs)

Allow Switching to Global Catalog if needed

Disable Nested Groups (Enabling it may slow down your access to cloud)

This is the root of the AD Forest and contains multiple sub-domains

Discover domain controller IP at runtime

Don't allow user auto-creation

Publish user's home drive

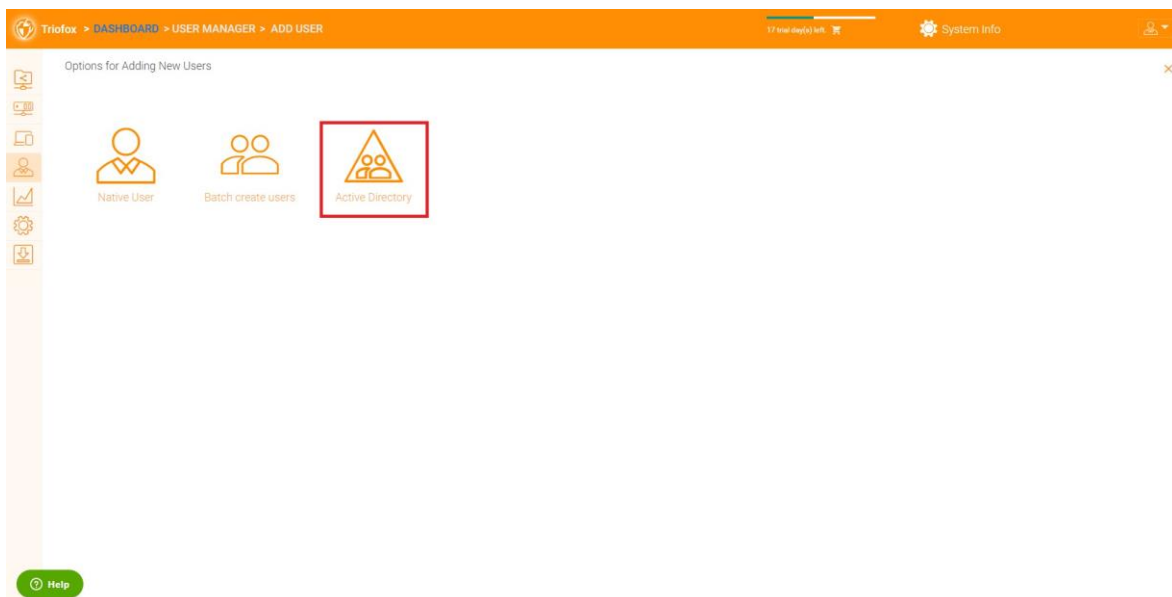
When unchecked, the user home drive space will be allocated from enterprise storage. When checked, existing user home drives will be automatically published from Active Directory.

The format of the organization unit is the OU's distinguishedName minus the DC suffix. For example, the following OU's property is:

```
distinguishedName => DC=tsys,DC=gladinet,DC=com
```

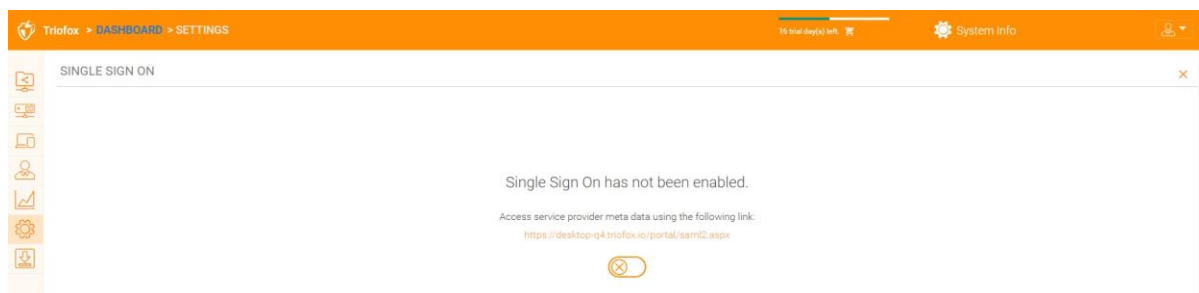
AD account auto provision, limiting to a specific AD group

From the User Manager, you can import the AD group, and the users in the AD group will be able to get the account automatically provisioned.



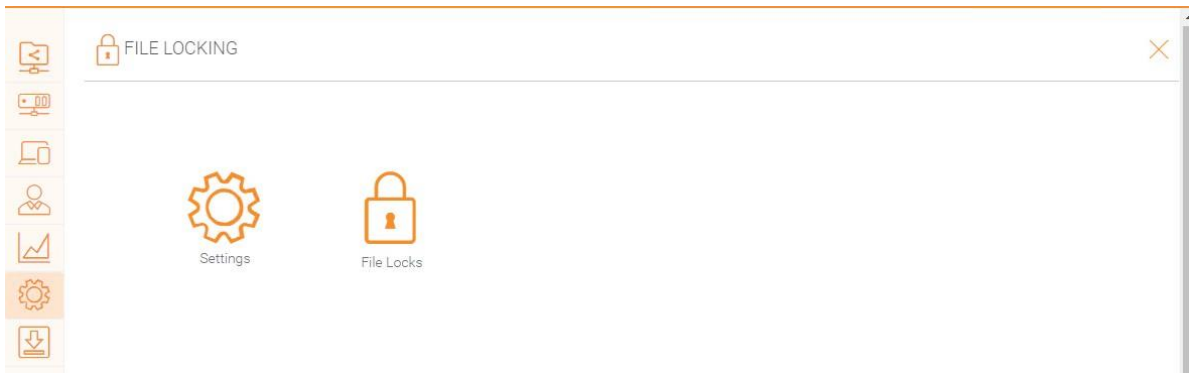
Single Sign-on

Single Sign on via SAML is a per-cluster setting.



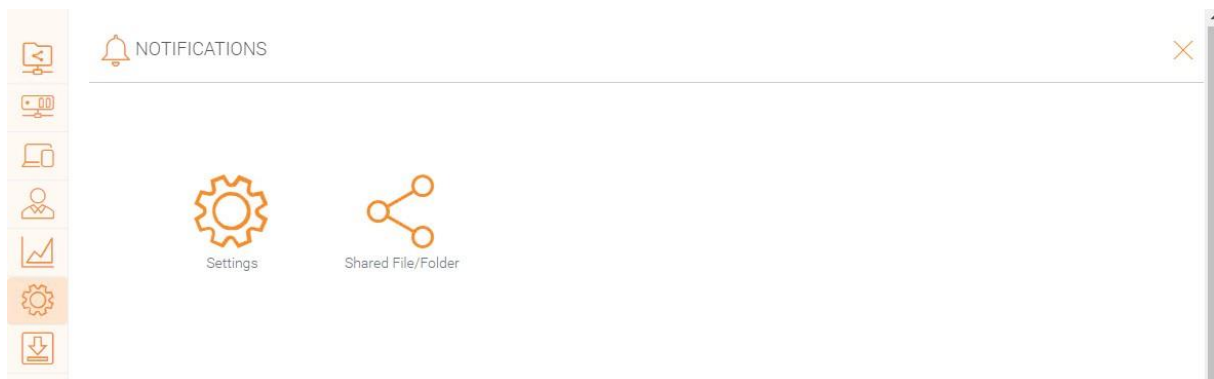
File Locking

File Locking is another critical component to ensure that users' changes are not overwritten by each other. Here you can enable or disable all file locking options.



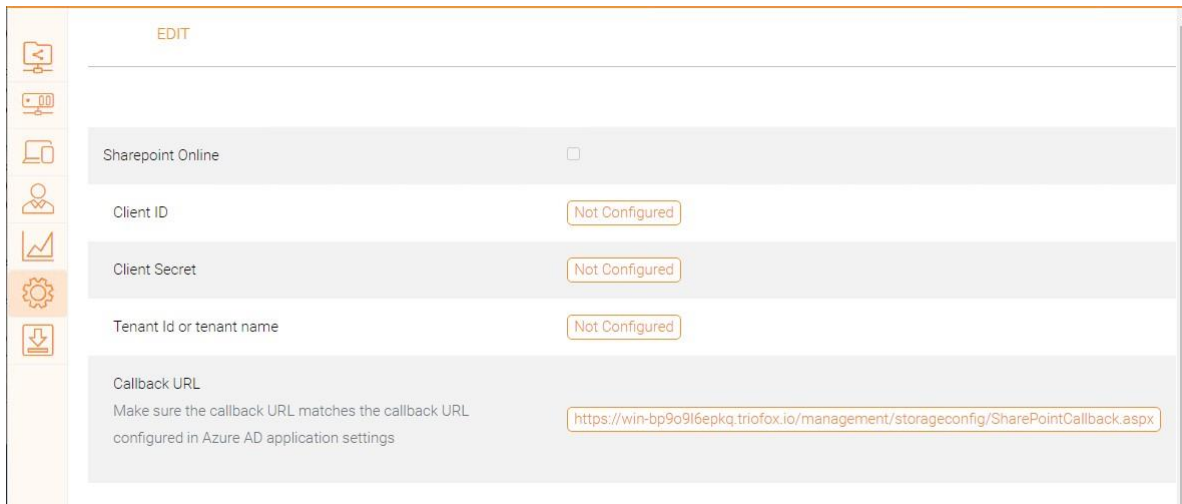
Notifications

Notifications is a critical component to ensure that users have control over what they can do with their notifications.



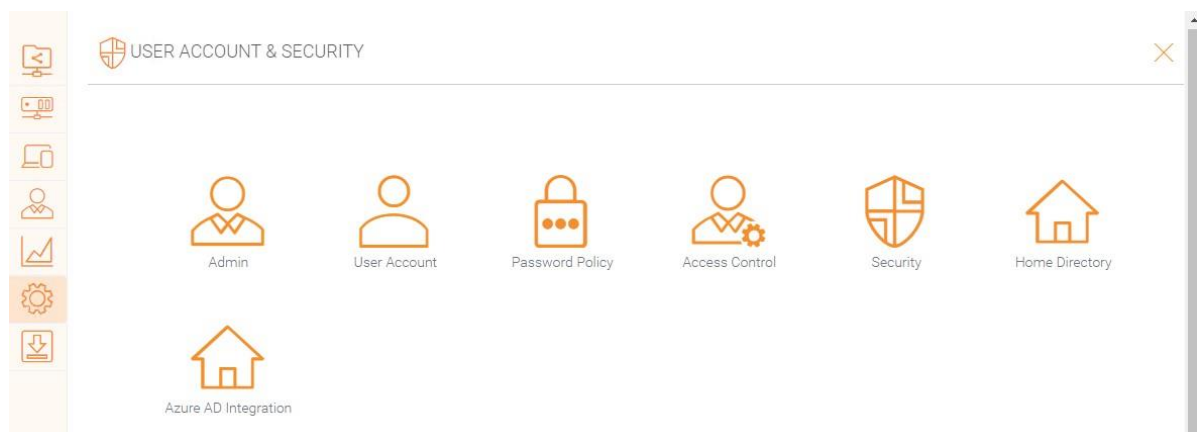
SharePoint Online Integration

Under "SharePoint Online Integration" you can integrate your SharePoint Online with Triofox.



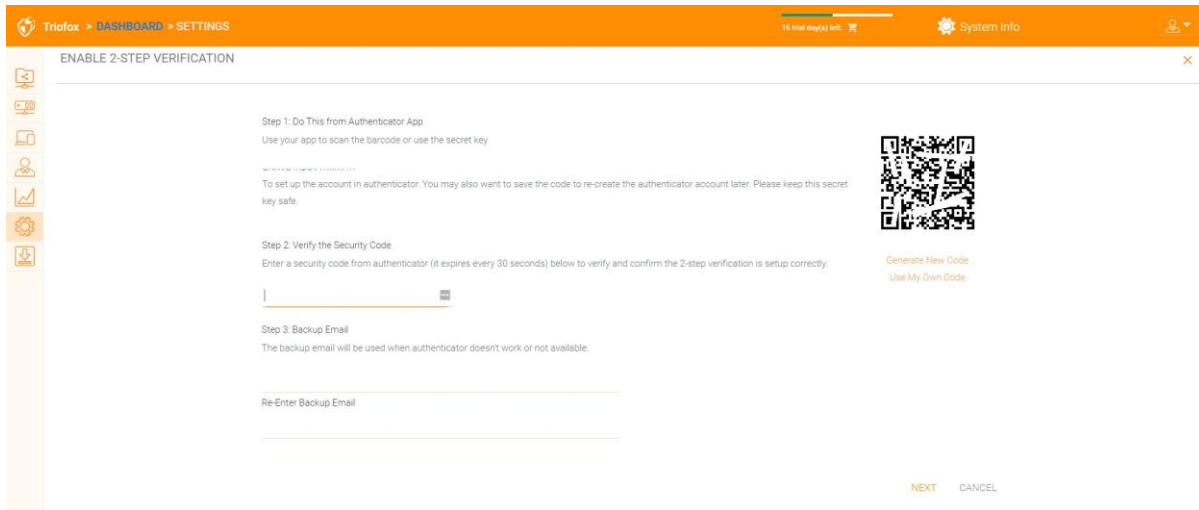
User Account & Security

Under "User Account & Security" you can control the security of the Tenant Administrators, the User Accounts, and the Password Policy. Next to that you can see the settings for Access Control, Security, Home Directory, and Azure AD integration.



2-Step Verification

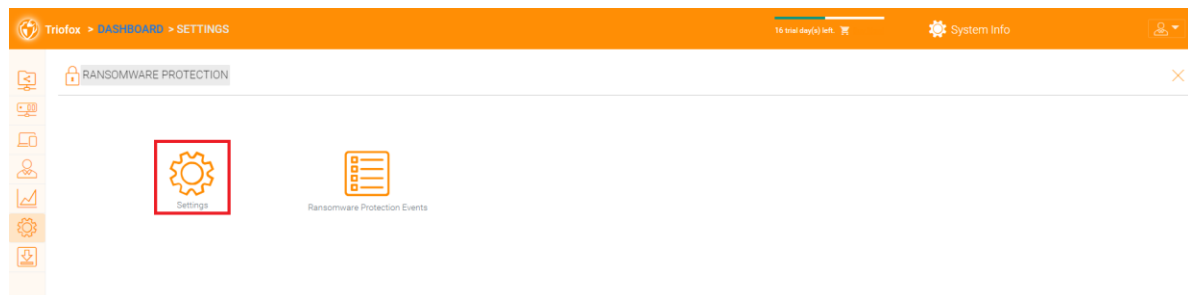
Enforce 2-step verification will force the users to set up 2-step verification via Google Authenticator, Microsoft Authenticator, Amazon MFA, or any other app that supports the same 2-step verification algorithm.



Ransomware Protection

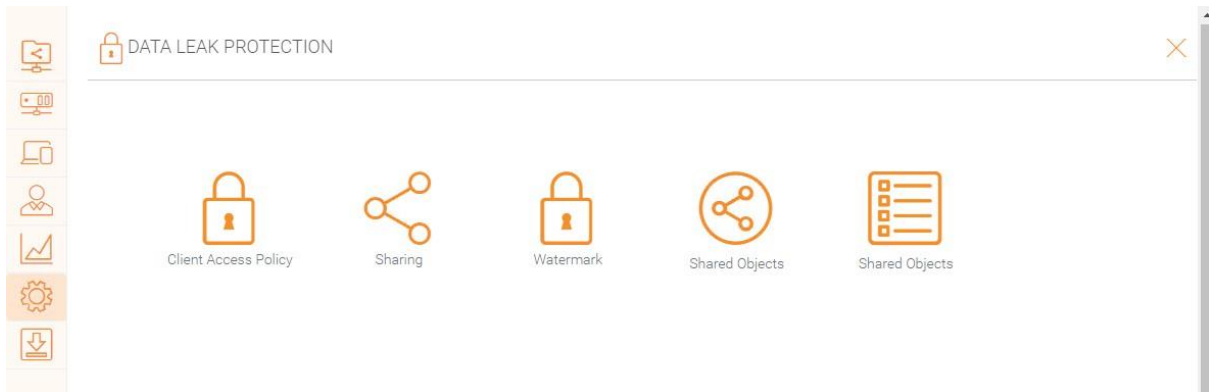
Triofox adds ransomware protection and an automatic alert mechanism to your file servers. It continuously monitors all Triofox clients for unusual activity and automatically shuts them down if it detects a possible attack.

You can enable ransomware protection by clicking Settings.



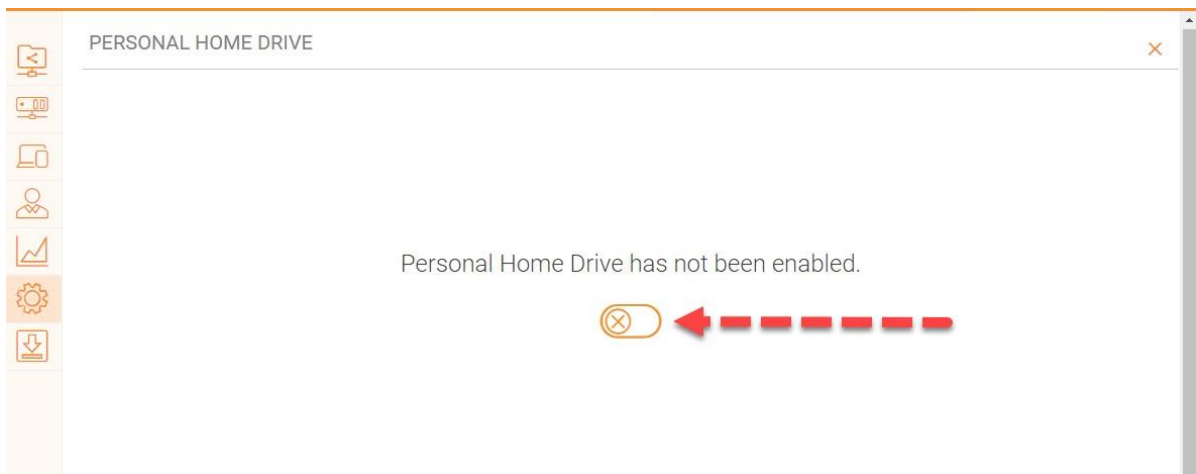
Data Leak Protection

Under "Data Leak Protection" you can control the Client Access Policy, Sharing, Watermarks, Shared Objects, and DLP Events.



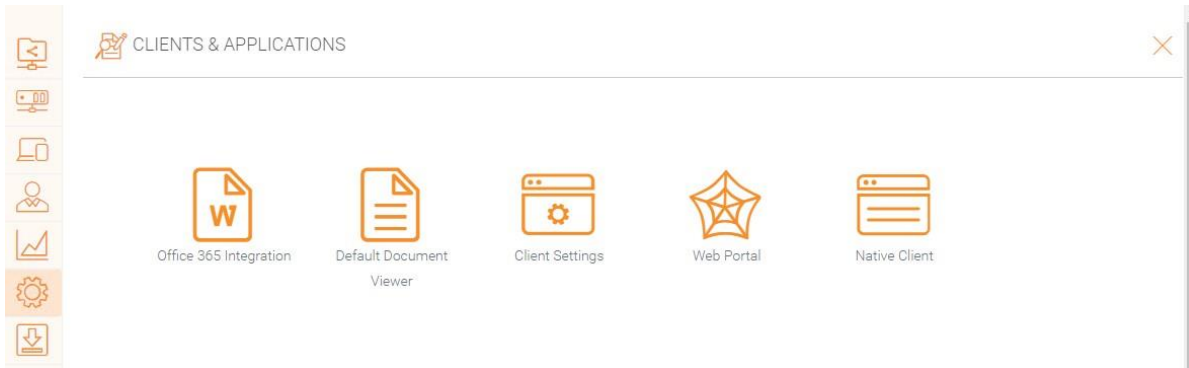
Personal Home Drive

Under "Personal Home Drive", you can enable access to your own personal drive aside from Triofox.



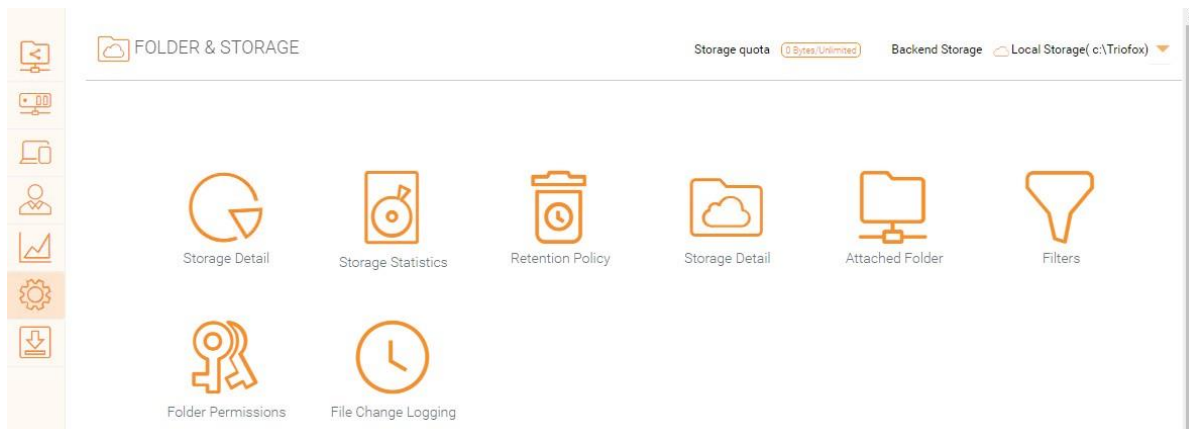
Clients & Applications

Under "Clients & Applications" you can integrate Office 365, change the Default Document Viewer settings, Client Settings, Web Portal Settings, and Native Client Settings.



Folder & Storage

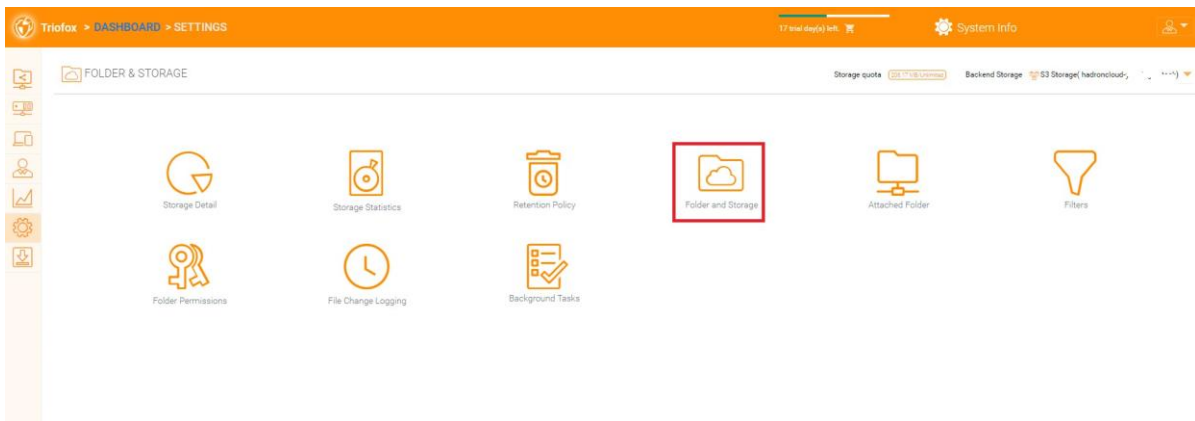
In the "Folders & Storage" section, you can change all the settings for your storage and folders. For example, Retention Policy and Folder Permissions.



Files and Folder Permission

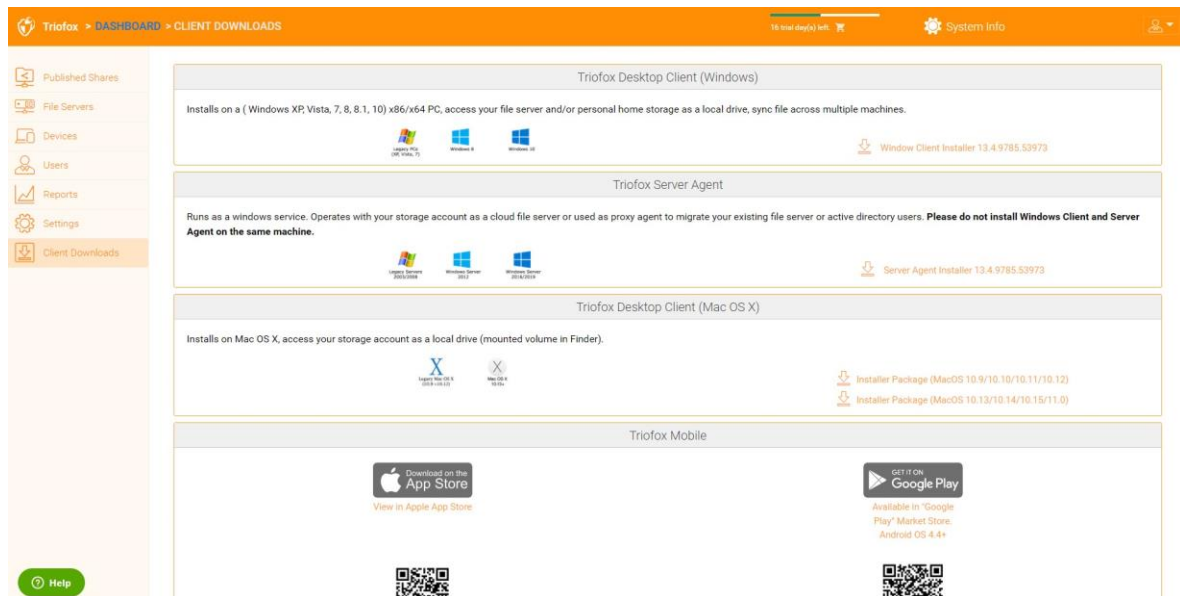
If your files and folders are located on a file server on the same local area network (LAN) as the Triofox server, it is best to delegate 100% of the file and folder permission to the NTFS permission.

If you are not using native NTFS permission. For example, if you use cloud storage services such as Amazon S3 or OpenStack Swift, you can use the Triofox folder permission.



Client Downloads

In this section you can find all Clients for download.



Cluster System Info



The System Information pane gives you access to additional settings, as well as information about your cluster, server farm, and client versions.

Cluster Info

In the cluster info pane, you can see the "Product Name" where you can change the branding of your cluster. The "Assigned License Count" area displays licensing details, including the license edition, number of users, cluster ID, and Triofox server version. Here you can upgrade your environment to a higher edition by clicking on the shopping cart next to your edition. Also, you can view and copy the Cluster ID.

Server Farm

In the Server Farm you can set up your External DNS, configure the settings for the Email Service, get the Database Information and view the number of Worker Nodes.

Server Farm	
External DNS	https://win-bp9o9l6epkq.triofox.io  
Email Service	Default >
Database Info	All-In-One: PostgreSQL (10.13) >
Worker Node Count	1 >

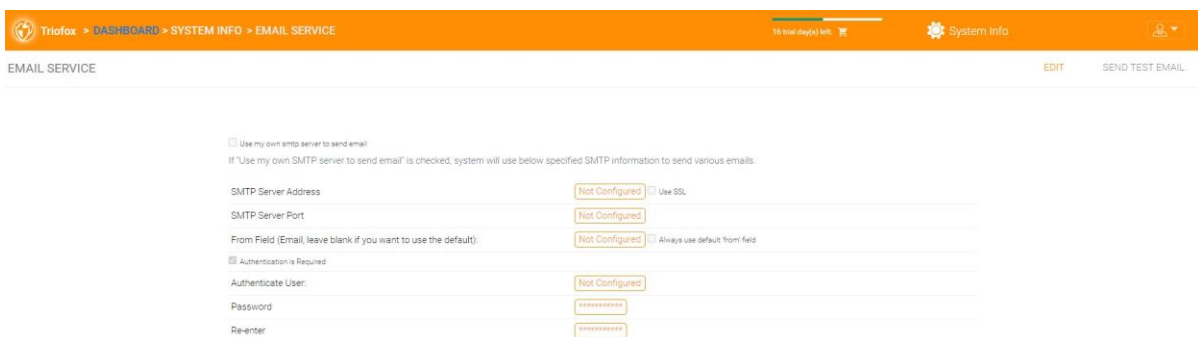
Email Service

In the Triofox solution, there are many places where the user needs to be contacted by email. The email service is used to set up the SMTP email service to send the emails.

By default, it works out of box using the default email service with the Cluster Server's customer support email address as the sender.

It is recommended to set up the SMTP service to use your own SMTP service for sending emails.

If your SMTP service does not require authentication, you can enter a dummy email in the Authenticate User field.



Triofox > DASHBOARD > SYSTEM INFO > EMAIL SERVICE

EMAIL SERVICE

Use my own smtp server to send email
 If "Use my own SMTP server to send email" is checked, system will use below specified SMTP information to send various emails.

SMTP Server Address Use SSL

SMTP Server Port

From Field (Email, leave blank if you want to use the default): Always use default from field

Authentication is Required

Authenticate User:

Password

Re-enter

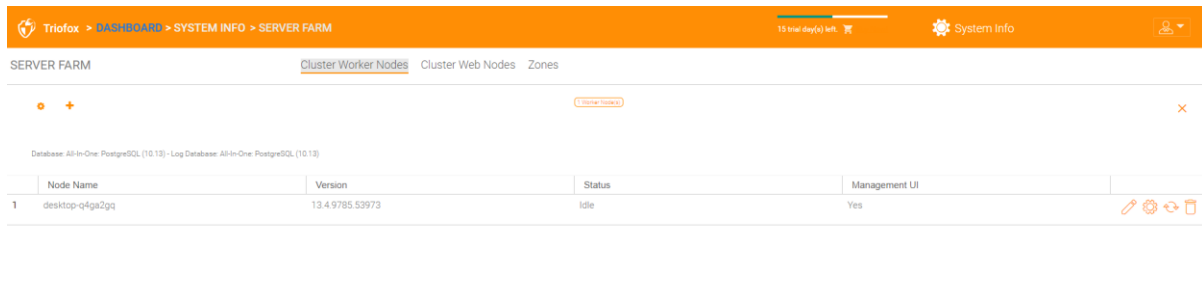
EDIT SEND TEST EMAIL

Worker Node Count

Cluster Server Farm has two types of nodes. One is "Worker Node", and the other is "Web Nodes".

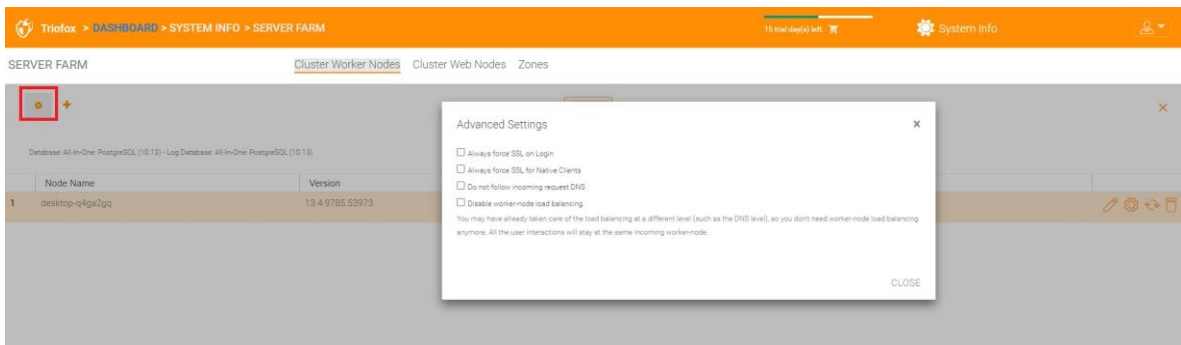
Cluster Worker Nodes

This type of node contains services such as the Web Browser Based File Manager, Storage Service Connectors, etc. Again, additional nodes can be added as the load increases. Since cache information resides on each node, users have an affinity for a single node once it is assigned. If the load balancer distributes users evenly across all worker nodes, the cache information can be present on all worker nodes.



Worker Node Settings

There are some settings that apply to all worker nodes. After clicking on the "Settings" icon, the "Advanced Settings" panel is displayed.



Always force SSL on login

In a production environment, almost 100% of the time you will need to enable the "Always force SSL on Login" option. If this option is checked and Triofox detects that the incoming connection is HTTP, it will do a redirect to HTTPS. If you enable SSL, you must first set up an SSL certificate.

However, if you have SSL-offload, such that SSL is offloaded to a hardware appliance, and after that, the incoming connection is HTTP between the hardware appliance and Triofox. In this SSL-offload case, you will NOT check "Always force SSL on Login" because it will create an infinite redirect loop because the incoming connection is always HTTP as far as the Triofox Server is concerned.

Always force SSL for Native Clients

In a production environment, almost 100% of the time you will need to enable the "Always force SSL for Native Clients" option.

Especially in the case of SSL-Offload, you MUST check "Always force SSL for Native Clients". Otherwise, the Triofox Server may think that the incoming connection is HTTP, so it will continue to encourage the native clients (such as Windows clients) to use HTTP instead of HTTPS.



Note

On iOS devices, Application Transport Security may be enforced by the operating system, and HTTPS must be used for an iOS application to connect to the Cluster Server.

Disable worker-node load balance

If you have your own load balancer, you will disable worker-node load balancing. The Cluster Server has built-in node-affinity load balancing that can be done on a per-user basis. If you have your own load balancer, you can have session affinity or just round-robin, either is fine.

Note

How to add a worker node?

Simply install the Cluster Server during the installation and point the Cluster Server to the same database. Once the Cluster Server worker node installation is complete, reboot. The web portal page appears and prompts you to add the worker node to the server farm.

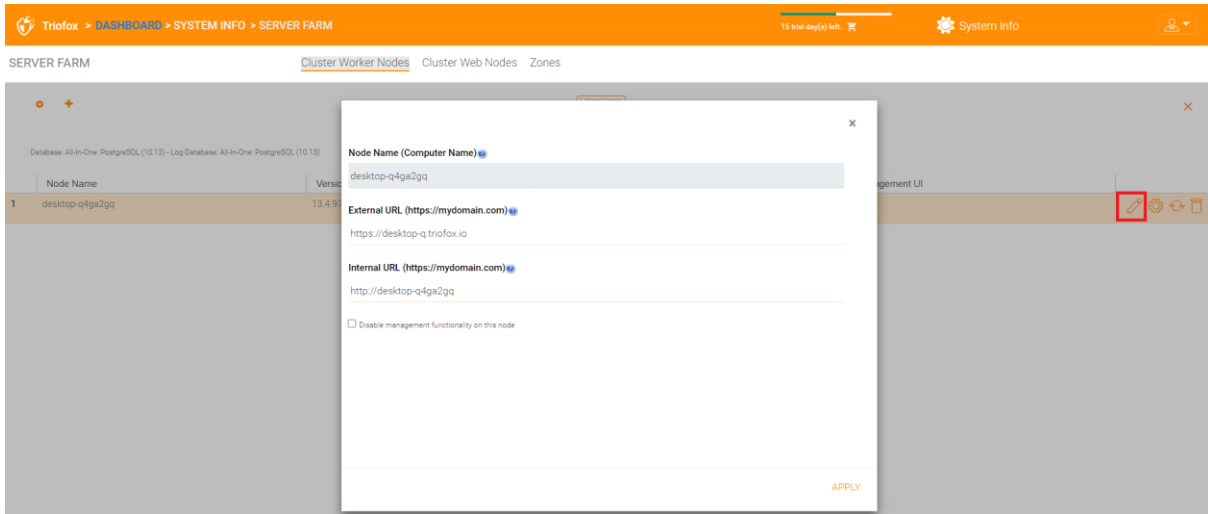
Warning

What happens if you have changed the Cluster Server Host Name?

In Windows Server 2012 and newer servers OS, a server that is newly provisioned is usually named similarly in the hostname format (WIN-ABCDEFGH). Sometimes it is desirable to change the name in the Control Panel -> Systems. If the Cluster Server is already installed, changing the name will make the Cluster Server add itself again with the new name. So, the next time you visit <http://localhost> on the Cluster Server after the server has been renamed, you will see that the worker node section contains both the node with the old name (which no longer exists) and the node with the new name (which is current and good). In this case, you simply need to remove the worker node with the old name.

Worker Node Properties

You may need to change the worker node properties when you set up SSL and the DNS name for the cluster.



Node Name

The **Node Name** needs to match the hostname of the worker node. If you rename the Windows hostname (NETBIOS name) of a worker node after installing the Cluster Server, it may happen that the Cluster Server displays a web page after rebooting, asking you to add the new worker node. In this case, you can add the new worker node and then delete the old worker node.

External URL

The **External URL** needs to match the external URL of the worker node. In a production environment, this is usually in the format `https://` and contains the DNS name of the node.

The External URL is an important property for email templates. After the Cluster Server installation is complete, the dashboard displays the warning message "External DNS has not been configured for this worker node. Some functionality may not work properly. Config Now".

The moment that you have finalized on the External DNS name of the Cluster Server, you must come here and configure the External URL property for the Cluster Server.

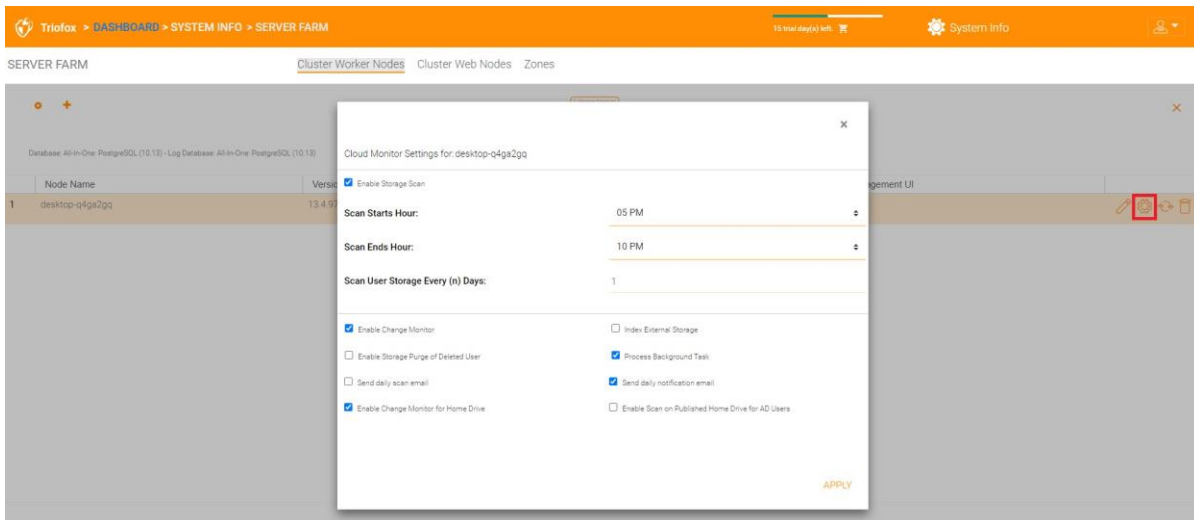
Internal URL

The Internal URL is the internal URL of the node, usually in the format `http://local-ip-address`. In later Cluster Server builds, this property is hidden and does not need to be set any more.

Disable management functionality

You can create an internal facing worker node (that doesn't have an external URL) and allow management functionality only on this worker node. This is a security feature.

Edit Cloud Monitor Setting



Enable Storage Scan

Enables or disables storage scan on the worker node. There is a Cloud Monitor service on the Worker Node. The service performs background monitoring and scans the storage from time to time to correct quota calculation and perform other maintenance tasks.

Scan Starts Hour

Normally, you set the start time for the scan sometime in the early morning, around 1 AM.

Scan End Hour

Typically, you set the end time for the scan to be sometime in the morning, such as 8 AM, before everyone gets to work. The idea is to use the idle time (when people are not at work) for scanning.

Scan User Storage Every (n) Days

Typically, you can set this to every week or every other week. So a number between 7 and 15 is appropriate.

Enable Change Monitor

If you enable Change monitor, the attached local storage, e.g., storage from file server network share, will be monitored and notification of file changes will be reported to remotely connected clients. This is typically required if your users modify documents both directly from the backend attached network share and from the front-end cluster access clients.

Index External Storage

This setting indexes storage services added through the "Storage Manager". The index is written to the files table in the database.

Enable Storage Purge of Deleted User

When a user is deleted from the system, the user's home directory is not immediately removed. In many cases, you may not want to delete it at all. For example, a user is deleted from the Cluster Server, but the user can still use the files and folders directly from the network.

Process Background Task

Specifies whether this particular node should process background tasks.

Enable Change Monitor for Home Drive

When Active Directory Home Drive integration is enabled, this allows Cluster Server to monitor changes on the home drive and notify remote client agents that the files/folders have been changed.

Send daily scan email

When storage scan is enabled, a daily scan email is sent to the cluster administrator about the scan result.

Cluster Web Nodes

Note

For a small deployment, it is not necessary to have web nodes. You can go directly to worker nodes since worker nodes are also web nodes by default.

The Account Management, Sign-in and Load Balancing services are installed on this physical (or virtual) machine. Depending on the load, you may need 1 to N such nodes. Typically, we recommend using 10+ worker nodes for each web front node. For small deployments, you can omit web front nodes and combine them into worker nodes. All the installation work is the same. If you do not need web front node, you do not need to assign them in Cluster Manager.

The screenshot displays the 'Cluster Web Nodes' page in the Triofox Cluster Manager. The breadcrumb navigation at the top reads 'Triofox > DASHBOARD > SYSTEM INFO > SERVER FARM'. The page title is 'SERVER FARM' with sub-tabs for 'Cluster Worker Nodes', 'Cluster Web Nodes', and 'Zones'. A 'Web Nodes' button is visible, along with refresh and add icons. Below is a table with columns for 'Node Name' and 'Version'. A help message at the bottom states: 'Nodes registered as a worker node, do NOT add it again as a web node. When you have a single-server/all-in-one deployment, add the node as worker node, instead of a web node. Only register dedicated web nodes here in a multi-node deployment.'

Example:

- ACME Corporation deploys two web front nodes `node1.acme.com` and `node2.acme.com`. Each node runs a copy of the Cluster Server connected to the same SQL database.
- ACME Corporation acquires a domain name (DNS) of `cloud.acme.com`, which is load balanced to `node1.acme.com` and `node2.acme.com`.

When users point their browsers to `https://cloud.acme.com`, they are directed to the login page of one of the nodes.

Note

NOTE 1: If you have hardware load balancing available, you do not need to use web nodes at all.

NOTE 2: Windows 2012/R2 comes with Network Load Balancing (NLB). If you use NLB, you do not need web nodes at all.

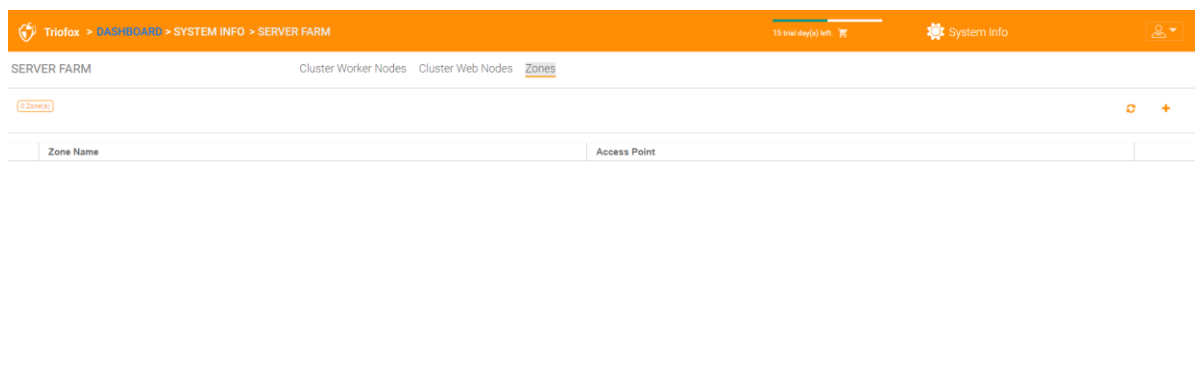
If you have an existing load balancer, you can basically omit the web nodes.

Zones

The concept of a zone is to connect your worker nodes to the location of storage. When you think about zones, you will first think about the storage location.

For example, I have storage in LA, so I have a LA zone. I also have storage in NY, so I have a NY zone.

You can also have worker nodes from different zones and assign users to a specific zone. If the user's home directory is from the LA zone, the user must be assigned to the LA zone.



Client Versions

Client Versions		
Windows Client	--/13.4.9785.53973	>
Server Agent	--/13.4.9785.53973	>
Mac Client	--/13.4.313	>

Windows Client

For Windows Client, Mac Client and Windows Server Agent, there is an automatic client update feature. Each upgrade package contains the updated clients. By clicking on the **Publish** button, the newer package can be published to the clients.

Each new Cluster Server upgrade includes the newer Windows client, Windows Server Agent, and Mac client. Cluster users can get the clients that are included in Cluster Server via the manual download. However, for existing users with clients already installed, these older clients are not automatically upgraded until the newer client packages are published.

Daily Upgrade Limit

This is a per worker node setting. For example, if you have 2 worker nodes and set the daily upgrade limit to 100, a maximum of 200 clients will be upgraded per day.

Apply to Users

This option is usually used for testing purposes before the client is published.

Do Not Apply to Users

This option is usually used for testing before the client is published and to exclude certain users.

Triofox > DASHBOARD > SYSTEM INFO > CLIENT VERSION MANAGER 13 trial days left System info

Windows Client Server Agent Mac Client

Please specify the windows client/server agent/mac client version you want to publish. The windows client/server agent will be upgraded automatically if its version is older than the specified version.

Windows Client Version: 13.4.9785.53973 PUBLISH

Windows Client Package: /portal/Pkgs/windowspkg.zip

Daily Upgrade Limit: 0 (Unlimited)
The auto client upgrade process will distribute the upgrades in evenly-spaced intervals each day up to the specified daily limit.

Apply to users: [email]1, [email]2, ...
specify the users whose clients will be upgraded. Leave it blank for all users to receive upgrades. (tenant admin email will include all users who belong to the tenant)

Do NOT apply to users: [email]1, [email]2, ...
specify the users whose clients will NOT be upgraded. Leave it blank for all users to receive upgrades.

Do not upgrade file driver

Current Published Version: --

Note

The Windows client out there has a process that runs as a Windows service in the background. The service checks in regular intervals of about 1-2 hours if a newer upgrade is available. Once a newer client package is published and discovered, the newer package is downloaded. However, if the client is still actively running, the replacement and upgrade will not occur until the client application is stopped and restarted. This usually happens when the user logs out of Windows or restarts their desktop.

If the Windows client software is actively running, a message may appear in the system tray asking the user if they want to restart the client software and get the newer version.

Once a client is published for automatic client upgrade, you can use **Unpublish** to stop the automatic client upgrade.

Server Agent

The Windows Server Agent can be published separately for automatic upgrade.

Triofox > DASHBOARD > SYSTEM INFO > CLIENT VERSION MANAGER 13 trial days left System info

Windows Client Server Agent Mac Client

Please specify the windows client/server agent/mac client version you want to publish. The windows client/server agent will be upgraded automatically if its version is older than the specified version.

Server Agent Version: 13.4.9785.53973 PUBLISH

Server Agent Package: /portal/Pkgs/windowspkg.zip

Do not upgrade file driver Do not restart server agent after upgrade

Current Published Version: --

Mac Client

The Mac client can be published separately for automatic upgrade.

The screenshot shows the 'Client Version Manager' interface for Mac Client. The breadcrumb navigation is 'Triofox > DASHBOARD > SYSTEM INFO > CLIENT VERSION MANAGER'. The page title is 'Mac Client'. Below the navigation, there are tabs for 'Windows Client', 'Server Agent', and 'Mac Client'. A message states: 'Please specify the windows client/server agent/mac client version you want to publish. The windows client/server agent will be upgraded automatically if its version is older than the specified version.' The form contains the following fields:

Mac Client Version (OSX 10.13/10.14):	13.4.313	PUBLISH
Mac Client Package:	/portal/Pkgs/Mac/MacClient.9.dmg.zip	
Current Published Version:		

Administrators

The "Administrators" option allows a Triofox administrator to change the cluster administrator's default email address, reset the password, and add additional administrators.

The screenshot shows the 'Administrators' interface. The breadcrumb navigation is 'Triofox > DASHBOARD > SYSTEM INFO > ADMINISTRATORS'. The page title is 'DEFAULT ADMINISTRATOR'. Below the navigation, there is a table of administrators:

	EDIT
Cluster Admin	EDIT
ahsana@triofox.com	EDIT RESET PASSWORD

Below the table, there is a section for 'Additional Cluster Administrators (add other users to administrators) (email1;email2):' with a text input field and an [EDIT](#) button.

Cluster Branding

You can access the cluster branding under **System Info**.

The screenshot shows the Triofox dashboard with the following sections:

- Cluster Info:**
 - Product Name: Triofox
 - Assigned License Count: Trial ends in 22 days
 - Cluster ID: KCYhAE1Y9RW6+cQ2hHQ2mVMSUqm#mpGzQzHRKxupV9U/zr/2fBwq2n2
- Server Farm:**
 - External DNS: https://desktop-q4ga2gq.triofox.io
 - Email Service: Default
 - Database Info: All-In-One: PostgreSQL (10.13)
 - Worker Node Count: 1
- Client Versions:**
 - Windows Client: --/13.4.9785.53973
 - Server Agent: --/13.4.9785.53973
 - Mac Client: --/13.4.313
- System Info Menu:**
 - Administrators
 - Cluster Branding** (highlighted)
 - Cluster Settings
 - Application Manager
 - Languages
 - Anti-virus
 - Reports
 - Multi-Tenancy
- Performance Metrics:**
 - Requests (Total): 273
 - Requests (Active): 0
 - Response Time: 414 ms
 - Active Upload: 0
 - Active Download: 0
 - Upload: 0 Bytes/S

In Cluster Branding, you can change the logo, bitmaps, and other branding-related information. There are two branding supports. One is the built-in self-service branding, which is fully controlled by the "Cluster Branding" settings in the "System Info". The other is the full-branding service. Both rely on "Cluster Branding" to change the appearance of the web portal.

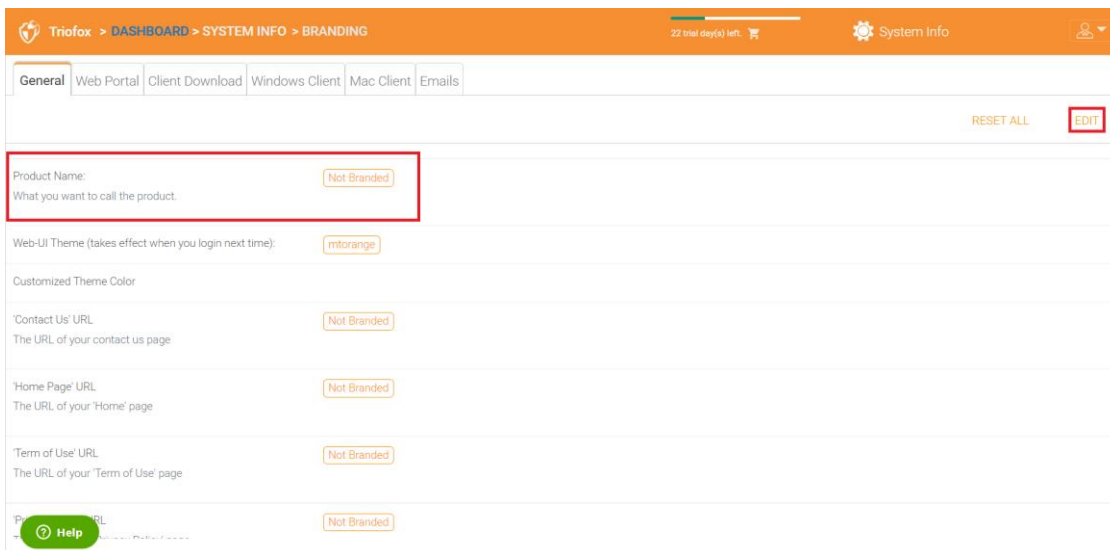
Built-in branding works with white-label clients, which upon the first connection to the cluster, will download the branding-related information and use the branding-related information. Compared to the full-branding service, full-branding clients burn artwork, logo bitmaps, and related information into the client binaries.

General

The General tab lets you specify the name and other settings as described below.

Product Name

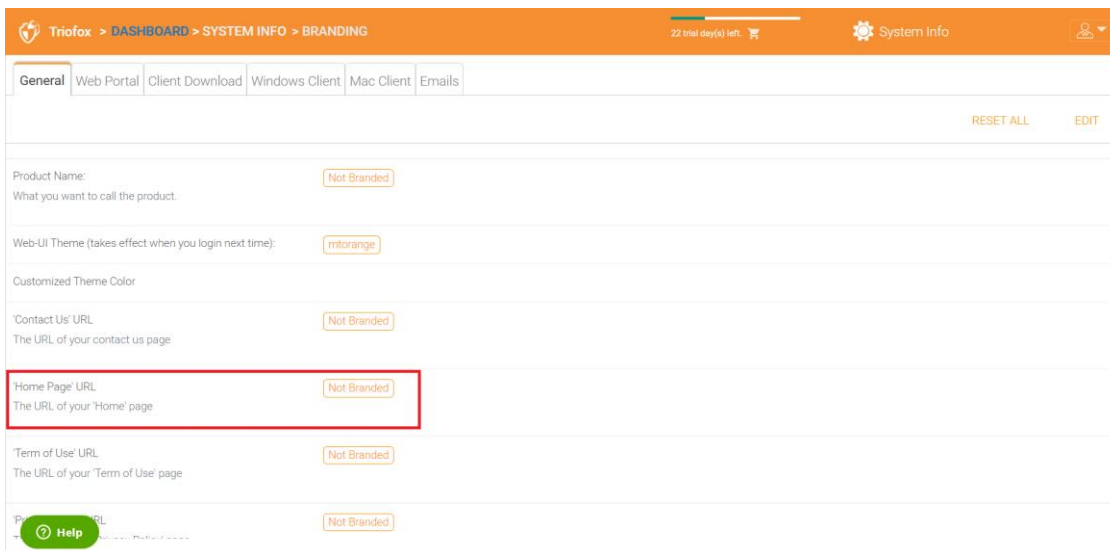
Here you specify what you want to call the product. This is the name that users will see when they log in to either the web portal or client applications. To access the branding settings, click the branding icon (1), then click "EDIT" (2), and then change the setting you want (3). Do not forget to save your settings. You can also choose a color theme that you want your users to see when they log in to the portal. You can choose a color theme that matches your company's colors.



The screenshot shows the 'BRANDING' settings page in the Triofox dashboard. The 'General' tab is selected. The 'Product Name' field is highlighted with a red box. The field contains the text 'Not Branded' and a description: 'What you want to call the product.' Other settings include 'Web-UI Theme' (mforange), 'Customized Theme Color', 'Contact Us' URL, 'Home Page' URL, 'Term of Use' URL, and 'Privacy Policy' URL, all currently set to 'Not Branded'. A green 'Help' button is visible at the bottom left. The top navigation bar shows 'Triofox > DASHBOARD > SYSTEM INFO > BRANDING' and '22 trial day(s) left'. The 'EDIT' button is highlighted with a red box.

Home Page URL

This is the URL of your "Home Page" page.



The screenshot shows the 'BRANDING' settings page in the Triofox dashboard. The 'General' tab is selected. The 'Home Page' URL field is highlighted with a red box. The field contains the text 'Not Branded' and a description: 'The URL of your "Home Page" page.' Other settings include 'Product Name', 'Web-UI Theme' (mforange), 'Customized Theme Color', 'Contact Us' URL, 'Term of Use' URL, and 'Privacy Policy' URL, all currently set to 'Not Branded'. A green 'Help' button is visible at the bottom left. The top navigation bar shows 'Triofox > DASHBOARD > SYSTEM INFO > BRANDING' and '22 trial day(s) left'. The 'EDIT' button is highlighted with a red box.

Copyright Statement

This is the content of your "Copyright Statement".

The screenshot shows the 'BRANDING' section of the Triofox dashboard. The breadcrumb trail is 'Triofox > DASHBOARD > SYSTEM INFO > BRANDING'. The page has a trial timer showing '22 trial day(s) left'. The 'General' tab is selected, and there are tabs for 'Web Portal', 'Client Download', 'Windows Client', 'Mac Client', and 'Emails'. On the right, there are 'RESET ALL' and 'EDIT' buttons. The settings list includes:

- Web-UI Theme (takes effect when you login next time): mtorange
- Customized Theme Color: (empty)
- 'Contact Us' URL: Not Branded (The URL of your contact us page)
- 'Home Page' URL: Not Branded (The URL of your 'Home' page)
- 'Term of Use' URL: Not Branded (The URL of your 'Term of Use' page)
- 'Privacy Policy' URL: Not Branded (The URL of your 'Privacy Policy' page)
- Copyright Statement: Not Branded (highlighted with a red box and a 'Help' button)

Web Portal

You can find **Web Portal** section under **Cluster Branding**.

Note

In previous builds, the icons worked best when the icon files were on the same server and the icons were referenced by a relative link.

For example, you can create a subfolder under the Cluster Server installation folder, such as the root/imagetest folder. The dimensions of all the icons for each setting in the web portal should match what is displayed for each setting. The branding of the icons and images require the icons and images have the same width/height as specified or the same aspect ratio if the resolution is higher.

In later builds, the icons used are what-you-see-is-what-you-get and you can upload those icon sets.

Application Icon

In the Web Portal section of the cluster branding, you can change the application icon. This is the image that appears next to the product name in the web portal.

The screenshot shows the 'BRANDING' configuration page for Triofox. The navigation bar includes 'Triofox > DASHBOARD > SYSTEM INFO > BRANDING', a trial timer '21 trial day(s) left', 'System Info', and a user profile icon. The 'Web Portal' tab is selected. The 'Application Icon' field is highlighted with a red box, showing a red-bordered input area with the text 'Application Icon' and 'PNG format recommended (32x32). Used by web portal.' To the right of this field is a preview of the current application icon, which is a shield with a heart inside. Other fields include 'Drive Icon', 'Logo', 'Login Background Image', 'IOS Client App ID', and 'Login Page Note', each with a preview or a 'Not Branded' status.

Drive Icon

This is the icon used for the Triofox drive. For example, in the tree view of the web portal.

This screenshot is similar to the previous one, showing the 'BRANDING' configuration page. In this view, the 'Drive Icon' field is highlighted with a red box. The 'Drive Icon' field has a red-bordered input area with the text 'Drive Icon' and 'The drive icon (16x16)'. The preview to the right shows a small version of the shield-with-heart icon. The rest of the page, including the navigation bar and other branding options, is identical to the previous screenshot.

Logo URL & Login Page Left Image

The screenshot shows the 'Web Portal' tab in the 'BRANDING' section. The 'Logo' field is highlighted with a red box. The page includes the following settings:

- Application Icon:** PNG format recommended (32x32). Used by web portal. (Image: Triofox shield icon)
- Drive Icon:** The drive icon (16x16). (Image: Triofox shield icon)
- Logo:** The logo image on the login page (300x50). (Image: triofox text logo)
- Login Background Image:** The background image on the login page.
- iOS Client App ID (used for Smart App Banners):** Not Branded
- Login Page Note:** Not Branded

Please follow the same steps for branding settings for “Login Background Image”, “File Share Stamp Icon”, “iOS Client App ID”, “Login Page Note”, “Change Password URL”, “Tutorial Page URL”.

Client Download

You can find **Client Download** section under **Cluster Branding**. You can also choose not to show the download link for some clients.

The screenshot shows the 'Client Download' tab in the 'BRANDING' section. The page includes the following settings:

- Download Page:** Windows Client, Server Agent, Mac Client, iOS Client, Android Client
- iOS Client Download Link:** Not Branded
- Android Client Download Link:** Not Branded

Mobile Clients Download Links

Once you have branded your own iOS client and/or Android client, you can point the download link to your own AppStore and Google Play.

Triofox > DASHBOARD > SYSTEM INFO > BRANDING

21 trial day(s) left. System Info

General Web Portal **Client Download** Windows Client Mac Client Emails

EDIT

Download Page

Windows Client Server Agent Mac Client iOS Client Android Client

IOS Client Download Link Not Branded

Android Client Download Link Not Branded

Windows Client

You can find **Windows Client** section under **Cluster Branding**.

Here you can specify the URLs for the application icon and the drive icon. You can also enter your company name under "Manufacturer Name" along with the "Contact Info" email. You also have the option to create your own branded MSI Windows client here. You can also use your own code signing certificate to digitally sign the MSI package. The advantage of creating your own MSI client package is that when users download and install the Windows client you provide, they will see your company name along with your branding during the client installation.

Triofox > DASHBOARD > SYSTEM INFO > BRANDING

21 trial day(s) left. System Info

General Web Portal Client Download **Windows Client** Mac Client Emails

EDIT

Recommended: use a single .ico file that contains multiple images (64x64, 48x48, 32x32, and 16x16) with 32-bit color depth (RGB/A)

Application Icon (ico) (32x32)
ICO format, used by Native Client

Drive Icon (ico) (32x32)
ICO format, used by Native Client

UI Language
Use OS Setting

Manufacturer Name
Not Branded

Contact Info
Not Branded

The Windows client supports multiple languages. Some language packs are included and shipped with Triofox. If you want to run the Windows client under a different language, you can set the UI language there.

After clicking the "Edit" button to edit the branding information of the Windows client, you can specify the EULA (End User License Agreement) and Code Signing Certificate.

The screenshot shows the 'Branding' section of the Triofox System Info interface. The breadcrumb trail is 'Triofox > DASHBOARD > SYSTEM INFO > BRANDING'. The page has a trial timer showing '21 trial day(s) left'. The 'Windows Client' tab is selected. At the top, there are buttons for 'SAVE SETTINGS AND BRAND INSTALLATION PACKAGE', 'RESET BRANDED PACKAGE', 'SAVE SETTINGS', and 'CANCEL'. A blue banner provides a recommendation: 'Recommended: use a single .ico file that contains multiple images (64x64, 48x48, 32x32, and 16x16) with 32-bit color depth (RGB/A)'. Below this, there are two 'Choose File' buttons for 'Application Icon (.ico) (32x32)' and 'Drive Icon (.ico) (32x32)'. The 'UI Language' is set to 'Use OS Setting'. The 'Manufacturer Name' field is empty. The 'Contact Info' field contains the email 'yueningliu19952@yahoo.com'. At the bottom, there is a 'Help' button and another 'Choose File' button.

EULA

The input is in an RTF file format.

Code Signing Certificate

You can acquire a code signing certificate from your code signing certificate vendor. Most SSL providers also offer code signing certificates. Make sure that you use SHA 256 (SHA2) as the hash algorithm for your digital signing certificate.

If your Code Signing certificate is already installed, you can also use the option - **Sign using cert in certificate store.**

MAC Client

You can configure the MAC client and MAC client installation package branding under here.

The screenshot shows the 'Mac Client' configuration page in the Triofox System Info interface. The breadcrumb trail is 'Triofox > DASHBOARD > SYSTEM INFO > BRANDING'. The page has a navigation bar with tabs for 'General', 'Web Portal', 'Client Download', 'Windows Client', 'Mac Client', and 'Emails'. The 'Mac Client' tab is active. Below the navigation bar is an 'EDIT' button. The main content area contains four configuration items, each with a description and a shield icon:

- Mac Client Application Icon**: Application icon in Mac Client Systray menu (128X128)
- Mac Client Drive Icon**: Mac Client Drive icon (.icns format)
- Mac Client Systray(Notification Area) Icon**: Mac Client Systray icon displayed on Notification Area (16X16)
- UI Language**: A dropdown menu currently set to 'Use OS Setting'.

Emails

There are many places in Cluster Manager where users need to be contacted via email. So, the **Emails** tab is used to set up the email templates used for contacting users via email.

The screenshot shows the 'Emails' configuration page in the Triofox System Info interface. The breadcrumb trail is 'Triofox > DASHBOARD > SYSTEM INFO > BRANDING'. The page has a navigation bar with tabs for 'General', 'Web Portal', 'Client Download', 'Windows Client', 'Mac Client', and 'Emails'. The 'Emails' tab is active. Below the navigation bar is an 'EDIT' button. The main content area contains a list of email templates, each with a plus icon and a title:

- Welcome Email for New Team User
- Welcome Email for New Guest User
- Email for File/Folder Share
- Request a File
- Notify External User that Shared File Changed
- Folder Change Subscription
- Sync Task Failed/Paused
- Fast Update Protection

At the bottom left of the page is a green 'Help' button.

Welcome Email for New Team User

The team user is a regular user in a cluster. This is the email template that is sent to the user when the user account is created.

Welcome Email for New Guest User

A guest user is a regular user in a tenant that does not have a home directory associated with it. Therefore, the guest user can only work in the files and folders shared by other regular users. This is the email template that is sent to the guest user when the guest user's account is provisioned.

Email for File/Folder Share

This is the email sent to a user when the user is about to receive file/folder shares.

Request a File

This is the email sent to a user when the user is about to receive an invitation to upload a file.

Notify external user that shared file changed

When a shared file/folder has been modified, this email is sent to the user who receives the shared files/folders.

Admin Reset User Password Email

This is the email that is sent to a user when their password is reset.

User Reset Password Email

This is the email that is sent to a user when the user resets the password for himself/herself.

New Sing-in Action Email

This is the email notification sent to the user when the user logs in from a specific machine.

Settings

This is where the reply email address is set. Normally, the email will be sent using the SMTP service set. However, if the reply address is different, you can set it here.

Cluster Settings

Cluster Settings

The screenshot shows the 'Cluster Settings' page in the Triofox dashboard. The breadcrumb navigation is 'Triofox > DASHBOARD > SYSTEM INFO > CLUSTER SETTINGS'. The page has a trial timer showing '21 trial day(s) left'. The settings are organized into tabs: 'Cluster Settings', 'Performance and Throttling', 'Timeouts and Limits', 'Languages', and 'Change Log'. The 'Cluster Settings' tab is active, displaying a list of 15 settings, each with an unchecked checkbox:

- Hide login failure message details
- Hide build number from login page
- Hide support button (only takes effect after login again)
- Hide 'Forgot your password' link on login page
- Don't retry when login failed
- Always display CAPTCHA on the web portal login page
- Show 'purge storage option' when delete user
- Don't send email notification to user when purge deleted content
- Don't send email notification to admin when purge deleted content
- Retrieve avatar from third party service (ie. Google)
- Hide file extension in web file browser
- Disable Windows Client Auto-Logon
- Allow personal data tagging
- Only allow access performance information from local host

A green 'Help' button is located at the bottom left of the settings list.

Hide Login Failure Message

If this option is enabled, the "Login failed" message will be replaced by a very generic "Login failed" message. If the option is not enabled, a more meaningful login error can be issued, such as user-not-found, authentication-error and so on. This is a security feature if you do not want to reveal too much information so that hackers can guess the reason for the failed authentication.

Hide build number from login page

This controls the build number on the login page of the web portal.

Hide support button

This hides the floating support icon.

Hide “Forgot your password” link on login

This option is most often used when Active Directory integration is enabled. The user then needs to forget and change his password in the normal Active Directory way and not in the way Triofox provides. In this case, it is recommended to hide the "Forgot your password" link.

Don't retry when login failed

This option is often used when the Active Directory user has a low failed-count on lock-out policy. If the user's password is incorrect, a few retries may lock the user's Active Directory account. The retry feature can be used when there is no Active Directory lockout or when the number of lockouts is high.

Show “purge storage option” when delete user

By default, when a user is deleted, the user's home directory storage contents are not touched for later use or review. If it is desired to delete the user's contents when the user is deleted, this can show the purge option.

Don't send email notification to user when purge deleted content

When the user deletes files, they are not actually deleted immediately. The purge is asynchronous and scheduled for a later time. This setting controls the notification.

Don't send email notification to admin when purge deleted content

When the user deletes files, they are not actually deleted immediately. The purge is asynchronous and scheduled for a later time. This setting controls the notification to the administrator.

Retrieve avatar from third party service (i.e. Google)

This is a usability feature that allows the user's image to be retrieved from Google.

Hide file extension in web file browser

This setting hides the file extension.

Disable Windows Client Auto-Logon

This is a security feature. The result is that every time the Windows client is closed, and the user tries to log in the next time, it does not remember the login token and the user must re-enter the credentials to log in.

Allow personal data tagging

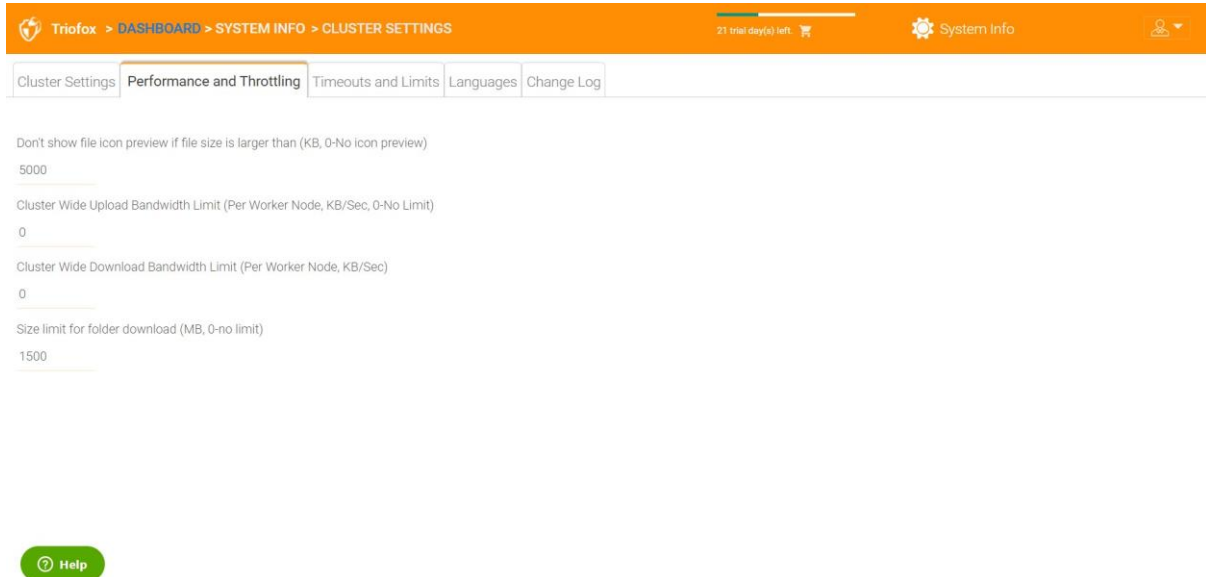
Attach local folder using in place versioned folder.

When synchronizing folders from remote PC/Mac to Triofox, using in place versioned folder will make the folder keep the same folder structure as the folder that is being uploaded. Otherwise, Triofox manages the folder contents on the server side in its own way.

Only allow access performance information from local host

Performance data can only be accessed from <http://localhost> and not from an external URL.

Performance and Throttling



Don't show file icon preview if file size is larger than (KB, 0-No icon preview)

This is used to control the generation of iconview thumbnail in the files and folders view of the web browser. Thumbnail generation takes CPU power from the Cluster Server. For large files, thumbnail generation can affect system performance. Therefore, it is recommended to limit the feature to a certain image size.

Cluster Wide Upload Bandwidth Limit (Per Worker Node, KB/Sec, 0-No Limit)

This limits upload bandwidth.

Cluster Wide Download Bandwidth Limit (Per Worker Node, KB/Sec)

This limits download bandwidth.

Size limit for folder download (MB, 0-no limit)

This is to prevent a user from downloading a very large folder and consuming all the resources of the Cluster Server.

Timeouts and Limits

Triofox > DASHBOARD > SYSTEM INFO > CLUSTER SETTINGS

21 trial day(s) left. System Info

Cluster Settings Performance and Throttling **Timeouts and Limits** Languages Change Log

Web Browser Session Timeout (minutes, 0 - never timeout): 120

Native Client Token Timeout (days, 0 - never timeout): 15

Mobile Client Token Timeout (days, 0 - never timeout): 15

Distributed Lock Idle Timeout (minutes, 0 - never timeout): 15

Send shared file change notification every n minutes(0 - send immediately): 5

Open third party web application in new window when the height of the web browser is less than 0

Max Device Count (Concurrent Device Count) for Each User (0-Unlimited): 0

Purge Device Entry n Days After Device Disconnected (0 - let system decides): 0

Maximum file search results: 25

[Help](#)

Languages

Triofox > DASHBOARD > SYSTEM INFO > CLUSTER SETTINGS

21 trial day(s) left. System Info

Cluster Settings Performance and Throttling Timeouts and Limits **Languages** Change Log

Allowed Languages:

- (Beta) Chinese (Simplified) - 简体中文
- (Beta) Chinese (Traditional) - 繁体中文
- (Beta) German (Switzerland) - Deutsch (Schweiz)
- (Beta) German - Deutsch
- (Beta) French - français
- (Beta) French (Switzerland) - français (Suisse)
- (Beta) Italian - italiano
- (Beta) Italian (Switzerland) - italiano (Svizzera)
- (Beta) Dutch - Nederland
- (Beta) Dutch (Netherlands) - Nederlands (Nederland)

Cluster Wide Default Languages:

⌵

[Help](#)

This section sets up the web portal languages and the client application languages for Windows client. We have automated the translation and provide the resource files that you can use to localize the web portal and clients in the language of your choice.

Change Log

Triofox > DASHBOARD > SYSTEM INFO > CLUSTER SETTINGS

21 trial day(s) left

System Info

Cluster Settings Performance and Throttling Timeouts and Limits Languages **Change Log**

Keep file change log for n days.

15

Email Address to Receive Cloud Monitor Messages:

Logging DB Connection String:

Logging DB Connection String (Read-only Replica):

Keep file change log for n days

This is a cluster-wide retention policy for the file change log.

The file change log resides in the SQL database. For deployments that use SQL Express, there is a size limit on the database. In the deployment guide, there is an option to split the file change log into a MySQL database or into another SQL database. This option is usually used to keep the SQL database size small.

Note

After the Cluster Server has been running in production mode for a while, we recommend that you check the file change log database table and the file index table to see how large these tables are.

Email Address to Receive Cloud Monitor Messages

From time to time, the Cluster Monitor service may send an email about status and alerts.

Logging DB Connection String

This is to split the file change log, device table, file index table, and audit trace table out of the main database and into a secondary database. The secondary database can be a Microsoft SQL Server or a MySQL Community Server.

The Cluster Server database is divided into a core part and a logging part. The core part can store the DB connection string that connects to the secondary database. This setting used to be in the web.config file.

Application Manager

You can also configure web apps under the "Application Manager" tab in Cluster Settings. This allows users to edit documents using the web apps. The apps here apply only to web portal-based editing.

Triofox > DASHBOARD > SYSTEM INFO > APPLICATION MANAGER 21 trial day(s) left. System Info

EDIT

Office Microsoft Office Web App
Microsoft Office Web App (Office Online Server is needed to edit word files)

Office Online Server Access Point (https://myoffice.com)
(Leave it blank to use Office365 online viewer) Not Configured

View only (check if your Web App Server doesn't allow editing)
 Use as default viewer

pixlr Pixlr Web App
 Use as default viewer

ZOHO Zoho Web App
 Use as default viewer

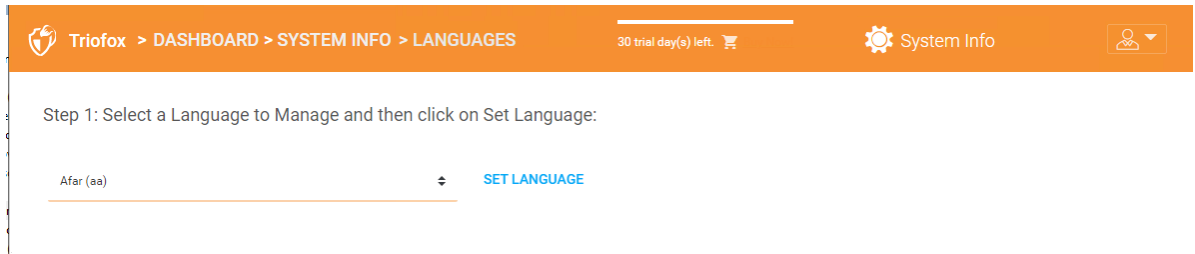
Zoho API Key Not Configured

Help

Once an application is activated, you can see the context menu entry in the web-based file and folder manager view.

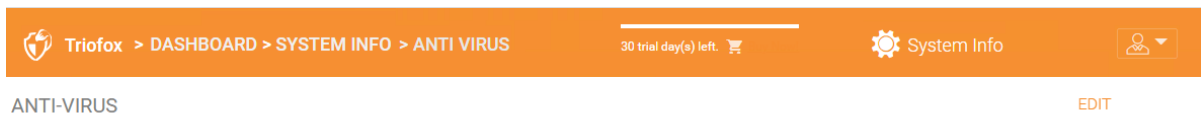
Languages

Under "Languages" you can set the language of your choice.



Anti-Virus

Under "Anti-Virus" you can activate your own Anti-Virus.



Anti-Virus Engine

file being uploaded via worker node will be scanned by the selected anti-virus software)

None

Cloud Backup

Cloud Backup

Note

With Triofox's Cloud Backup, you can turn your Triofox server into a backup appliance or create a self-hosted backup solution with the ability to back up endpoints and restore folder permissions.

In this section, you will learn how to enable backup for file shares and endpoint devices, and how to access and restore the files in the backup.

Enabling Cloud Backup

Cloud Backup is enabled on a cluster-wide basis. Instead of purchasing an expensive backup appliance, your Triofox server takes on the role of the virtual appliance, allowing you to create a self-hosted backup service or use Triofox's hosted environment to secure the offsite copies of your data.

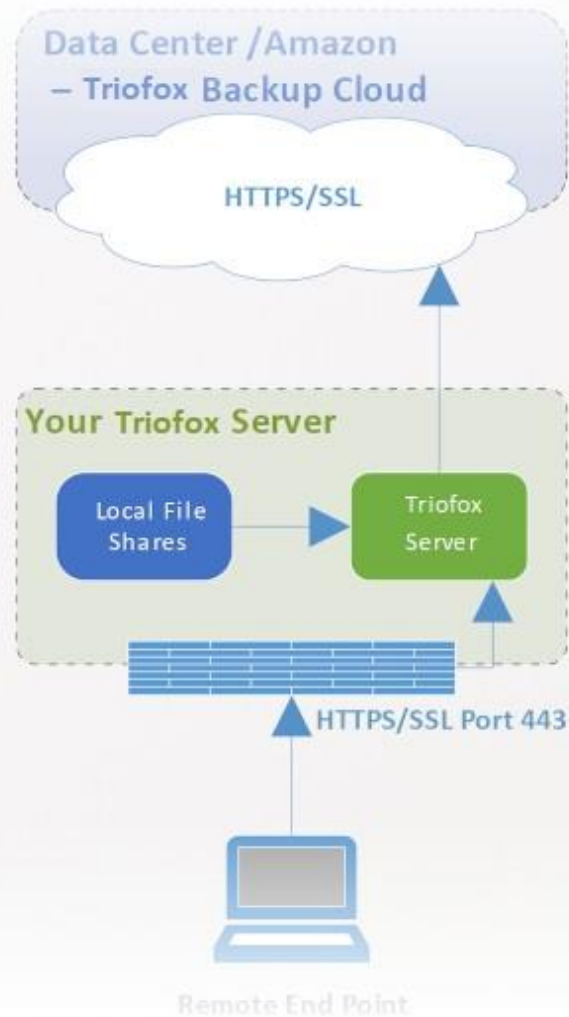
Backing Up File Shares

You can back up file shares from the local file server using your Triofox server as a conduit to the Triofox backup cloud, or you can define your cloud backup destination if you want to use a different storage service.

Backing Up Endpoint Devices

Folders and file shares on remote PCs and servers are backed up using existing Triofox agents to take advantage of existing HTTPS/SSL connections that are rigorously architected to maintain connectivity and reliability.

The following data flow illustrates how the basic architecture functions for this solution works.



Note

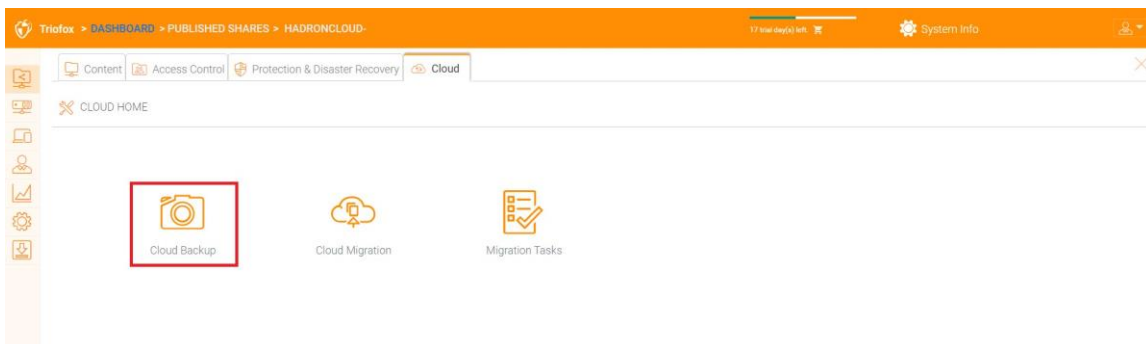
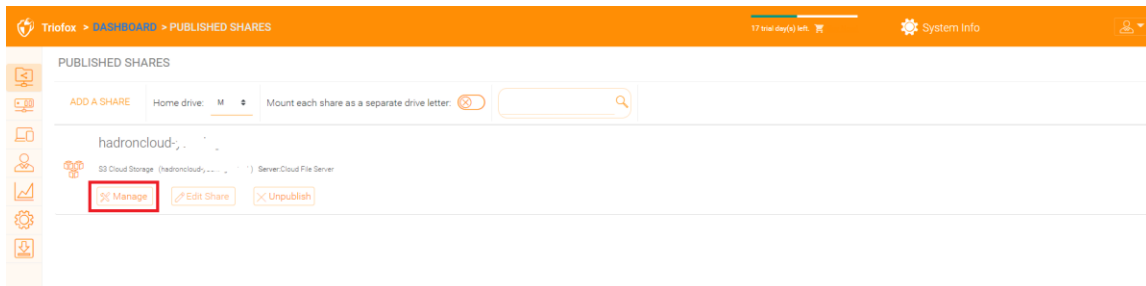
Traditionally, enterprises use on-premises backup appliances to obtain backup sources from servers and desktops on the company network. This is a very secure setup because the backup data resides within the appliance. However, it presents a challenge for remote devices because they are not always inside the company network and the VPN (a virtual private network) of remote devices is not always on to observe certain backup schedules.

On the other hand, cloud backup solutions such as Carbonite and CrashPlan can back up remote devices directly to the cloud, solving the remote backup problem. However, the backup destination is in an opaque location controlled by a third party. This becomes problematic when there are business policies that prevent data replication to third-party controlled locations.

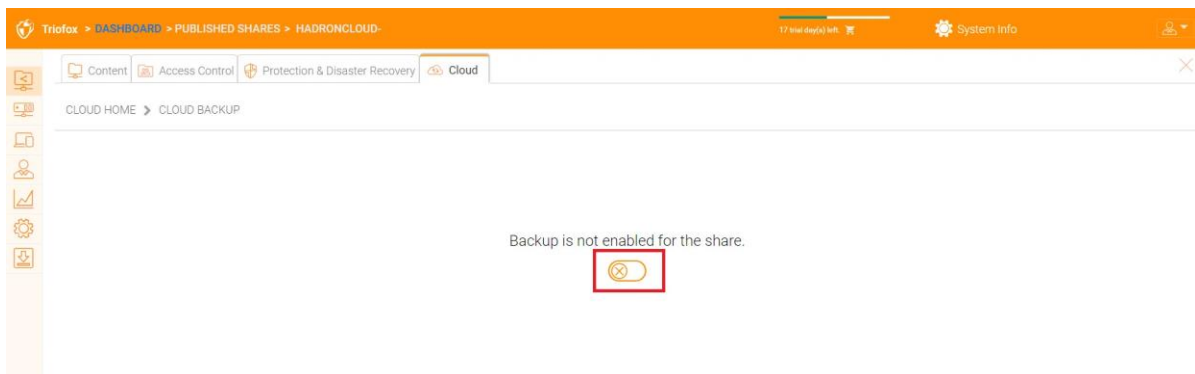
Triofox Cloud Backup solves both of these problems. First of all, the Triofox server maintains the connection to remote PCs and file servers via HTTPS/SSL, so the connection is always on. This means that remote PCs and file servers can always use Triofox's communication channel and data channel to back up via the Triofox backup appliance. And because Triofox's cloud backup is storage agnostic and allows you to back up to a storage service you control, you can now provide continuous backups of your file servers and endpoints to a storage service you control or the Triofox defaults.

Enabling Cloud Backup

Go to Published Shares -> Manage Share and select Cloud Backup.



Then you can enable Cloud Backup by clicking the button below.



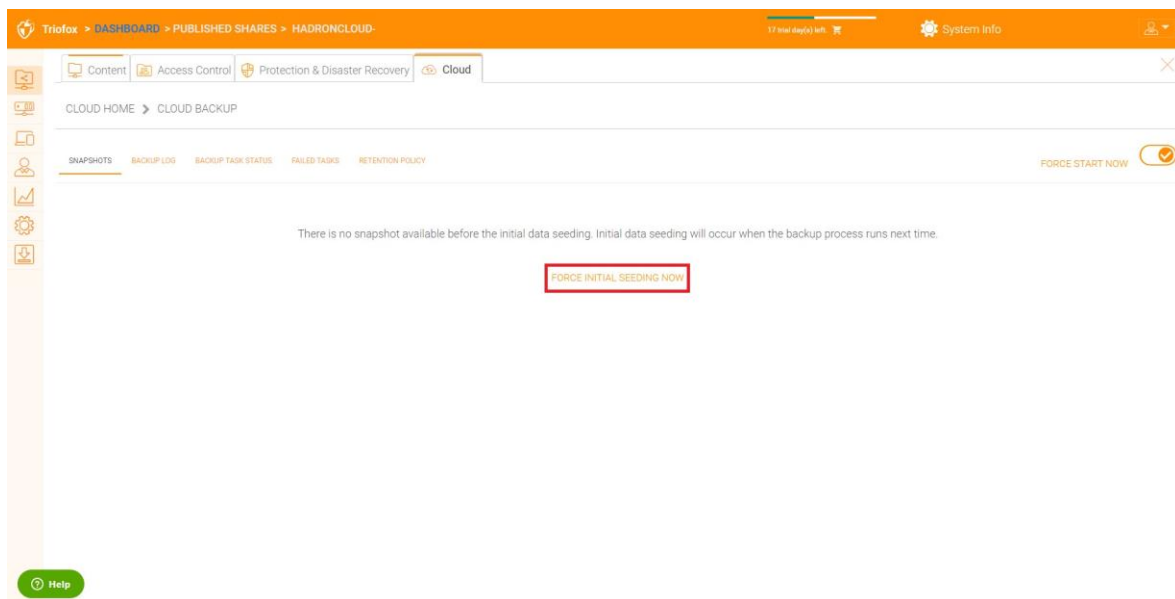
Cloud Backup Settings

Cloud Backup Snapshots

Once enabled, Cloud Backup is stored in snapshots. The snapshot must be initially seeded, and new snapshots are created to capture updates to the data set. The data can be restored from any snapshot.

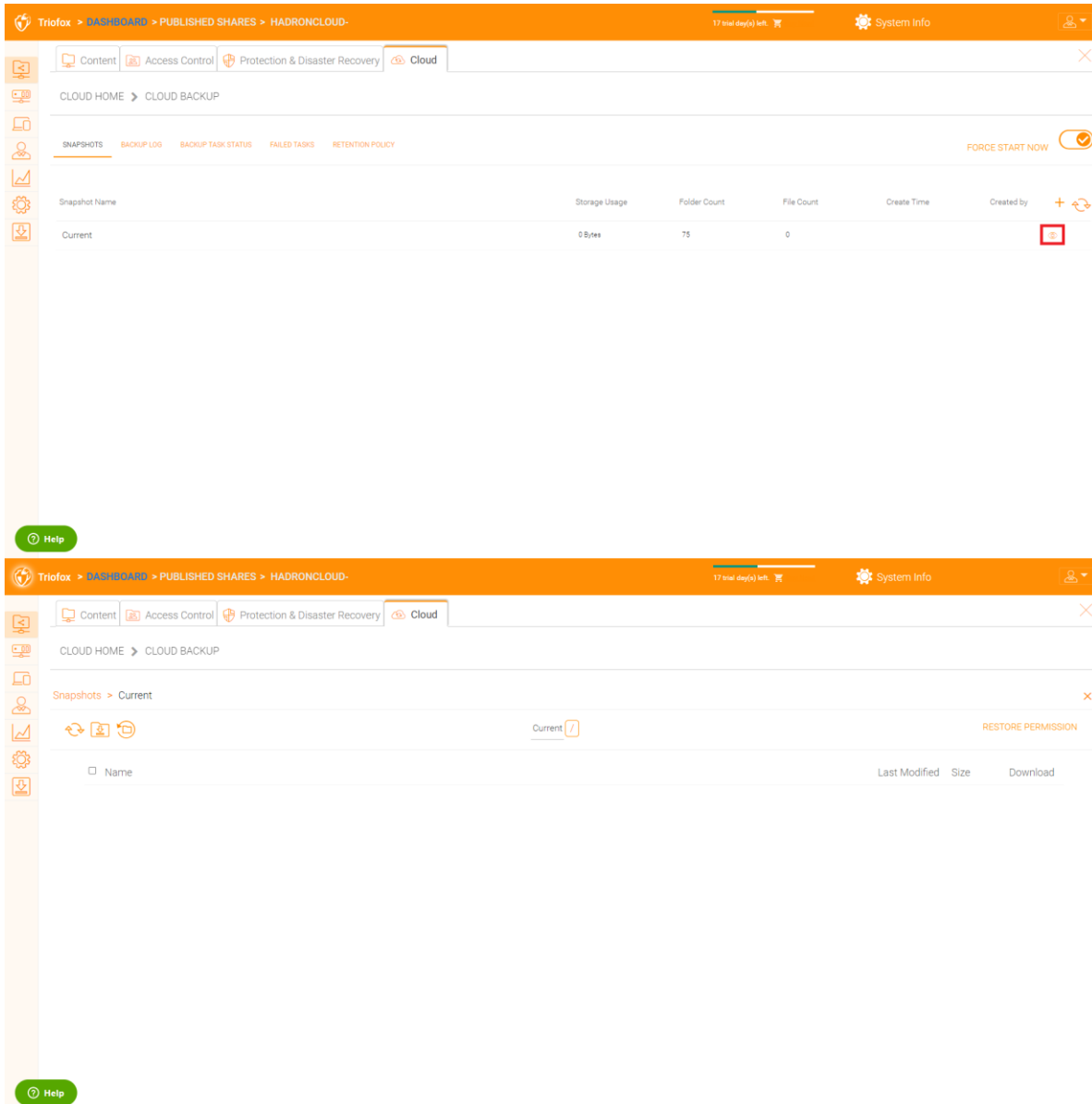
Seeding a Snapshot

Go to Cloud Backup -> Snapshots and click "Force Initial Seeding Now".



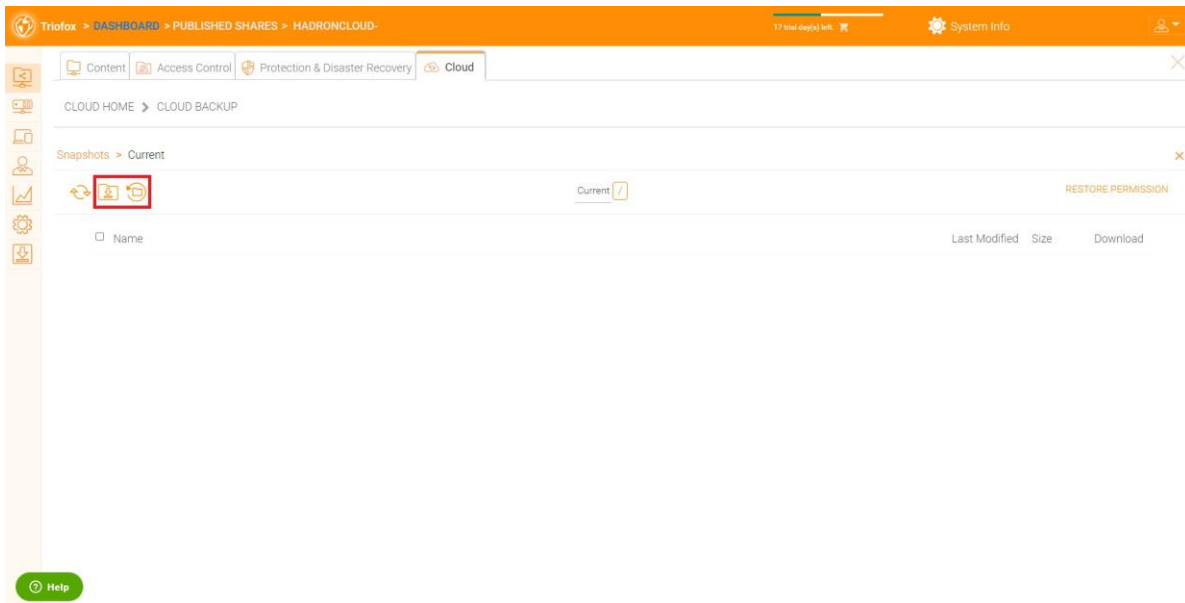
Browsing a Snapshot

To browse a snapshot, click the icon that looks like an eye on the right side of the listed snapshot. You can then navigate through the folder hierarchy in the snapshot to download and restore files and folders using the action icons at the top left of the page. You can use check boxes to filter the list of items to which the action is applied:



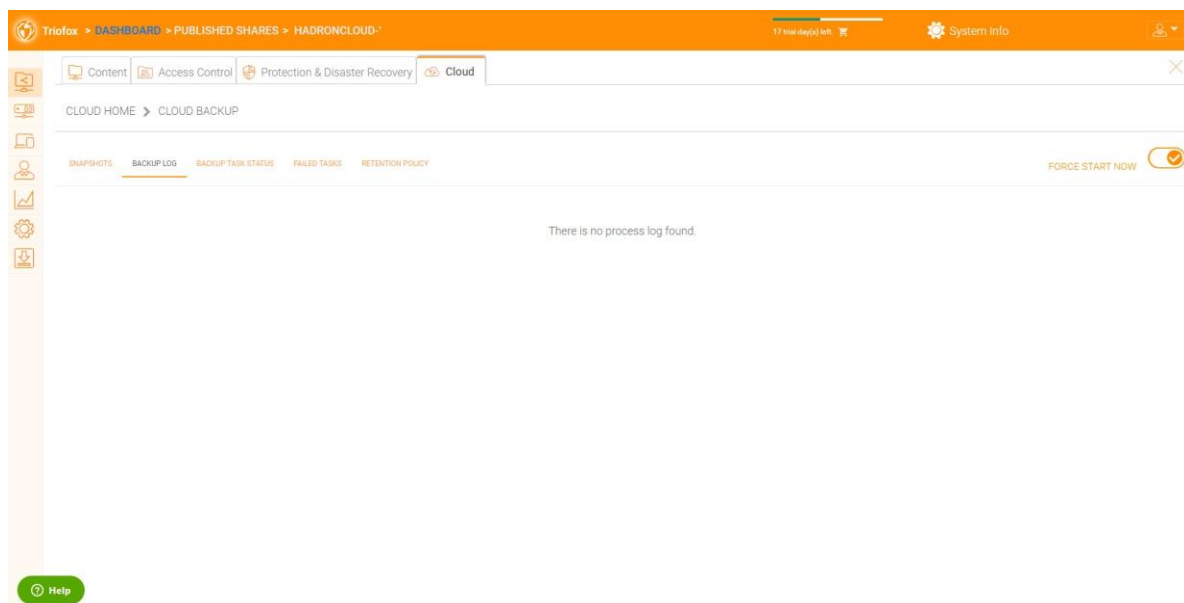
Downloading and Restoring from a Snapshot

For example, in the image below, you can click the highlighted icon to restore the selected items:



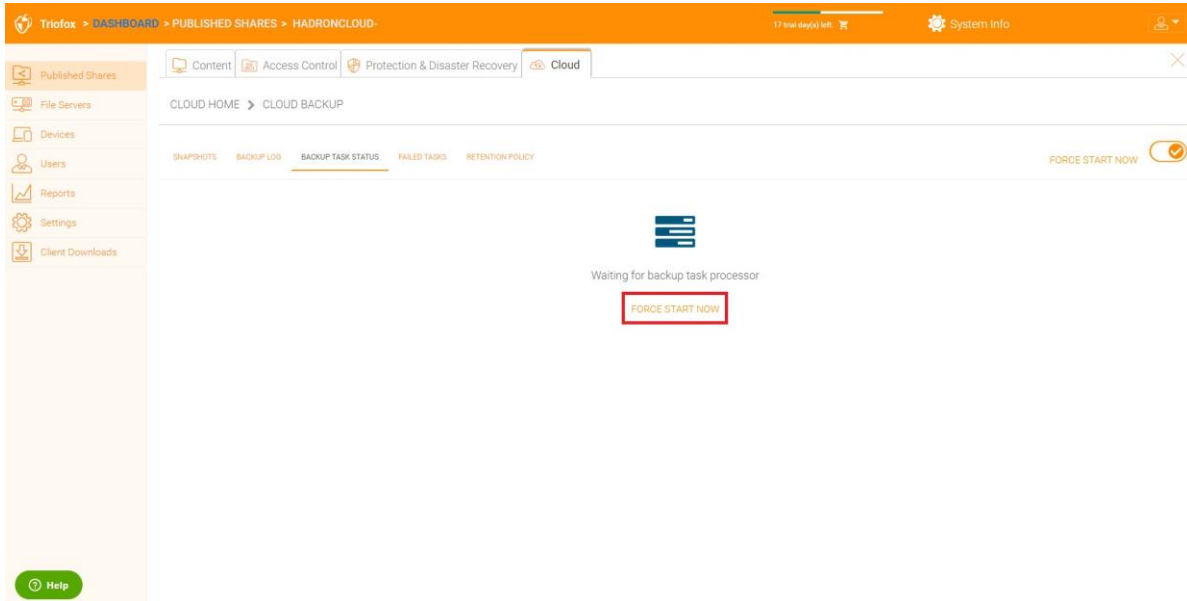
Backup Log

On this page you can browse the backup logs.

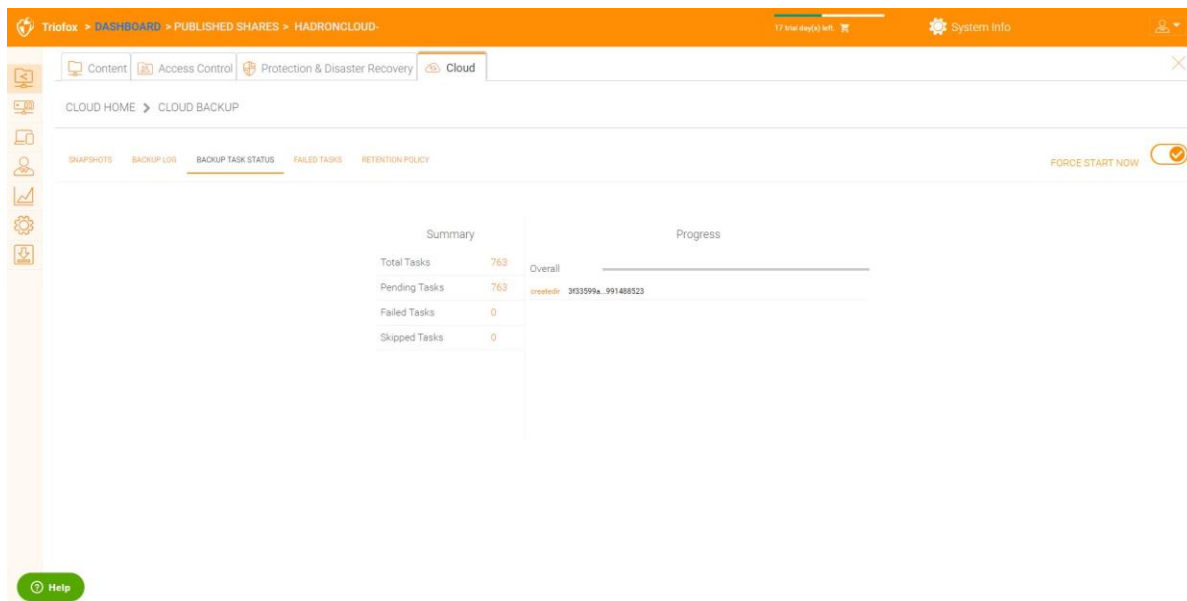


Backup Task Status

You can go to Backup Task Status -> click “Force Start Now” to start backup tasks.

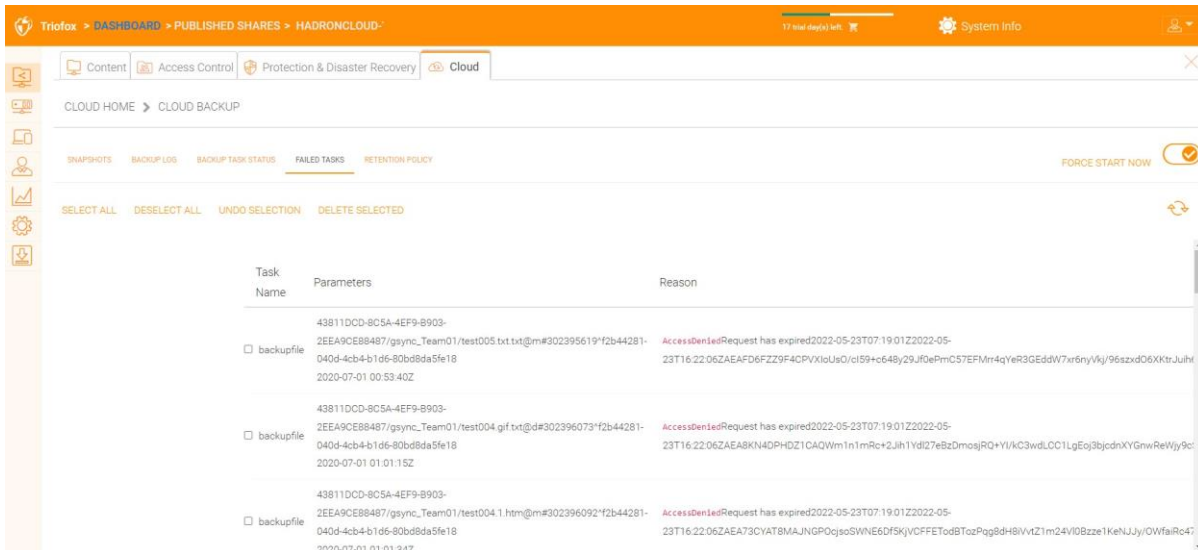


When backup tasks start, you can see the progress bar with progress details.



Failed Tasks

After the backup job is finished, the failed tasks are displayed here and you can manage the tasks.



Retention Policy

There are three retention policies.

"Keep last n snapshots" defines the maximum number of snapshots allowed at a given time. However, this setting can be overridden by the value of "Keep snapshots for at least n days" if it is not 0. For example, you may want to only keep the last 2 snapshots available, but if the system is configured to keep a snapshot for at least 30 days, a daily snapshot could result in 30 snapshots being created before any one is deleted.

