WhiteStar Files

Secure File Transfer

Installation and User’s Guide

Table of Contents

1. Introduction - What is WhiteStar Files (WSF)?

Businesses need to electronically transfer large files that contain highly sensitive information without worrying that the information within those files is being compromised. Illegal appropriation of these files could be highly damaging to a company's customers in addition to causing financial ruin to the company itself. Today's businesses are forced to utilize extremely inefficient manual means, such as physically breaking files up on to numerous disk drives and transporting them by hand or compromising security by transferring them with legacy solutions that have known exploits and vulnerabilities. Likewise, most current tools are either limited in the size of files they will transfer or work so slowly that they become prohibitive to be productive.

Standard file transfer tools, such as Secure Copy (SCP), require user accounts to be created, holes in firewalls to be configured, and have inherently slow transfer rates with limitations on file sizes. Cloud-based transfer tools have less limiting file size restrictions but require an intermediary step of storing files in the Cloud - increasing the surface area of attack to hackers (and also assume the cloud-based provider deletes these files after the transfer completes). While there exist some peer-to-peer VPN solutions, they are extremely slow, difficult to setup and maintain, and do not provide the required flexibility that businesses require, especially in a mobile environment. Likewise, manual "sneaker-net" solutions are extremely expensive and require a high degree of trust in the individuals transporting the data.

Additionally, legacy tools offer no ability to audit the path of each file, with integrated meta-data monitoring tools. This becomes especially important with data compliance regulations, where each and every person who interacts with that file needs to be accounted for, along with where that individual file goes. Having integrated sensors built into your file transfer system protects against potential data compliance issues.

Therefore, there is a need to move high value files efficiently and securely, preventing exposure to data leaks or hackers; and to do it all at a low cost. Additionally, these files need to be able to be sent anywhere in the world, without leaving data on any intermediary servers, as they make their way from source to destination.

WhiteStar Files is our solution to the problem. It utilizes full end-to-end encrypted file transfers, to and from virtually any device, anywhere in the world, with security natively built in. It runs on our hybrid peer-to-peer WhiteStar Network which operates as a "Network as a Service" for secure applications. Equally important, file transfer speeds are similar to local file transfer rates but traverse the network in such a way as to be completely impervious to interception. Files transfer from point-to-point with no intermediate file retention, with built in fault tolerance should the link fail, preventing the need to resend the entire file. WhiteStar Files also integrates the WhiteStar Sensor Suite allowing users to monitor/visualize the movement of files as they traverse the WhiteStar network.

2. WSF - Solution Overview

WhiteStar Files is comprised of**:**

Administrator's Dashboard - a web-based console used to manage your WSF licenses plus grant and revoke access to members of your team (providing them with the proper credentials to connect to remote WSF servers). Additionally, the Dashboard integrates control of the servers, as well as the WhiteStar Sensor Suite.

WSF Client - a secure file transfer application that interfaces directly with the WSF Server service running on remote devices. The WSF Client allows transparent access to devices running locally within your intranet or remotely (via the internet) to any device the client has been granted access to. Once transfers are complete, the user simply exits from the WSF Client application and all secure network connections are torn down automatically.

WS Stardrop - a secure file transfer application that interfaces directly with the WSF Server service running on remote devices. Stardrop allows both IOS and Android mobile devices the ability to transfer files (one way) directly to WSF Servers they have been granted access to. Once transfers are complete, the user simply exits from the WS Stardrop application and all secure network connections are torn down automatically.

WSF Server - a secure service that executes on a device where files are being transferred from or to. This service provides the WSF user a secure interface between the Server device and the user's Client application. The WSF Server can be started and stopped, as needed, providing the Server device administrators the ability to enable/disable remote WSF access on demand. Depending on the customer's procedures for external access to their devices, their administrators may want to keep this service stopped and *only start it when file transfers are required on a particular device*.

WhiteStar GTS Database – an optional addition to the WhiteStar Files ecosystem, the GTS is a database that automatically privately tabulates information about the traffic on your WhiteStar Files deployment. The GTS makes metadata about transfers moving over the network searchable to your organization by way of a specific read key.

WhiteStar Sentinel Malware Protection – An optional addition to the WhiteStar Files ecosystem, Sentinel automatically detects malware embedded in files moving over your Files deployment and enacts various resolution methods like quarantining or sanitization. Sentinel is also capable of redacting PII and other sensitive information to ensure private information stays private.

Figure 1 illustrates a basic representation of how WhiteStar Files Client users connect to WSF Server devices (both on the same intranet and seamlessly through firewalls and the internet).

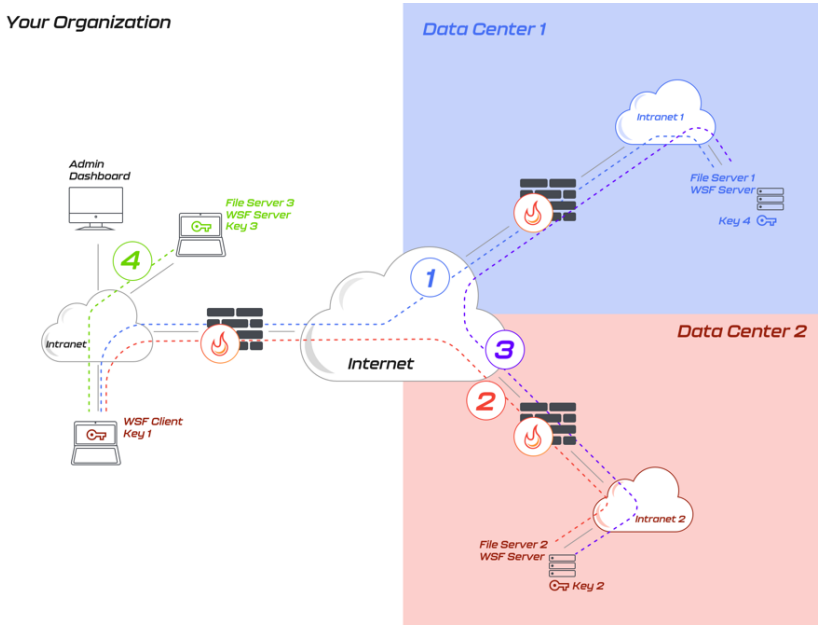


Figure 1

As illustrated above, the WSF client can transfer files to and from devices within its own intranet (#4), to and from devices across the internet to itself (#1 and #2), and between two different devices (at two different data centers - #3) – all from the same WSF client.

2.1. Teams – Subdividing Teams

Customers typically only allow "specific" users with WSF Clients access to transfer files to and from one of their server devices. The WSF system fully supports this concept by providing the administrator with the ability to grant access to a single user or sub-divided members within an organization into **Trusted Teams** dedicated to accessing specific server devices.

Take, for example, an organization with four (4) WSF users. The administrator may want to grant access to individual users to transfer files (and connect to) individual server devices or create a small **Trusted Team** of WSF users permitted to a transfer to/from a specific set of server devices. They may also want to have a *generic Trusted Team made up of all WSF users* who can connect to any Server devices. Figure 2 illustrates an administrator who has created three (3) teams [this is done by assigning a **WhiteStar Trusted Team Tag** – or multiple Trusted Team Tags – to their WSF Client users]. How to accomplish this is discussed later in this document.

- **Trusted Team #1** (Purple: with 2 WSF Client users) has been established to connect to and transfer to/from a single "Purple" server device at Data Center 1 by both Client users.
- **Trusted Team #2** (Green: with 3 WSF Client users) has been established to connect to and transfer to/from "Green" server devices at all 3 Data Centers. Note that Client #'s 1

and 2 are members of both Team #1 and #2 and therefore can connect and transfer files to/from any “Green” and “Purple” devices in all Data Centers.

- **Finally, Trusted Team #3** (Red: with only 1 WSF user) has been established to connect to and transfer to/from a single “Red” server device in Data Center 3.

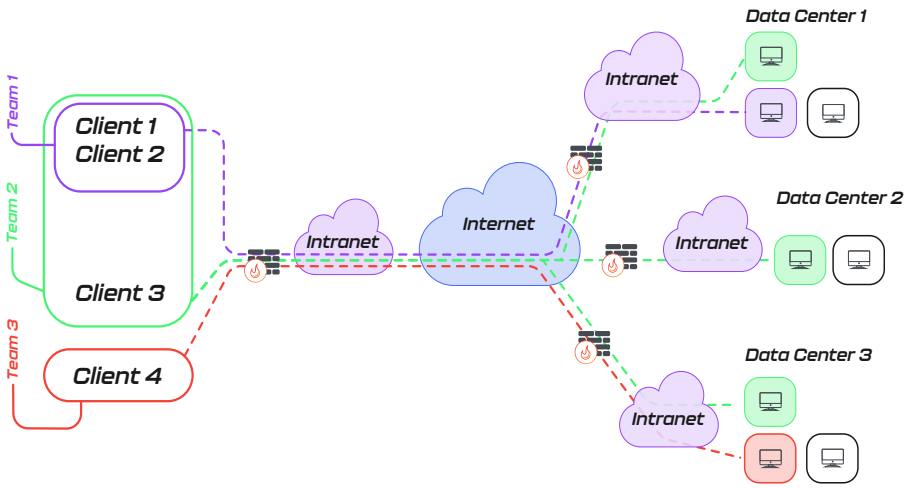


Figure 2

Note: the administrator creates Trusted Teams Tags (Tags) on their **[WhiteStar Administrator Dashboard]** by assigning WhiteStar Trusted Team Tags to their users to delineate which Trusted Team(s) they are a member of. For a customer to grant access to a WSF Server device, they must log on to the particular device and grant access (e.g. via their Server interface) to the corresponding WhiteStar Trusted Team Tag which represents the Trusted Team they want access granted to.

3. Minimum System Requirements

3.1. Software

3.1.1. WSF Client

- Windows 10 or higher
- Mac OS 10.9 or higher
- Red Hat Enterprise Linux 8 or higher
- CentOS Stream 8 or higher
- Debian 10 or higher
- Ubuntu 18.04 or higher
- Rocky Linux 8 or higher

3.1.2. WSF Server

- Windows 10 or higher
- Mac OS 10.9 or higher
- Red Hat Enterprise Linux 8 or higher
- CentOS Stream 8 or higher
- Debian 10 or higher
- Ubuntu 18.04 or higher
- Rocky Linux 8 or higher

NOTE: You must have Telnet installed and enabled on your device in order to properly interact with a WhiteStar Files Server. If your device does not have Telnet installed, or it is not enabled, please follow your operating system's instructions on installing or enabling Telnet in order to interact with the WSF Server.

Customized WSF Server implementations for devices (other than Linux based systems) are available upon request. Please reach out to WhiteStar Communications to investigate how we can assist you with these at ***info@whitestar.io***.

3.2. Hardware – WSF Client

Operating System	Minimum Requirements
Windows OS	• 1 Ghz or faster processor with 2 or more cores (64 bit compatible) • 4 GB RAM • 64GB or larger storage device
MAC OS * * *Both* X86 and Apple Silicon where applicable	• 1 Ghz or faster processor with 2 or more cores (64 bit compatible) • 4 GB RAM • 64GB or larger storage device

Linux flavors	• 1 Ghz or faster processor with 2 or more cores (64 bit compatible) • 4 GB RAM • 64GB or larger storage device

4. The WhiteStar Administrator Dashboard

The WhiteStar Administrator Dashboard is the interface a company uses to allocate application subscriptions to WhiteStar Files users, create and assign WhiteStar Trusted Team Tags (which provide access for WSF Client users to WSF Server devices), and maintain the company's profile information. A WhiteStar Trusted Team Tag is the company's "***token***" to gaining access to specific WSF Server devices and must be assigned to individual WhiteStar Files Client users in order for them to be granted access to a Server device.

To access the Administrator Dashboard, a designated company administrator must visit the WhiteStar Communications website at **https://www.whitestar.io** and click the "***Sign In***" button at the top right hand corner of the web page (see Figure 3).

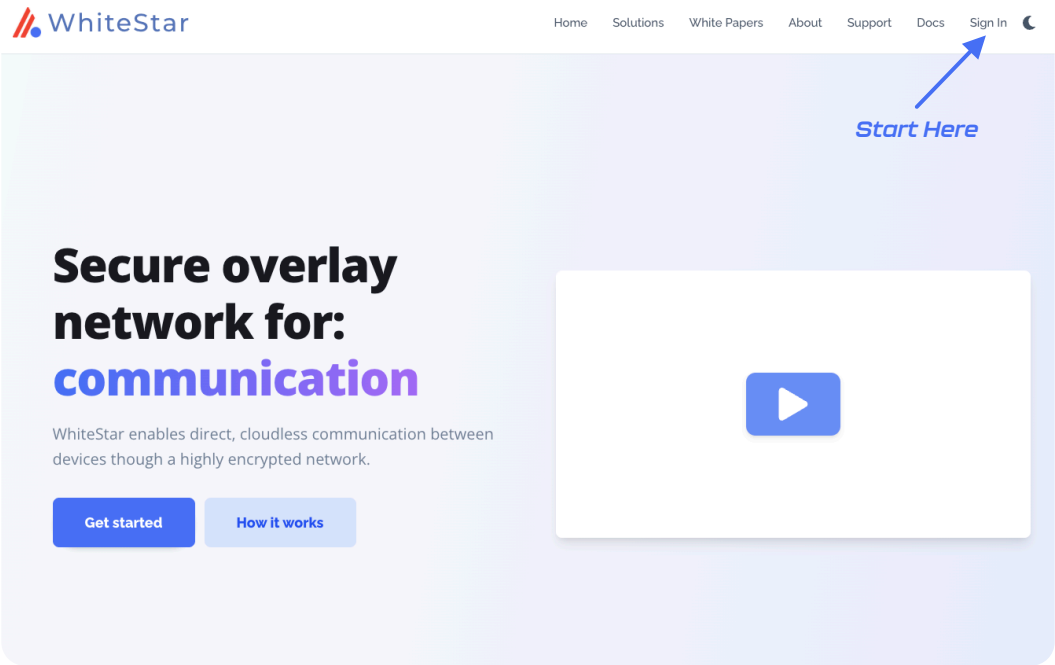


Figure 3

After clicking "***Sign In***", the administrator is presented a screen prompting them to log in (see **Error! Reference source not found.**). If they already have a WhiteStar administrator account, they can enter their email address and password information and hit "***Continue***", or they can click on "***Continue with Google***" to use Sign in with Google (Google Single Sign On (SSO)). If an account has not been established for the admin, they can sign up by clicking the "***Sign Up***" link on the screen. For additional details on obtaining an administrator's account, please refer to section 5 below.

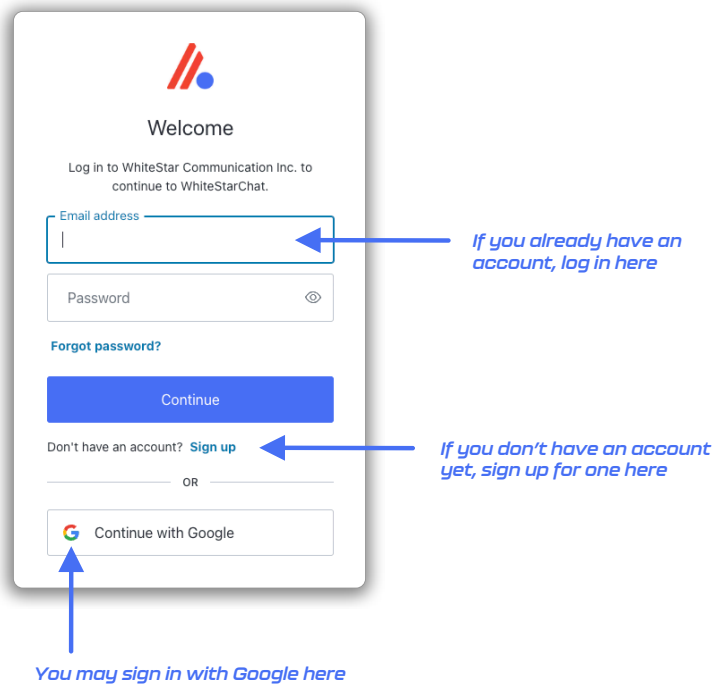


Figure 4

NOTE: If you have been assigned administrator credentials for more than one organization, you must use the drop down list on the top left hand side of the administrator's panel to select the proper organization you currently want to administer (see Figure 6).

4.1. Administrator Dashboard - Orientation

Once successfully logged in, the administrator sees their dashboard (see Figure 5), which has multiple functions. The lefthand column of the ***Administrator Dashboard*** is used to toggle the main functions of the page: (1) manage users (WhiteStar Files users who are utilizing the WhiteStar Client application), (2) view billing information, and (3) view company profile information.

The middle section of the page provides a summary of the total number of licenses that are available, who they are assigned to, options to bulk upload or add individual users, and assign Trusted Team Tags to users.

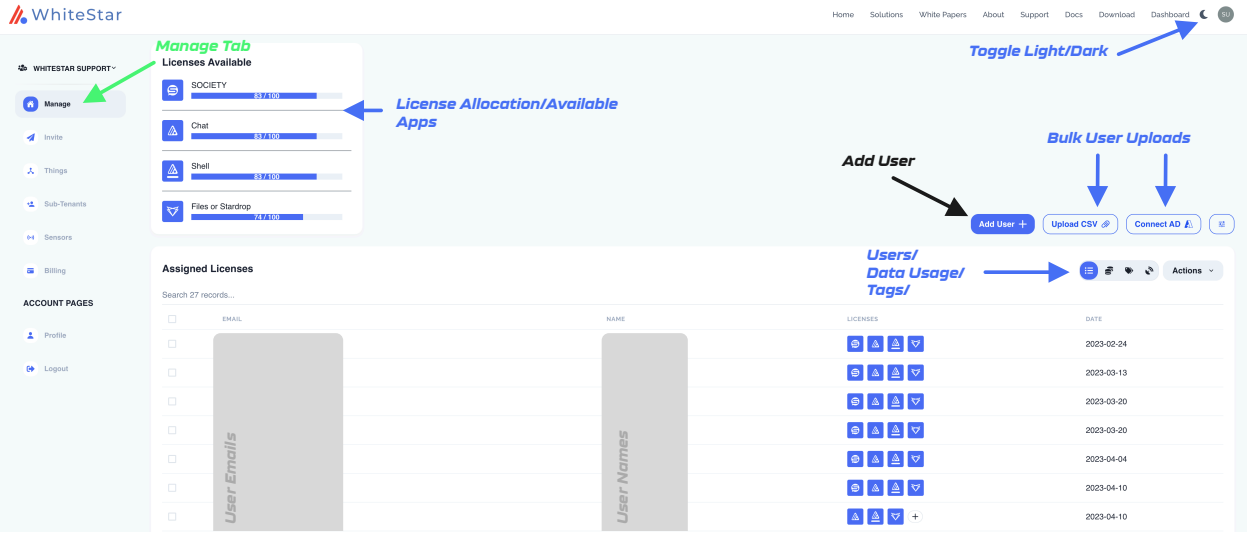

WhiteStar
Home
Solutions
White Papers
About
Support
Docs
Download
Dashboard
Manage Tab
Toggle Light/Dark
WHITESTAR SUPPORT
Manage
Invite
Things
Sub-Tenants
Sensors
Billing
ACCOUNT PAGES
Profile
Logout
Licenses Available
SOCIETY
Chat
Shell
Files or Stardrop
License Allocation/Available Apps
Bulk User Uploads
Add User
Add User
Upload CSV
Connect AD
Users/ Data Usage/ Tags/
Actions
Assigned Licenses
Search 27 records...
EMAIL
NAME
LICENSES
DATE
User Emails
User Names
2023-02-24
2023-03-13
2023-03-20
2023-03-20
2023-04-04
2023-04-10
2023-04-10

Figure 5

5. Signing up for an Administrator Account

If you have not already signed up for a WhiteStar Administrator's account to administer your organization, you will need to prior to doing anything else. When signing up for a WhiteStar Administrator Account, the user has two options to create their account:

1. Enter an email address and password (which must be verified) OR
2. Log in with Google

If option #1 is chosen, the user enters their email address along with a ***strong*** password (see Figure 6). Once the information is entered, click the "***Continue***" box.

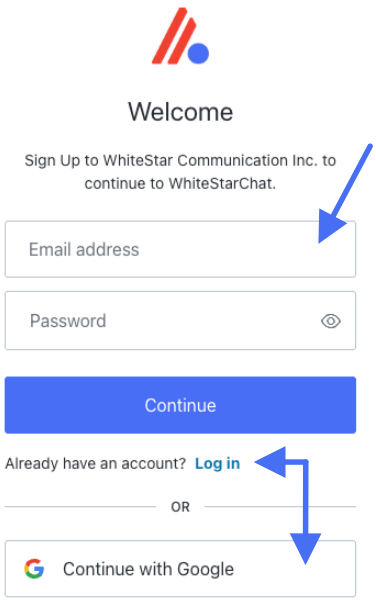


Figure 6

A verification email is sent to the address provided in order to verify ownership (see Figure 7).

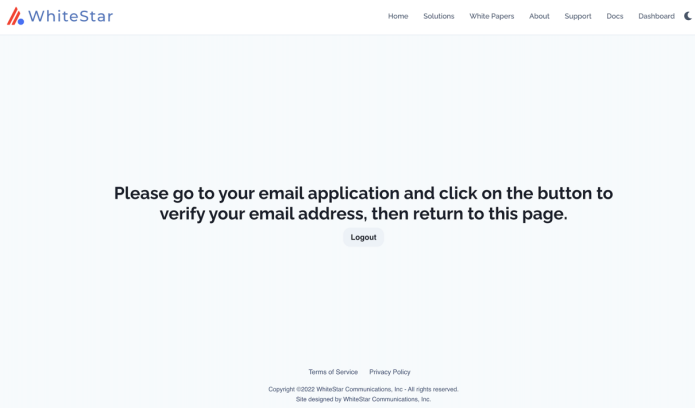


Figure 7

Go to your email application and click on the appropriate button (see Figure 8) to verify your email. If this step is not executed, the administrator account will not be created.

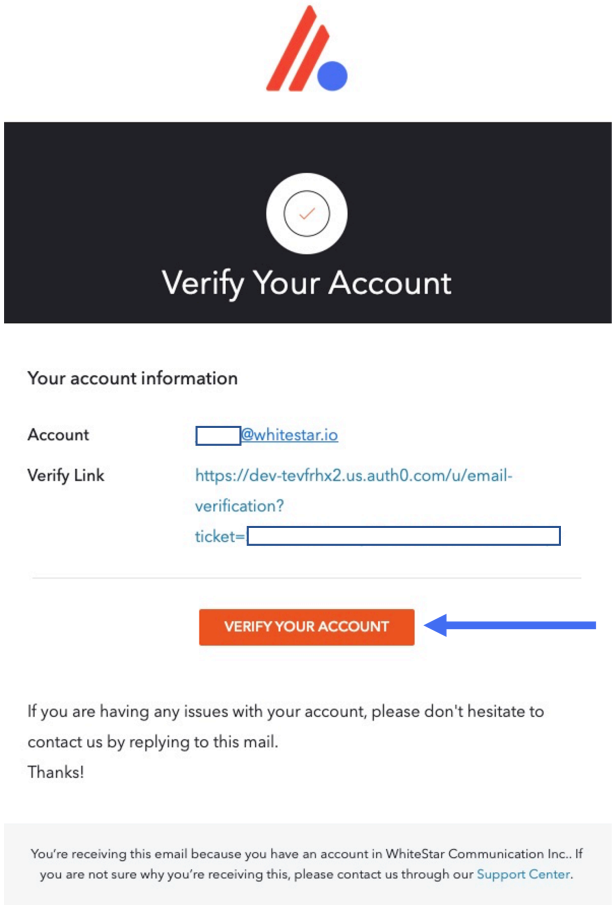


Figure 8

When creating a password for a WhiteStar Administrator Account, *please use good security practices*. It is suggested that the password be *at least* 8 characters in length, of which three characters ***must*** be an uppercase letter, a number, and a special character. This will help to protect your password from intrusion.

If option #2 is chosen, simple log in with your Google credentials and you will be brought directly to the Administrator dashboard.

Note: WhiteStar ***<u>does not store your password anywhere</u>***, and you are responsible for the safe storage of your password. You may consider using a quality password manager to store your WSF password. If you lose your password, you must zeroize, or reset, your WSF Client and rebuild your user identity from scratch.

5.1. Adding New WhiteStar Files Users

5.1.1. Add an Individual User

To add, or assign a license for an application for a new user or team member in your organization, click on the ***"Manage"*** link in the left column of the main administrator web page and then click on ***"Add User"*** in the main body (see green arrows in Figure 5). This allows the administrator to authorize WhiteStar Files users to use the WhiteStar Files Client application (by adding their email address to the list of authorized members of an organization). The WhiteStar Files users themselves use their email address during the WSF Client installation process to activate this license.

After clicking on "***Add User***" in the main screen, the "***Add New User***" screen is presented to the admin. The only required field on this panel is the email address, but it is highly recommended that the WhiteStar Files users name be entered as well. Once the information is entered, click the "***Submit***" button (see Figure 9).

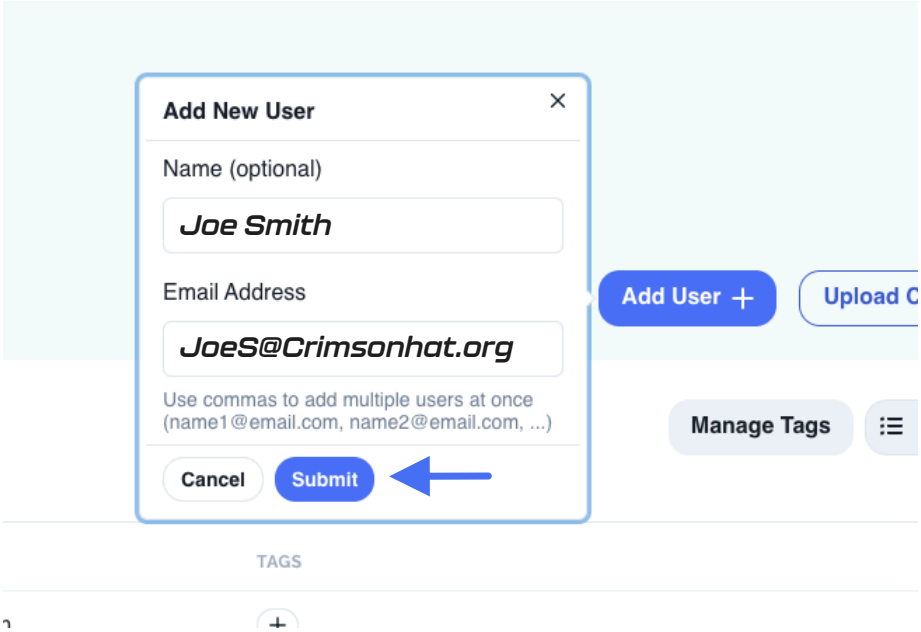


Figure 9

The administrator is then prompted to assign an available license to this new user (see Figure 10). Click "***Okay***" to assign the license.

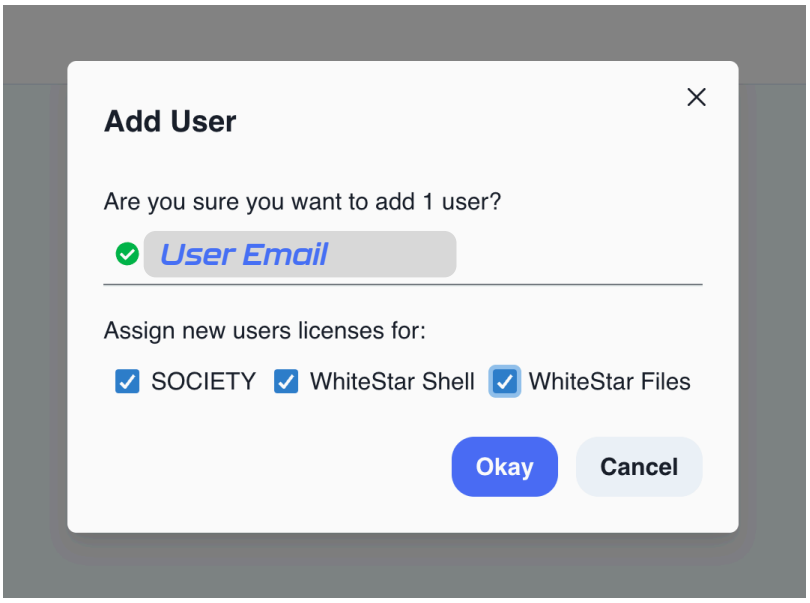


Figure 10

Check the boxes for the WhiteStar applications being assigned to the user. Depending on which WhiteStar application(s) your company has purchased, you may see one or more applications available for selection on the screen.

Prior to assigning licenses to your users, ensure your WhiteStar account has enough available licenses for each application. The main screen under "***Manage Users***" indicates your current and available-to-be-assigned license count for each of your WhiteStar applications (see Figure 11).

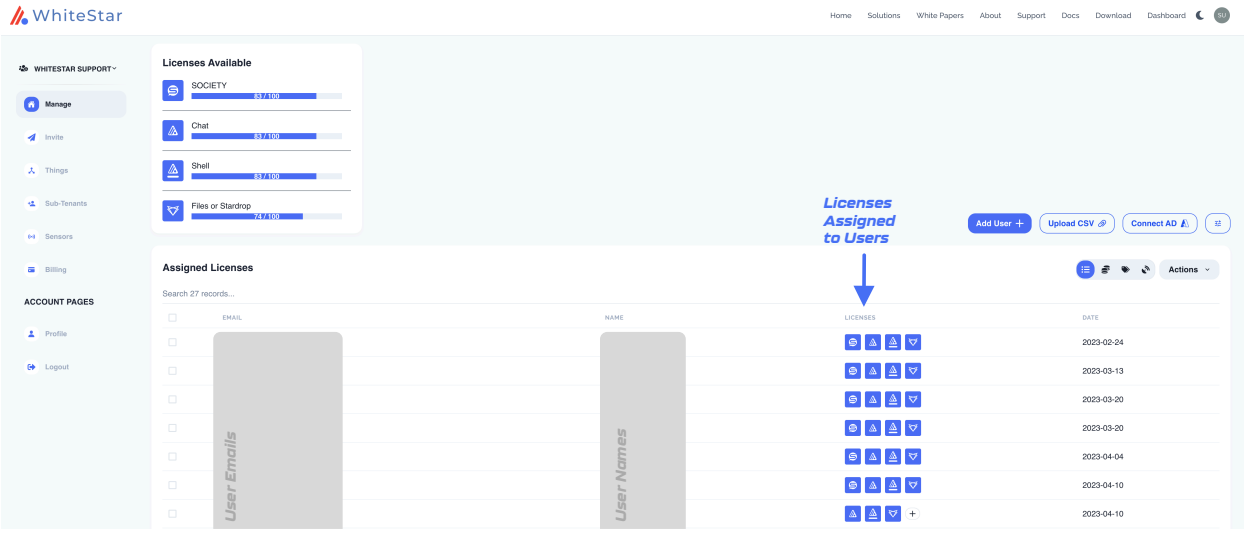


Figure 11

If the administrator wants to bulk upload new WhiteStar Files users into the dashboard, there are two ways to achieve this: (1) via upload of a ***CSV file*** or (2) via direct access to your ***Active Directory*** (AD) server.

5.1.2. Add Users via bulk Upload CSV (Comma Separated Values)

To add a list of users via a bulk CSV upload, click on the "***Upload CSV***" on the main Dashboard screen. The administrator is presented with the appropriate file picker for their operating system to choose the file, from the hard drive, they want to have uploaded.

The only column that is required in the CSV file is the support user email addresses. Administrators may optionally include the WhiteStar Files users' names and/or tag names that should be assigned to each user (these should match the names of existing tags that have been created, separated by commas). Inclusion of a header row in the CSV is optional. Once the CSV is uploaded, the administrator is presented with a preview of the uploaded data and asked to select which column corresponds to which field: ***Email, Name, and Trusted Team Tags***. Current column assignments can be seen in the first row of the preview table.

The administrator is prompted first to select the Email column. If the default selection is incorrect, the administrator may tap on the correct column in the preview table to re-select it, otherwise they may simply press the **"*Next*"** button to continue. This process may be repeated to select the column corresponding to the Name and Trusted Team Tags fields on the subsequent steps. The user may simply press **"*Next*"** to skip these steps if the fields are not included in the CSV upload. Once all three fields have been assigned to their corresponding columns, the user may press **"*Submit*"** to continue the bulk license assignment (see Figure 12).

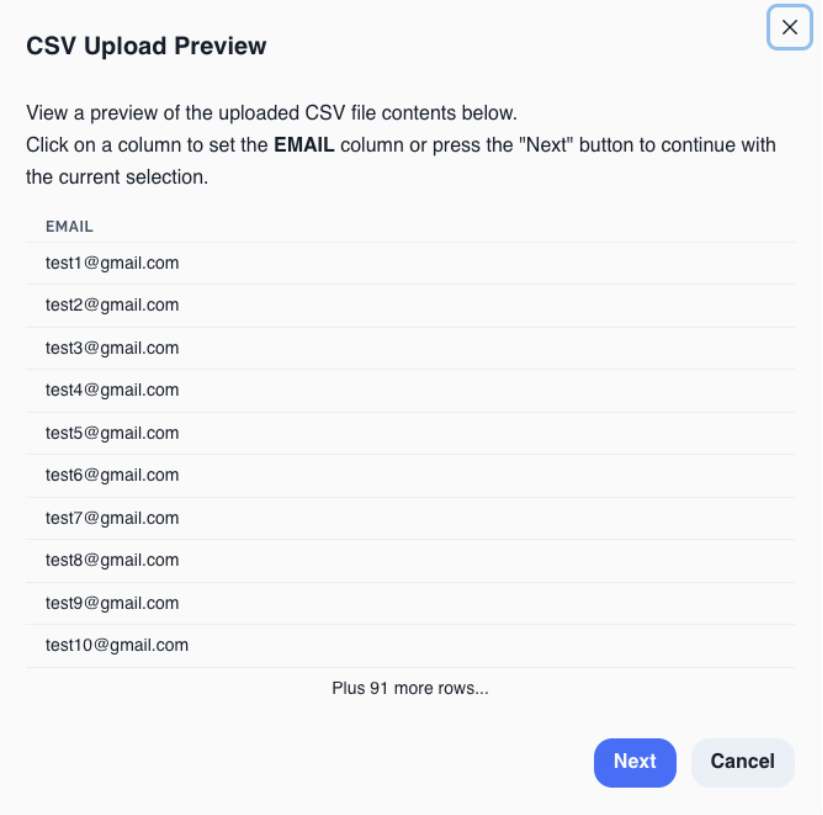


Figure 12

After the administrator clicks "**Submit**", they are presented with a list which summarizes the information that has been read in from the CSV file (see Figure 13). The list is broken down by:

- The top list shows the email addresses that are in the CSV which are new to the system (need licenses) **and have available licenses** ready to assign to them (green circle checks).
- The second list are email addresses that are in the CSV file, new to the system, need a license but will **exceed the current total licenses available** to assign (red exclamation point circle). The email addresses are added, and licenses assigned, but you need to increase your account licenses in the next billing cycle.
- The third list are email addresses in the CSV file which **already have a valid assigned license** in the system (yellow exclamation point).
- Finally, the administrator is told the total number of email addresses that have licenses assigned to them in the system **but were *not* present in the CSV file**. The administrator can either have the system delete these email addresses during this process (toggle on) or leave the toggle off and retain those email addresses (and licenses being assigned) in the system.

Figure 13

Once the administrator is satisfied with the list presented, click the "***Okay***" button to execute the upload and save the changes.

5.1.3. Add Users via bulk Upload Active Directory (AD)

This feature is currently under development and is in ***Open Beta***. WhiteStar supports a bulk upload of users via an Active Directory integration. Please click the "***Connect AD***" button on the Dashboard and follow the on-screen prompts to upload users from AD.

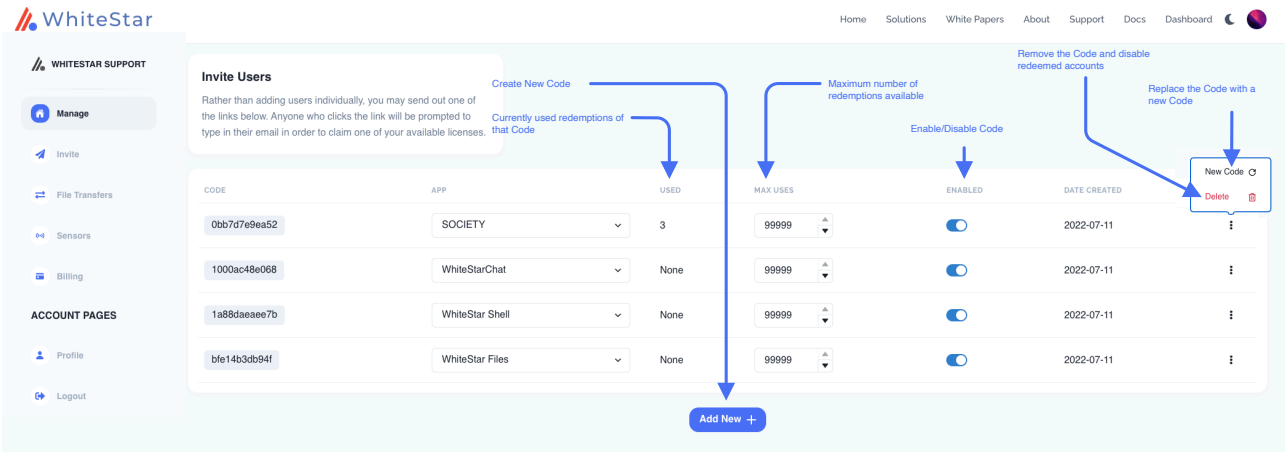


Figure 14

The administrator can also add new users via the Invite tab on the side of the Dashboard. On this tab Administrators can generate a claim code which can be redeemed for a WhiteStar subscription. Generate a new code using the "***Add New +***" button on the bottom of the Dashboard, which will generate a new code. This code has a settable number of redemptions, which Administrators can set using the "***Max Uses***" counter. Enable and disable the code from being redeemed using the toggle. Additionally, if you need to replace the code with a new number, you can do so by clicking the ellipses (**…**) button on the right-hand side of the screen and selecting "***New Code***".

If you want to remove the code entirely, the same ellipses menu has a "***Delete***" button that will remove the code from the Dashboard. If the Administrators have users who have claimed a code that they then delete, those users will stay subscribed. If the administrator needs to remove those users from the corporate WhiteStar account, the administrator may do so under the "***Manage***" tab.

5.2. Removing a User from the System

If the administrator needs to remove a user from your organization (and zeroize the information on their device), they must log into the WhiteStar Administrator dashboard, click on "***Manage***" in the lefthand column, and then click the check box next to the user(s) they wish to delete/zeroize. The administrator must then click on the "***Actions***" button and selects either "***Remove Selected***" (to delete the user from the system and free up their license) or "***Zeroize Selected***" (to delete the user from the system, free up their license, and delete all the WSF Client data from their device). If "***Zeroize Selected***" is chosen, a confirmation screen is presented (see Figure 15) to ensure this is the action the administrator truly wants taken. Understand that any user zeroized will have ALL of their locally stored WSF Client information, and any network connection information, ***deleted permanently***. Zeroization cannot be undone, but the administrator can always set up a new account for that user if needed.

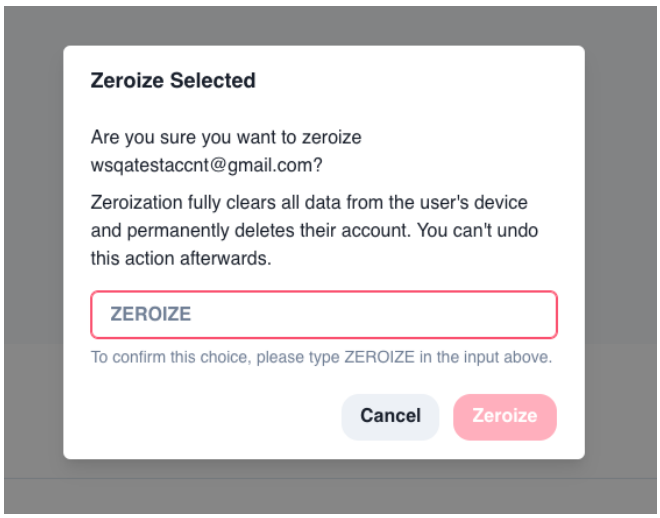


Figure 15

Zeroization is useful if a user forgets their password; their user account can be zeroized and set up again from scratch - note that within WhiteStar, passwords are ***never*** stored in a centralized repository, ***nor*** can Administrators reset user passwords (this is for security purposes, as it prevents malicious actors from tampering with other user's credentials).

5.3. Sub-Tenants

On your WhiteStar Dashboard, you may find that you need to administer your WhiteStar Applications differently for different clients. By going to the Sub-Tenants page on the left-hand side, you can create new Organizations, or Sub-Tenants, which you can control individually. This allows you to silo each Sub-Tenants assets individually for organization and information hygiene purposes. After creating a new Sub-Tenant, you will see that new Sub-Tenant listed under the organizations drop-down on the upper left-hand side of the screen.

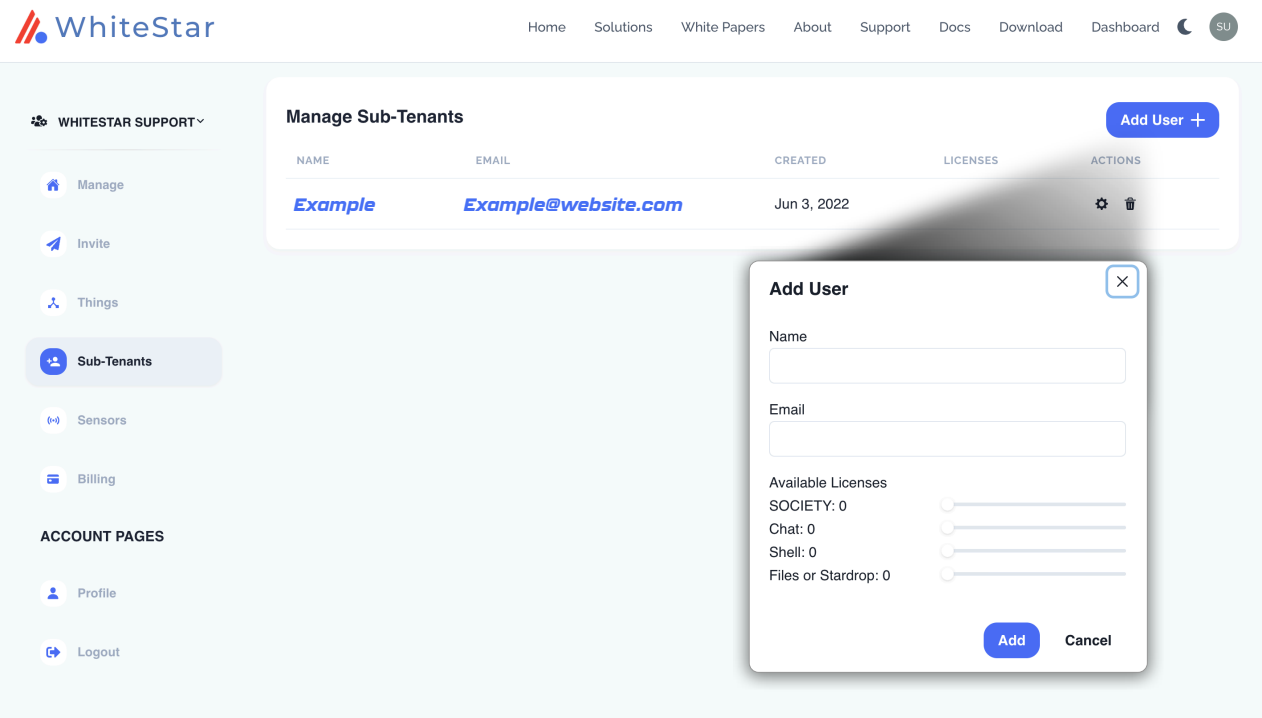


Figure 16

It's important to note that your overall organization may have a certain number of licenses available which can be apportioned to each Sub-Tenant that you oversee. On the Sub-Tenant creation screen, you can adjust the number of licenses each Sub-Tenant may use.

5.4. Trusted Team Tags – Providing Access to Server Devices

Permission to access a device's WSF Server service is granted by unique identifiers referred to as ***Trusted Team Tags*** (Or just Team Tags, or Tags for short) in the WhiteStar system.

Trusted Team Tags are created on the Administrator Dashboard and assigned to WSF users either individually or to groups of WSF users. In order to access a particular Server device, it is the customer's responsibility to log into the admin dashboard, add the Server to their account, and assign the Trusted Team Tag to that server. Refer to Maintaining the list of Trusted Teams Who Can access a Device for more details on how to perform this action.

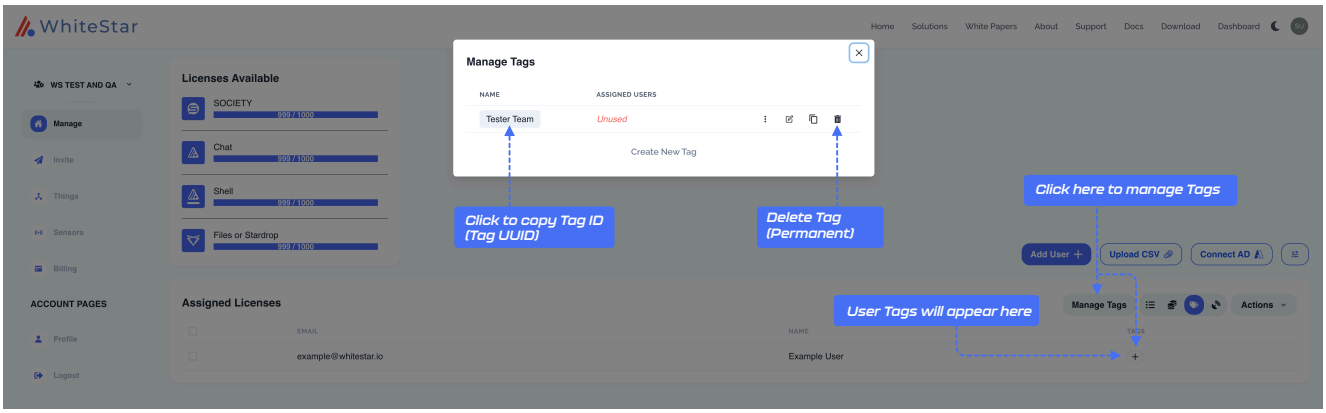


Figure 17

Creating Trusted Team Tags and assigning them to WhiteStar Files users is quick and easy. The administrator first logs in to the Administrator dashboard and clicks on "***Manage***" in the lefthand column. In the main portion of the screen there is a three-way control switch (see Figure 18) on the right-hand side of the ***"Assigned Licenses"*** table that allows you to see the Team Tags applied to a given user's account.

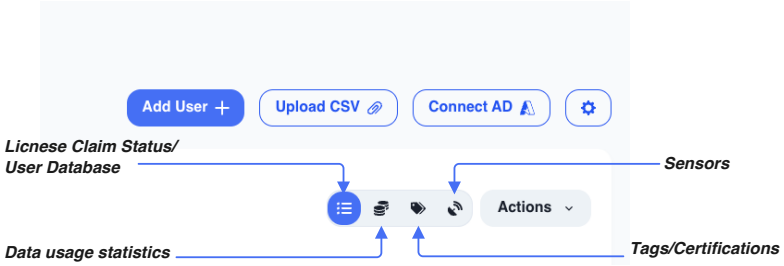


Figure 18

Toggle this switch, and you'll see a row appear in the names list that will allow you to add Trusted Team Tags (see Figure 19).

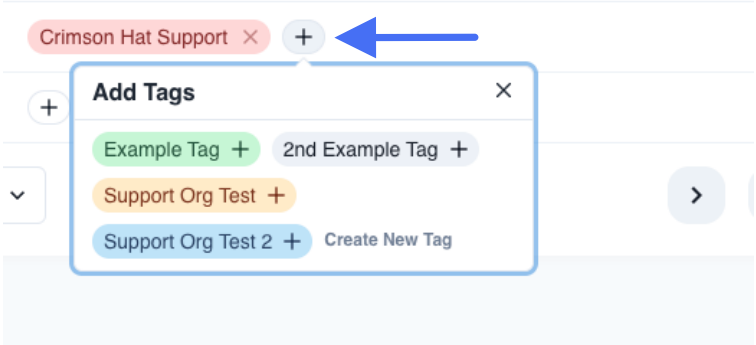


Figure 19

Press the "***Plus***" button. If there are currently no Trusted Team Tags created for your organization, you can create one here and apply it to the WhiteStar Files user. For ease of use, Trusted Team Tags can be colorized to provide a better visual delineation of which users have permission to access which customer devices. Trusted Team Tags can be edited once they are created by clicking **"*Manage Tags*"**. This will allow you to change the Trusted Team Tag name and color, as well as view it's unique identification code.

Removing a Trusted Team Tag from a user removes their ability to access the devices associated with that Trusted Team Tag. Likewise, removal of the user also *automatically* removes the Trusted Team Tag from their account.

Each Trusted Team Tag, when created, is assigned a unique code, which is required by the WSF Server. You can find this CODE by clicking **"*Manage Tags*"** after you created the Trusted Team Tag, or by clicking on the Trusted Team Tag in the user list.

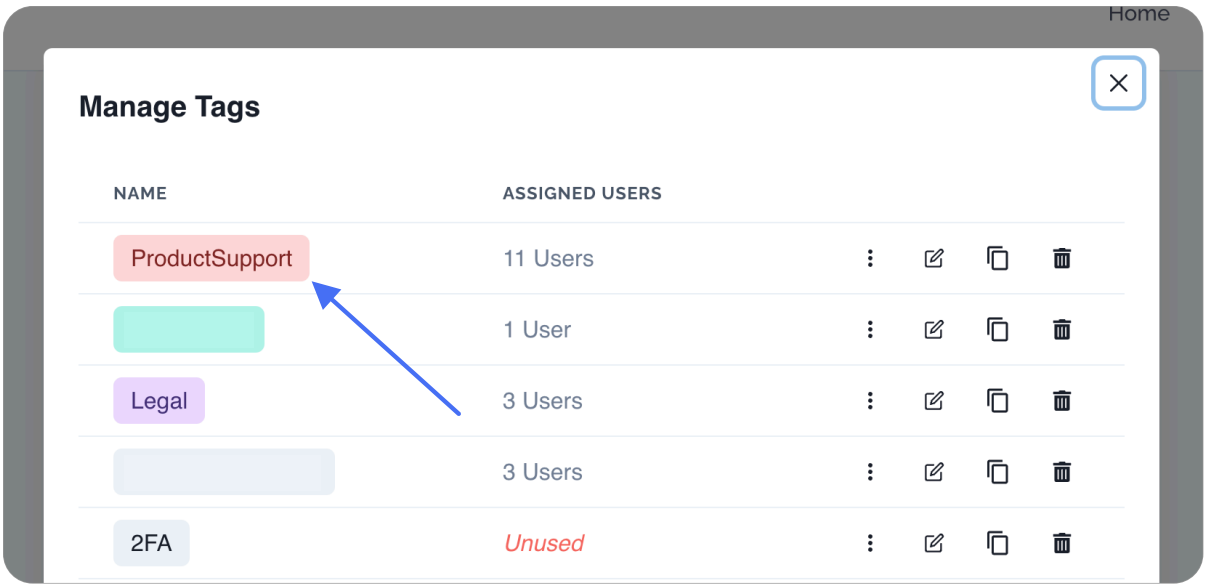


Figure 20

Clicking on the **code or the Team Tag Name** will automatically copy the code to your clipboard. You can then share the code with the network/server administrator of the customer device for them to grant access into their WSF Server interface. After the code is installed correctly, the WSF Client remote terminal is able to access the WSF Server.

WhiteStar applications also understand certain "***Feature Tags***", which are a style of Tag, which when applied to a Federation, cause that Federation to receive certain special features in applications (for example, a 2FA Tag will cause the application to require a 2FA authentication upon login, or Sensor Reports will enable the WhiteStar Sensor Suite to monitor that Federation's traffic, etc).

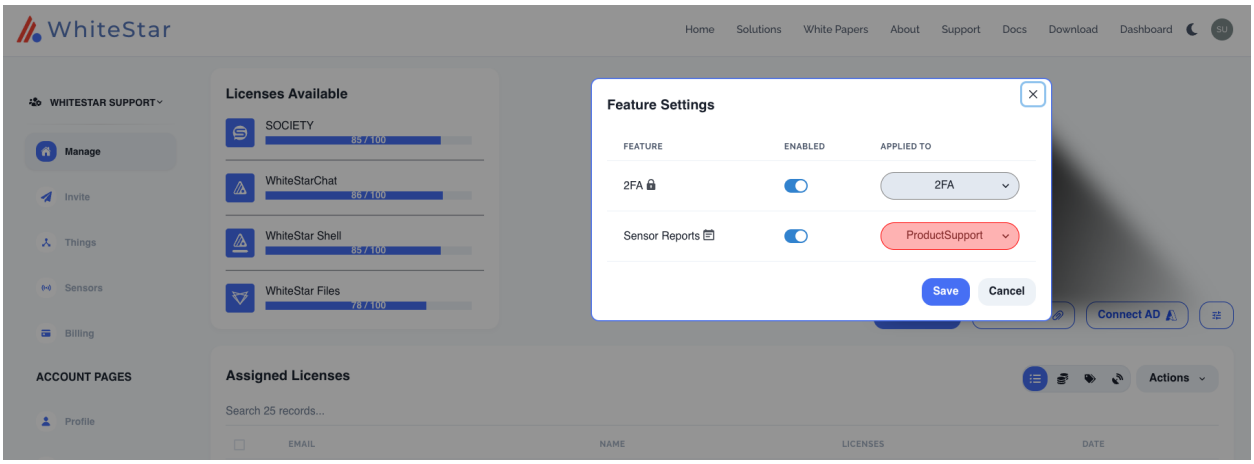


Figure 21

As shown in Figure 21, you can access Feature Tags from the manage portal on the Dashboard near the righthand side of the screen. This will bring up the Feature Tags available to you as an administrator. You can apply these to a Tag and enable and disable the feature if needed. ***We suggest creating a specific Tag for each Feature, which you can then apply selectively to the Federations you manage (for example, creating a 2FA Tag that can be applied to certain Federations who you believe need to have multi-factor authentication.)***

5.5. Trusted Team Tags – Adding Additional Functionality

The administrator has the ability to add properties to Trusted Team tags which, in turn, provide clients (assigned these tags) additional functionality (e.g. turning on email notifications when files transfers complete or running antivirus scanning against transferred files). To add additional properties to a Trusted Team tag, the administrator must:

1. ***Log in to the WhiteStar administrator's dashboard*** at www.whitestar.io (top right hand of web page)

2. Click on the "***Manage***" from the left-hand column

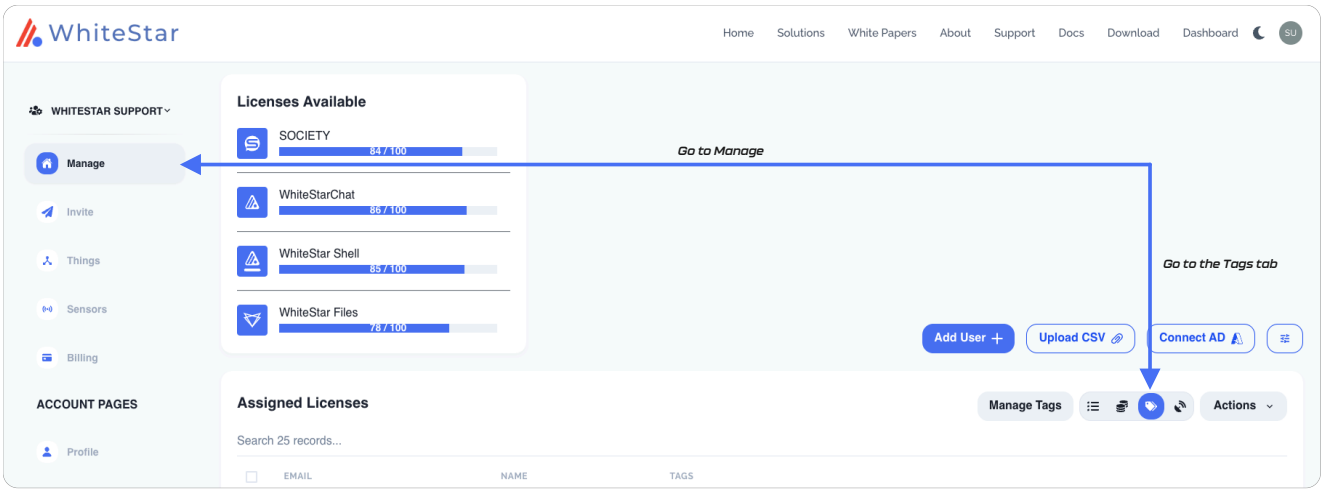


Figure 22

3. Click on the "***Tags***" selection

4. Click on "***Manage Tags***"

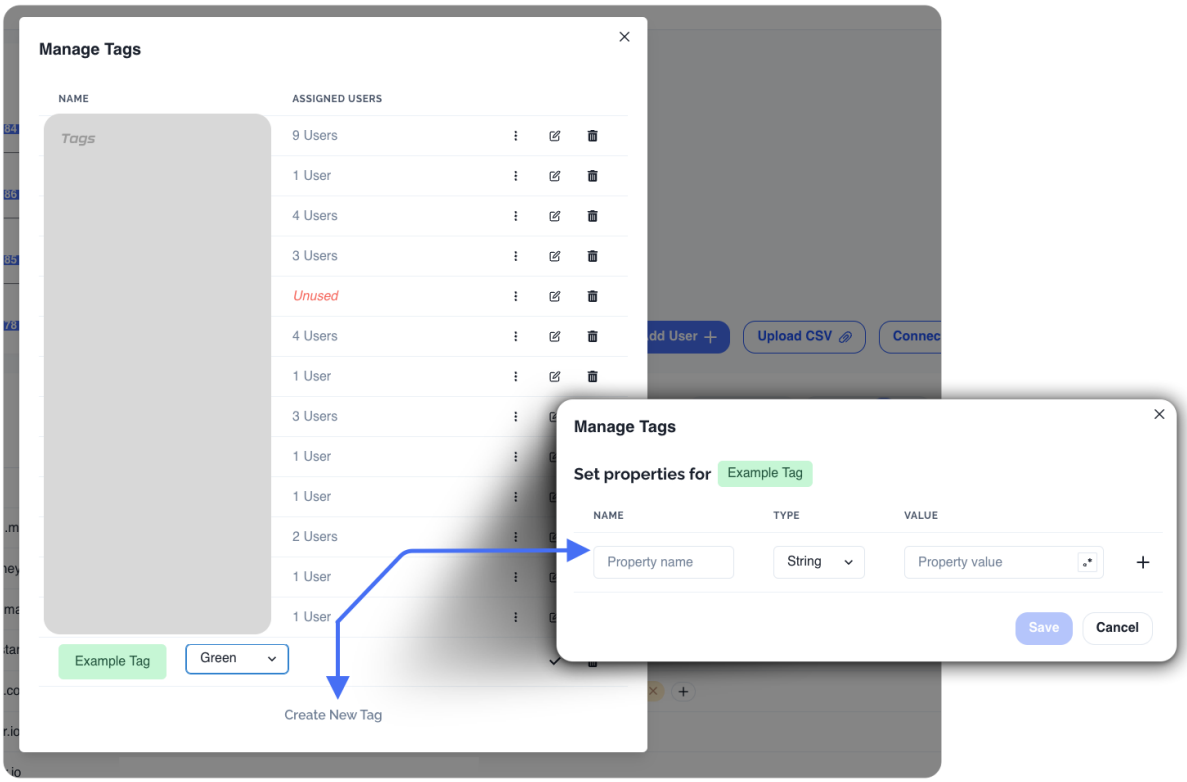


Figure 23

5. Once the list of Trusted Team Tags is presented, click the three vertical ellipses for the Tag you want to add properties to "***set additional properties***"

6. Enter the ***property name, type, and value*** (see sections below).

5.6. Trusted Team Tags – Best Practices

The maximum character limit of a Tag is 30 characters. When creating Tags, it's important to remember to name them something memorable and clear, but also to be concise and to the point. It's recommended to not overload the name of a Tag – Afterall, ***there is no limit on the number of Tags that can be created***.

Here's an example: a team of people are working on a project called ***Super-Mega-Ultra Project Number 457851-127***. This is a very long project name, and internally different members of the team refer to the project by different names. Some members use the ***numeric designation***, some members call it ***Super-Mega-Ultra Project***. Two Tags can be thus created, one that's called ***Super-Mega-Ultra Project*** and the other Tag called ***457851-127***. Both can point to the same File server, and as such have the exact same purpose, but it allows users to more easily find the correct server or project they're posting files back to.

In general it's recommended to not use special characters in Tags – keep them alphanumeric. Always remember that Tags can be used for multiple applications as well; while this document pertains to WSF, the same Tag can be used with any number of WhiteStar apps as well.

5.7. Trusted Team Tags – Duplicating Tags

Under the ***Manage Tags*** screen, there is a button to ***duplicate*** a Tag. This may be useful for quickly taking a single Tag and creating a duplicate for additional users and/or servers. When duplicating Tags, the new tag is created with the label "***Copy***" in its name but can be easily renamed. Note that ***all properties on the duplicate Tag will be cloned from the original Tag***, and it will be an exact one-to-one replica, save for the fact that the newly created clone Tag ***will have a unique Tag ID***.

Cloning is useful if, for example, the administrator wants to create multiple Tags with the same type of permissions but wants to apply these Tags to different file servers for proper data hygiene.

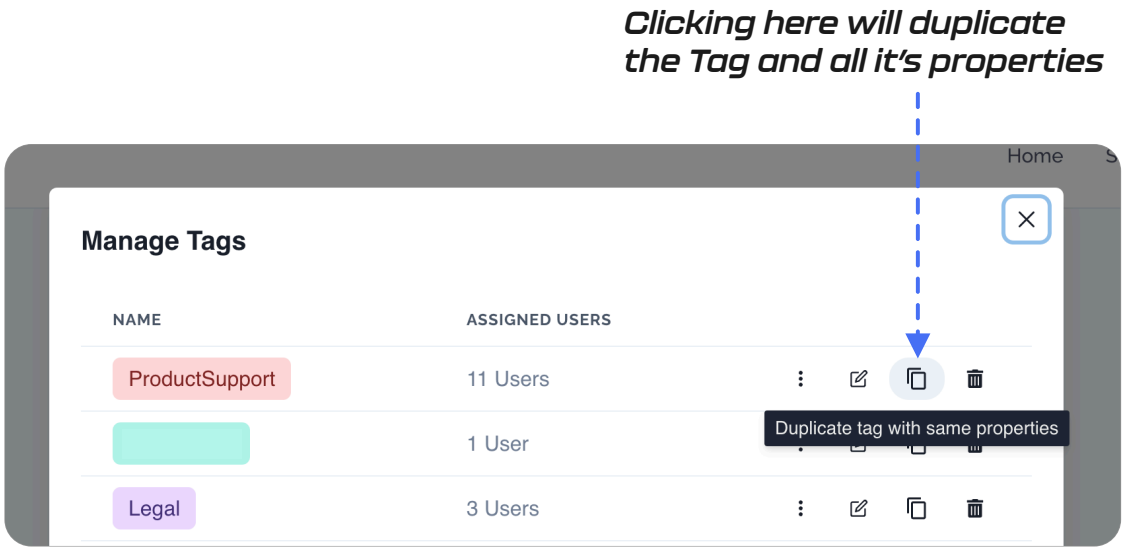


Figure 24

5.8. File Transfers – Notifications and Automation

5.8.1. Email notifications

WhiteStar Files has a built in facility to notify interested parties (via email) when files are transferred to/from specific Servers. In order to enable this feature the administrator must add additional properties to a Trusted Team Tag that has been given permission to transfer files to/from the subject Server. When "fileNotify" is enabled (on), the recipients in the To, CC and BCC lists receive an email with the subject line (provided in the Trusted Team Tag) each time a file is transferred to that server or retrieved from that server. If the person *initiating* the transfer is listed in any of the To, CC or BCC fields, they **do not** receive the email (since they originated the transfer). The following fields must be added to the Trusted Team Tag which gets assigned to users who can transfer files to/from a server:

Property Name	Property Type	Description
fileNotify	Boolean	This turns email notifications on and off. This property is **mandatory** for this feature to work.
fileSubjectLine	String	The text string that is placed in the subject line of the email sent.
fileToField	List	The list of fully qualified email addresses to be placed on the email's To list.

fileCcField	List	The list of fully qualified email addresses to be placed on the email's carbon copy (CC) list.
fileBccField	List	The list of fully qualified email addresses to be placed on the email's blind carbon copy (BCC) list.
fileExportStrategy	String	When transferring files, the admin can decide whether files with the same name are either replaced (overwritten) or the original is kept (with the file being transferred renamed to a similar name annotated by a numeric value). The two accepted values are: • **replace** (overwrite the old file with the file being transferred) • **keep** (maintain the original file and rename the file being transferred). This is the default behavior if the property is not specified.
mediaConverterEnabled	Boolean	If the user desires media (such as photos) to arrive on the target server in a particular format, the WS Files client will do the conversion for them prior to transferring them. This property is **mandatory** for this feature to work.
convertImagesTo	String	If mediaConverterEnabled is set to TRUE, media files will be converted to this file format prior to transferring files to a server. Current format conversions to that are supported are: • jpeg • png This property is **mandatory** for this feature to work.

To temporarily suspend email notifications, the administrator must toggle the "***fileNotify***" property to the "off" position which suspends email being sent until toggle back to the on position.

The email generated with each transfer contains the following information:

- Name and email address of the originator of the transfer
- Total number of files transferred (including the total size of the transfer)

- The timestamp of the transfer
- The content tracking UUID (to be used if content tracking is enabled)
- The location of where the files originated from and where the were transferred to
- The list of files transferred

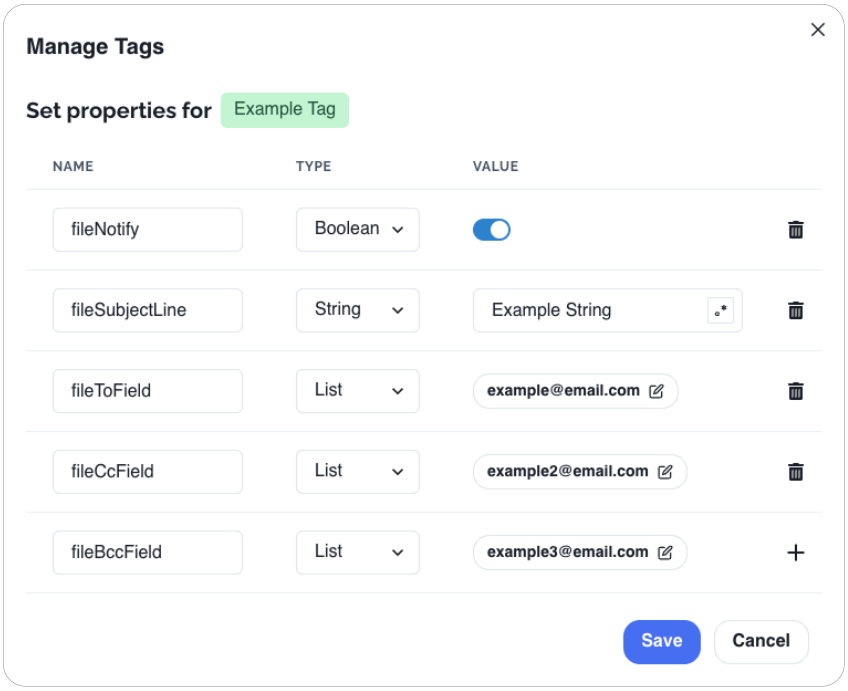


Figure 25

5.8.2. Automation Web Hooks

In order to accommodate client specific automation, WhiteStar files supports the ***calling of webhooks*** once a file transfer has completed. In order to enable this feature the administrator must add additional properties to a Trusted Team Tag that has been given permission to transfer files to/from the subject Server. The administrator must have the uniform resource identifier (URI) of that identifies the web resource that will execute the automation on completion of the file transfer.

Property Name	Property Type	Description
fileWebHookUri	String	URI to call
fileWebHookMethod	String	Put, Get, Post, Delete – method for URI call, used with webhook
fileWebHookHeader	Map	map of key/value pairs to put in the webHook header (optional)

You can edit this on the ***Manage Tags*** section of the Dashboard. Once you have defined your webhook, click save and the webhook's URI will be called each time it is triggered in WSF.

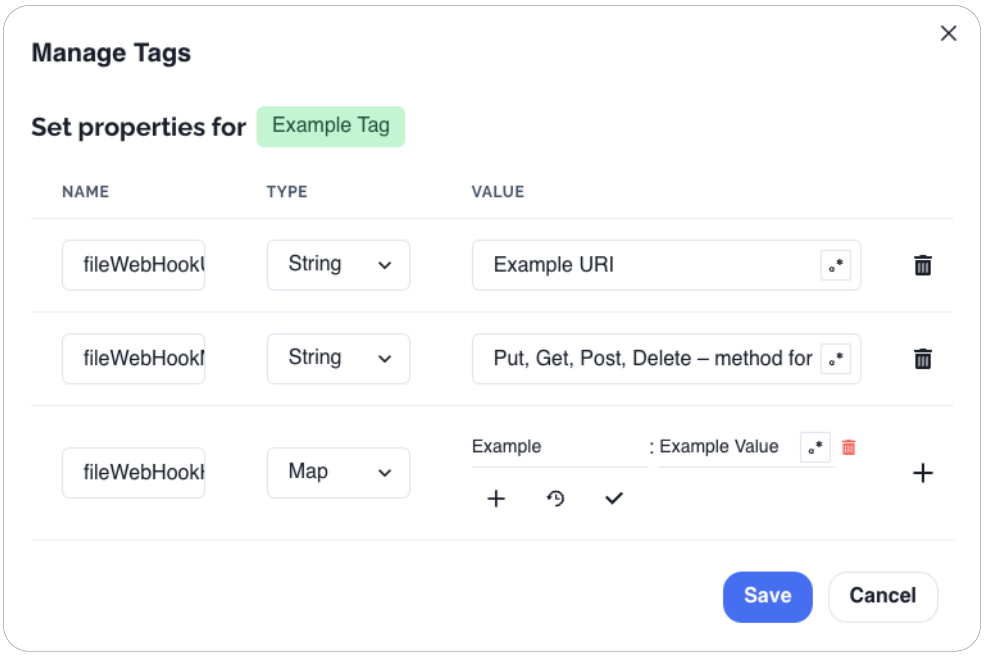


Figure 26

5.9. Sentinel File Antivirus / Data Loss Prevention

Threat Detection / Mitigation

Companies frequently ingest files from outside their organization potentially exposing themselves to malicious malware or viruses attached within them. WhiteStar Files has built within the WSF Server the ability to scan these files once they successfully reach the Server, which is called WhiteStar Sentinel. After a successful file transfer, a multitude of malware/antivirus engines actively scans the files and, if enabled, quarantines (creates a password protected zip) those which contain malware or viruses.

Sentinel is not a part of the base WSF system and must be activated separately in order to take advantage of it. If you are not currently subscribed to WhiteStar's Threat Detection and Mitigation services, and would like to add this capability to your WhiteStar software, please contact info@whitestar.io. WhiteStar highly recommends adding this to your WSF deployment if you:

- Regularly interface with external clients, contractors or entities who have files of indeterminate origin
- Are operating in an environment where there are known hostile actors
- Are in possession of a large number of old files that may contain malicious code

- Operate with SOP's that dictate a high security posture that requires virus scanning at all times
- Your business needs to maintain data protection compliance for legal reasons
- Have particularly sensitive and irreplicable data that, if lost, would be a critical loss to your organization
- Your organization, for whatever reason, has decided they do not want multiple external copies of data stored in redundant data storage (not recommended)

Data Loss Prevention (DLP)

In addition to malware / virus detection, WSF Server can also be configured to run a sophisticated Sentinel Data Loss Prevention engine against newly ingested files. This engine searches for sensitive data (such as Social Security Numbers, credit card numbers, or other Personal Identifying Information) and redacts it (physically replacing the text with a black box) from the file. Both a redacted and unredacted copy of the file is saved allowing the user to choose which file they'd like to work with. WhiteStar Sentinel DLP prevents unwanted data leaks and may be a requirement for your organization, particularly if your organization operates with a requirement to provide compliant data handling services.

Similar to Sentinel Threat Detection / Mitigation, this feature is not a part of the base WSF system and must be activated separately in order to take advantage of it. If you are not currently subscribed to WhiteStar's DLP services, and would like to add this capability to your WhiteStar software, please contact info@whitestar.io.

5.9.1. Sanitization / Quarantine

When Sentinel is enabled and configured, WhiteStar Files has the ability to take 2 actions once files have been transferred: (1) run antivirus against the files and (2) run data loss prevention sanitization (e.g. the ability to redact personal and sensitive information). These features require additional licensing and are not a part of the base WhiteStar Files package. Please see your Sales representative to have these features added to your account (info@whitestar.io).

Once enabled, the following fields must be added to the Trusted Team Tag which gets assigned to users who can transfer files to/from a server:

Property Name	Property Type	Description
sanitizationAction	String	When antivirus is run against files, the administrator has three options on how this feature operates. The three options (and values which must be set for this property): 1. **none** - sanitization is disabled

		2. **sanitizeAndKeep** – sanitize files and keep the original 3. **sanitizeAndReplace** – sanitize files and replace the original with the sanitized file
quarantineAction	String	The administrator also has the ability to determine what action is taken with the original file once a virus is detected. Two accepted values: 1. **none** - disabled 2. **quarantine** – quarantine the file
quarantinePassword	String	If the administrator chooses to quarantine a file, WhiteStar files will zip the file to ensure it cannot infect the host computer. When zipping, WSF zips the file with a administrator assigned password to ensure accidental running of the file is prevented.

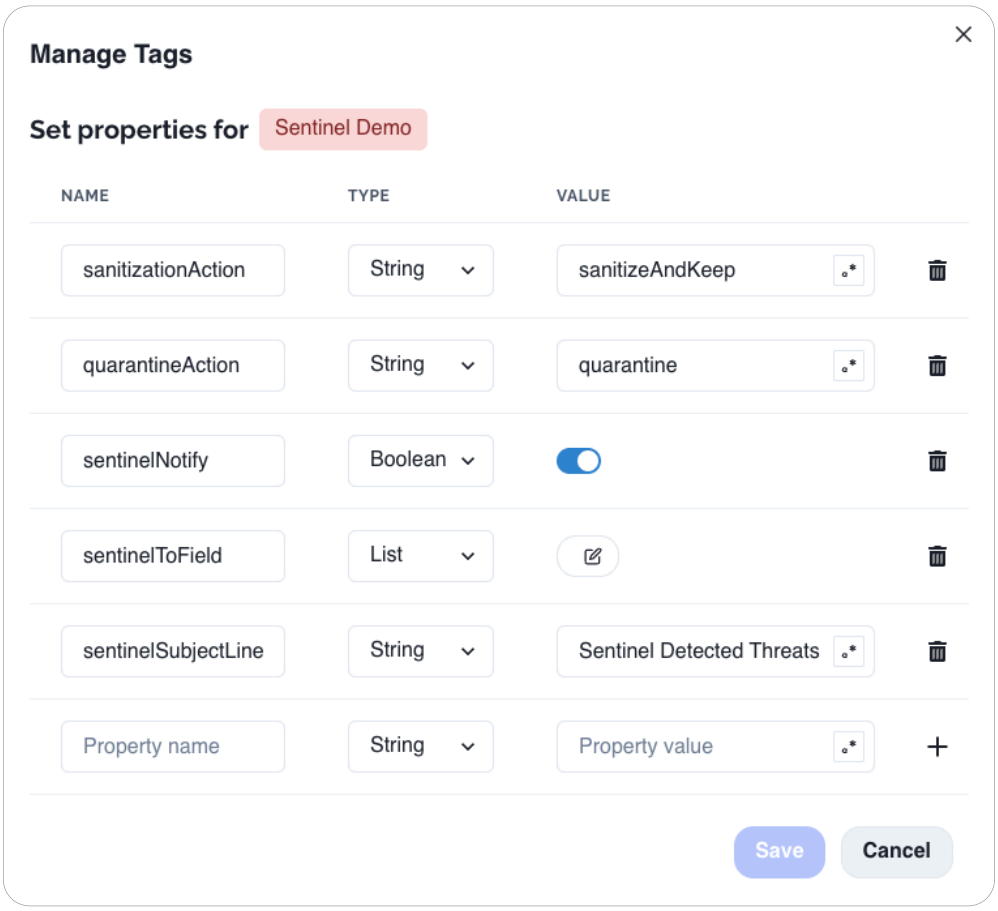


Figure 27

To adjust the Sentinel settings of individual folders on any given file server, navigate to the server detail page, under ***File Management***, then select ***the threat detection icon*** on the right-hand side of the screen. Clicking on this will bring up a dialogue box.

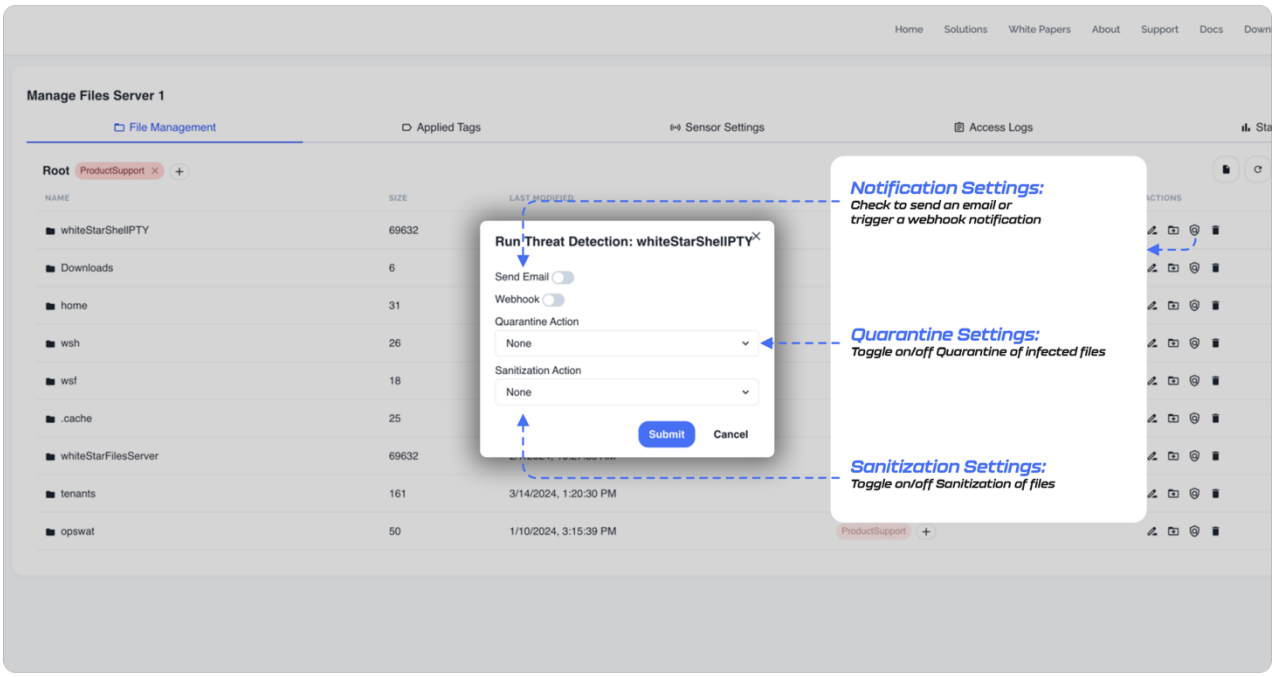


Figure 28

On this box, there are three options that control the Sentinel threat detector. They control how you will receive notifications (or if you will receive notifications), and turns on and off the quarantine and sanitization settings.

5.9.2. Email Notifications

WhiteStar Files has a built in facility to notify interested parties (via email) when antivirus scanning and or sanitization has completed. In order to enable this feature, the administrator must add additional properties to a Trusted Team Tag that has been given permission to the subject Server the files reside on. When "***sentinelNotify***" is enabled (on), the recipients in the To, CC and BCC lists receive an email with the subject line (provided in the Trusted Team Tag) each time antivirus scanning / sanitization on the server has completed. The following fields must be added to the Trusted Team Tag:

Property Name	Property Type	Description
sentinelNotify	Boolean	This turns notifications on and off. This property is **mandatory** for this feature to work.
sentinelSubjectLine	String	The text string that is placed in the subject line of the email sent.

sentinelToField	List	The list of fully qualified email addresses to be placed on the email's To list.
sentinelCcField	List	The list of fully qualified email addresses to be placed on the email's carbon copy (CC) list.
sentinelBccField	List	The list of fully qualified email addresses to be placed on the email's blind carbon copy (BCC) list.

To temporarily suspend email notifications, the administrator must toggle the "***sentinelNotify***" property to the "***off***" position which suspends email being sent until toggle back to the on position.

5.9.3. Automation Web Hooks

In order to accommodate client specific automation, WhiteStar files supports the ***calling of webhooks*** once a file s antivirus scan / sanitization has completed. In order to enable this feature the administrator must add additional properties to a Trusted Team Tag that has been given permission to transfer files to/from the subject Server. The administrator must have the uniform resource identifier (URI) of that identifies the web resource that will execute the automation on completion of the file transfer. The following fields must be added to the Trusted Team Tag:

Property Name	Property Type	Description
sentinelWebHookUri	String	URI to call
sentinelWebHookMethod	String	Put, Get, Post, Delete – method for URI call, used with webhook
sentinelWebHookHeader	Map	map of key/value pairs to put in the webHook header (optional)

5.10. Managing Sensor Groups

Natively built within the WhiteStar Network Operating System is a feature offered to administrators to track the movement of content while it traverses the WhiteStar network, track interactions between WhiteStar cohorts, and log diagnostic messages generated within the WhiteStar system for debug purposes. In the case of WhiteStar Files, the administrator *can* enable the tracking feature to record exactly where and when files traverse the WhiteStar network during transfer (although it's important to note, this is *optional*).

A high-level description of the three major sensor types:

Content Sensor - collects metadata about the content traversing the WhiteStar network including application type the content is being sent on, the type of content being generated, the data and time the content is traversing the network, source and destination information, etc.

Cohort Sensor **-** collects information about the Federations on the network and their relationships to each other (WhiteStar Cohorts).

Log Sensor **-** diagnostic sensors used to detect faults or other network issues for debugging.

Visualizations of the data collected are available in different styles and form factors including geographic maps, pie and line charts, 3D graphs, etc. Providing these visualizations enable administrators, in the case of WhiteStar files for example, to easily represent the flow of file content over the network, along with detailed log information about the content sensor outputs (displayed in a table below the visualizer) – see Figure 29.

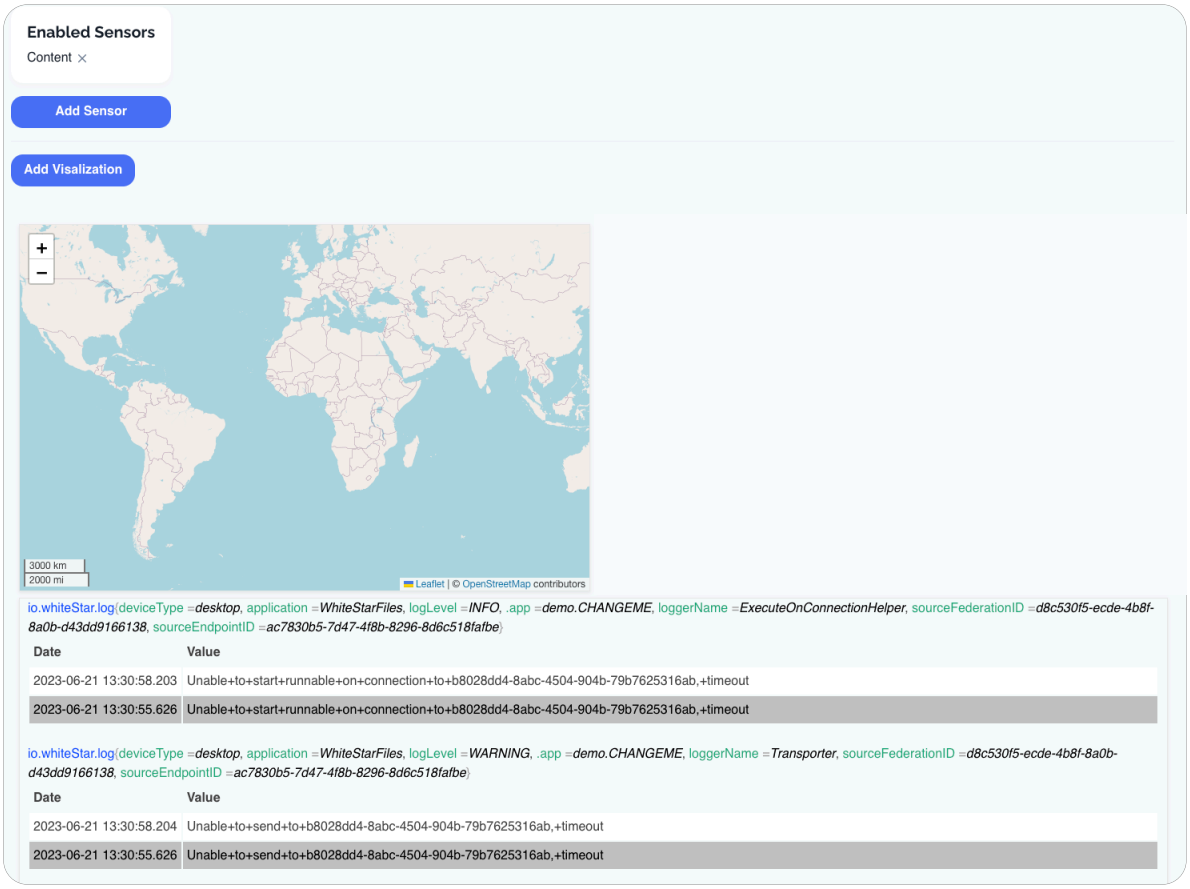


Figure 29

Best practices: It is recommended to keep sensor groups ***as simple and to the point as possible*** to avoid confusion.

For example, if your company needs to monitor the flow of data between Cohorts, avoid adding a Content sensor to the same sensor group as well. If your primary concern is geographic data sovereignty, and your company wants to ensure that no data leaves a particular region of the world (e.g. leaving the Eurozone as per GDPR), use the map visualizer and don't crowd the UI with charts or graphs. Finally, if your company is concerned with the volume of traffic over time, the map visualizer isn't particularly useful, and instead the line chart is better suited to plot the relevant information.

There are no limits to the number of sensor groups that can be created, therefore, making ***concise sensor groups with tight constraints*** on the type of information and their visualizations helps improve the usability of the application.

5.10.1. Adding a Sensor Group

On the main sensor group tab of the Administrator's Dashboard, the sensor groups that have been defined by your organization are presented in tabular form. This includes the title at the top, a description of the sensor group (both of which can be edited at any time so they're descriptive of the sensor's function, in case the function of the sensor needs to be altered at some point), along with the read and write tokens for the sensor group. If your organization needs to grant permission to read information from the sensor, the read token can be given to the counterparty that needs access to the information.

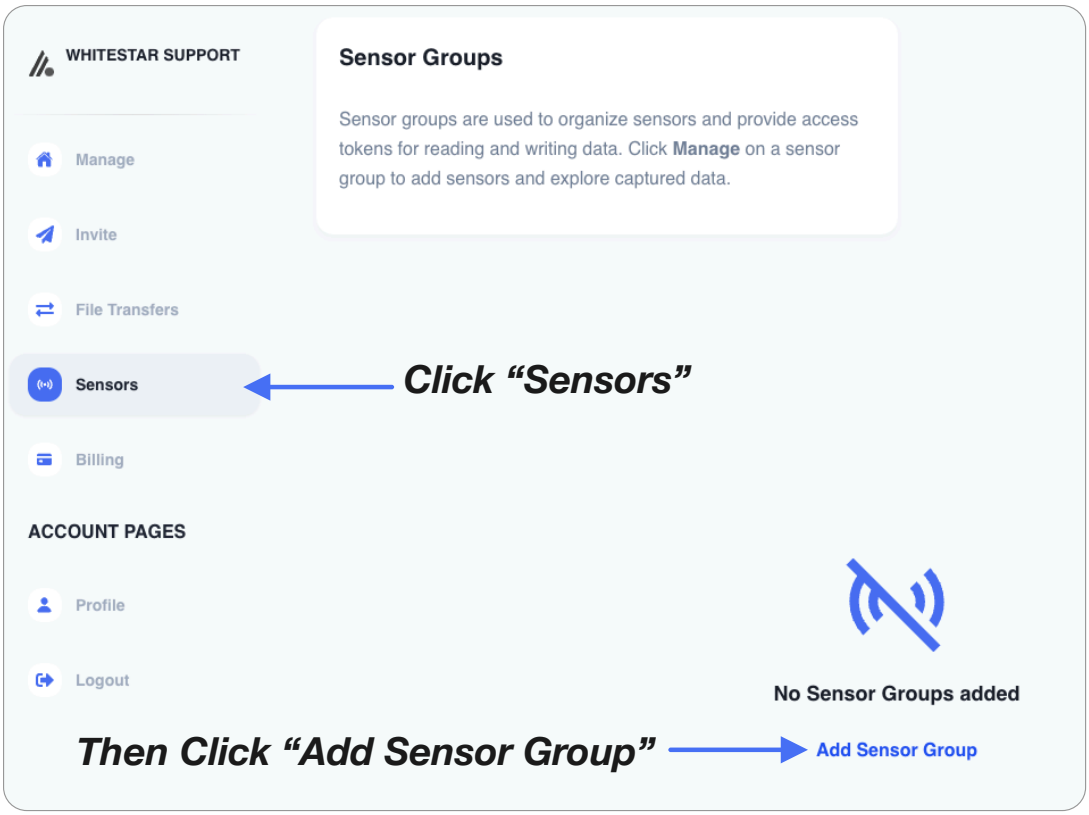


Figure 30

To add a new sensor group, from the left-hand navigation menu, click on "***Sensors***" (see Figure 30). Name your sensor group and give it a description, then click "***Add a Sensor Group***" (see Figure 31).

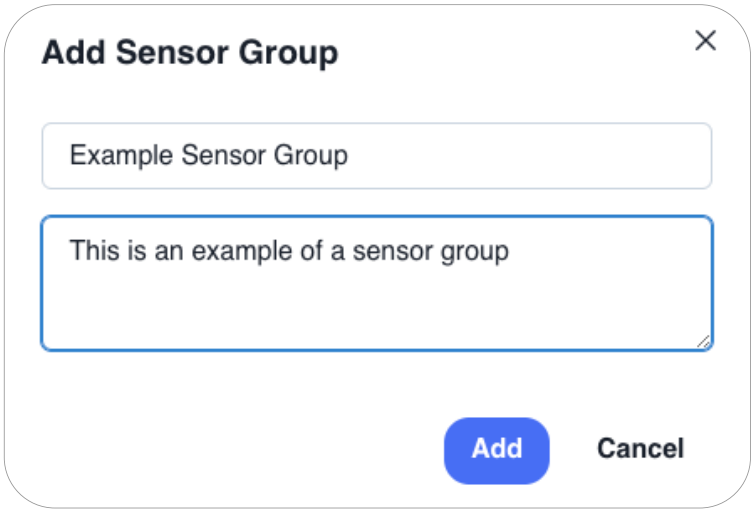


Figure 31

Once successfully created and implemented, the sensor group information is displayed along with the Read and Write tokens needed to access the ***WhiteStar GTS*** (Geo Time Series) database (see Figure 32).

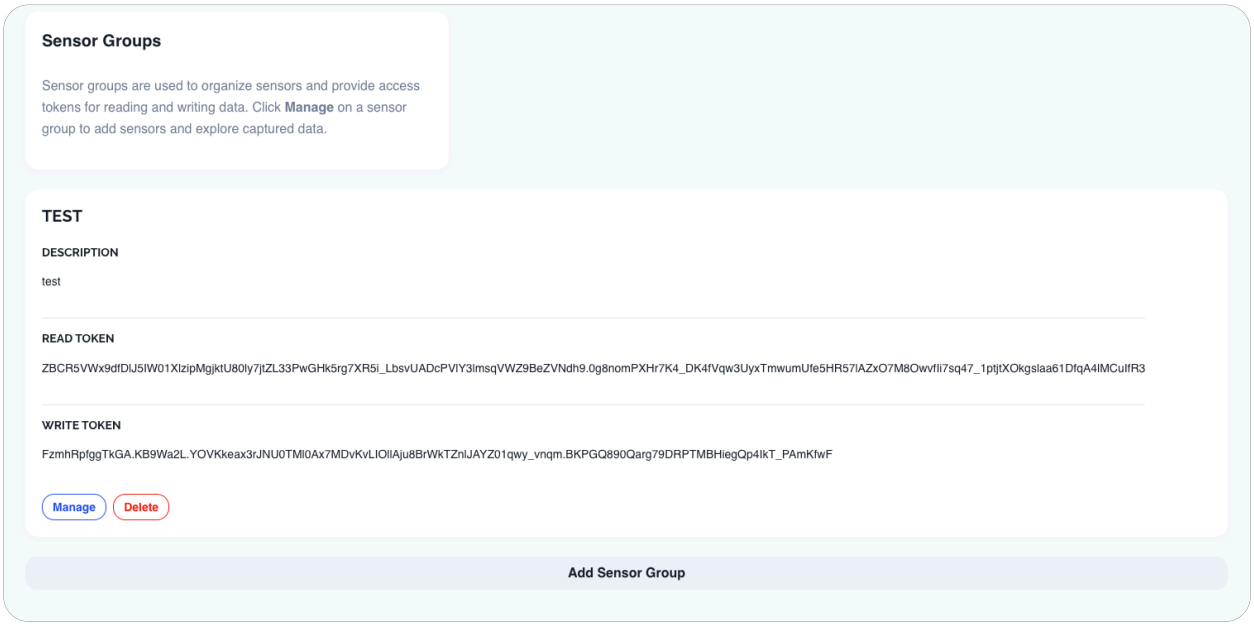


Figure 32

Write tokens are required to post information to the GTS database while ***Read Tokens*** are mandatory when creating visualizations, via the administrator's dashboard, on the data that is collected. Read tokens can also be used in the event an organization wants to cooperatively share their data (provide read access to) with another business.

Creating a sensor group automatically generates a sensor group Tag. When collecting data for Cohort sensor groups, these tags will need to be added to the users within the organization the administrator desires to track.

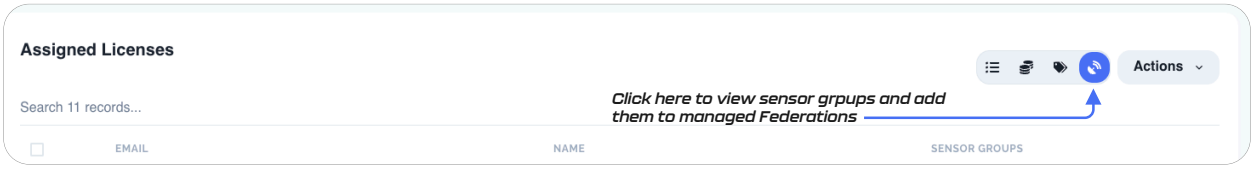


Figure 33

5.10.2. Deleting Sensor Groups

Deleting sensor groups is done via the sensor group tab (see Figure 33). Click on the "***Sensor Group***" tab and there will be "***Delete***" button the administrator can click to delete the group. Note that if you delete a sensor group, it also deletes all the information collected by that sensor.

Be aware, there is ***no way to recover data once the sensor group has been deleted***, so it's not generally recommended that you delete sensor groups.

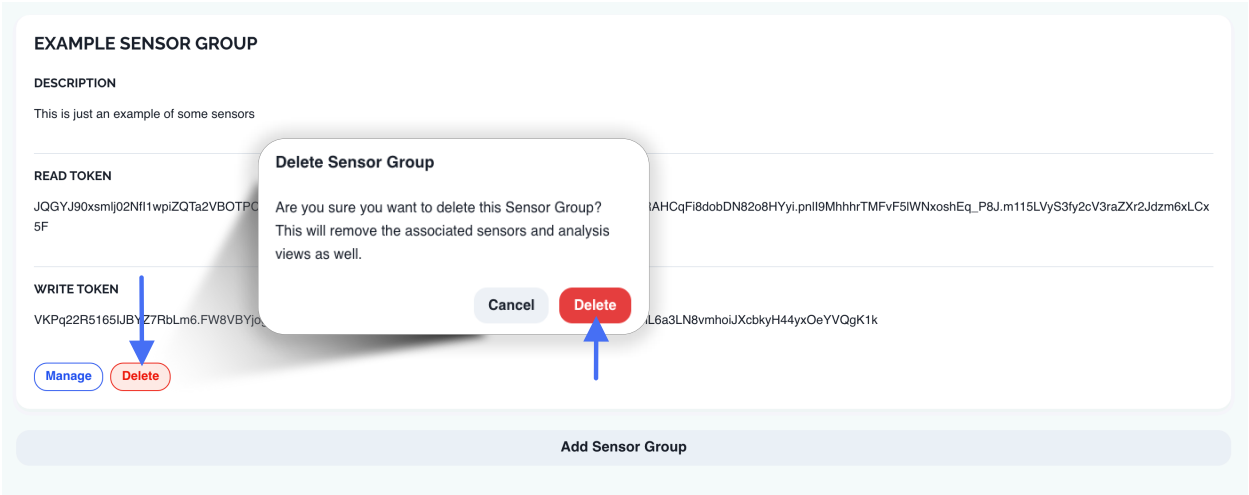


Figure 34

5.10.3. Adding Sensor Visualization

To add a visualizer, click on the "***Add Visualization***" button and select from the drop-down menu which kind of visualization you'd like. You can select from various types of graphs and charts, as well as a map to be able to easily see content moving in physical space.

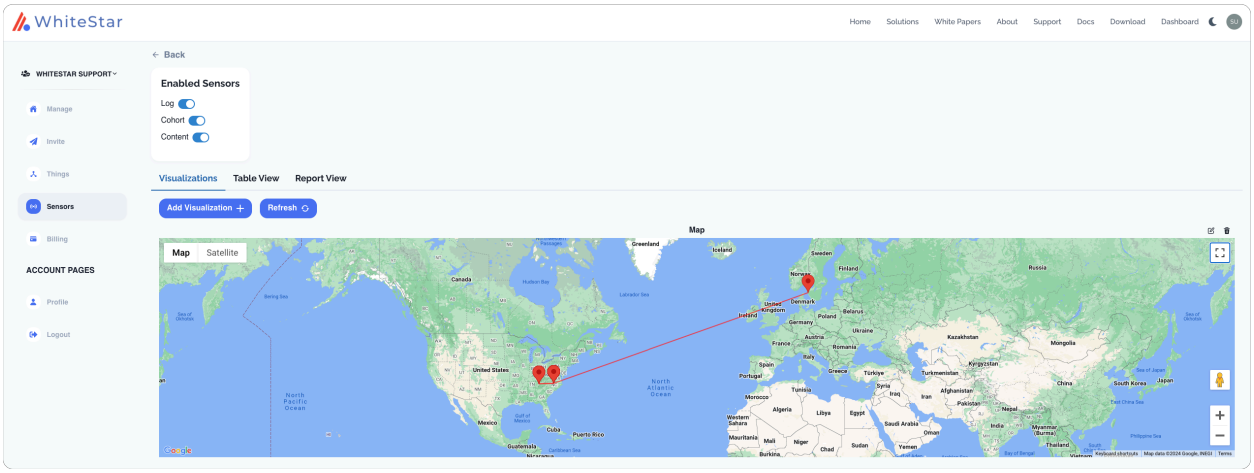


Figure 35

If you need to generate a table of datapoints from your sensor dataset, you can either see the raw data listed on the Table tab, or generate a specific search result using the Report view.

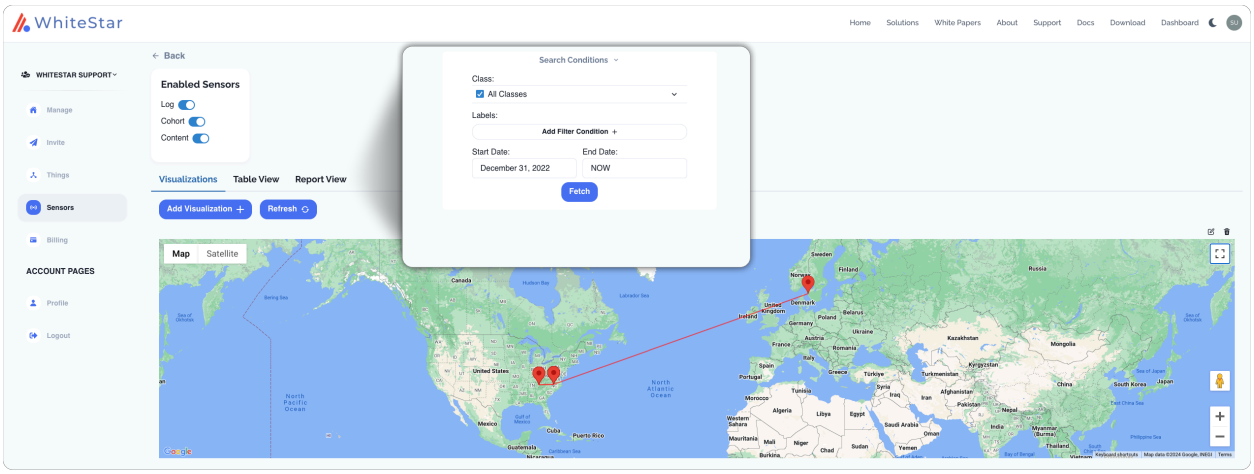


Figure 36

You may also add additional visualizers as needed, keyed to specific classes of information if necessary. Simply go to the visualization page and add visualizers as needed.

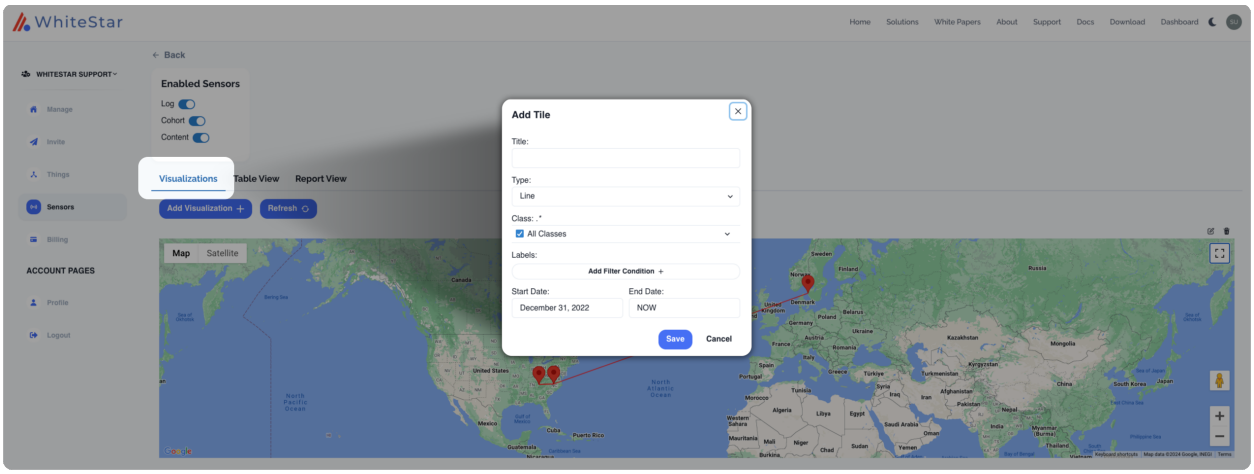


Figure 37

5.10.4. Deleting Sensor Visualization

To delete a visualization, right-click the visualization and choose "***Remove Visualization***" or click the small X in the top right-hand corner of the visualization.

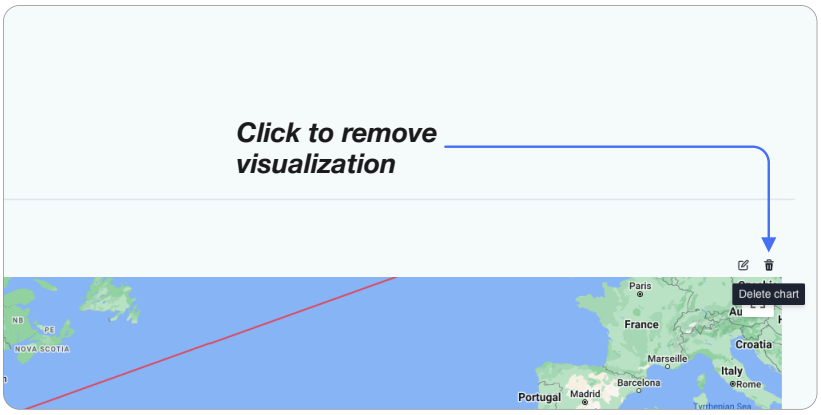


Figure 38

5.11. Accessing/Updating the Administrator Profile

From the main screen of the Dashboard navigate to the left-hand column under "***ACCOUNT PAGES***" and then click on "***Profile***" (see Figure 39). The administrator will find information about the organization including total licenses purchased, total licenses assigned to users, total licenses claimed by users, etc. Additionally, the administrator can modify which notifications they want to receive via email (e.g. low on licenses, out of licenses, etc.). There is also contact information to get in touch with their WhiteStar representative.

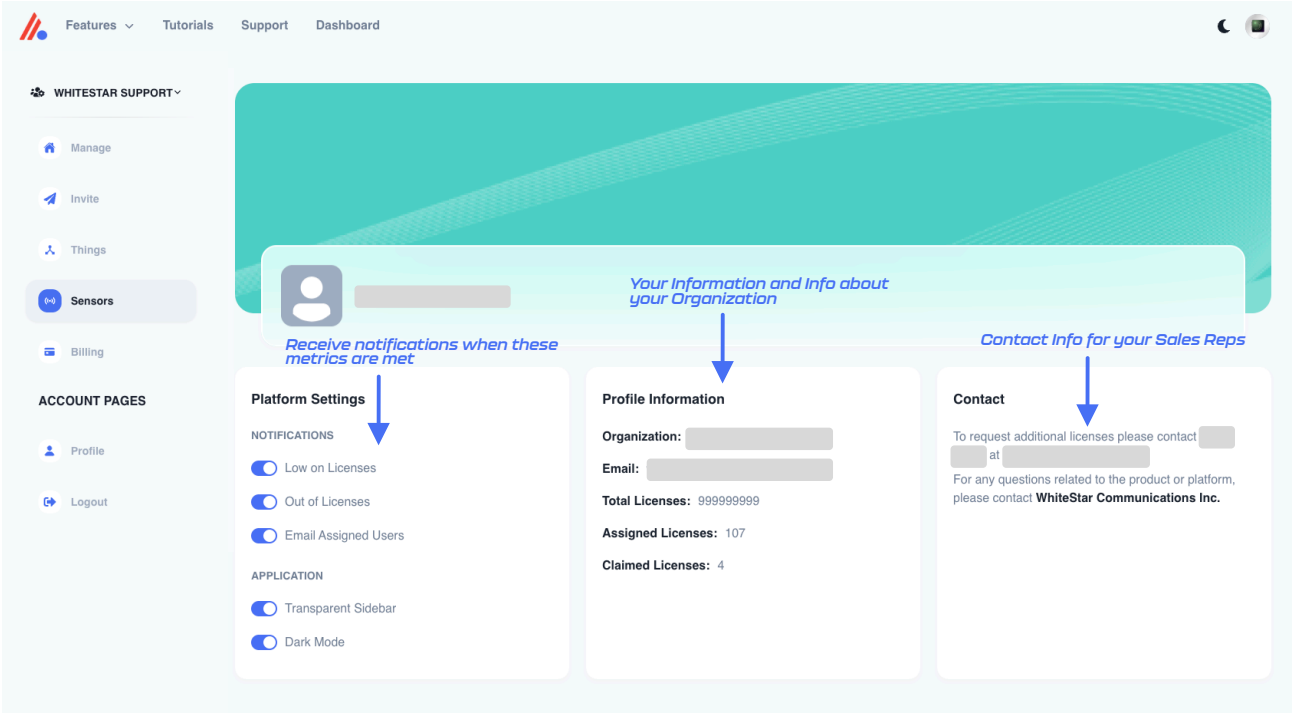


Figure 39

6. Installation of WSF Client

For a WhiteStar Files user to connect to a Server device (running the WSF Server software), they first need to install the WSF Client component on to the machine they want to connect from. The WSF Client component runs on Microsoft Windows, Apple macOS (both Intel and Apple Silicon), and Linux desktops.

Open a web browser and navigate to the following WhiteStar website: https://whitestar.io/download/wsf/client/. The user is presented with a link to download the WSF Client component for the operating system they are currently running on. If not, select the appropriate link for the operating system you want and download the installation package.

Ensure that there are the correct user privileges on the local device to install software on it. You may notice that on certain macOS devices, you will have to allow third-party developers to install software on your device. Click on the "**?**" Button and your Mac will automatically show a popup prompting you to follow it to the Controls/Security and Privacy settings to allow permission.

Open the folder where the WSF installer package was saved.

Click on the download package to ***run the installer***. You are brought to the following screen (see Figure 40):

Figure 40

Click on the "***Next***" button to begin the installation.

Read and accept the Terms of Service by clicking on the "***I accept the agreement***" and then click on the "***Next***" button (see Figure 41).

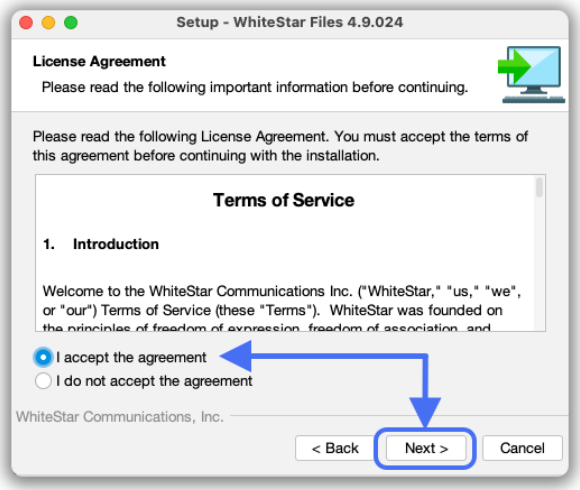


Figure 41

Choose the directory for the application to be installed into, and then click the "***Next***" button (see Figure 42).

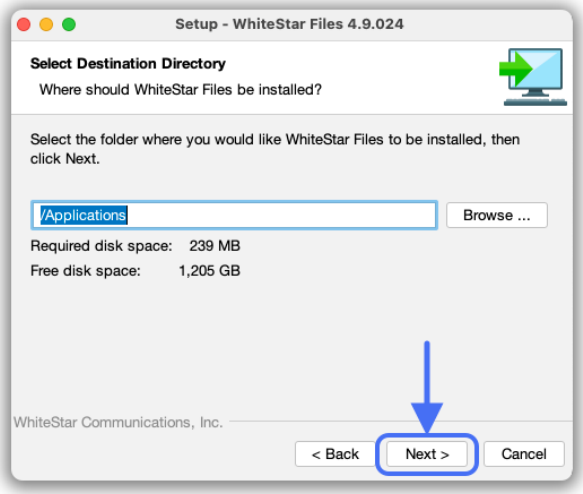


Figure 42

Click the "***Finish***" button to complete the installation (see Figure 43).

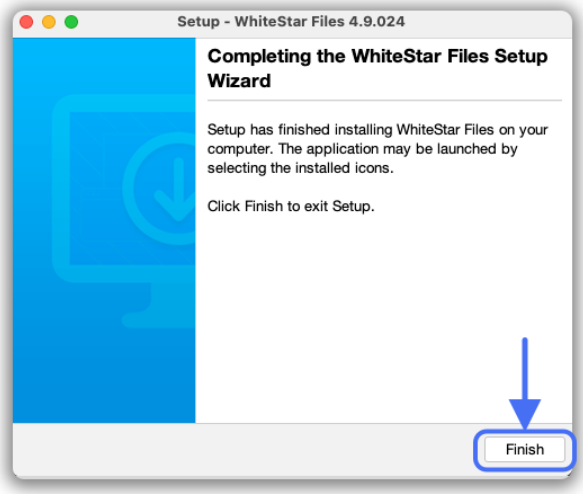


Figure 43

The first time the user starts the WSF Client program they are brought to the registration screen (see Figure 44). Enter your name and company email address (2x) and click the "***Request Confirmation Code***" button to have a confirmation code send to your email address.

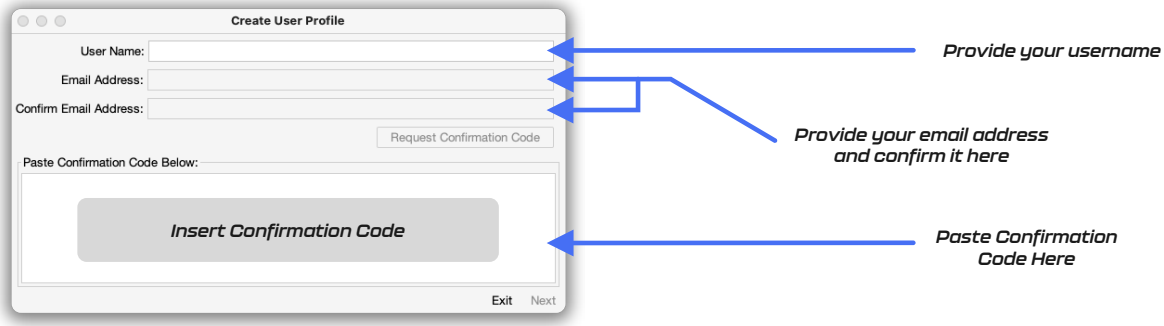


Figure 44

NOTE: Company administrators must have previously assigned a license to your email address. If one has not been assigned, please contact your system administrator to have one assigned or the confirmation code that is sent will **not** activate your account, and you will arrive at a screen prompting you for a subscription.

Go to your email client and look for an email from vortex@whitestar-vortex.com with the subject line of "***WhiteStar Validation Code***" (check your spam folder if you don't see the email within 2-3 minutes). Open the email and copy the **entire** confirmation code (including the

single quotes) from the email into the copy buffer (typically highlight the entire code and hit **Cntl-C/Cmd-C**). Go back to the WSF Client installation screen (see Figure 44) and paste (typically hit **Cntl-V/Cmd-V**) the confirmation code into the appropriate box (see Figure 45 as an example).

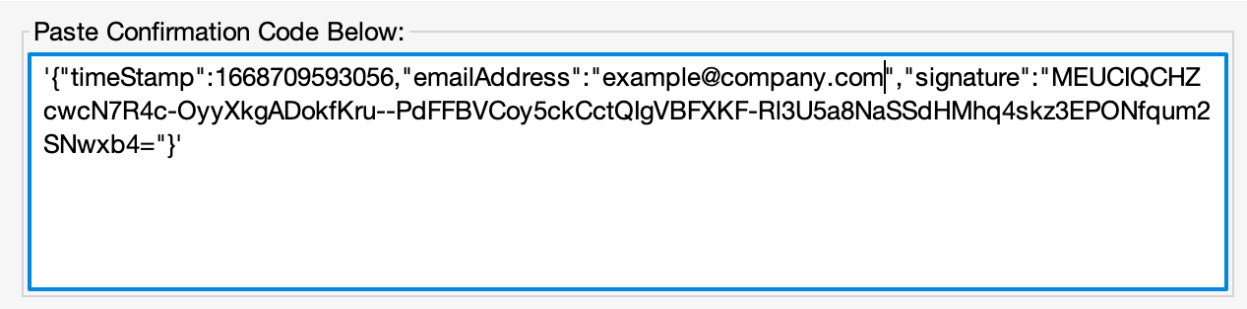


Figure 45

Alternatively, if your computer permits this function, the user can left click (and hold) on the QR code provided in the email, and drag/drop it in to the validation box (in Figure 44).

Click the "***Next***" button. You will then be prompted to create a password for your account. This password is ***never*** stored at WhiteStar Communications *or* with your local system administrator, so it is up to each user to remember their password. There is *no* "password reset" capability with WSF Client. If you lose your password, see the section in this guide on resetting your account.

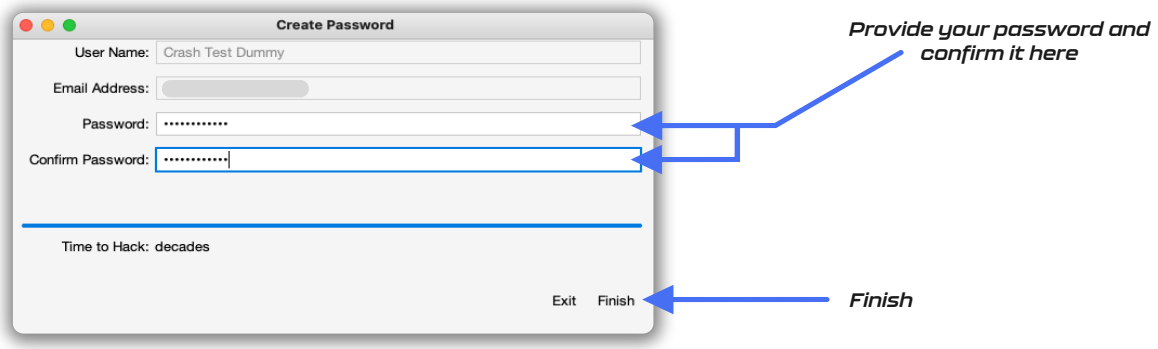


Figure 46

If your administrator requires you to create a ***2FA code***, you will see a QR code popup that can be scanned using your Authenticator app to create a shared secret.

After entering a ***strong*** password and confirming it (generally recommended practice is to use at least once capital letter, one special character, one number and between 8-13 digits), click the "***Finish***" button to complete the installation (see Figure 46).

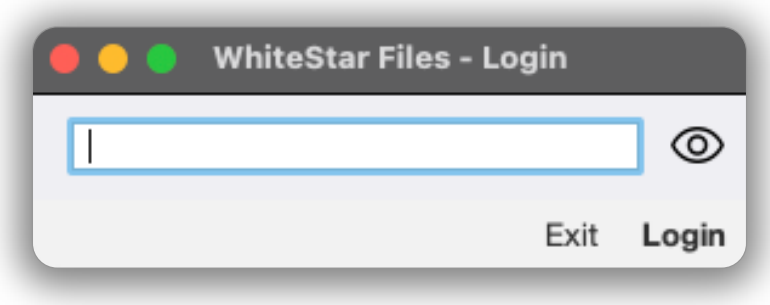


Figure 47

If you already have created an account on WhiteStar Files, and are returning the application, you are prompted to log in to the application (see Figure 47), and do not need to set your account up a second time.

Note: WhiteStar Files will remember the exchanged file jobs that it has completed in the work queue. After you log back into the application, you will see previously completed tasks on the bottom portion of the application (see Figure 48).

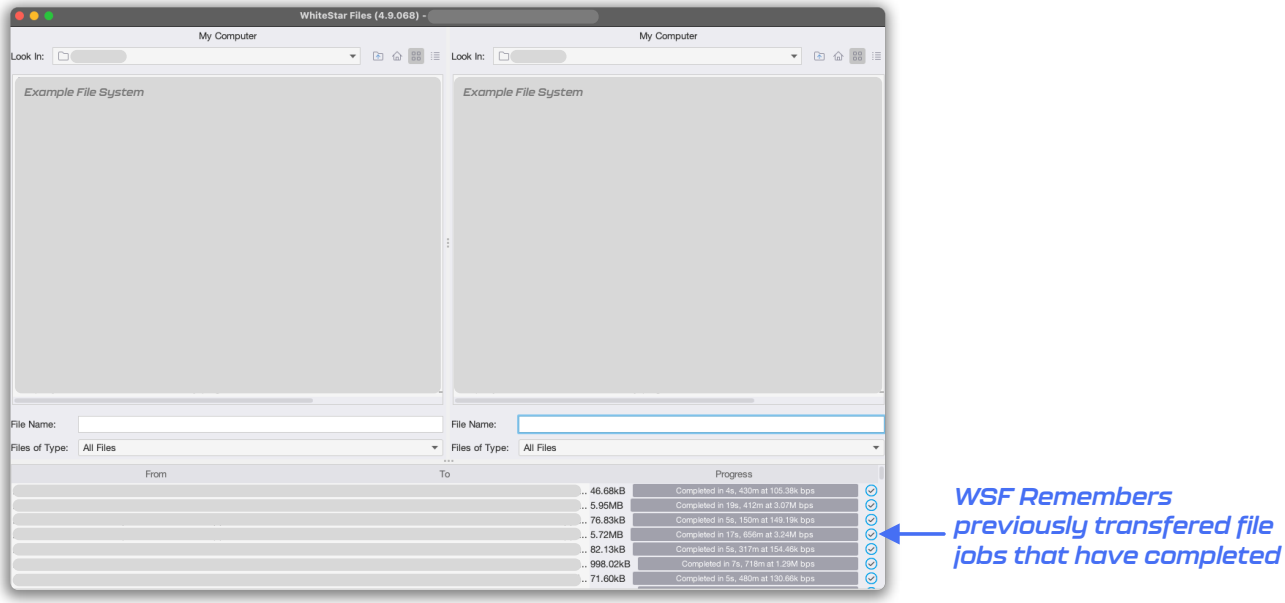

WhiteStar Files (4.9.068) -
My Computer
Look In:
Example File System
File Name:
Files of Type:
All Files
From
To
Progress
.. 46.68kB
Completed in 4s, 430m at 105.38k bps
.. 5.95MB
Completed in 19s, 412m at 3.07M bps
.. 76.83kB
Completed in 5s, 150m at 149.19k bps
.. 5.72MB
Completed in 17s, 656m at 3.24M bps
.. 82.13kB
Completed in 5s, 317m at 154.46k bps
.. 998.02kB
Completed in 7s, 718m at 1.29M bps
.. 71.60kB
Completed in 5s, 480m at 130.66k bps
WSF Remembers previously transfered file jobs that have completed

Figure 48

7. Running the WSF Client

When running the WSF Client for the first time, the user is prompted to register an account. Please see *Installation of WSF Client* above for details on how to install and register an account.

For a WSF Client to connect to a WSF Server on a remote device, the system administrator must first create a Trusted Team Tag and assign it to the WSF Client user. This Trusted Team Tag must also be enabled on the WSF Server device for the WSF Client to connect to it. Trusted Team Tags serve as a "token" that grants access permissions to users.

If you are experiencing issues connecting to a device, first ensure that you have been authorized to do so by verifying with your administrator that the Trusted Team Tag for this device has been created and assigned to your ID. If that is confirmed, double check on the device that the Trusted Team Tag (via the WSF Server interface) has been authorized.

To connect to a device, click on the ***WSF Client*** icon on your desktop (or in your computer's Applications folder). The first action taken is to verify that the user has an active subscription. If one is not present, the user remains on the "Waiting for subscription…" screen until one has been assigned and activated (see Figure 49).

Ensure that you have a subscription.

If you do not yet have a subscription you will see this screen.

Figure 49

If the user has a valid subscription, they are prompted to enter their password, and are brought to the main WSF Client screen (see Figure 51). Both the left and right panes display the file system of the current device you are running the client on.

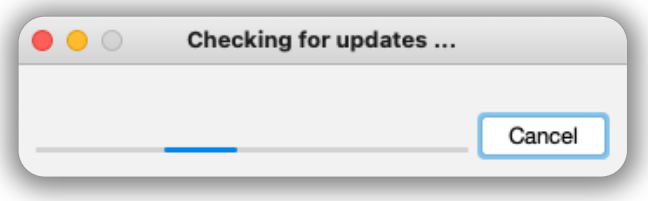


Figure 50

WhiteStar Files automatically checks for updates each time you launch the application (see Figure 50).

Initial startup view

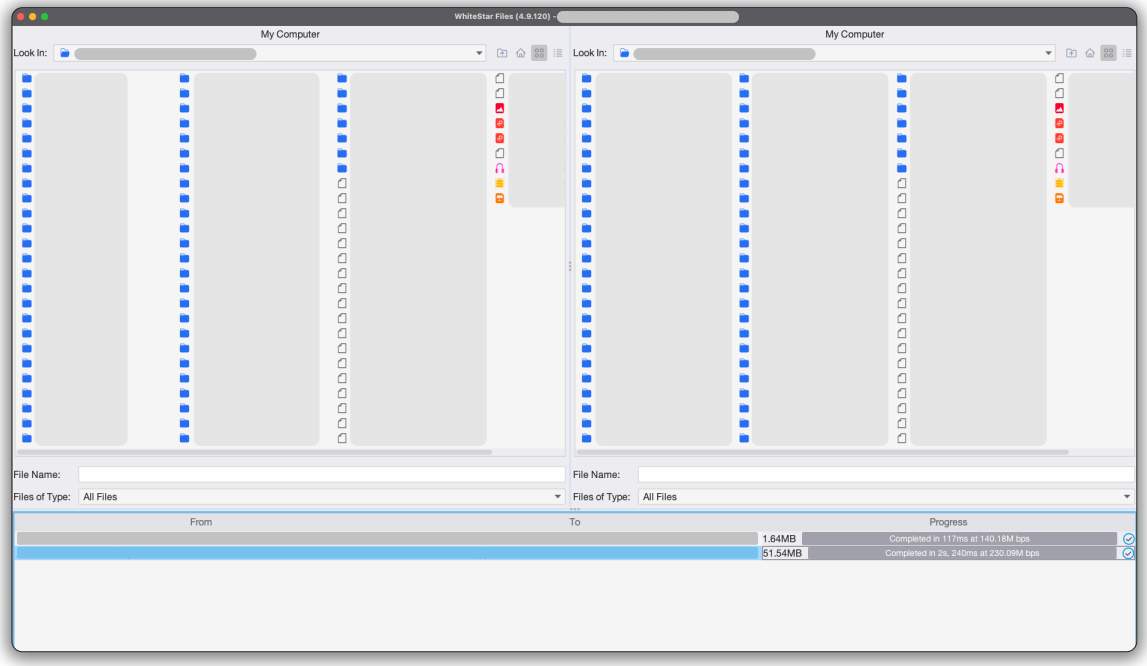


Figure 51

7.1. Transferring Files – Supported Scenarios

WSF is used to initiate files transfers in the following scenarios:

1. From a file system on a device to another location on the <u>same</u> device
2. To/From your local file system and a remote device
3. To/From a remote device to another remote device

When starting the WSF Client application for the first time, both top panes display your local file system. ***Either*** pane can display the local file system or a remote device's file system. The top of each pane indicates the current device it is displaying (e.g., "This Computer" for the local file system).

Figure 52 provides an example of the WSF Client transferring a file from the local file system to another location on the same device. In this scenario, transferring files locally ***moves*** the file from its initial location to the destination – as opposed to copying the file. Using your mouse, simply navigate to the file you wish to move, click (and hold) on the filename, and then drag/drop the file from one pane to the directory you want it moved to on the other pane. This drag/drop capability works bi-directionally.

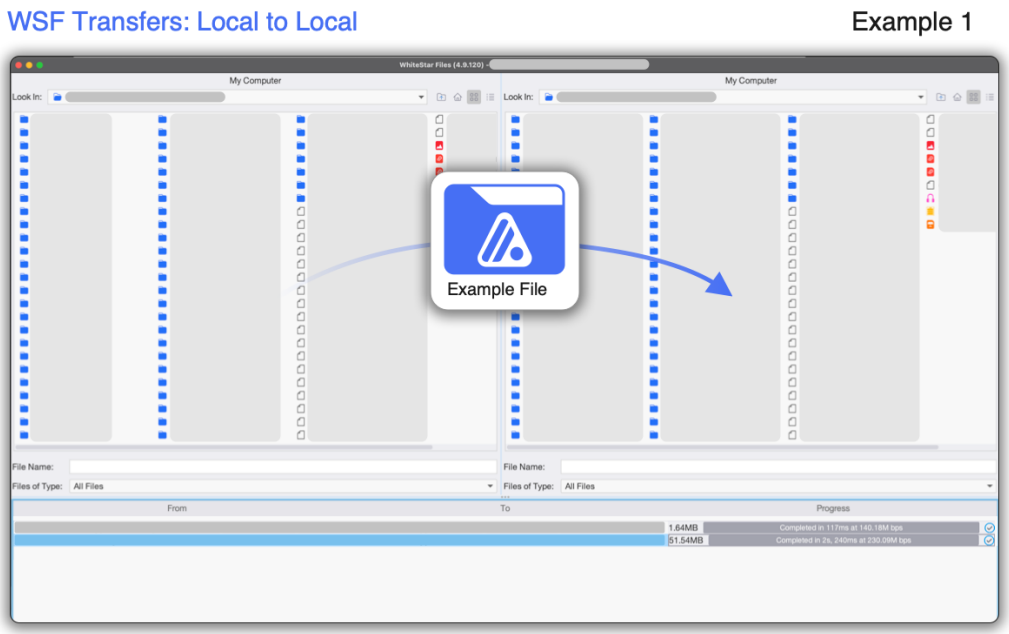


Figure 52

Figure 53 provides an example of the WSF Client transferring a file from the local file system to a file system on a ***remote*** device. Again, drag/drop files from either the local file system to the remote device, or from the remote device to the local file system. When dealing with remote devices the file is ***copied*** (not moved) during the transfer.

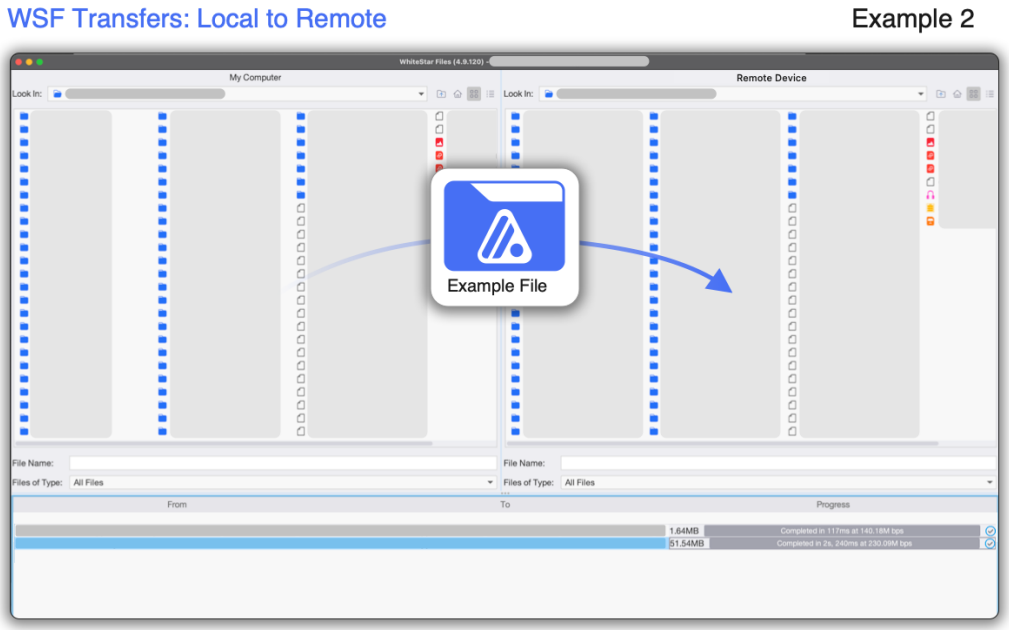


Figure 53

Figure 54 provides an example of the WSF Client transferring a file from one ***remote*** device to another ***remote*** device. Here the user first connects to each remote device individually and then transfer files between them. When dragging/dropping between two different remote systems, files are ***copied*** from one device to the other.

For all transfers via WSF, until the transfer has fully completed, ***no content is available on the receiving device***.

WSF Transfers: Remote to Remote Example 3

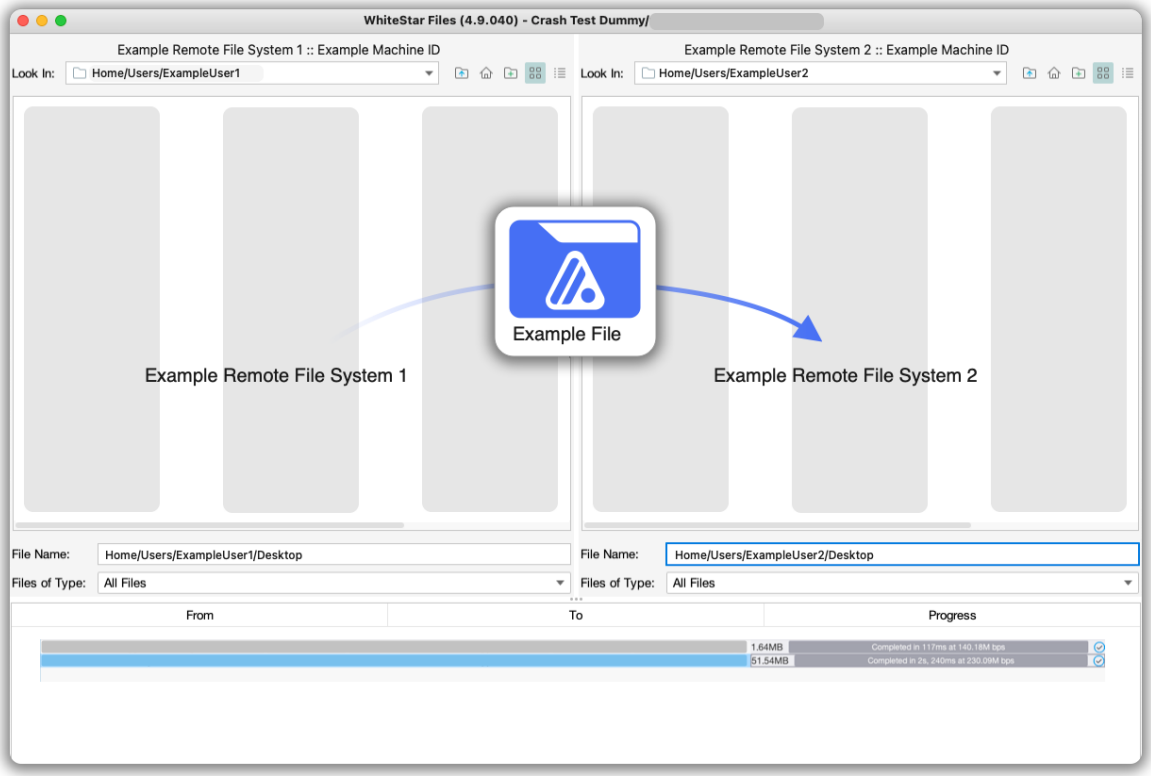


Figure 54

7.2. Transferring Files – Controlling the Transfer Queue

As the transfer action is progressing the user can control the progress of the transfer queue. ***Right-click on the queue***, which brings up a pop-up menu of options. Options include *Force Run*, *Abort Transfer*, and *Delete* transfers from the queue.

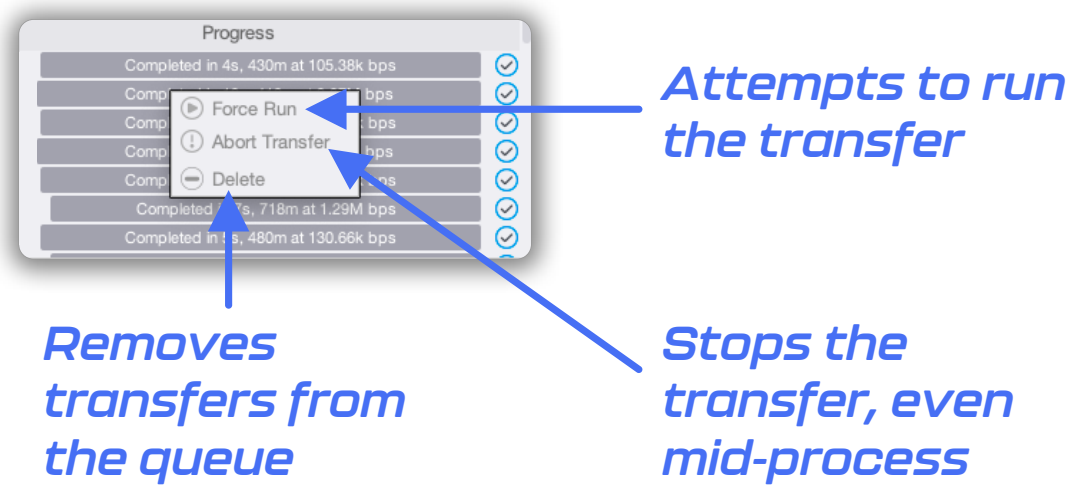


Figure 55

Force Run immediately runs the transfer if it is stopped or paused. ***Abort Transfer*** stops a current transfer in progress. ***Delete*** removes the transfer from the work queue.

To invoke these options, the user selects a particular job (or multiple jobs) in the lower transfer queue pane by selecting them with their mouse. After completing the selection, right-click on any of the highlighted jobs to display the pop-up menu of options.

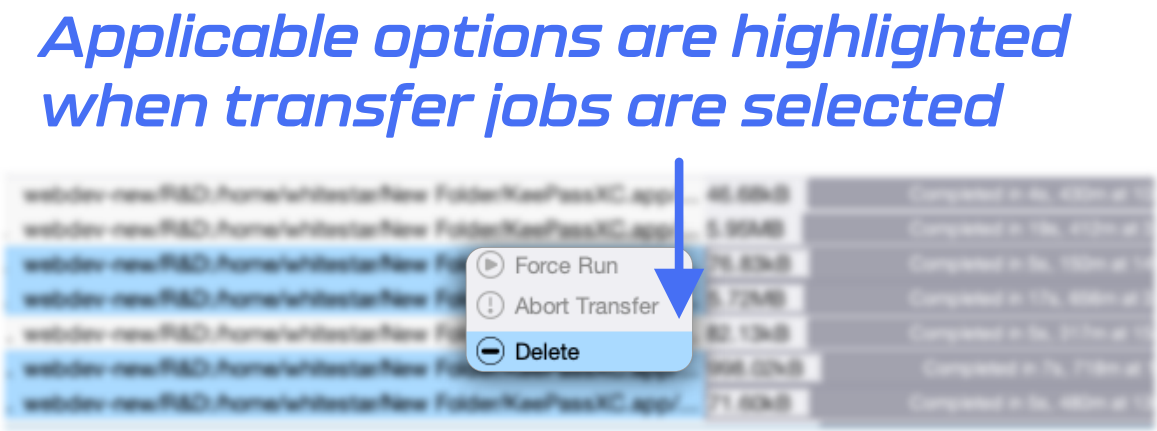


Figure 56

In the case of ***Deleting*** transfers, the user is also required to confirm the deletion.

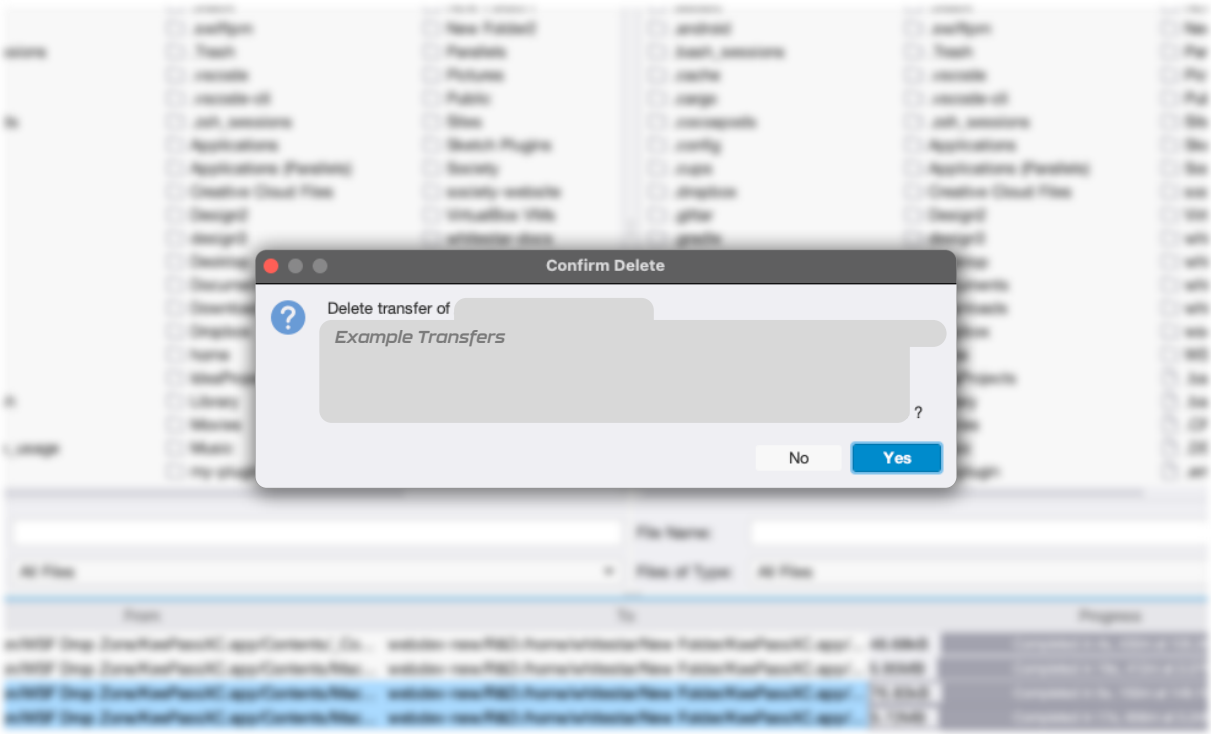


Figure 57

After selecting ***"yes"***, transfers are permanently removed from the WSF transfer queue. The user cannot delete transfers that are currently in progress, instead they must first Abort the transfer and then delete them from the queue.

7.3. Connecting to a Remote Device

In order for the WSF Client to transfer files to/from a remote device it must first establish a secure connection with that device. A Trusted Team Tag must be in place – assigned to the user and enabled on the remote device – prior to attempting to connect.

To connect to a remote device, right click on either upper windowpane window and select "***Open remote connection***" (see Figure 58).

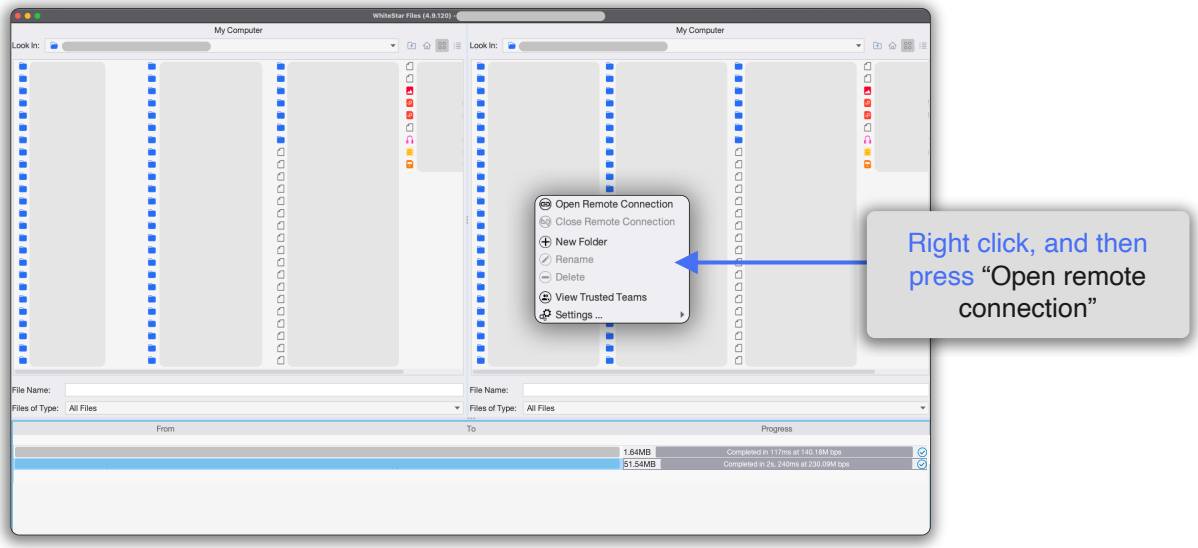


Figure 58

The user is presented with a list of remote devices they have been granted access to. Select the device from the list (see Figure 59) to initiate the connection. If the desired device is not displayed in the list, contact the administrator of that device to have them grant this WSF Client user access.

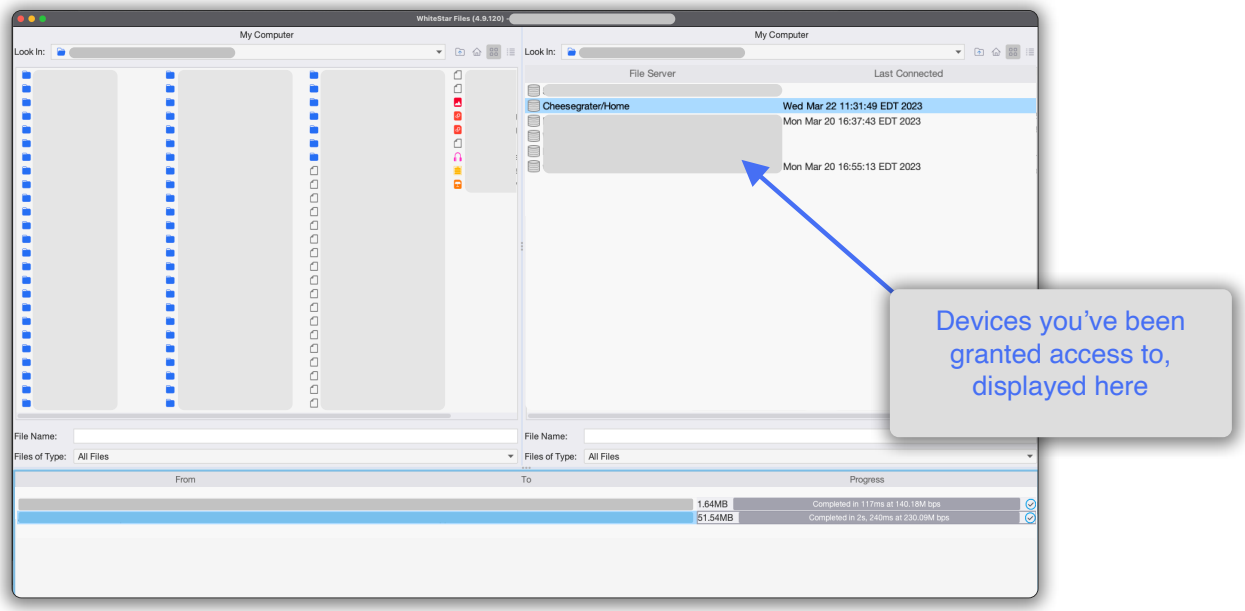


Figure 59

Once the connection is established the WSF Client presents the file system of the remote device in the pane selected.

There are two types of connections on WSF between the client and server: Peer-to-Peer or Tunnel. WhiteStar first attempts to create a Peer-to-Peer connection, indicated on the application by a green icon, which is considered the optimal connection. This allows devices to communicate directly between each other, increasing transfer speeds between the devices.

Figure 60

If the client and server are unable to connect via ***Peer-to-Peer***, they are connected using a Tunneled connection, which routes packets with assistance from the WhiteStar Network. This connection maintains a high transfer speed, but requires slightly more overhead, and thus is less optimal than a Peer-to-Peer connection.

WSF is designed to act as a good citizen and will not over utilize your network while you are using the application. This is especially important for mobile environments, where mobile devices may not have as robust of a network connection as a wired desktop environment. WhiteStar is specifically designed to deal with these issues by responsible network management.

7.4. Disconnecting a Remote Device

Upon completion of file transfers, simply right-click on the connection panel pane and select the ***Close Remote Connection*** button from the drop-down list (see Figure 61). Alternatively, if the user has completed all file transfers, they can shut down the WSF application which automatically severs all connections between the client and servers.

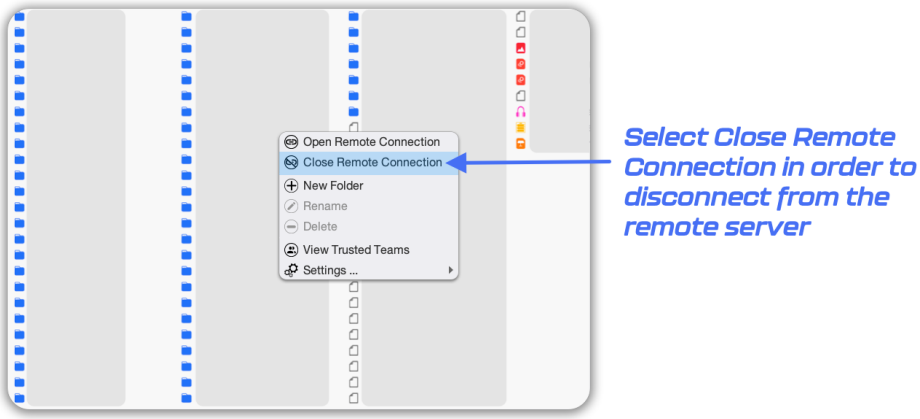


Figure 61

7.5. Creating New Folders

Users occasionally need to create folders for organizing files transferred on another device. In order to create a new folder, navigate to the directory you want to create this folder in. Right-click with your mouse in the pane and select ***New Folder*** (see Figure 61). This creates a temporary folder called "New Folder" on the device. Select the new folder and right-click on it (selecting "***Rename***") to change the name of the folder (see Figure 62).

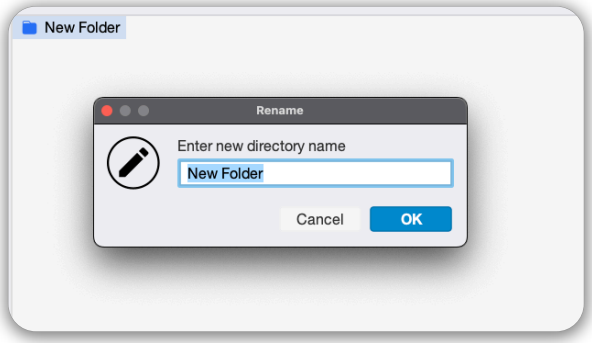


Figure 62

7.6. Deleting Files / Folders

At times files or folders need to be deleted from the device the WSF client is connected to. To delete a file or a folder, select [highlight] the target file(s) or folder(s) with a single left click of the mouse, then ***right-click*** to open the drop down and select ***Delete***. This user is prompted to confirm the delete (see Figure 63).

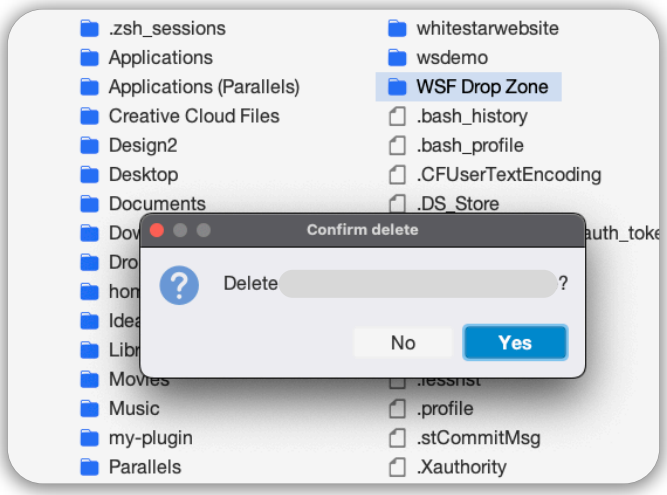


Figure 63

7.7. Navigating the Directory / Changing the View

To navigate the WSF client application directory structure view, the user clicks on the buttons in the **top right-hand corner of the screen** (see Figure 64).

- To traverse to the parent directory of the current directory, click on the "***go up one level***" button [icon of a file folder with an arrow pointing up].
- To return to the home [top level] directory of the server, click on the "***home***" button [icon of a house].
- To toggle the directory structure view between the list view or grid view, click on the appropriate button.

Figure 64

7.8. Viewing Trusted Teams Assigned to User

For a list of ***Trusted Team Tags*** that have been assigned to the user, right click on the application window and select "View Trusted Teams" (see Figure 65). Team Tags that have been granted are listed in the popup box. When users need to access a remote server, they should provide one of these Team Tags to the administrator of the server they are attempting to connect to. The administrator must add this Trusted Tag to the ***Trusted Devices*** list on the server for access to be granted.

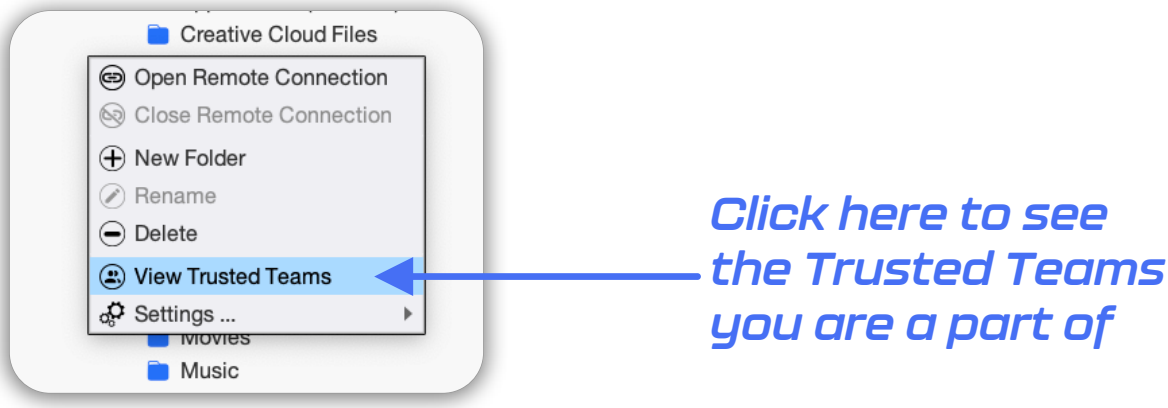


Figure 65

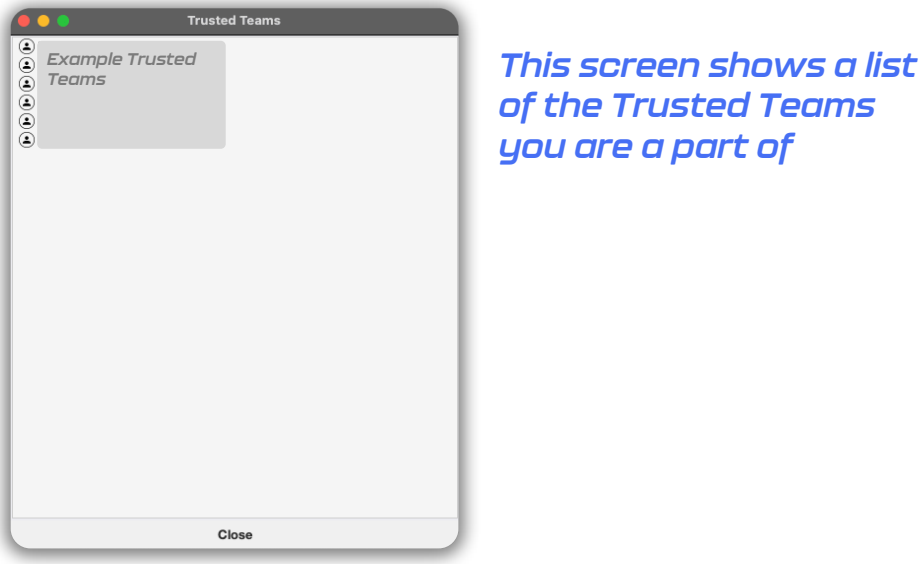


Figure 66

7.9. Setup Authenticator – Resetting your 2FA Authentication

In order to reset your 2FA Authenticator, right click on the WSF Client in either of the two connection windows and scroll down to the Settings menu. Then click "***Setup Authenticator***".

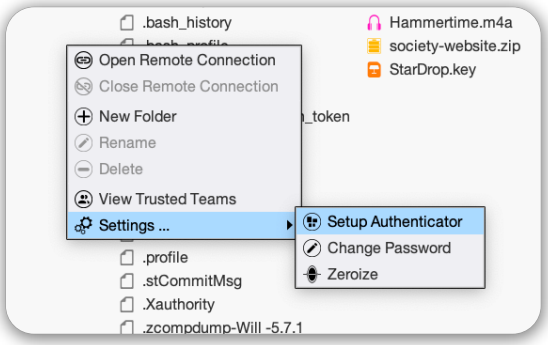


Figure 67

You will then be displayed with a QR code that you can scan from your Authenticator app. Once you have added your secret key to your Authenticator, you can then click "***done***". This will function with any Authenticator app (Google, Microsoft, etc.)

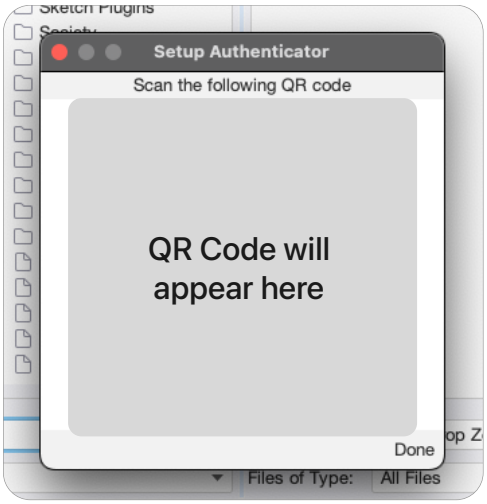


Figure 68

If you already have an Authenticator entry on your Authenticator app for WSF, you will need to delete the previous entry for WSF.

7.10. Changing your Password

To change your password, right click anywhere in the main connection window of WSF and scroll to the "***Settings***" option. Then click "***Change Password***".

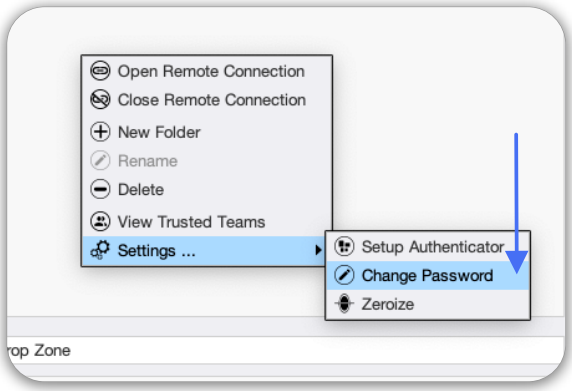


Figure 69

Then enter your new password, and confirm the same new password in the second box. Once you have the new password you wish to change to, click "***Change***".

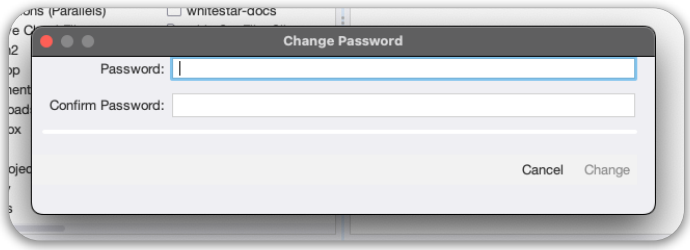


Figure 70

The next time you log in, your password will be changed.

7.11. Zeroizing your Application

If the user wants to completely remove their WSF account, and securely delete all information that have been generated on this device, they can do so by clicking on the "***Zeroize***" in the right click menu.

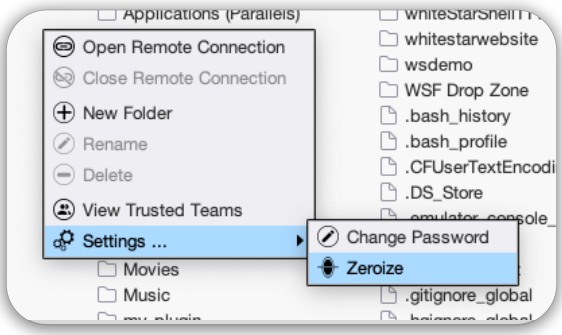


Figure 71

You will then see a prompt to Zeroize the application, which will reset the application and delete all information and data about the user profile the Application has stored.

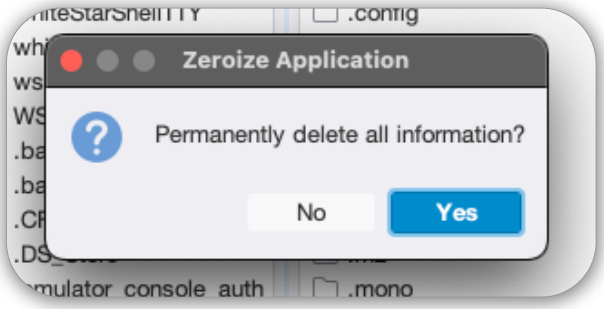


Figure 72

At this point, upon relaunching the application, you will need to set up a new profile and user information, beginning from the start.

7.12. Displaying Transfer Status

When a file is moved or copied to a remote server, WSF displays the sender and receiver file paths at the bottom of the application, along with a progress bar as the file progresses from one device to the other (see Figure 73).

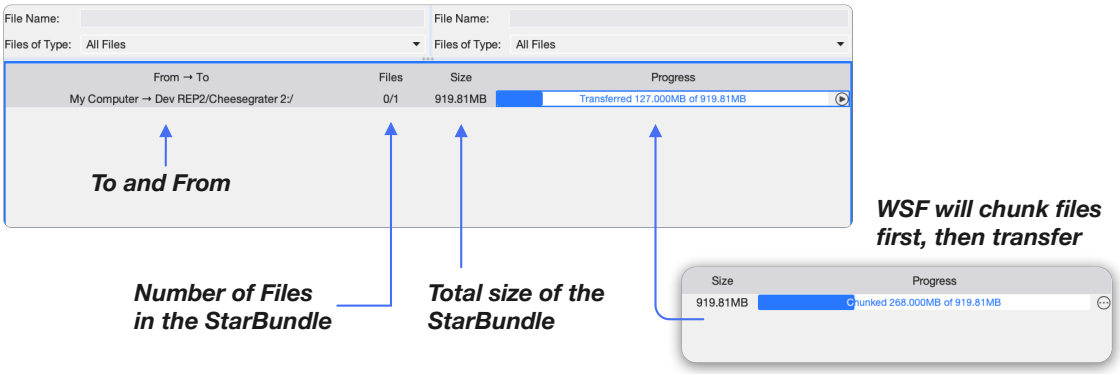


Figure 73

If transferring multiple files, the user sees files queued (no status in the progress bar) until they sequentially begin to move from sender to receiver.

Note: by default, WSF will ***copy*** files when transferring files between devices, leaving a copy on the sending device, and creating a new copy on the receiver. When moving files on the same device/locally, WSF will ***move*** the file from the source to the destination.

8. Installation / Configuration of WSF Server

For a WhiteStar Files user to connect to a Server device (running the WSF Server software), an administrator needs to install the WSF Server component on to the machine they want WSF Client users to connect to. The WSF Client component runs on Microsoft Windows, Apple macOS (both Intel and Apple Silicon), and Linux systems.

8.1. Installation on Linux Server

Installation of the WSF Server software is accomplished via the built-in Linux DNF or YUM package managers.

The system administrator will need to execute the following two commands to add the WhiteStar repository and then install the software. Each requires root privileges.

```
# sudo dnf copr enable -y whitestar/wsf

# sudo dnf install -y wsf
```

From here, the admin manages the WSF Sever by way of the online ***WhiteStar Administrator's Dashboard*** (see below).

8.2. Installation on Mac OS or Windows

Open a web browser and navigate to the following WhiteStar website: https://whitestar.io/download/wsf/server. The user is presented with a link to download the WSF Server component for the operating system they are currently running on. If not, select the appropriate link for the operating system you want and download the installation package.

Ensure that there are the correct user privileges on the local device to install software on it. You may notice that on certain macOS devices, you will have to allow third-party developers to install software on your device. Click on the "**?**" Button and your Mac will automatically show a popup prompting you to follow it to the Controls/Security and Privacy settings to allow permission.

Open the folder where the WSF installer package was saved.

Click on the download package to ***run the installer***. You are brought to the following screen

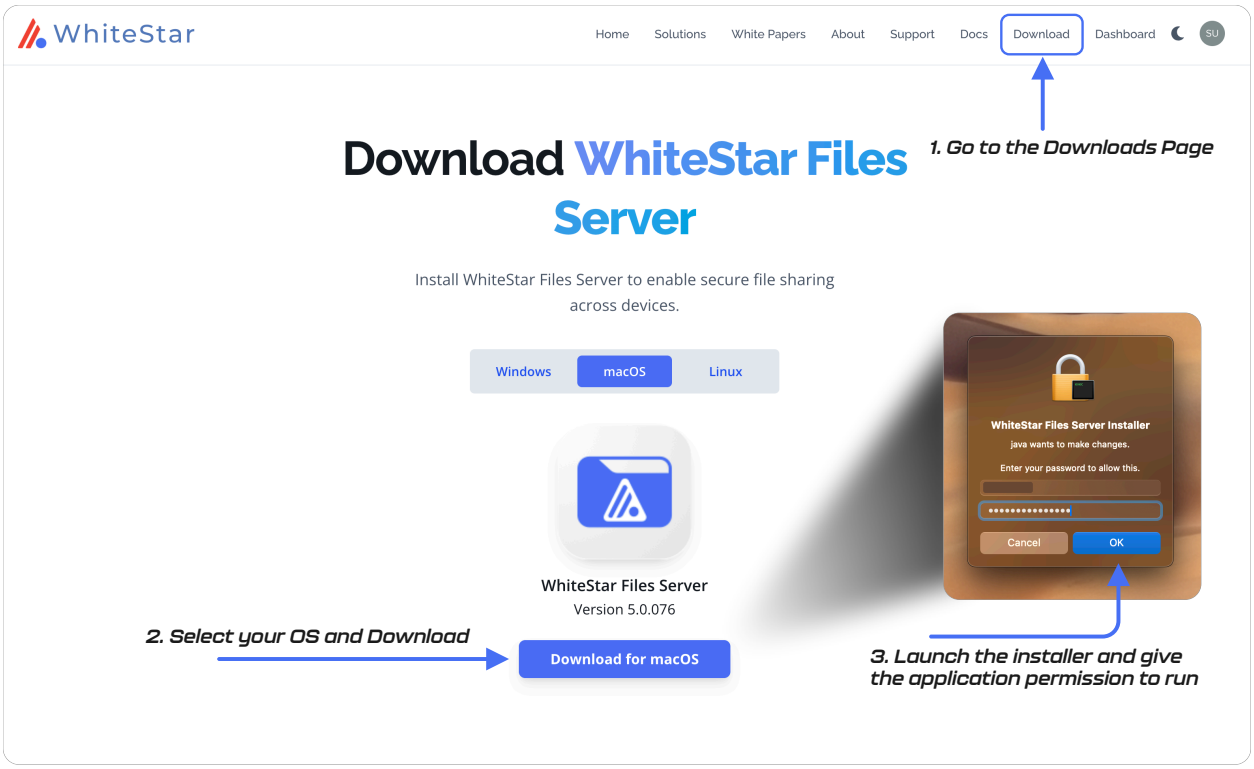


Figure 74

Once you launch the installer and give the installer permission to run, follow the prompts on the screen to complete the installation.

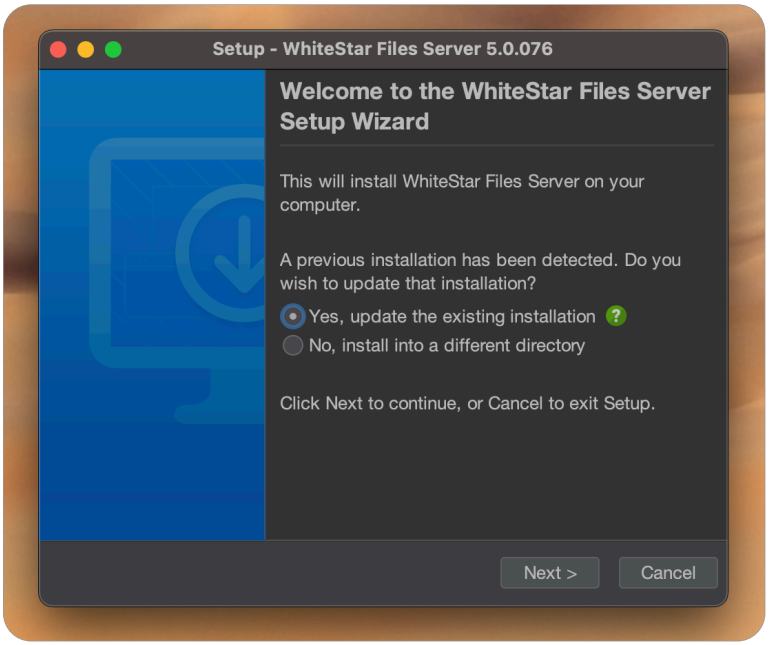


Figure 75

From here, the admin manages the WSF Sever by way of the online ***WhiteStar Administrator's Dashboard*** (see below).

8.3. Configuration and Use of WSF Server

Once the WSF Server has been successfully installed, the device administrator can:

- Configure which threat detector the WSF Server is utilizing and where it resides:
  - Linux:
    - Edit the /etc/systemd/system/wsf.service file
    - Find the "ExecStart" command line
    - Add/Edit the threat detector class to run:
      - Default: -dthreatDetectorClass=io.whiteStar.api.OPSWAT
      - Mock detector: -dthreatDetectorClass=io.whiteStar.api.MockThreatDetector
    - If the threat detector is NOT on the same machine as the WSF Server, the admin must provide the IP address of the machine it is running on (on the ExecStart command as well)
      - -DOPSWATBaseUrl=http://xx.xx.xx.xx:8008
  - MacOS and Windows:
    - Edit the WhiteStarFilesServer.vmoptions file
    - Add a line at the bottom for the threat detector class to run:
      - Default: -dthreatDetectorClass=io.whiteStar.api.OPSWAT
      - Mock detector: -dthreatDetectorClass=io.whiteStar.api.MockThreatDetector
    - If the threat detector is NOT on the same machine as the WSF Server, the admin must provide the IP address of the machine it is running on (on the ExecStart command as well) by adding another line to the file (not the same line as the threat detector class)
      - -DOPSWATBaseUrl=http://xx.xx.xx.xx:8008

- While logged directly in to the device the WSF Server is running on:
  - enable and disable the WSF Server service running on the device (See section Starting and Stopping the WSF Server Service)
  - view the unique ID of the device which is used to claim the device from the administrator's dashboard (See
  -
  -
  - Viewing the Unique ID of the WSF Server Device)

- From the administrator's dashboard:
  - maintain the list of trusted team tags which can access the device, and specifically which directories on the device they have access to

- configure notifications to be sent when files are transferred
- configure web hooks to be executed when files are transferred

This can be done from the WhiteStar Administrator's Dashboard. Simply navigate to the "***Things***" tab on the lefthand side and then select the "***Thing***" (device) you wish to interact with. If your WSF server isn't yet connected to your Dashboard, visit the section Viewing the Machine ID of the WSF Server Device.

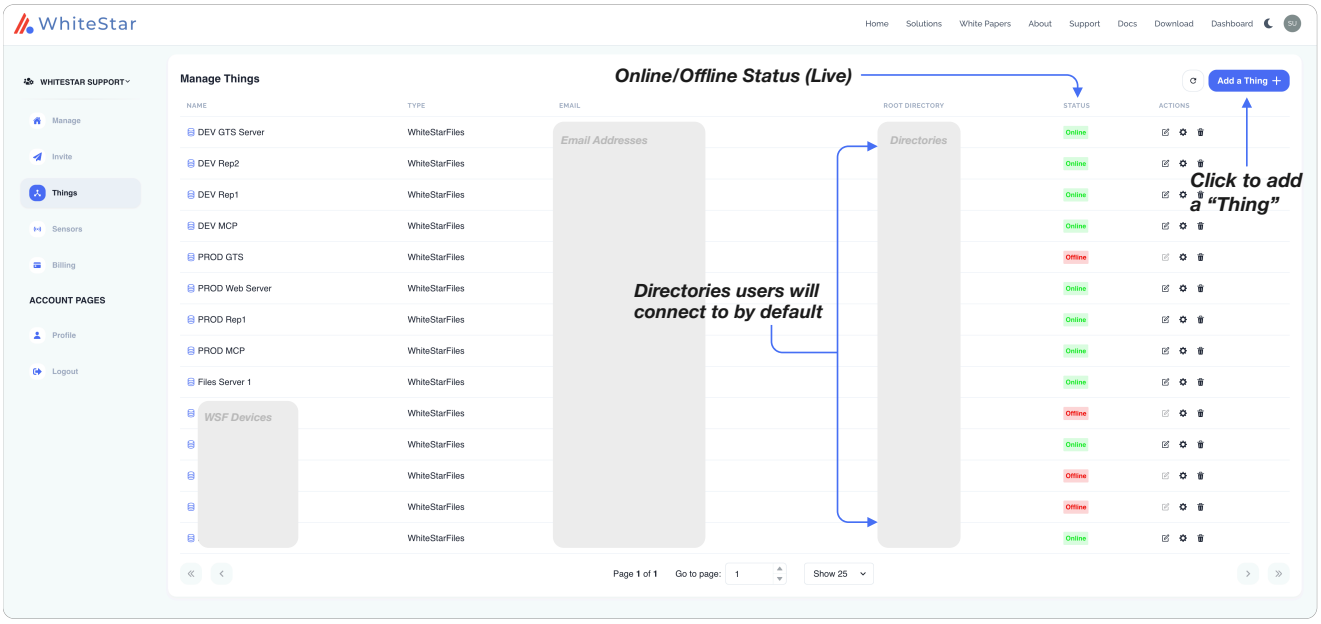


Figure 76

From the "Things" tab on the Dashboard, you can view and manage your "Things", or devices. WhiteStar refers to them as "Things", as in the "Internet of Things", but with WSF we are concerning ourselves with servers. Click on "***Add a Thing***" in the upper righthand corner of the screen, which will bring up a screen to add a "Thing".

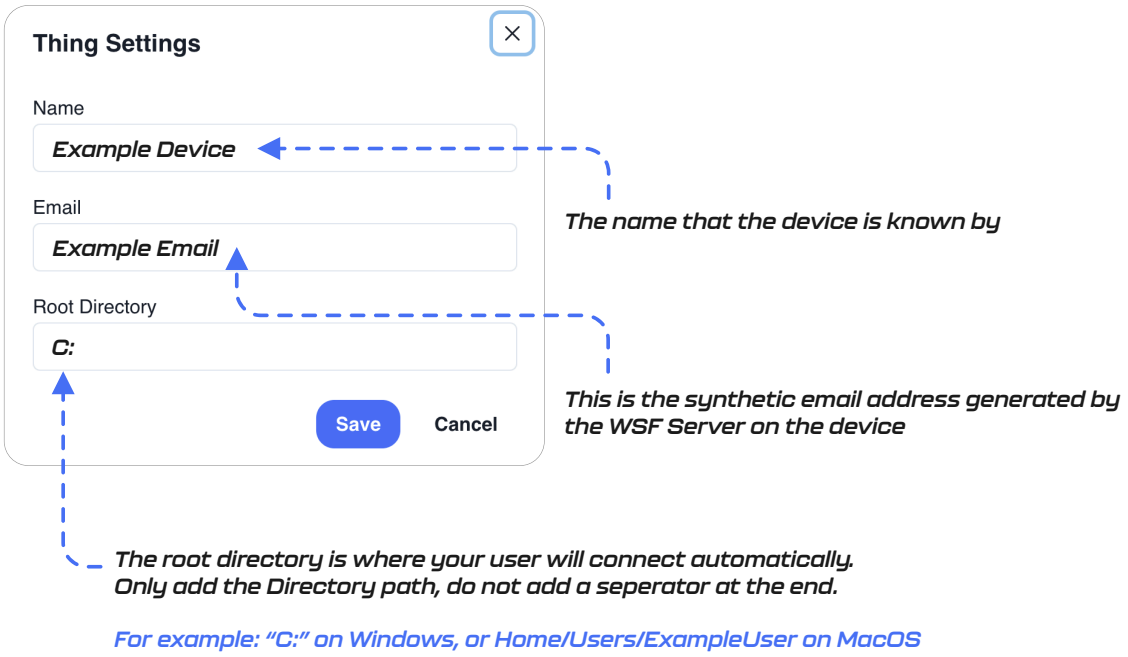


Figure 77

The administrator is presented with a screen pop up as represented in Figure 77. This configuration panel requires the administrator to enter the server name (free form text field), the synthetic email address generated by the WSF Server of the device that is to be managed (please see "

Viewing the Unique ID of the WSF Server Device" below to obtain the synthetic email address), and the fully qualified path of the root directory where the WSF Server will connect to.

NOTE: each operating system will have different OS-specific eccentricities regarding which directories the WSF Server can access. Be aware that WSF *will not be able to access*, for example, individual user desktops on MacOS, or the documents folder of Windows. We generally recommend setting up a "***Drop Zone***" folder at the user level or above on devices to allow for the best compatibility and ease of use.

After clicking "***Add***", your new WSF server will be placed in your list of "Things". From here, the administrator will have access to set Trusted Team Tags on the server. Click the small "***pencil***" icon on the righthand side of the screen to proceed to the server control page, then, at the top left of the screen, press the "***+***" button to add a Tag. Select a Tag, then click okay. Now any Federation with this Tag will be able to connect to this device.

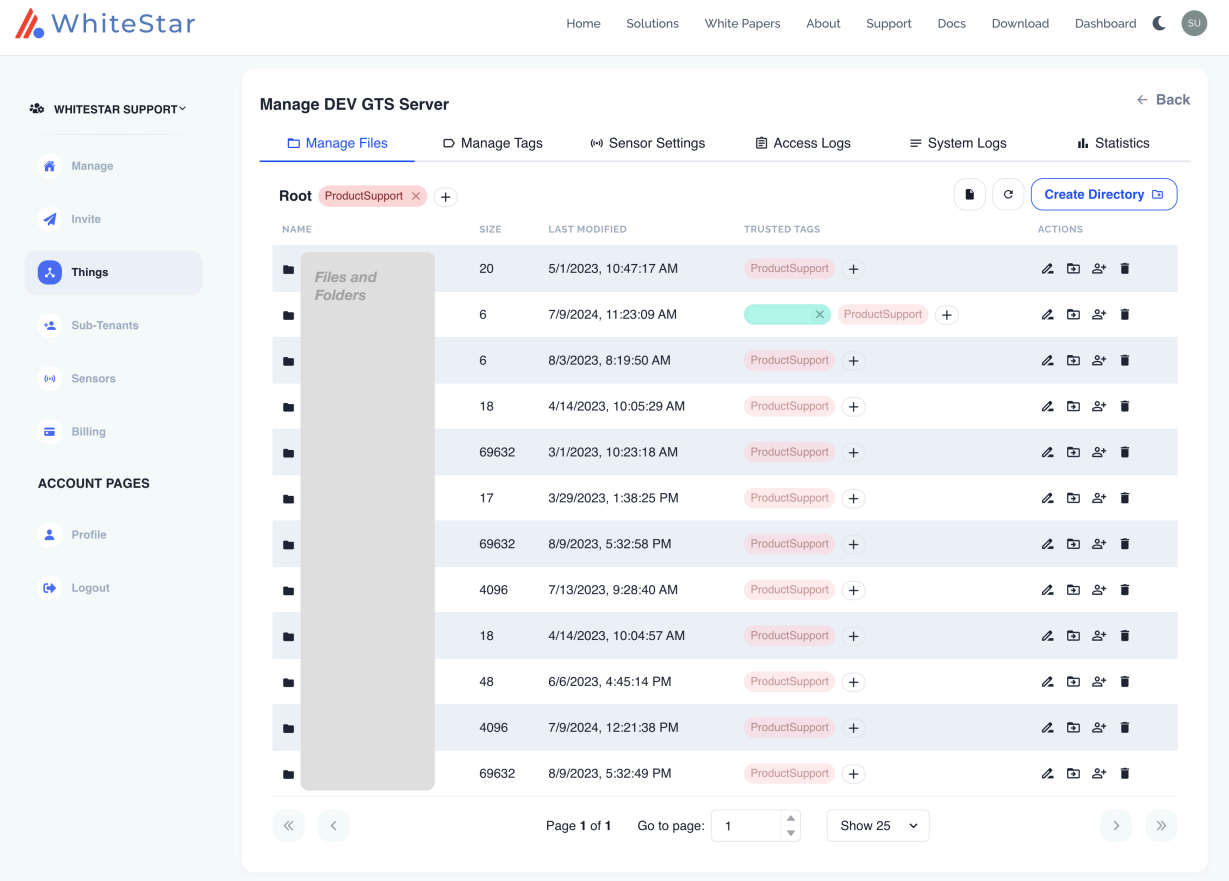


Figure 78

At the top of the screen, you can remotely access logs from each server. This will enable you to see who has logged onto the server, who has StarDropped files to the server, which files were Dropped, etc. It can also be useful for diagnosing potential issues with the server remotely. Both system and access logs are available.

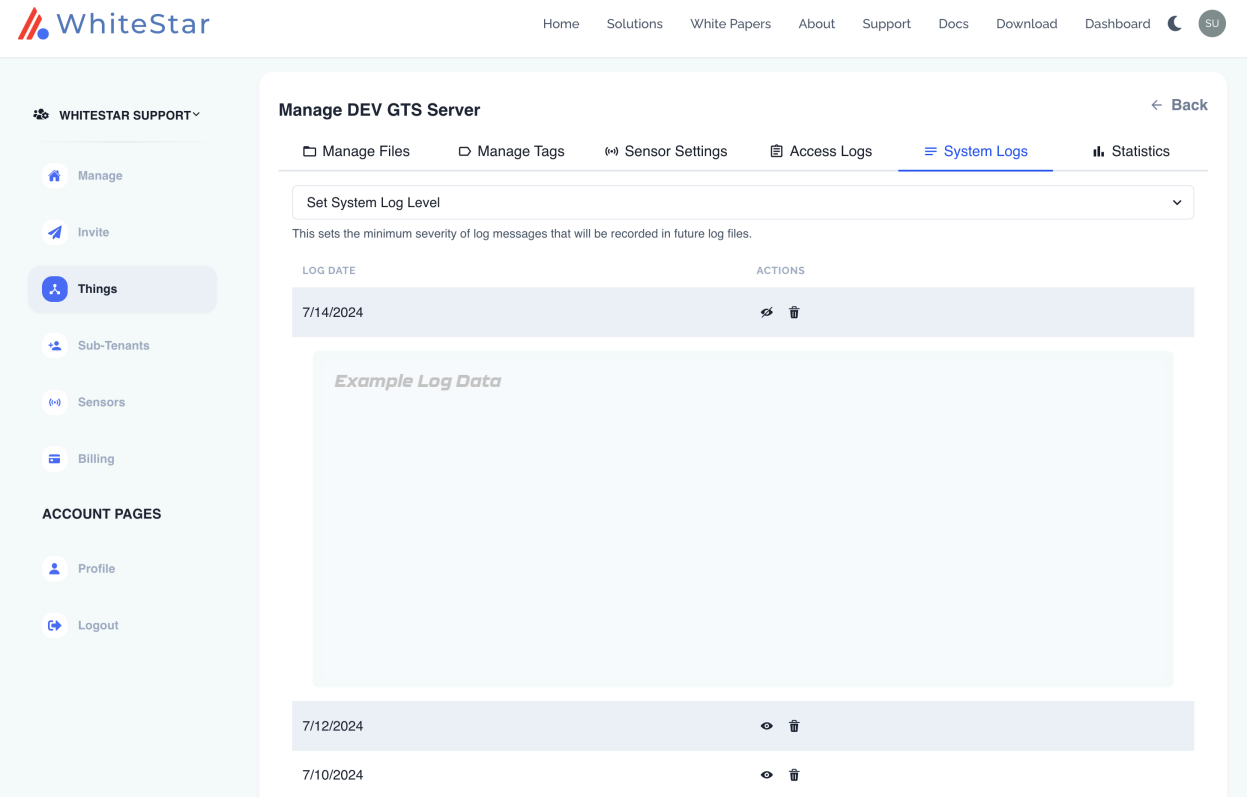


Figure 79

When looking at the individual device overview screen, we can see (from left to right) that there are individual folders, the size of each folder, the time it was last modified, the Tags allowed to access that individual folder (if you need even finer control over who may access individual folders on a particular device) and a series of options on the righthand side. In addition, at the top righthand corner, there is a toggle to show or hide individual files (instead of just folders), a refresh button and a button to create a new directory (or folder).

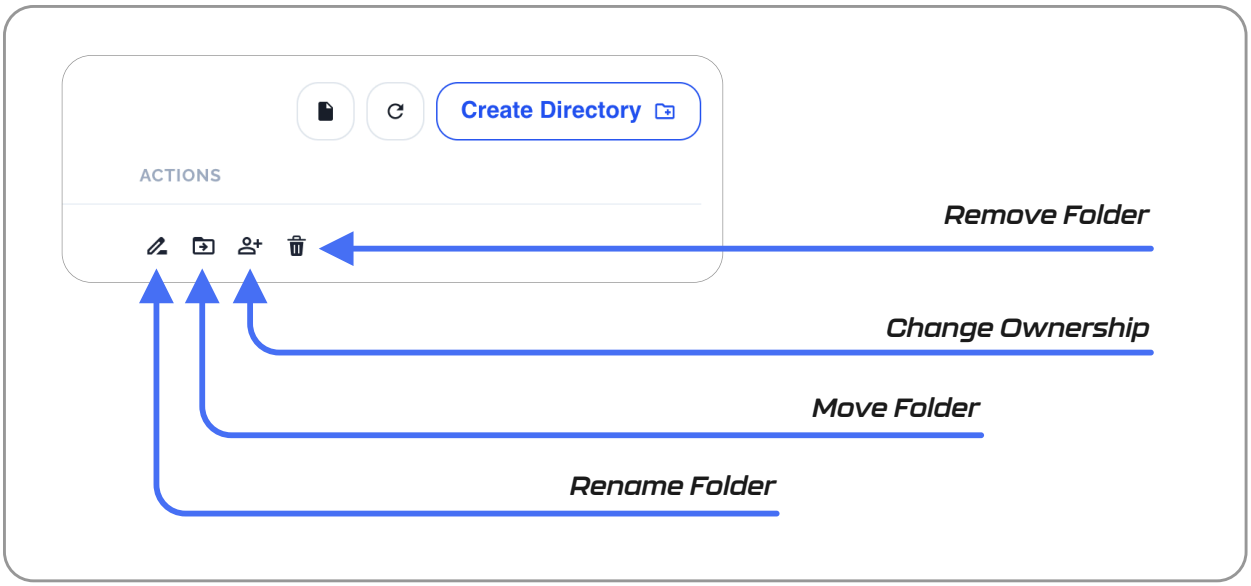


Figure 80

The actions that are on the righthand corner are as shown in Figure 80.

Clicking on Rename Folder will allow you to rename the folder. Moving the folder will allow you to define a new path for the folder, as shown in Figure 82.

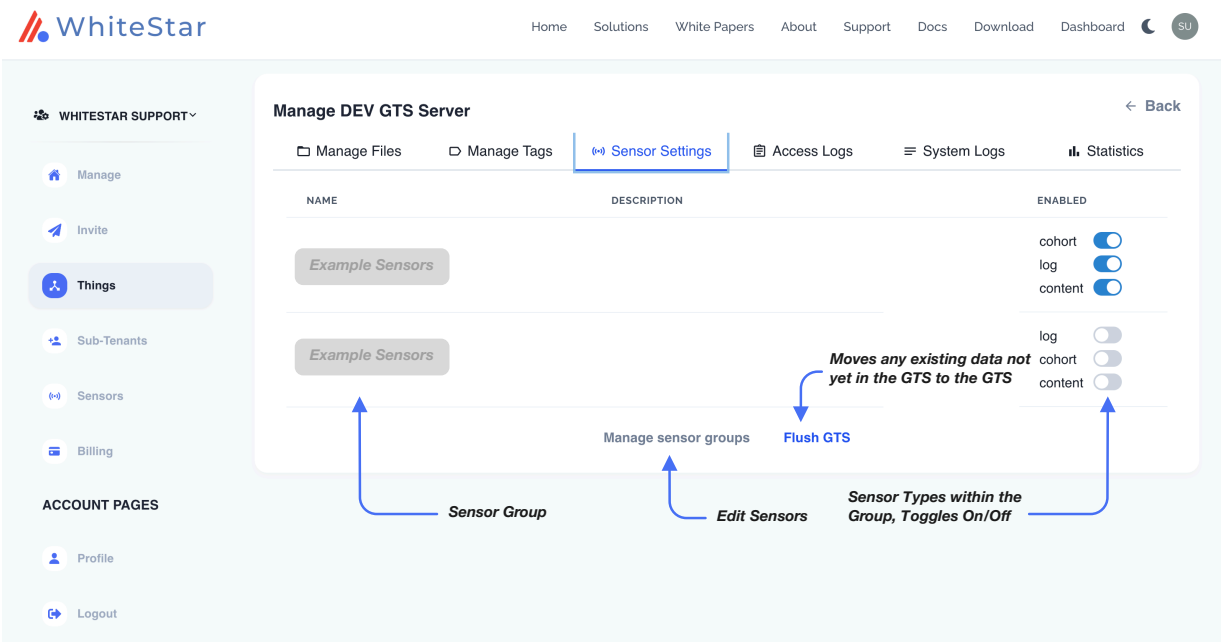


Figure 81

On the sensors setting page, working from left to right, is the name of existing sensor groups, the sensor group description, access logs and the ability to turn on and off particular types of sensors within the group. There are also buttons at the bottom of the screen that will enable a

flush of un-backed-up data to the GTS database. Additionally, there is a button that will take the user to the sensor group management page.

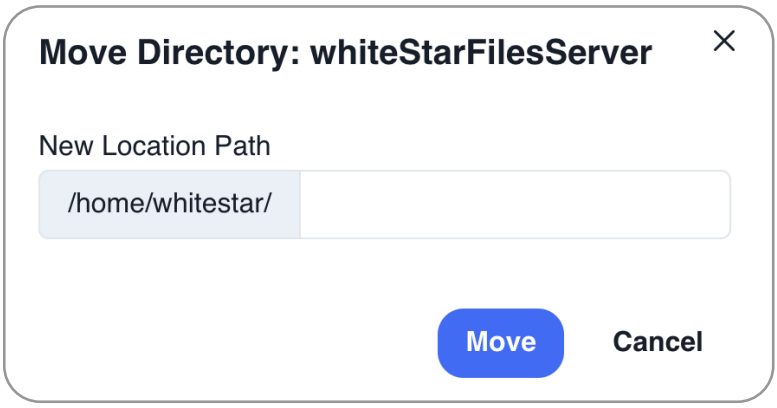


Figure 82

If you need to change the ownership of the folder, simply click the “Change Owner” button (Figure 83) and you can define the new owner of the folder. The ownership can be conferred on both existing and new owners, if need be. Keep in mind the owner of a folder may do things like remove/delete folders, change permissions, etc.

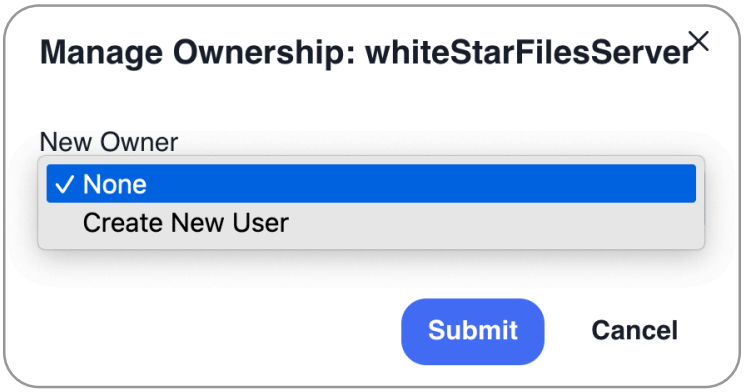


Figure 83

When creating a new user, make sure to enter a valid email and name for the user of that you wish to make the new owner of the folder.

8.4. Up/Down Notifications for WSF Servers

WSF Servers can send users a notification when they go on or offline, so the user can understand that the server is either capable or not capable of receiving files. The server notifications can be accessed from the device menu.

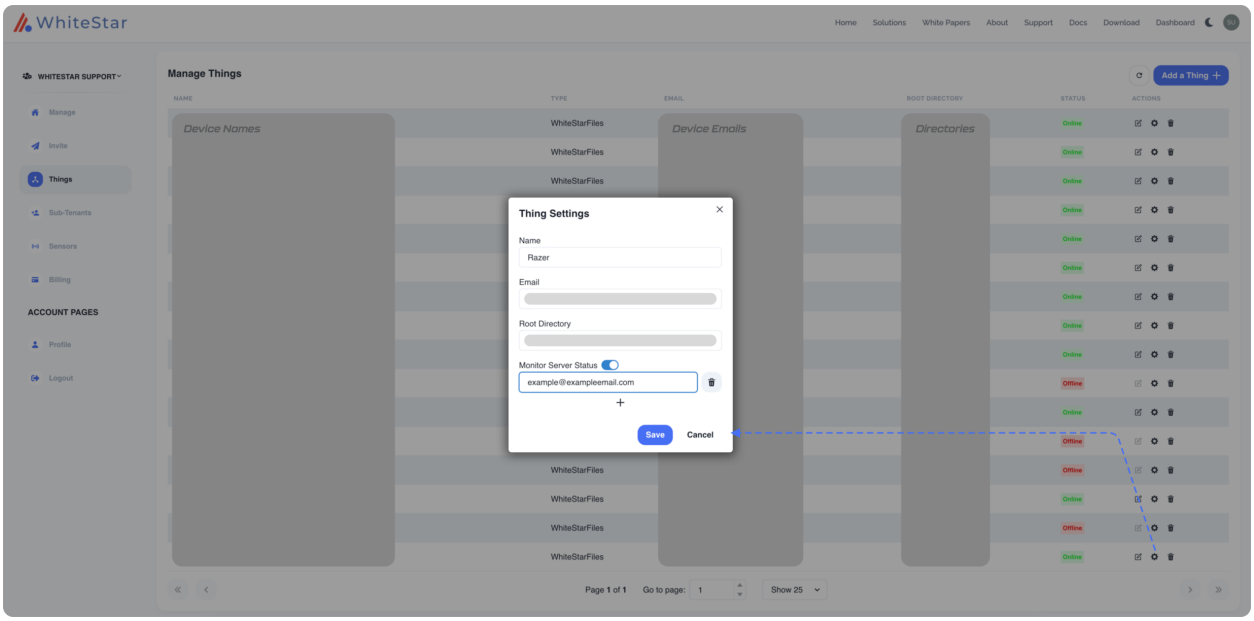


Figure 84

By pressing the “gear” icon on the righthand side of the devices page, you can access the “Thing Settings” page. Checking the toggle box at the bottom of the dialogue box will create a field for an email address. After entering in a valid email address and hitting “save”, the WhiteStar Vortex email server will send a notification email to that address when the server goes on and offline.

This can be useful for detecting issues with a server going down, knowing when updates to servers start and finish, and in the event you have a mobile server, you can know when the server is capable of receiving a transfer.

8.5. Starting and Stopping the WSF Server Service

The WSF Server service runs securely on the remote device and only allows connections by trusted teams specifically configured for that device. The service can be kept running at all times, or toggled on and then off for only the time a WhiteStar Files client requires access to the device.

To start/stop the WSF Server service:

- Log in to the device the WSF Server has been installed on

- Open a terminal or shell and run the following commands:
  - ***Linux*** (must be run as sudo)
    - Start: systemctl start wsf.service
    - Stop: systemctl stop wsf.service
  - ***Windows***

    - Start: net start WhiteStarFileServer
    - Stop: net stop WhiteStarFileServer
  - ***MacOS*** (must be run as sudo)
    - Start: sudo /Applications/WhiteStar\ Files/WhiteStar/WhiteStarFilesServer start
    - Stop: sudo /Applications/WhiteStar\ Files/WhiteStar/WhiteStarFilesServer stop

If WhiteStar Sentinel is licensed and installed on the WhiteStar Files service, it will need to started manually. This is added to the WSF start command as an optional when starting WhiteStar Files on the device:

```
-DthreatDetectorClass=io.whiteStar.api.OPSWAT
```

Currently WhiteStar Sentinel is configured to use Opswat API's by default, which may run locally or remotely, depending on how the deployment is configured. Optionally, if using the Opswat scanning system on a different device other than the device running WhiteStar Files server on, users can specify the URL here:

```
-DOPSWATBaseUrl=http://localhost:8008
```

The Opswat scanner needs a certain amount of time to scan files. This is defaulted to 20 minutes, however If additional time beyond 20 minutes to process information for large datasets is needed, one can manually define the duration that the process will be given by entering in the following command:

```
-D OPSWATHttpDuration=20
```

If needed, a manually specified API key on the server for security purposes can be specified using the following optional:

```
-D OPSWATApiKey=<the key>
```

8.6. Viewing the Unique ID of the WSF Server Device

Each "***Thing***" (WSF Server device) within the WhiteStar network is referred to by its unique ID (currently its WhiteStar email address). This email serves as your identification for the WSF service, and you will need to enter this email address onto the Dashboard under "Things" to allow the Dashboard to interact with the WSF Server.

- Open a terminal window on your OS. These instructions will be valid for *all* operating systems.

- Type ***telnet localhost 42526*** (ensure Telnet is installed and enabled, if it is not, install and enable Telnet, as it may not be installed or enabled by default on certain, especially Windows operating systems).

- Once you see the prompt from a successful connection to the service, type ***wai*** ("*Who am I?*"). You will be presented with 3 pieces of information: Federation, member, and email address.

```
Connected to localhost.
Escape character is '^]'.
Enter ?l to list available commands.
wai
WhiteStarFiles> I Am
Federation [[redacted]] member [[redacted]] email [[redacted].WhiteStarFiles@vortex.com]
```

Figure 85

- The administrator will need to highlight and copy the entire email address into the copy buffer in order to add the Server to the list of "Things" that get managed by their organization.

8.7. Zeroizing the WSF Server interface

If the administrator wants to completely remove the WSF Server account, and securely delete all log files that have been generated on this device, they can do so by:

- Open a terminal window on your OS. These instructions will be valid for *all* operating systems.

- Type ***telnet localhost 42526*** (ensure Telnet is installed and enabled, if it is not, install and enable Telnet, as it may not be installed or enabled by default on certain, especially Windows operating systems).

- Once you see the prompt from a successful connection to the service, type ***zero*** ("*zeroize")*

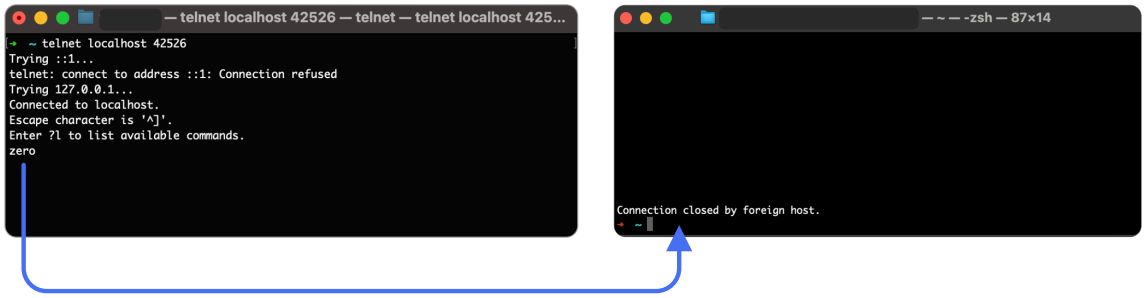


Figure 86

8.8. Maintaining the list of Trusted Teams Who Can access a Device

In order for a "Thing" (e.g. WSF Server) to be accessed by a WSF Client, the system administrator of the device must add trusted team tags to it via the administrator's dashboard.

To add a trusted team tag:

- Log in to the Admin Dashboard (from the WhiteStar web page: https://www.whitestar.io)
- Click "***Things***" on the lefthand side of the screen, which displays all devices that have been claimed by your organization
- Find the "Thing" you wish to grant a Trusted Team Tag to, and click on the ***pencil icon*** on the righthand side of the screen to manage that "Thing's" options
- Navigate to the directory you which to grant access to. If you want to grant access to the entire server, there is a ***"+"*** button at the top of the page which will allow you to add the Trusted Team Tag to the "root" of the server device
- Once you have navigated to the directory you want to add the Trusted Team tag to, under the "***Trusted Tags***" column on the web page click on the "***+***" sign and add the tag you have previously created. Keep in mind that the administrator must have created the Trusted Team Tag prior to attempting to add the Tag to the "Thing"
- Users who have this Trusted Team Tag assigned to them ***will now be able to access this device, and the folders it has been assigned to***

In order to grant access to a specific directory, when adding a Tag to a "Thing", you will be able to define a path for the user to "land" on when connecting to that server. It's important to

define the path (for example on Windows: C:\username or MacOS: /Users/username , etc.) otherwise the user will be able to connect to the root directory of the machine. This can be ***extremely important for limiting access to a particular device***, as a user will not be allowed to go "above" the directory they connect to.

Note: if the administrator wants to allow the WhiteStar Files user to access the device, they must ensure the WSF Server service is running on the box (see Starting and Stopping the WSF Server Service).

If, at any time, the administrator wants to remove access for a particular Trusted Team from the Server, they need only click on the "garbage can" icon to the right of the team (see **Error! Reference source not found.**) and access is removed for that team.

8.9. Maintaining WSF Server Software

8.9.1. Update on Linux Server

In order to keep the WhiteStar Files Server up to date, the device's administrator must issue the following command (during their routine maintenance window):

```
# sudo dnf update -y wsf
```

This command automatically checks the versions of WhiteStar software (or any of its dependencies) currently installed to determine if they need to be updated. If updates are required, the new version is automatically downloaded and installed on the device. If the current version is up to date, the administrator will receive a command response indicated there is "Nothing to do".

8.9.2. Update on Mac OS or Windows

In order to keep the WhiteStar Files Server up to date, the device's administrator must download the latest software from the WhiteStar website and follow the install directions (similar to the initial installation).

Open a web browser and navigate to the following WhiteStar website: https://whitestar.io/download/wsf/server. The user is presented with a link to download the WSF Server component for the operating system they are currently

running on. If not, select the appropriate link for the operating system you want and download the installation package.

Ensure that there are the correct user privileges on the local device to install software on it. You may notice that on certain macOS devices, you will have to allow third-party developers to install software on your device. Click on the "**?**" Button and your Mac will automatically show a popup prompting you to follow it to the Controls/Security and Privacy settings to allow permission.

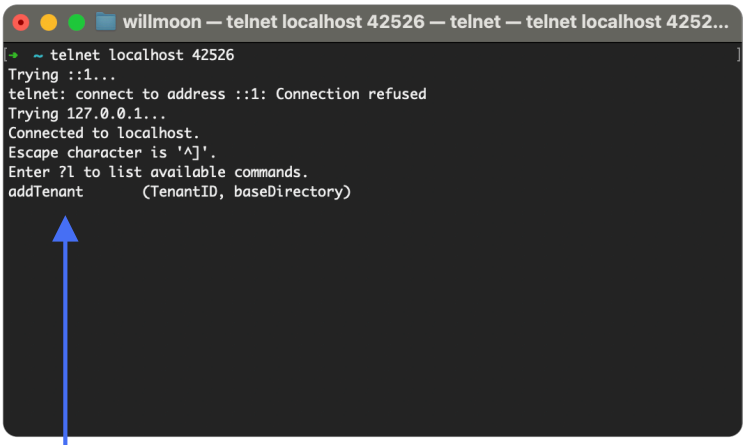
9. Tenants on WSF Servers

When administering your WSF server, you may need to allow multiple organizations to have access to your server, but you may want to keep them entirely separate. This is known as having multiple "tenants". Think of it like an apartment building, where every tenant of the building has their own separate, private space to keep their belongings in. In this case, a server may allow multiple parties to access entirely private directories that are separate on your device, preventing them from being able to interact with directories they're not allowed to access, but allowing them full reign over the directories they are allowed.

9.1 Adding Tenants

You may have multiple ***Tenants*** on a WSF server. Defining tenants is optional; without defining more than one tenant, by default a WSF server is considered to have a single tenant.

To add a tenant on a WSF server, on the device, telnet into the service (recall: telnet localhost 42526 will launch the WSF server interface). From here, type the command addTenant followed by a space, and a TenantID, a space, and the directory the tenant should connect to when connecting to the server. Spacing these pieces of information out with either a space or a comma is acceptable.



Use command addTenant + (TenantID, baseDirectory)

TenantID = a FederationID you wish to add
baseDirectory = Directory you wish Tenant to connect to

TenantID's are simply a WhiteStar ***FederationID***, used to define a tenant on a WSF server. Any FederationID will work for this purpose; when added to a WSF as a tenant, it is known as a TenantID.

The ***baseDirectory*** is the directory that the user will connect to when connecting to a WSF server. This is definable on a tenant-by-tenant basis, since some tenants will need to be placed in their own directories, but you may have yet other users whom need to be given access to a more broadly constrained file system.

9.2 Deleting Tenants and Content from Tenants

It's very important to note that when deleting the tenant, there is the option to leave the tenant's files on the server or delete them, thus it's prudent to take care when deleting a tenant from a WSF server.

When deleting the tenant, use the "***deleteTenant***" command. To properly define the command, add the TenantID after a space. There is a Boolean option to tell the WSF server to delete, or not, the content owned by the tenant from the server. By default, and if this Boolean is not defined, the function is set to false, which leaves the files on the server rather than deleting them. If the Boolean is set to true, the files associated with that tenant are deleted from the server.

10. Help

Typing the help command on the command line of a WSF server device will bring up the help menu. Type ***"?help (command name)"*** and WSF will print out instructions on how to use each command, their context and s brief description of what each command does.

11. Uninstall and Deactivation

macOS – Go to the applications folder on your computer and locate WhiteStar Files within the folder. Drag the application into your trash bin and then empty the trash bin. This will delete the WhiteStar Files application locally.

Windows – Go to the control panel, then add/remove applications, then search for the WhiteStar Files on the page and locate the application. Then click the ellipses (three dots) on the right-hand side of the screen and there a drop-down menu is presented. Select uninstall, and follow the on-screen prompts to remove the program from the PC. Then go to C:/Users/*yourusername*/whiteStarFilesClient and delete this directory. Empty the OS trashcan. The application is now fully deleted.

Account Reset - If you lose or forget your password, you will need to reset your application. Follow the above instructions for uninstallation, then reinstall the application and proceed through the sign-up process again. This will reset the user's account. Assuming you use the same email address to re-register your account, your Trusted Teams Tags and subscription will automatically be applied to the account. Note: depending on your system admin settings, you may need an admin password signature to remove or reinstall software on your device.

12. FAQ

Q: Why do I need a subscription?

A: WhiteStar bills for the use of our software. In order to use WhiteStar Files the user will need a valid subscription that has been activated by their administrator.

Q: What is the WhiteStar Network?

A: The WhiteStar Network is a hybrid peer-to-peer overlay network that directs secure communication between devices without Cloud servers. For more information, please see the WhiteStar Communications web page at https://whitestar.io

Q: I lost my password for WhiteStar Files. What should I do?

A: WhiteStar applications never save your password on your device or to an external repository. If a WSF Client user cannot remember their password they must fully delete, and then reinstall, the WSF Client software.

Q: Our firm just let go of an employee. How do I make sure that they no longer have access to WSF or WhiteStar tools?

A: The first thing a WSF administrator must do is deactivate the license, via the WhiteStar Administrator dashboard, that is associated with this user. This will disable the user from accessing WSF or any WhiteStar tools. If the administrator wants to completely remove the user from the system, they can use the Zeroize feature available to them in the dashboard.

Q: How can I contact customer support?

A: Go to your WhiteStar Administrator's dashboard and click the "**Support**" tab at the top of the screen. It will take you to the support portal, where you can send a question or put in a support ticket.

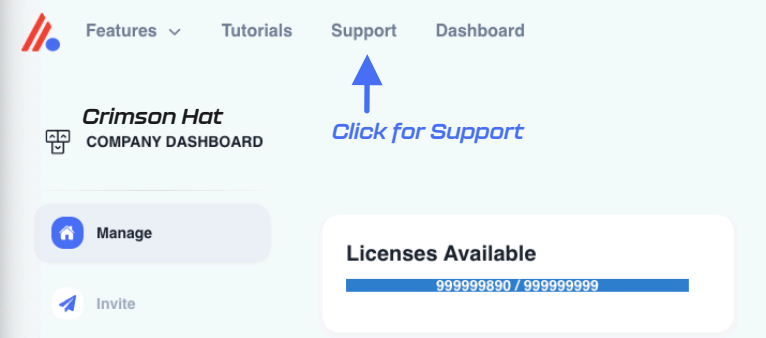


Figure 87

Q: Why do I need a Trusted Team Tag to connect to a device?

A: WhiteStar Trusted Team Tags are unique identifiers, created by your organization's administrator, to identify an individual user, or team of users, within the support organization. This Trusted Team Tag is then used by a customer to grant access to a device within their network – thus permitting **only** that user, or team, the ability to connect to their WSF Server device. A Trusted Team Tag asserts (to your customer) that your company and users are a trustworthy entities capable of accessing their devices. Any attempt to connect to a device without the correct Trusted Team Tag in place results in a failed connection attempt.

Q: What is WhiteStar Files?

A: WSF is WhiteStar's file transfer solution which accomplishes encrypted high-speed file transfers, of any size, to and from the WhiteStar Files Client and Server components.

Q: What's a Tenant?

A: A Tenant is a user, organization or individual, who is allowed to access a server. There can be multiple tenants on a single server.

Q: Why does WSF generate an email address during setup?

A: The email address generated synthetically during initial setup of your WSF server contains your server's Federation ID, which is used to help identify the server on the WSF network. This email address is only ever used a single time – during initial startup. In order to find your server, the email address is fed into the WhiteStar Core, which allows it to associate your WSF server as a "Thing" on your Dashboard. You will need a Tag to control access permissions on the device, however.

Merely adding the “Thing” to your Dashboard does not also allow users to access that WSF server. Keep in mind, only once a Tag is added to the server can anyone with that Tag access the server, and only users with that Tag may access the server. Servers can have multiple Tags with multiple permission sets (IE: one Tag allows access to the top levels of a file directory, whereas another Tag may only allow access to a restricted subfolder and not allow the user to “go higher” in the directory tree).

Q: What’s a “Thing”?

A: The term “Thing” derives from the term “Internet of Things”, and simply refers to any device on the network that is not a human (or a Federation a human controls). They’re called “Things” because they could be any kind of device - in the case of WSF this primarily refers to servers – but within WhiteStar a “Thing” could also be something like a light switch, garage door opener or a security camera.

Q: What does Zeroize mean?

A: WhiteStar contains a process called Zeroization, where a device is Zeroized. On a WSF server, the command “**Zero**” will cause the server to Zeroize, and the WSF client contains a zeroize command on the right click menu. Zeroization removes all of the locally stored information from WSF, deleting the user account, password and any connections that the user has, effectively resetting the program to “zero”.

Q: Why would I want to use sensors on the WS Dashboard?

A: Sensors are an important, albeit optional feature of WhiteStar applications, and are woven into the very fabric of the WhiteStar Network. The WhiteStar Network is content aware, being able to understand the types of content moving over the network. From time to time, it may be beneficial to understand what kind of traffic is traversing your WSF deployment. It can be very helpful, for example, to know the types of files, their size, the source and destination, their geographic location, whether those transfers were repeats, etc, for the purposes of auditing or workflow improvement.

The sensors contained within WhiteStar can be turned on and off at will and are fully optional. Your organization may not need sensors to monitor the content of your WSF deployment, thus it’s entirely possible to not apply them. However, for those organizations with data handling, sovereignty and retention compliance requirements, WhiteStar sensors can be an invaluable air in proving compliance with those requirements in the event of an audit.

13. Troubleshooting

I cannot connect to a WSF Server device

If you have successfully started the WSF Client, and are being denied a connection to a particular WSF Server device, there are several things to verify:

1. First confirm that your administrator has attached the proper WSF Trusted Team Tag, granting access permission to this device, to your user id.
2. Next ensure that the customer has granted access to the WSF Trusted Team Tag (the same one your administrator created in #1 above) on the WSF Server device that is attempting to be accessed.
3. Confirm with the customer that the WSF Server software is installed and enable on the device. Also confirm that the device has the ability to reach the internet.
4. Confirm that the local device running the WSF Client can connect to the internet.
5. If your company is running its' own WhiteStar Core Network, make sure that both the MCP and Replicators are running and online.

My Client is stuck trying to "validate" the session. What can I do?

Ensure that the clock on the WSF Client device is set correctly. WhiteStar applications require a precise true-to-time measurement in order to synchronize. If you have manually set your device's clock, try setting it to automatically adjust.

The WSF Client won't launch

Make sure that there are no instances of the WSF Client currently running in the background. Only one instance of the WSF Client is permitted to be running on a particular device.

The WSF Client shows a blank screen after connecting and doesn't accept keyboard input

Terminate the current instance of the WSF Client Shell and restart. If, after restarting, you still cannot interact with the WSF Client Shell, it may be because there is another user currently connected to the WSF Server you attempted to connect to. Check with other team members, who are also permitted to connect to this Server devices, to ensure they are not currently connected.

The other potential reason you would see this issue is if the WSF Server has been disabled on the remote device. If this is the case, you should have been prompted with another safeguard to prevent connection to an offline device, however that safeguard may have not triggered. Ensure the remote device's Server is currently on, kill your instance of WhiteStar Files, and retry your connection.

The WSF Client believes I have no subscription

Double check with your administrator that your subscription is valid on their Dashboard. If the problem is present for only a single user, find their name in the Dashboard and check the box next to their name. Then under "Actions" select "Reset Subscription", which will revalidate their subscription. If the problem is present for many users, ensure that your WhiteStar account is currently in good standing.

The WSF Server doesn't show any current connections but there's someone currently connected to the device

Ensure that all devices are connected to the internet and that there is sufficient bandwidth for the devices to operate. You may have issues with connectivity when there is very little bandwidth available. Turn your Server off and then back on, then reassess whether you see the online devices. Have your remote user disconnect and reconnect by rebooting their Client and reconnecting to your Server.

I cannot add more members to my WhiteStar dashboard

You may be limited by the number of available subscription seats that you have available. If you're attempting to add more members than you have subscriptions available, and are running into a hard cap of the number of members you may add, please contact WhiteStar Sales for an additional allotment of subscription seats.

If you have sufficient subscriptions to cover the additional team members, you may already have the team member(s) you're attempting to add in your member roster. Search your roster and ensure that you do not already have these members in your list.

14. Glossary

ACRONYMN / TERM		Definition
CSV file		Comma separated values file, typically used with Microsoft Excel
Federation ID	Synonymous with Machine ID	A unique identifier on the WhiteStar Network, which makes you and your devices routable on the network. A Federation is made up of all of your Endpoints, both devices you interact with and IoT devices. Federations can be Tagged to give them special permissions. With a Federation, all properties of the Federation are applied to all member of the Federation.
Server	WSF Service for Remote Transfers	The WSF Server is a service that runs on a remote server that replicates all commands it receives from a user's Client into the server's terminal.
Google SSO	Google Single Sign On	Sign in with Google, using Google's authentication services for your account management with WhiteStar
Files	WhiteStar Files, WSF	WhiteStar's native anywhere-to-anywhere, always encrypted, unlimited-file-size, platform agnostic file transfer system.
Client	WhiteStar Files local Client, WSF Client	The WSF Client is your local interface with the WSF Server. It allows the user to see a multi-pane view of two different file systems, either two remote file systems from two other devices, or one remote and the user's local device, in order to move files between devices. The WSF Client also shows batch-send progress during the transfer process.
WSF	WhiteStar Files	The WhiteStar Files is the name for the entire Server/Client/Dashboard solution.
Zeroize		Zeroization permanently deletes not only your Endpoint and Federation ID from the WhiteStar Network, it also tells the entire network that any information sent from your endpoint is also null, and thus should be deleted. This results in a complete deletion of you and your WhiteStar Network identity, *as if you were never part of the network in the first place*.

Trusted Team (Team)		A Trusted Team or Team for short is a certified Team that is allowed to access a Server by way of a Team Tag. The Team Tag functions as a certificate that asserts that the Team is trusted and valid. Each member of the Team has a unique cryptographic key used to access the WSF Server, since WhiteStar never uses group cryptography.
Trinary	Trinary Switch	Having three states
Trusted Team Tag	Team Tag, Tag, Certification	The Team Tag is what denotes the user is part of a Trusted Team. Also known as a certification, the Team Tag is conferred upon a member of a Team to assert their trustworthiness
Dashboard	WhiteStar Dashboard	The administration panel used for controlling the members of an organization, their data usage and their associated Team Tags.
License	Subscription	Your allowance of usage of the WhiteStar Network. Each user needs a license in order to utilize WhiteStar services.
Society	WhiteStar Chat	WhiteStar's encrypted private messaging system. Society is a commercial offering built for individual private chats, WhiteStar Chat is a centrally managed enterprise version of the application.
Logs	Log Files	A detailed written record of what tasks your computer is currently working on or has completed.
UUID		Another form of unique identification that can identify a machine, device or endpoint
Vortex		WhiteStar's privacy-centric email server, used for account verification
Trust-Based		All information is encrypted in-flight and at-rest, with no group cryptography. This makes the surface-area of potential attack vectors 1, which is theoretically the lowest possible while still allowing for communication between devices. Endpoints are granted specific access by way of pair-wise relationships.