WhiteStar Shell

Secure Remote Terminal Interface

Installation and User's Guide

Table of Contents

1. Introduction - What is WhiteStar Shell (WSH)?

Sometimes things break - software goes awry, mistakes are made - and you need provide support to your customers. The trouble is your organization needs to allow support technicians, both on-staff and third-party, remote access to devices within a corporate network (for diagnostic purposes), without exposing those devices to the risk of outside penetration by unwanted individuals. Furthermore, direct interactive access is best - the ability to actively view/collect log files or run diagnostics real time on the devices in question - and once diagnostic log files are generated, securely retrieving them is another major problem.

The overall remote support landscape is complicated. Devices may be on-premises, in the Cloud or running as a virtual machine. They may be assigned private IP addresses with very limited reachability. They may be behind multiple firewalls. Standard tools like SSH [secure shell] require holes in firewalls to function, as well as user accounts with sufficient permissions to diagnose and repair a problem. Customers are very reluctant to open their network up to allow such access - nor do they want to provide a “phone home” facility that constantly sends information back to their vendors. Furthermore, Cloud-based management systems have enormous attack surface areas, and most other tools do not account for, or enforce, technician segmentation (the ability to limit exactly which support personnel can access a particular customer's device). You may also find that companies are extremely hesitant to allow any of their sensitive corporate data to be stored in any Cloud-based management or support platform.

WSH, running on WhiteStar’s trust-based overlay network, gives your organization the ability to provide real time first or third-party support without creating a security risk to your customer's network infrastructure. By maintaining a robust trust-based ecosystem, WhiteStar allows your organization to provide support without the need to open your customer's firewalls or request user accounts with special privileges. Additionally, WSH provides for the designation of trusted support providers by customer, allowing you to securely segregate which of your staff can actually connect to a particular customer's devices.

While providing the ability to securely access devices within a customer's enterprise network, WSH also provides the ability to transfer any size file - like a system log - to and from devices in a totally secure fashion. This means your support staff can access files from a customer's devices securely, without the fear that data (potentially containing sensitive user and device data) may be leaked online, protecting your customer against potential data exfiltration.

Finally, WSH maintains its own log files for each command issued on the remote device. This provides your customers a running record of what was done on their device (should they want to see what the support organization did), while also providing a running log that can be leveraged by support technicians in order to retrace their steps during debug. This level of transparency creates a high level of trust between the support staff and the client.

2. WSH - Solution Overview

WhiteStar Shell is comprised of **three parts:**

Administrator's Dashboard - a web-based console used to manage your WSH licenses plus grant and revoke access to members of your team (providing them with the proper credentials to connect to your customer's remote servers and devices).

WSH TTY (remote terminal) - a secure terminal that interfaces directly with the WSH PTY service running on a customer's device (emulating a shell as if you were running on the device locally). The WSH TTY allows transparent access to the device being diagnosed allowing the technician to use the tools he/she would use locally to diagnose and fix issues via a shell interface. If files need to be securely retrieved from or sent directly to the device being diagnosed, WhiteStar's Enterprise Files capabilities are built right in to the WSH TTY component to accommodate this. Once complete, the technician simply disconnects or exits from the WSH TTY terminal and all secure network connections are torn down automatically.

WSH PTY (pseudo-terminal) - a secure service that executes on the customer's device being diagnosed. This service provides the service technician a secure interface between the customer's device and the technician's TTY terminal. The WSH PTY can be started and stopped, as needed, providing the customer's device administrators the ability to enable/disable remote WSH 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 diagnosis is required on a particular device.

Figure 1 illustrates a basic representation of how WSH TTY users connect to end customer devices via the WSH PTY (seamlessly through firewalls and the internet).

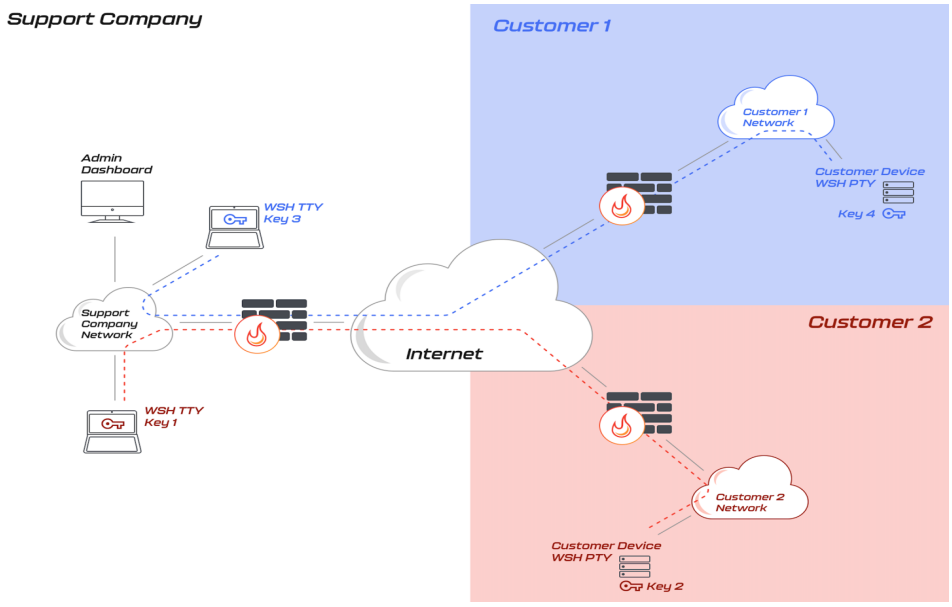

Figure 1

2.1. Support Teams – Subdividing Teams

At times customers request that only "specific" service technicians diagnose their systems. In other cases, companies charge a premium to establish separate service sub-teams dedicated to individual customers. The WhiteStar Shell system fully supports this and provides the system administrator the ability to grant access to a single technician (for an individual customer) or sub-divide members within their organization into teams dedicated to particular customers.

Take, for example, a support organization with five (5) service technicians. The administrator may want to grant access to individual technicians to provide support (and connect to) individual customers' devices or create a small team of service technicians dedicated to a particular customer. They may also want to have a generic team made up of all service technicians who can connect to any customer's devices. Figure 2 illustrates an administrator who has created four (4) teams [this is done by assigning a WhiteStar Team Tag – or multiple Team Tags – to their technicians. How to accomplish this is discussed later in this document].

- Team #1 (with 3 service technicians) has been established to connect to PTY devices for Customer #1.
- Team #2 (with 2 service technicians) has been established to connect to PTY devices for Customer #2. Note that technician #2 is a member of both Team #1 and #2 and therefore can connect to devices in both customer environments.
- Team #3 (with only 1 service technician) has been established to connect to PTY devices for Customer #3.
- Finally, Team #4 (with all service technicians as team members) has been established as the generic group for all new customers for this company and Customer #4 has been assigned to use it.

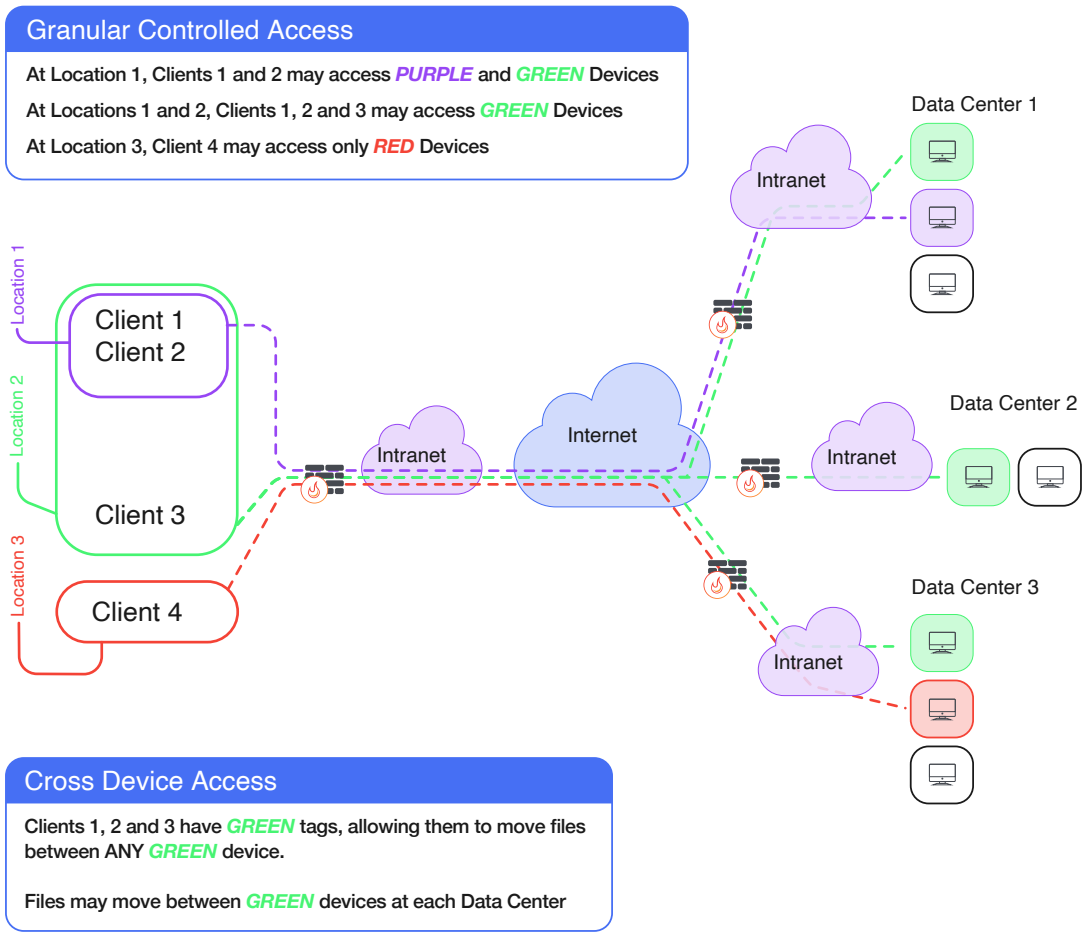

Figure 2

Note: the Service Company administrator creates support teams in their WhiteStar Dashboard by assigning WhiteStar Team Tags to their technicians in order to delineate which “team” or “teams” they are a member of. For a customer to receive support, they must log on to the particular device requiring support and grant access (e.g. via their PTY interface) to the corresponding WhiteStar Team Tag which represents the trusted team they want access granted to.

3. Minimum System Requirements

3.1. Software

3.1.1. WSH TTY

- 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. WSH PTY

- 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
- Cockpit (web-based graphical interface for servers). Please visit **https://cockpit-project.org** for more information on how to install and setup Cockpit.

Customized WSH PTY 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.

3.2. Hardware – WSH TTY

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 for allocating application subscriptions to support technicians, creating and assigning WhiteStar Team Tags (which provide access for the technicians to access customer's devices), and maintaining the company's profile information. A WhiteStar Trusted Team Tag (Tag) is the company's "token" to gaining access to specific devices on a customer's network, and must be assigned to individual service technicians in order for them to be granted access to a customer's 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).

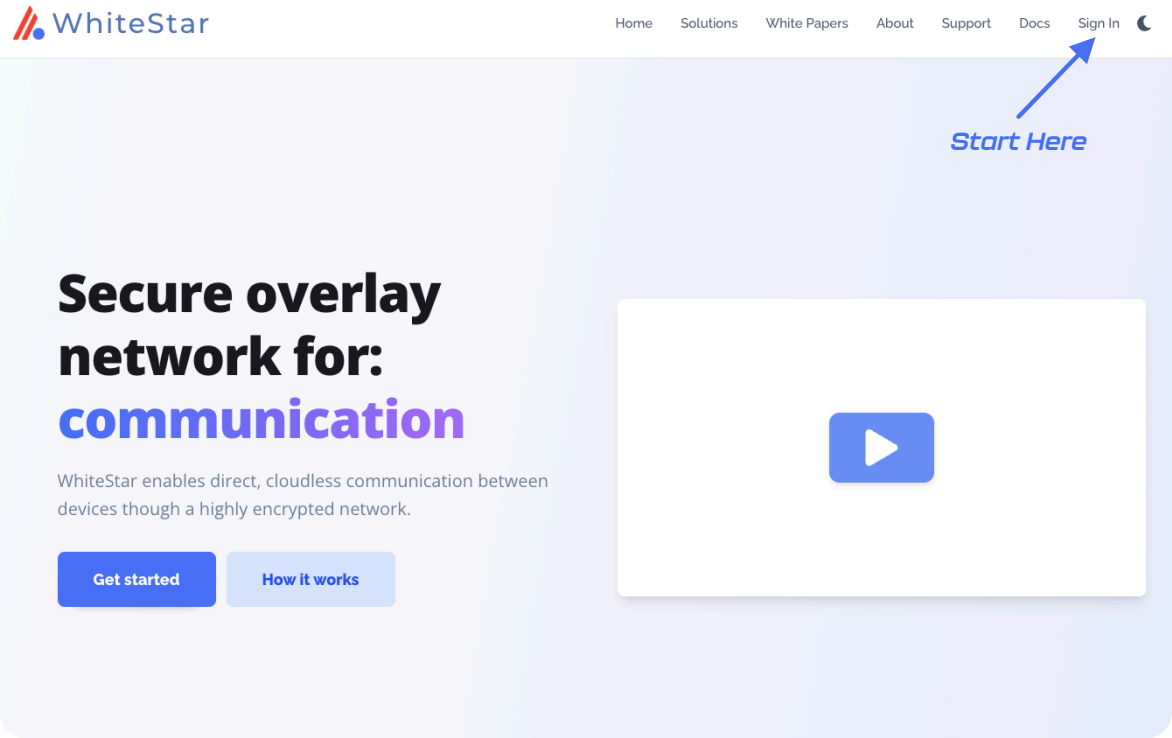

Figure 3

After clicking "Sign In", the administrator is presented with a screen prompting them to log in (see Figure 4). If they already have an WhiteStar administrator account, they can enter their email address and password information, and hit "Continue" or they can click on "Continue with Google" to leverage Sign In with Google and its use of 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 (see Figure 4). For additional details on obtaining an administrator's account, please refer to section

Signing up for an Administrator Account below.

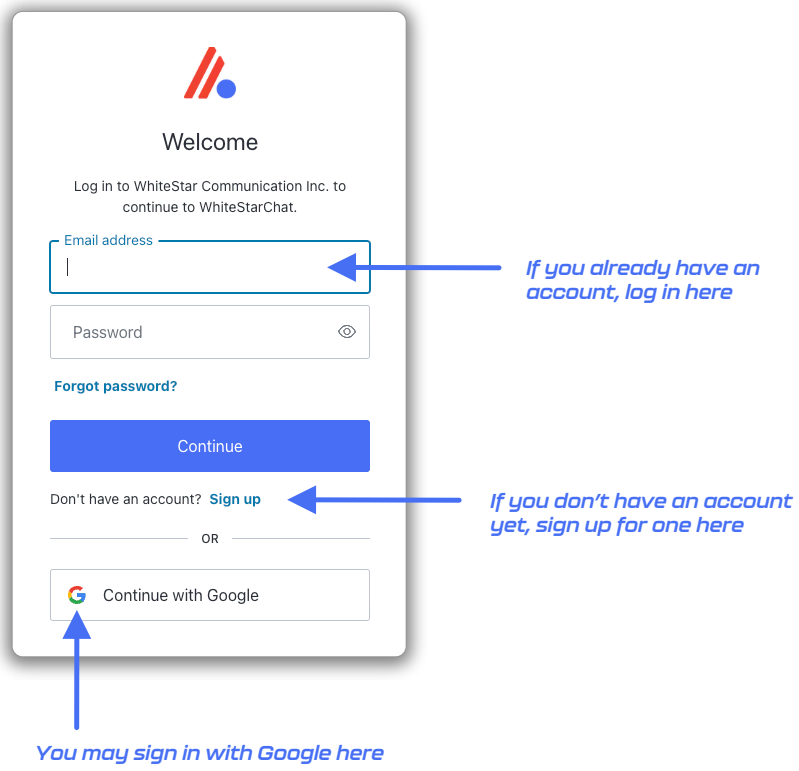

Figure 4

4.1. Administrator Dashboard - Orientation

Once successfully logged in, the administrator is presented with their dashboard (see Figure 5) which has multiple functions. The left-hand column of the Administrator dashboard is used to toggle the main functions of the page: (1) manage users (support technicians who will be utilizing the WhiteStar TTY 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 Tags to users.

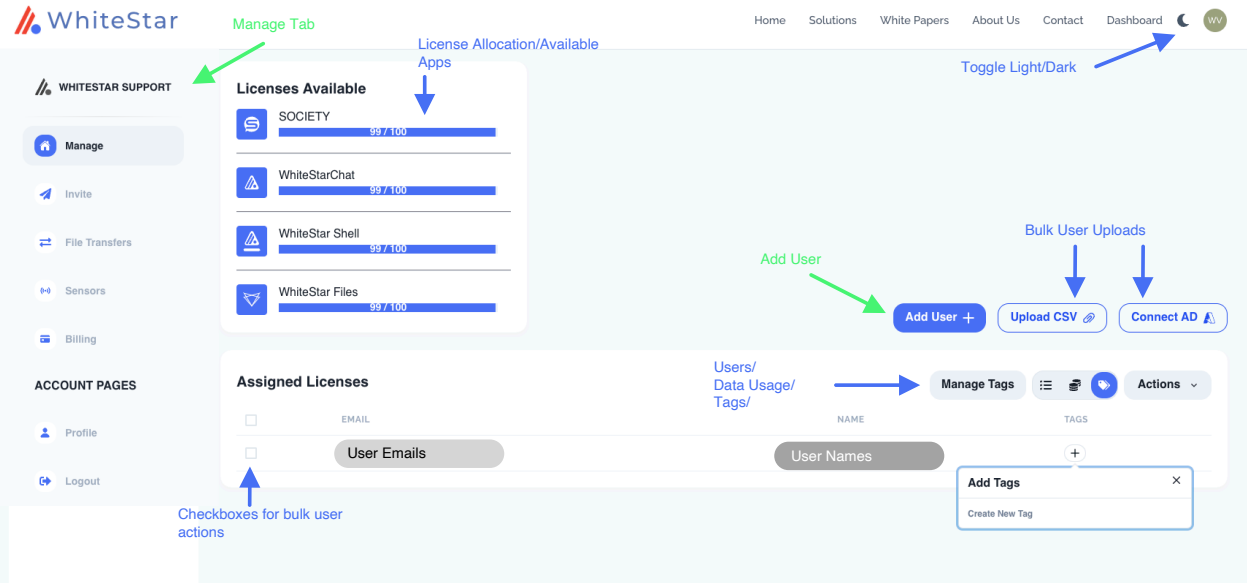

Figure 5

5. Signing up for an Administrator Account

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.

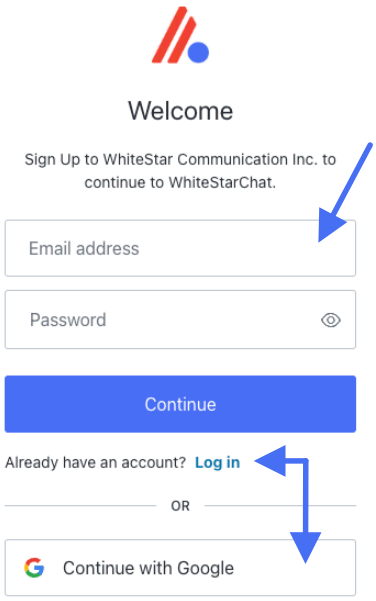

Figure 6

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

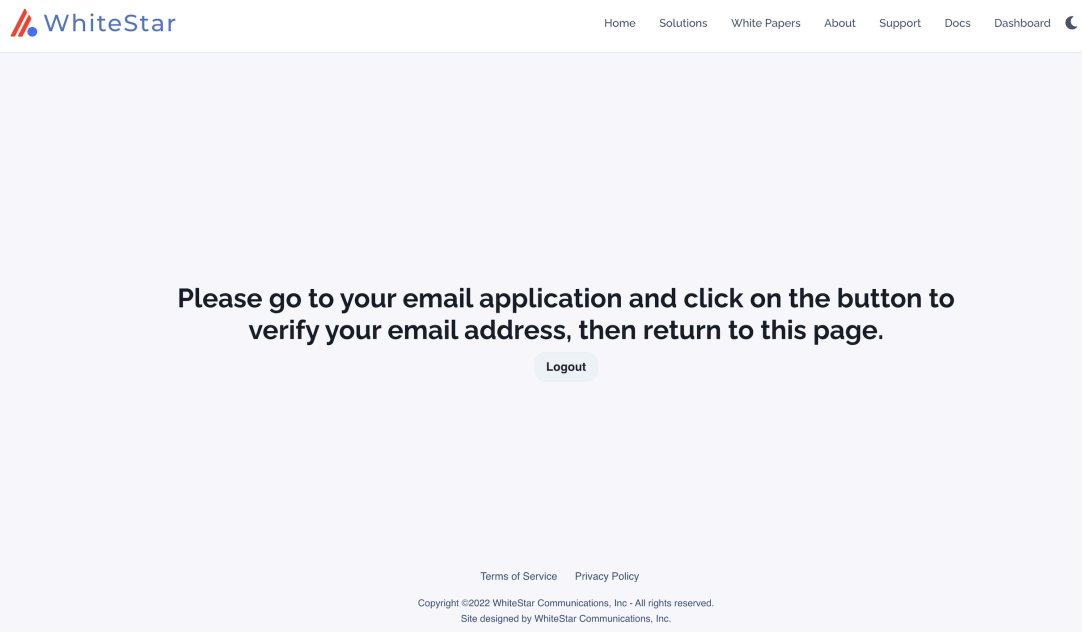

Figure 7

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.

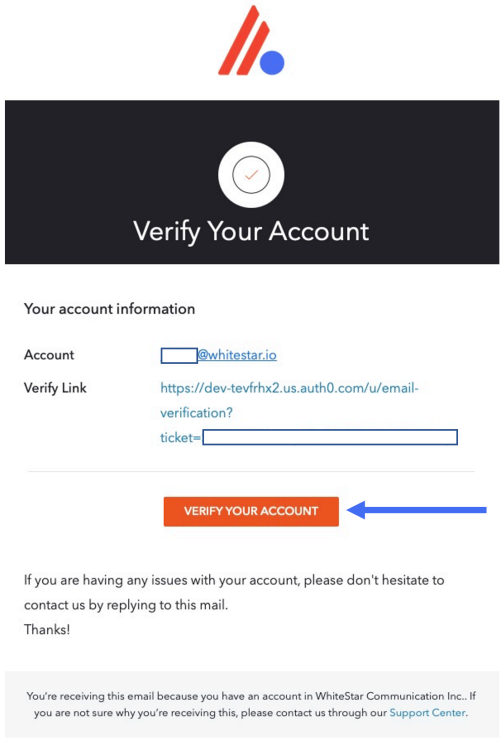

Figure 8

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

5.1. Adding New Support Technicians

5.1.1. Add an Individual Technician

To add, or assign a license for an application for a new technician 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 support technicians to use the WhiteStar TTY application (by adding their email address to the list of authorized members of an organization). The support technicians themselves use their email address during the WSH TTY 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 support technicians name be entered as well. Once the information is entered, click the "**Submit**" button (see Figure 9).

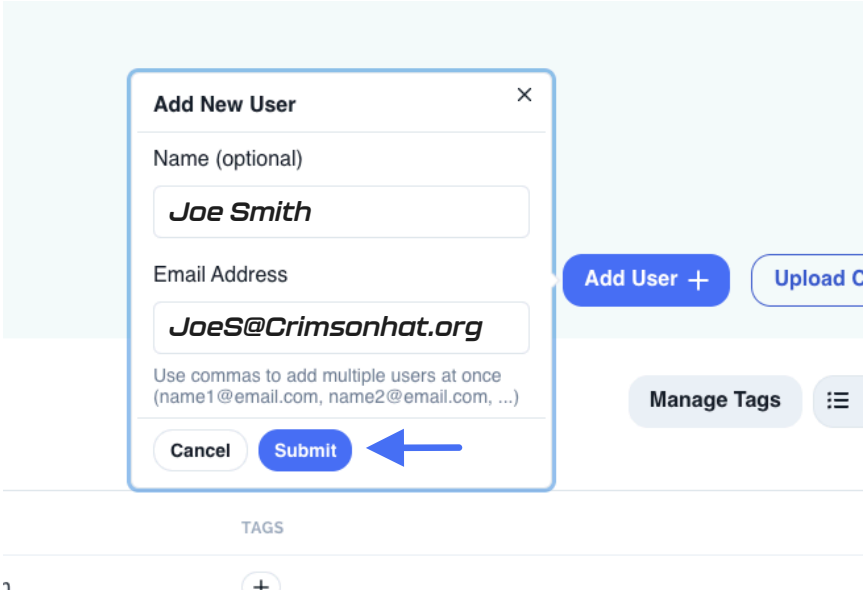

Figure 9

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

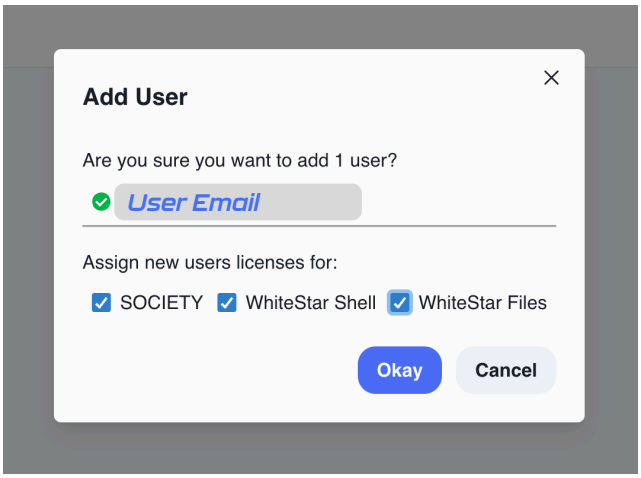

Figure 10

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).

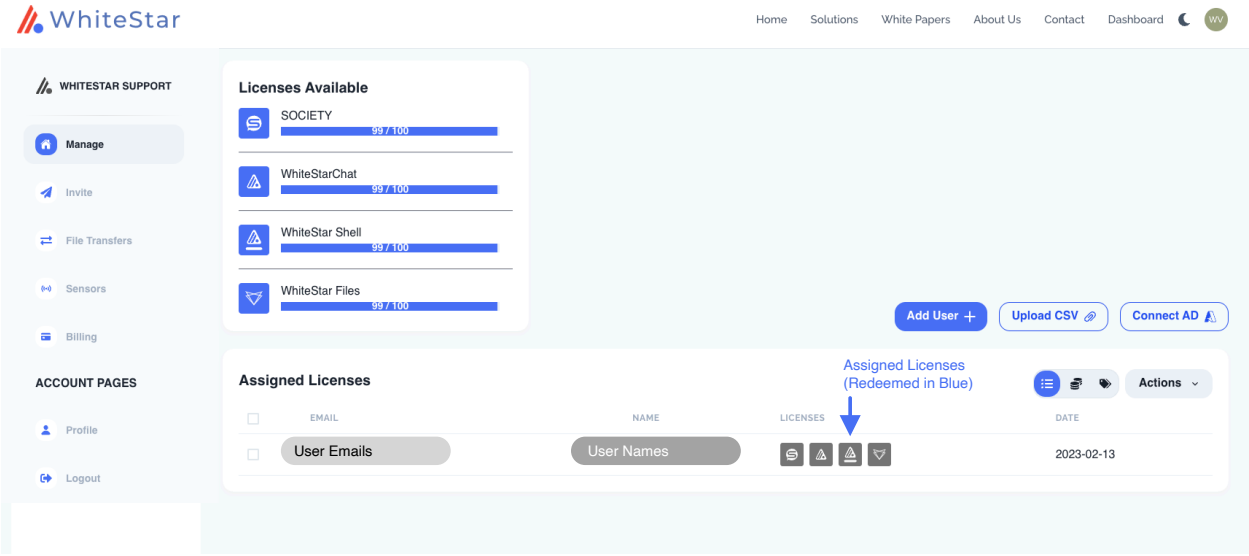

Figure 11

If the administrator wants to bulk upload new support technicians 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 Technicians 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 technician email addresses. Administrators may optionally include the support technicians' names and/or tag names that should be assigned to each technician (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 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 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).

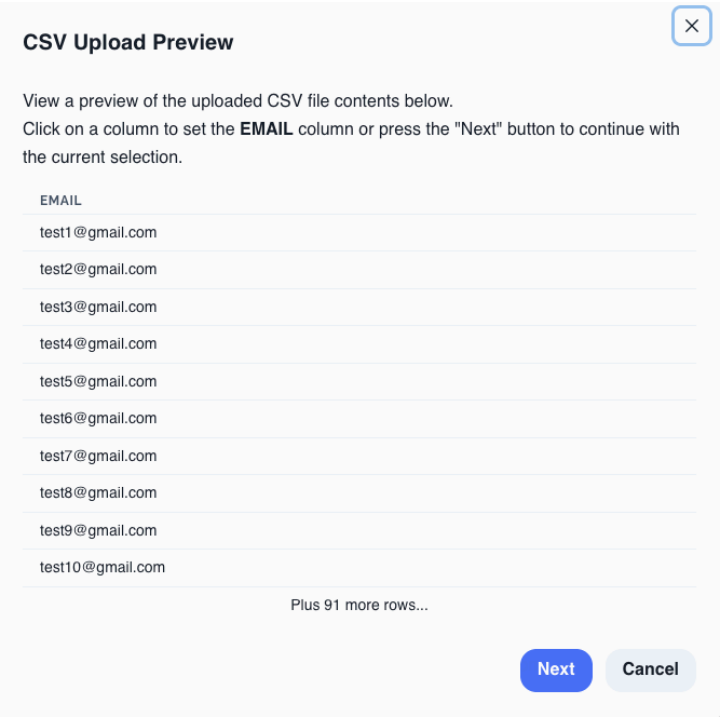

Figure 12

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 available to assign (red exclamation point circle). The email addresses are added, and licenses assigned, but you are expected to increase (and pay for) these additional licenses.
- 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.

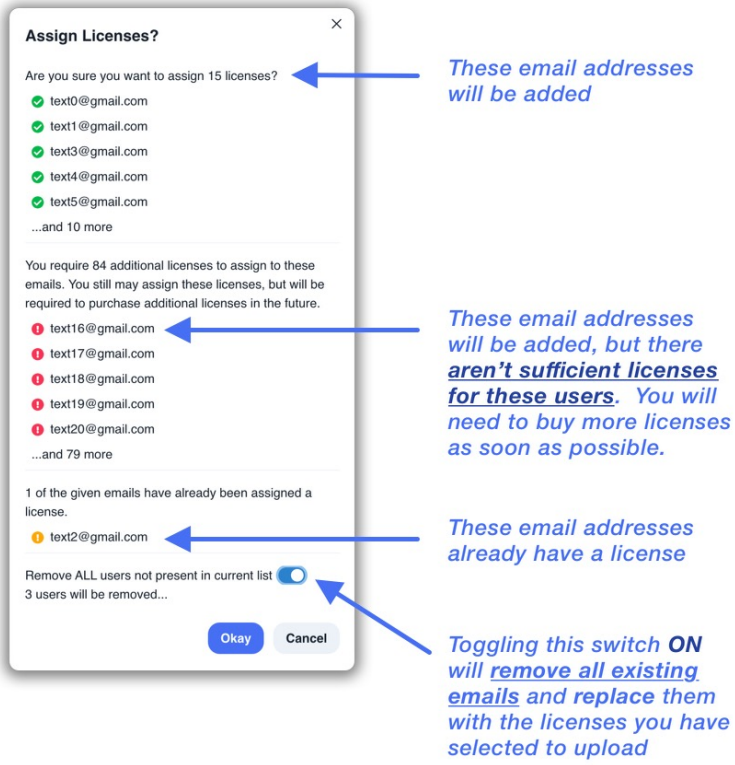

Figure 13

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 Technicians via bulk Upload Active Directory (AD)

This feature is currently under development and is in Open Beta. WhiteStar supports a bulk upload of technicians 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.

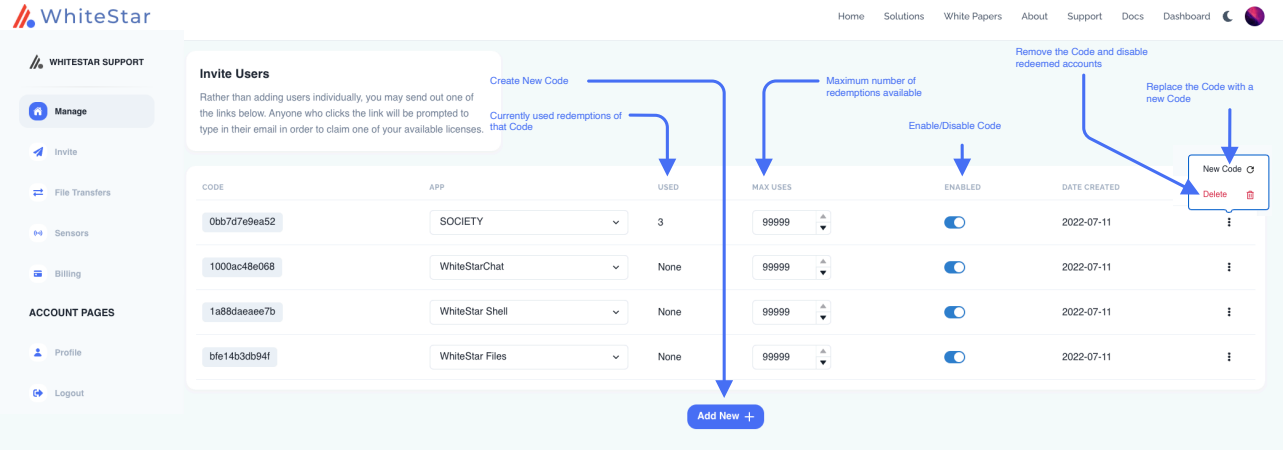

Figure 14

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 left-hand 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 WSH TTY 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 WSH TTY 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.

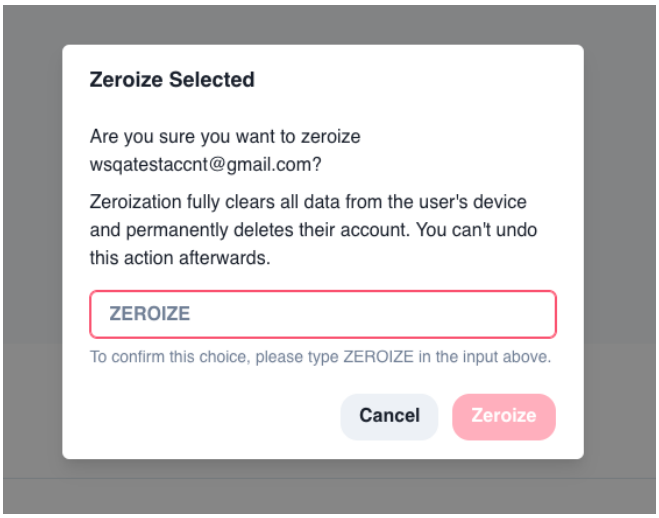

Figure 15

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. Tagging – Providing Access to Customer PTY Devices

Permission to access a device's WSH PTY service is granted by unique identifiers referred to as **Team Tags** in the WhiteStar system.

Team Tags are created on the WSH Administrator Dashboard and assigned to service technicians either individually or to groups of service technicians. In order to access a particular customer's device, it is the customer's responsibility to log into the device they wish to grant access to, navigate to the Cockpit console, and specifically add the Trusted Team Tag which has been assigned to the service technician they are wanting accessed granted to (the service technician may have to share the name of the Team Tag with the customer in order for them to choose the proper one). This will allow any technician with that Team Tag to access the customer device. Refer to Maintaining the list of Trusted Teams Who Can access a Device for more details on how to perform this action.

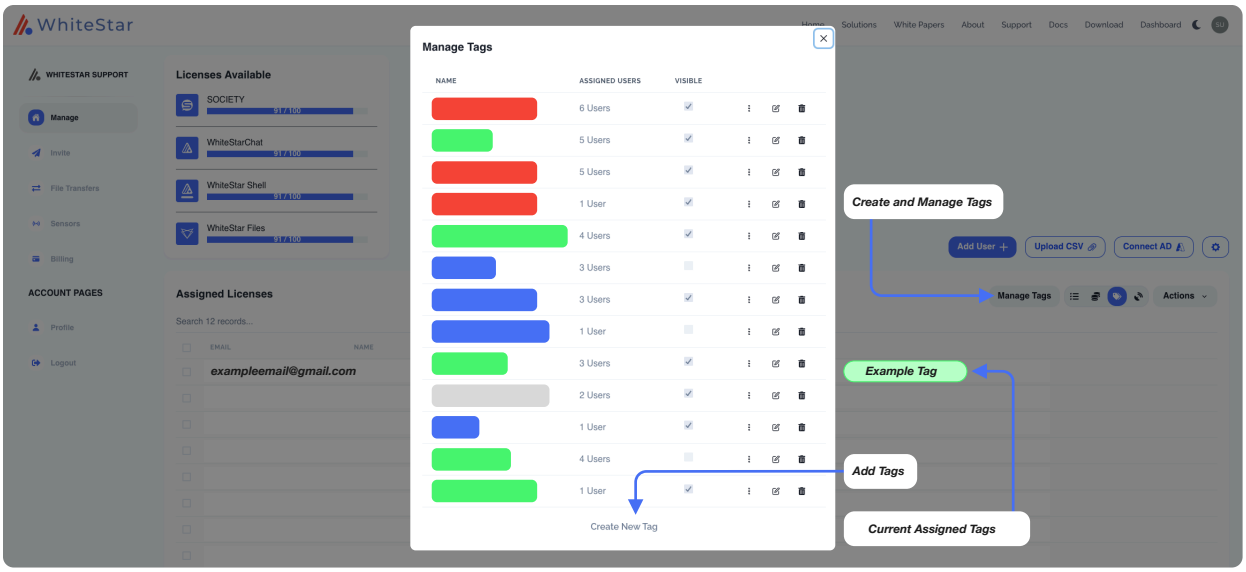

Figure 16

Creating Team Tags and assigning them to support technicians is a simple task. The administrator first logs in to the WSH Administrator dashboard and clicks on "**Manage**" in the left-hand column. In the main portion of the screen there is a trinary control switch (see Figure 17) on the right-hand side of the **"Assigned Licenses"** table that allows you to see the Team Tags applied to a given technician's account.

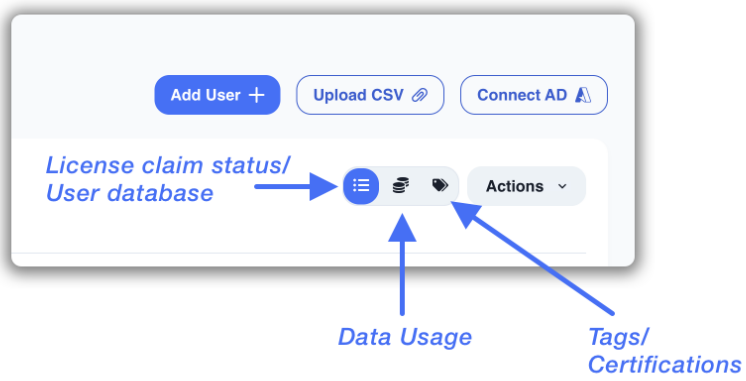

Figure 17

Toggle this switch, and you'll see a row appear in the names list that will allow you to add Team Tags (see Figure 18).

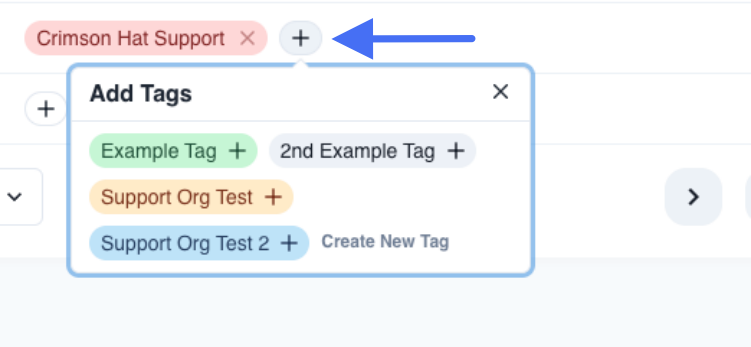

Figure 18

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

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

Each Team Tag, when created, is assigned a unique code, which is required by the WSH PTY plugin in Cockpit to grant any user with that Team Tag access the WSH PTY on the server. You can find this CODE by clicking **"Manage Tags"** after you created the Team Tag.

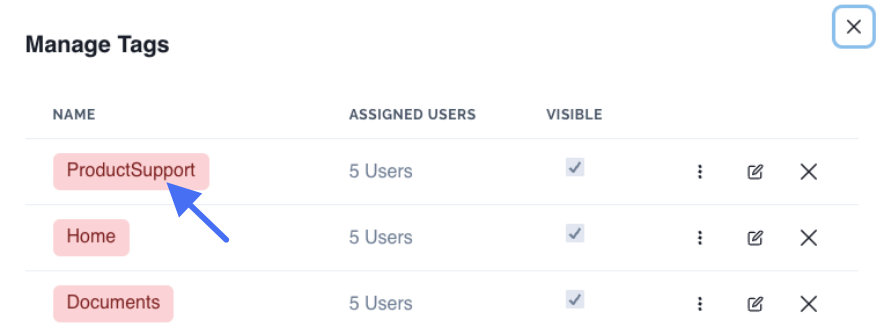

Figure 19

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

As you can see in Fig. 19, there is a checkbox to enable Tag visibility. Visible Tags are searchable on the MCP and can be selected by PTY users on their Cockpit interface. An invisible Tag won't be searchable but can still be manually input into the interface.

5.4. Accessing the Profile

From the main screen of the Dashboard navigate to the left-hand column under "**ACCOUNT PAGES**" and then click on "**Profile**" (see Figure 20). 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.) and who to contact at WhiteStar with questions.

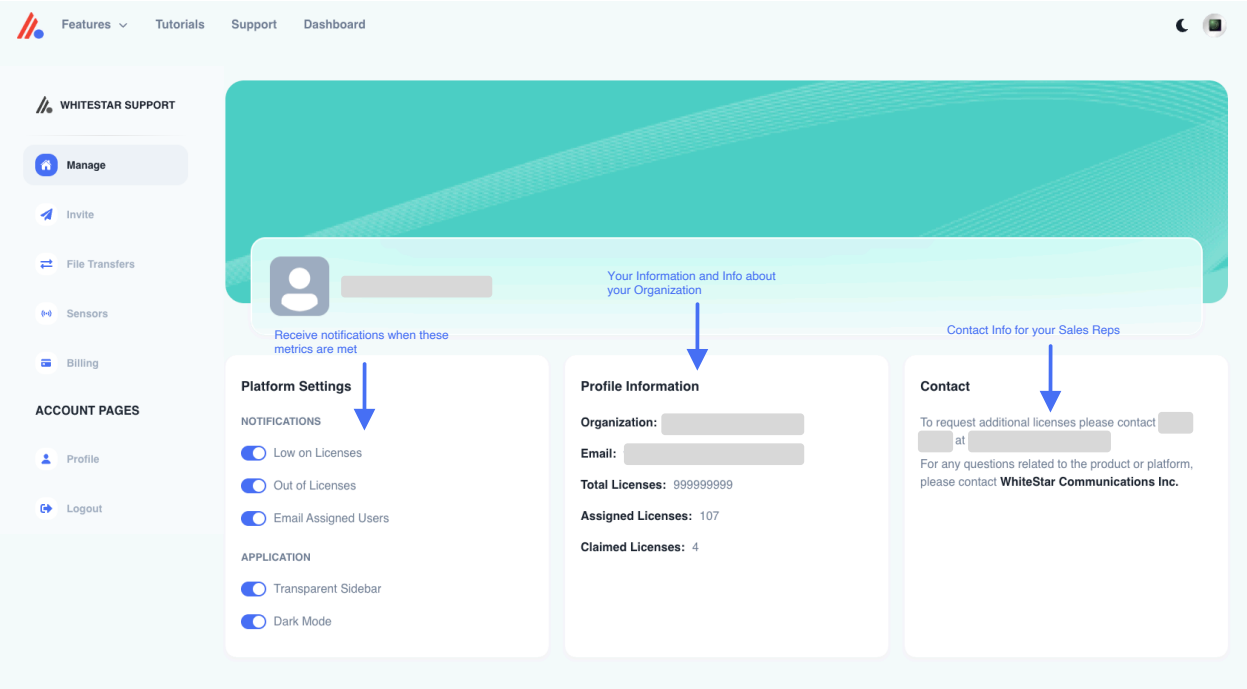

Figure 20

6. Installation of WSH TTY

For a service technician to connect to a customer's device (running the WSH PTY), they will first need to install the WSH TTY component on to the machine they want to connect from. Currently the WSH TTY component runs on Microsoft Windows, Apple macOS, or Linux desktops.

Open a web browser and navigate to the following WhiteStar website: **https://whitestar.io/download/wsh/tty/**. The user is presented with a link to download the WSH TTY 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 WSH installer package was saved.

Click on the download package to run the installer. You are brought to the following screen (see Figure 21):

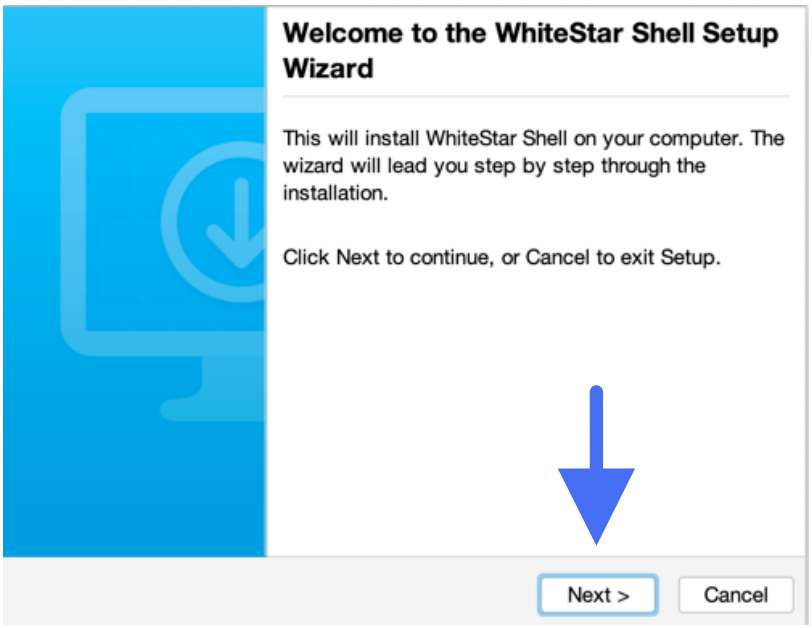

Figure 21

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 22).

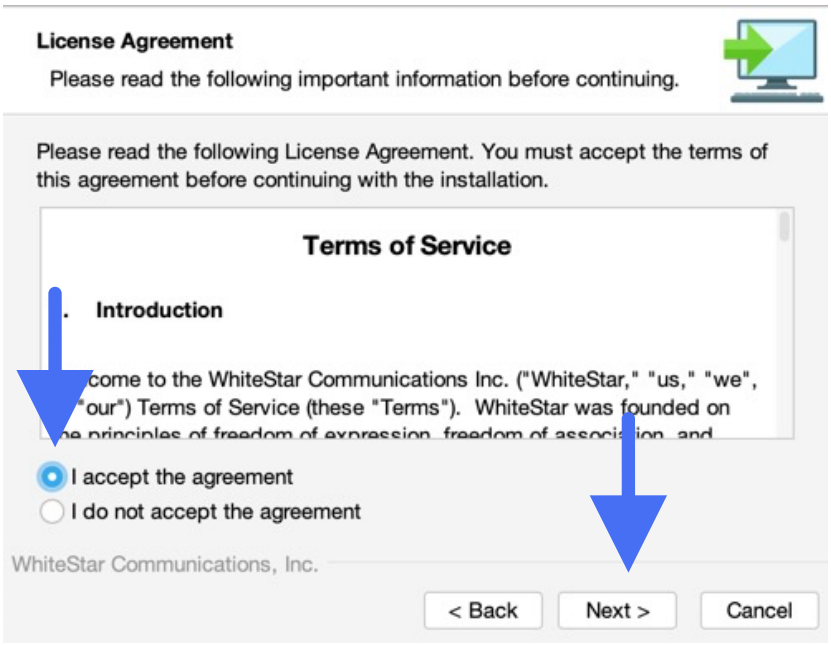

Figure 22

Choose the directory for the application to be installed into, and then click the "**Next**" button (see Figure 23).

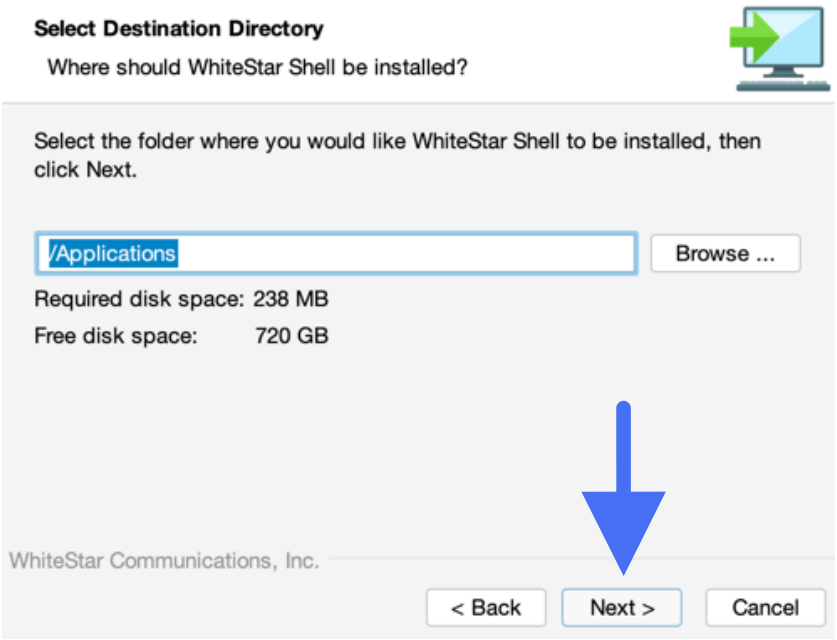

Figure 23

Click the "**Finish**" button to complete the installation (see Figure 24).

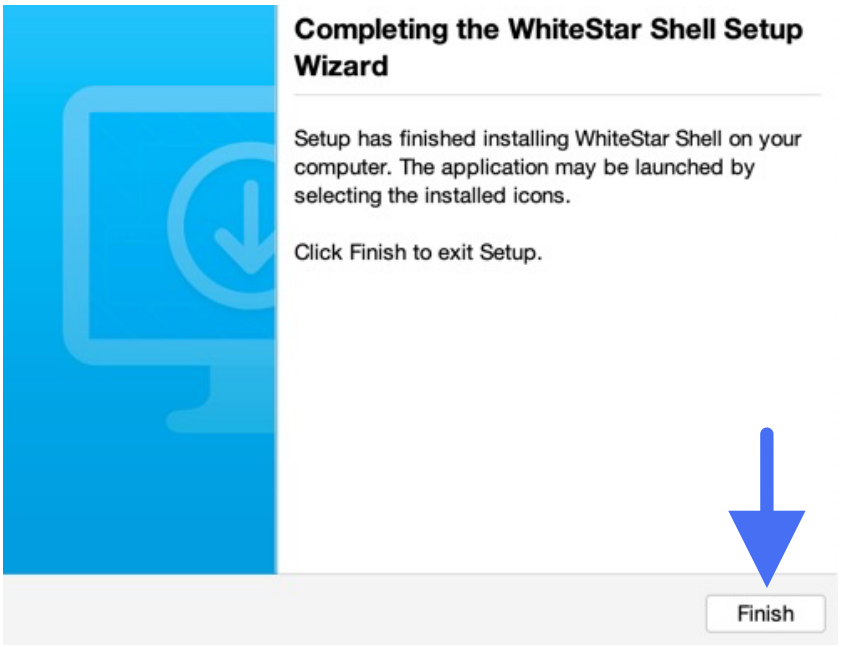

Figure 24

The user is then be brought to the registration screen (see Figure 25). 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.

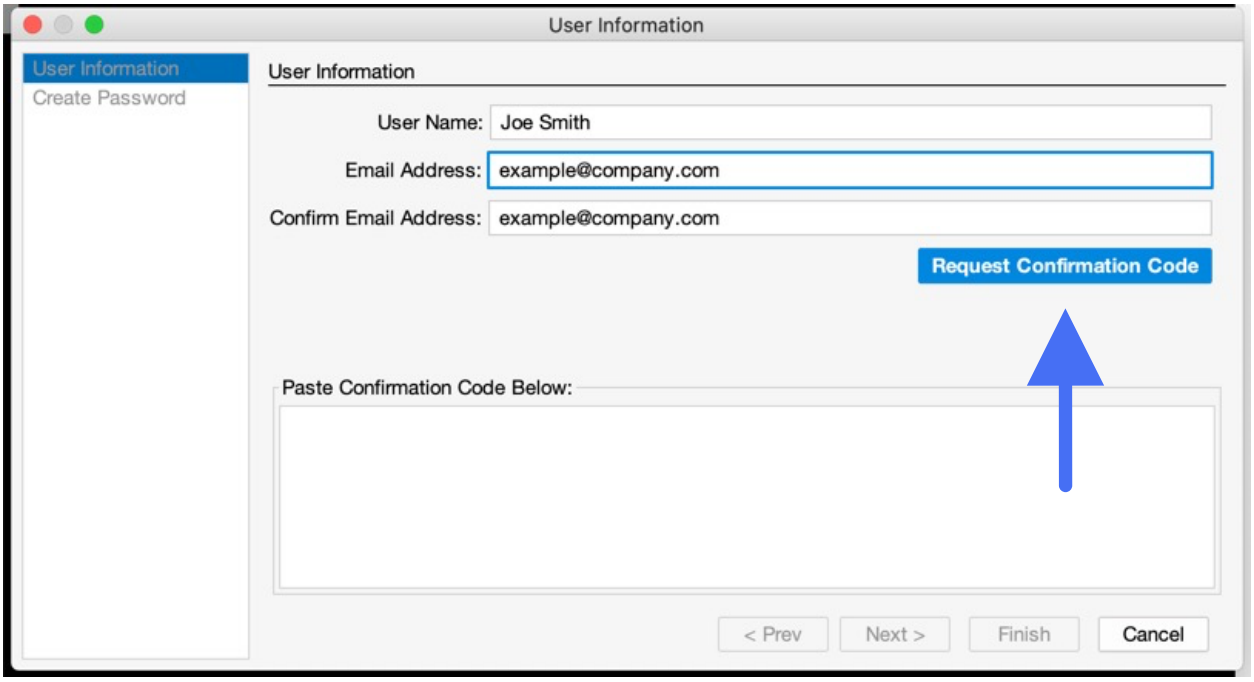

Figure 25

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.

Go to your email client and look for an email from vortex@whitestar-vortex.com with the subject line of "WhiteStar Validation Code" (check you 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 WSH TTY installation screen (see Figure 25) and paste (typically hit Cntl-P/Cmd-P) the confirmation code into the appropriate box (see Figure 27 as an example).

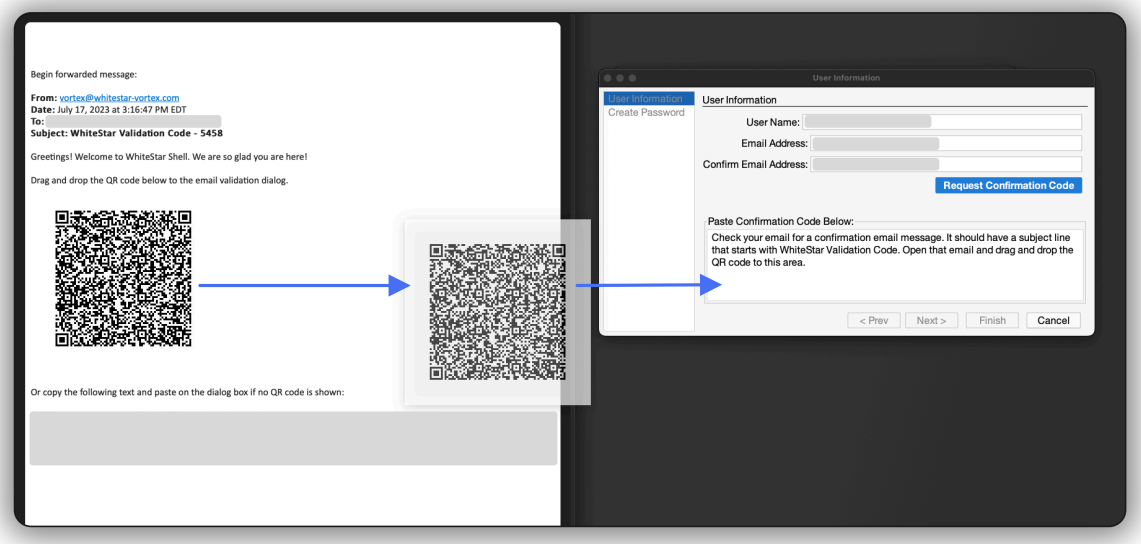

Figure 26

You can drag and drop the QR code that comes in the WhiteStar authentication email into the validation box on the TTY signup page. Barring that, you can also copy/paste the confirmation code into the box manually.

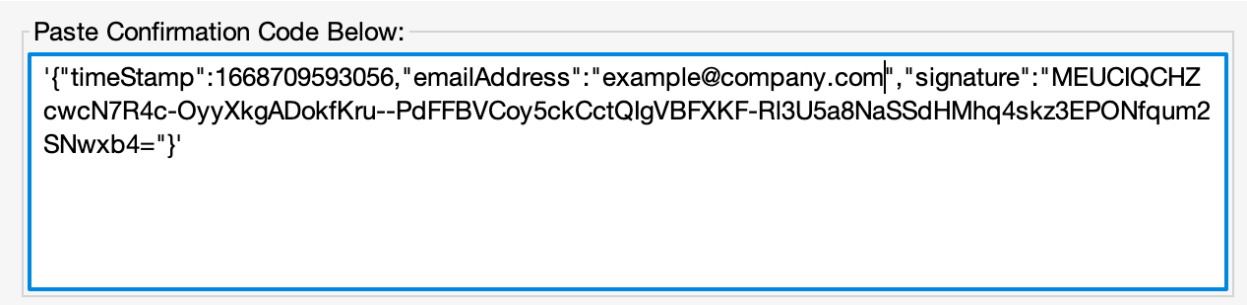

Figure 27

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 technician to remember their password. There is no "password reset" capability with WSH TTY. If you lose your password, see the section in this guide on resetting your account.

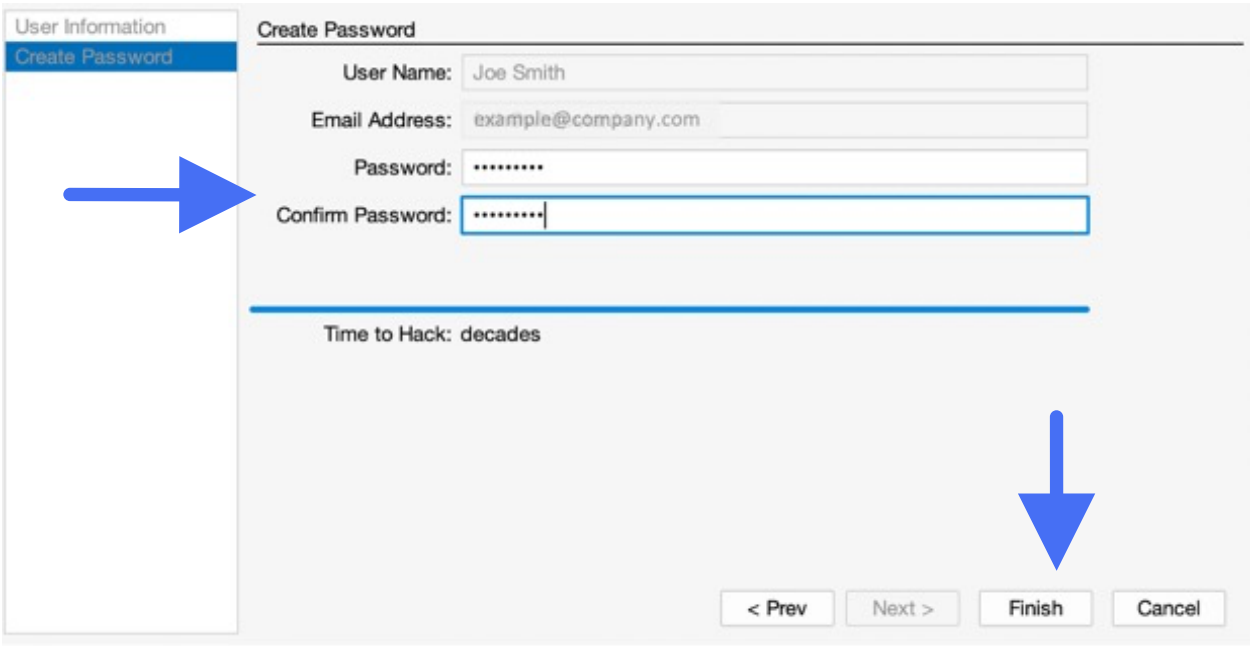

Figure 28

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 28).

7. Running the WSH TTY Client

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

In order for a WSH TTY client to connect to the WSH PTY on a customer's device, the customer support system administrator (for the team of support technicians) is required to create "**Trusted Team Tags**". These "**Trusted Team Tags**" are used by customers, on their WSH PTY interface, to enable secure access for your organization to securely access their devices. If you are experiencing issues connecting to a customer's devices, first ensure that you have been authorized to do so by verifying with your administrator that the "**trusted Team Tag**" for this customer has been created and enabled for your ID. If that is confirmed, double check with the customer that they have authorized this "**trusted Team Tag**" (via the WSH PTY interface) on the device they are seeking diagnostic help for.

To connect to a device, click on the **WSH TTY** icon on your desktop.

If there isn't a valid subscription when starting the WSH TTY application, the user is informed it is waiting for an active subscription (see Figure 29). If you receive this message, ensure your system administrator has a subscription attached to your email address, otherwise you won't be able to use WSH TTY.

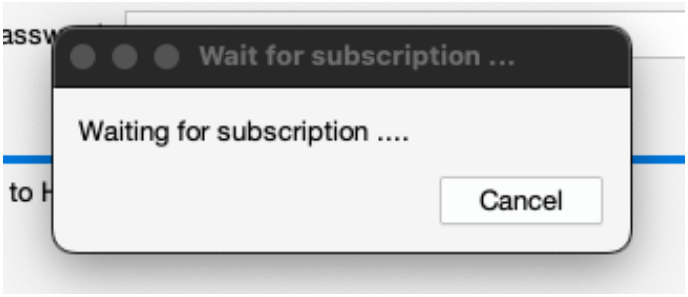

Figure 29

If the user has a valid subscription, they are prompted to enter their password (see Figure 30). To make a secure connection to the exact customer device, the customer will need them to provide support staff with that device's Machine ID. It can be found by the customer on their WSH PTY cockpit interface for the device they want support staff to connect to. Please see *Viewing the Machine ID of the WSH PTY Device* above to assist the customer with finding this ID.

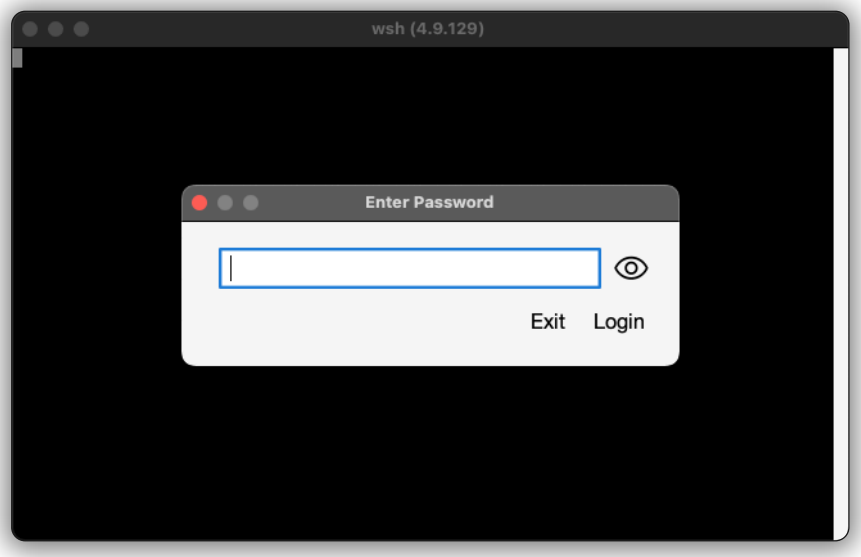

Figure 30

Once the proper machine ID is retrieved for the device, enter it into the "**Machine ID**" field (see Figure 31) and then click the "Connect" button.

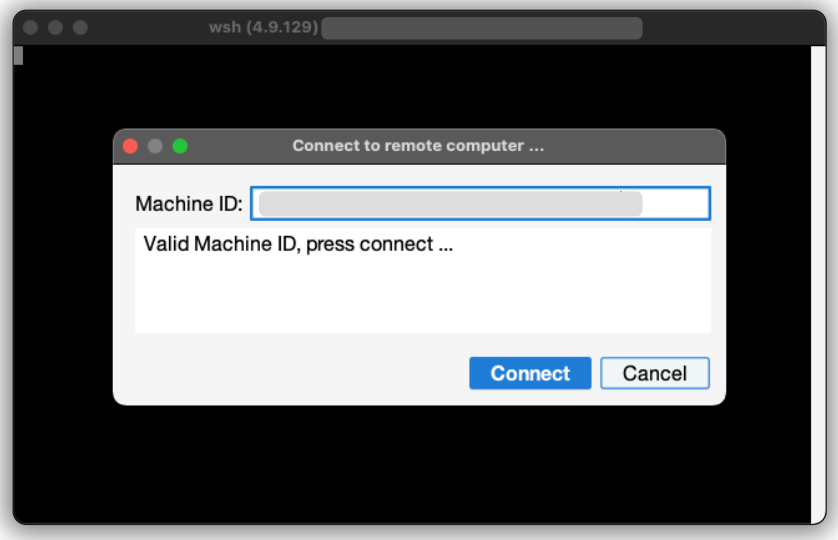

Figure 31

WSH PTY will automatically connect the user to that device and initialize the WSH PTY terminal (see Figure 32). The WSH PTY is a pseudo-terminal on the server allowing service technicians to interact with the server as if the user were using a local terminal on the device.

Figure 32

All traffic sent between the WSH PTY and TTY is encrypted and thus completely secure. Commands are logged on the customer's device in order to provide transparency for the customer and also have a running record for the service technician. Once the technician is finished, the connection between the user's local device and the server is broken automatically.

In order to show Trusted Team Tags, right click on the terminal to show Teams. The Trusted Teams the user is a member of are listed in a popup box. If users need to access a particular PTY, users may provide TTY certificates to administrators to add to the **"Trusted Devices"** list on the PTY.

7.1. WhiteStar Enterprise Files – Transferring Files To/From PTY Device

WSH includes WhiteStar's secure file transfer system known as **WhiteStar Files** built into the WSH TTY. Right click (with the mouse) on the WSH TTY terminal windowpane to see the options to **send and receive** [get] files to and from the WSH PTY device (see Figure 33). All files sent or received via WhiteStar Files are encrypted during flight and at rest ensuring complete security. File transfers have a progress bar, along with a cancel button to stop a file transfer before it completes. When downloading files, the technician can specify which folder the file goes into or let it default to the downloads folder on your computer.

7.1.1. Sending a File to the Remote Machine

On the WSH TTY, right-click (with your mouse) within the TTY windowpane and select "**Send File** …" (see Figure 33).

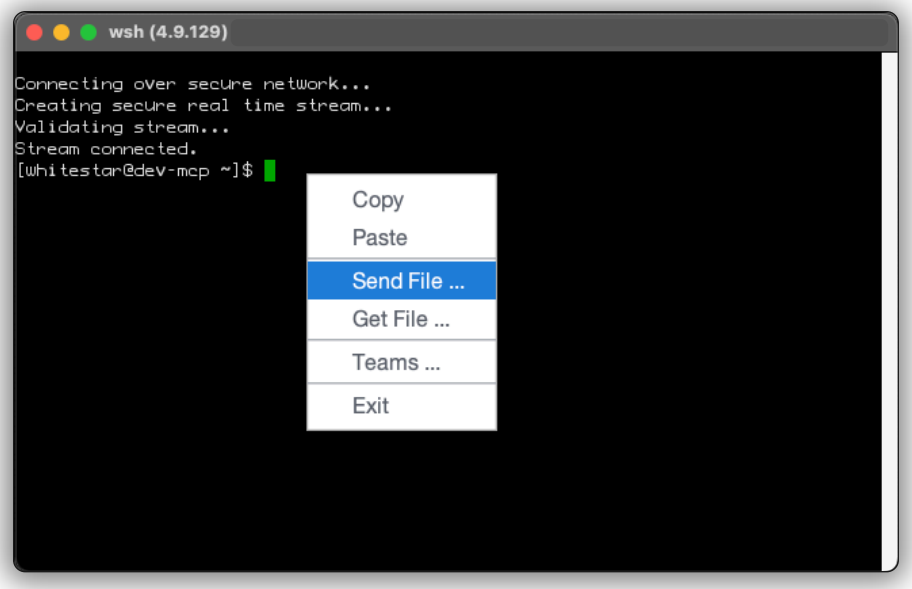

Figure 33

This action displays a file browser of your local computer (see Figure 34).

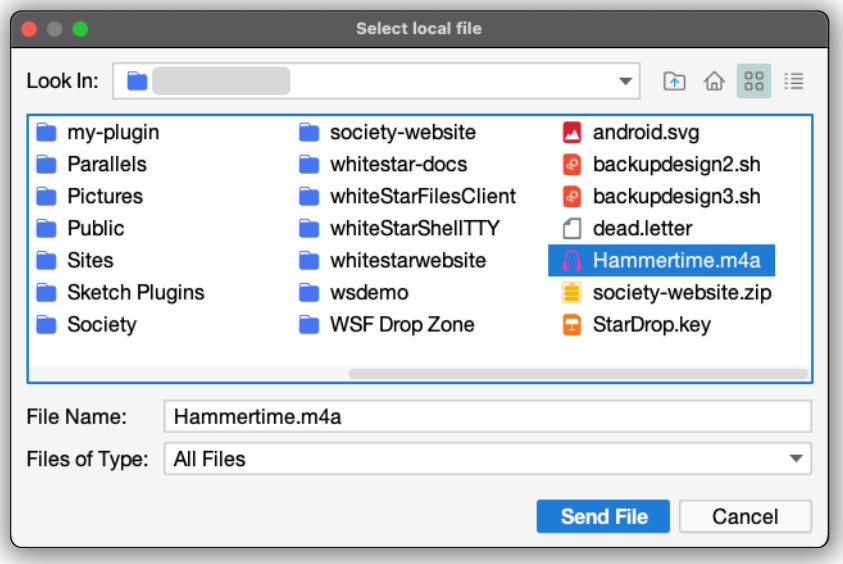

Figure 34

Next navigate to the directory of the file you wish to send and select it by double clicking (with the mouse) on the file name. Once selected, click the "**Send File**" button to initiate the transfer of the file to the WSH PTY device. A progress bar is displayed on the WSH TTY providing real time status. Once the file transfer is complete, the file can be found in the remote device's Downloads folder for the white star user (/home/whitestar/Downloads).

7.1.2. Viewing your Trusted Teams Tags

In order to view the Trusted Teams Tags you have associated with you WSH account, right click the TTY window and scroll down to "Teams".

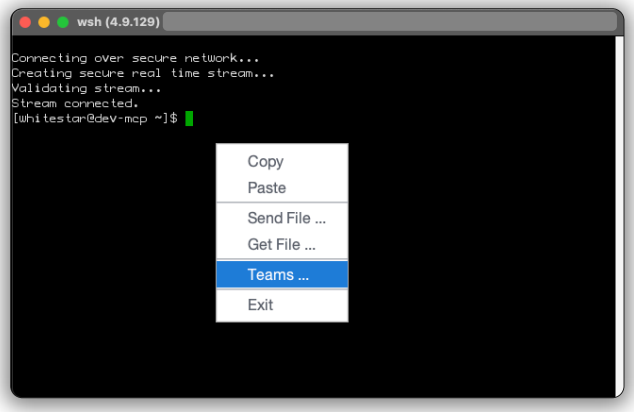

Figure 35

Then click "Teams". This will view the current assigned Teams Tags that are associated with your account. When you're finished, click "Finished".

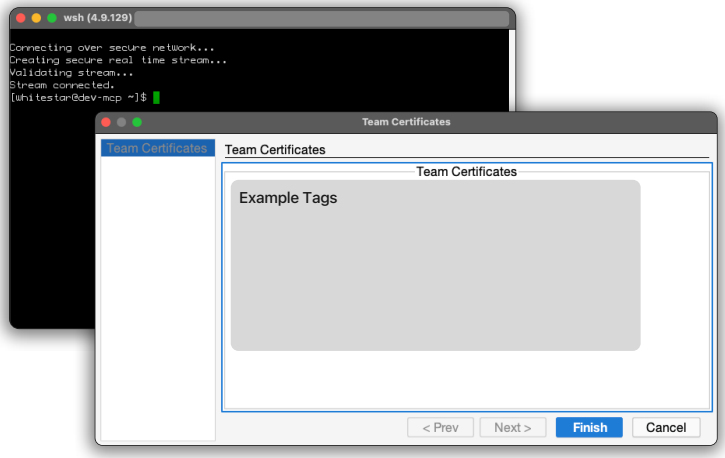

Figure 36

7.1.3. Receiving a File from the Remote Machine

On your WSH TTY, right-click (with your mouse) within the TTY windowpane and select "**Get File** …" (see Figure 24). This action displays a file browser of the remote WSH PTY device.

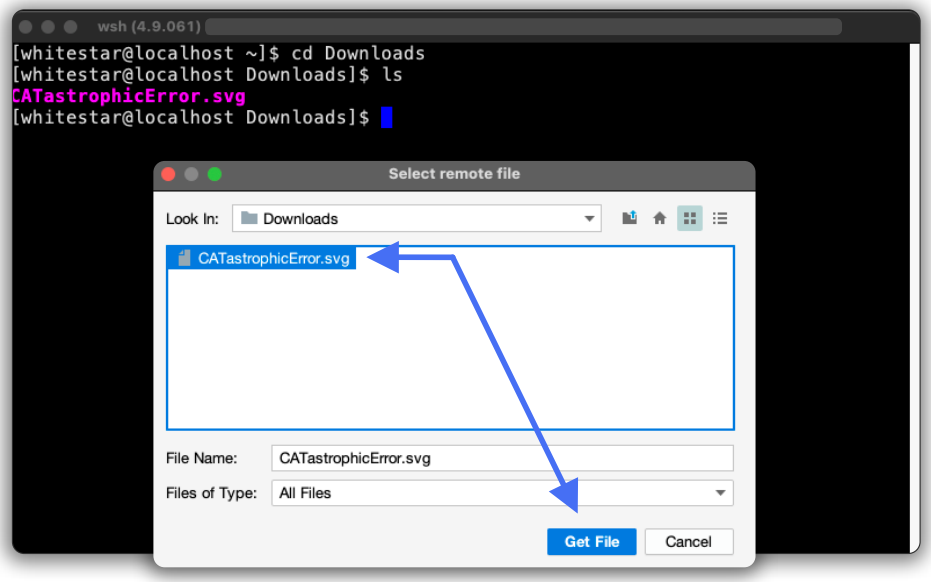

Figure 37

Next navigate to the directory of the file you wish to receive and select it by double clicking (with your mouse) on the file name. Once selected, click the "**Get File**" button to initiate the transfer of the file to the WSH TTY device.

A progress bar is displayed on the WSH TTY providing real time status. Once the file transfer is complete, the file can be found in the local device's Downloads folder for the administrator user (/Downloads).

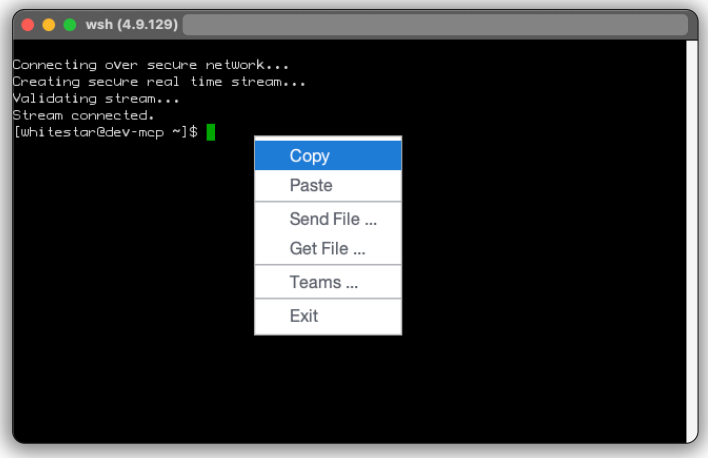

Figure 38

You can right-click to copy and paste data in and out of the TTY.

Typing the “exit” command into the TTY will close all network connections and exit the application (Fig. 35).

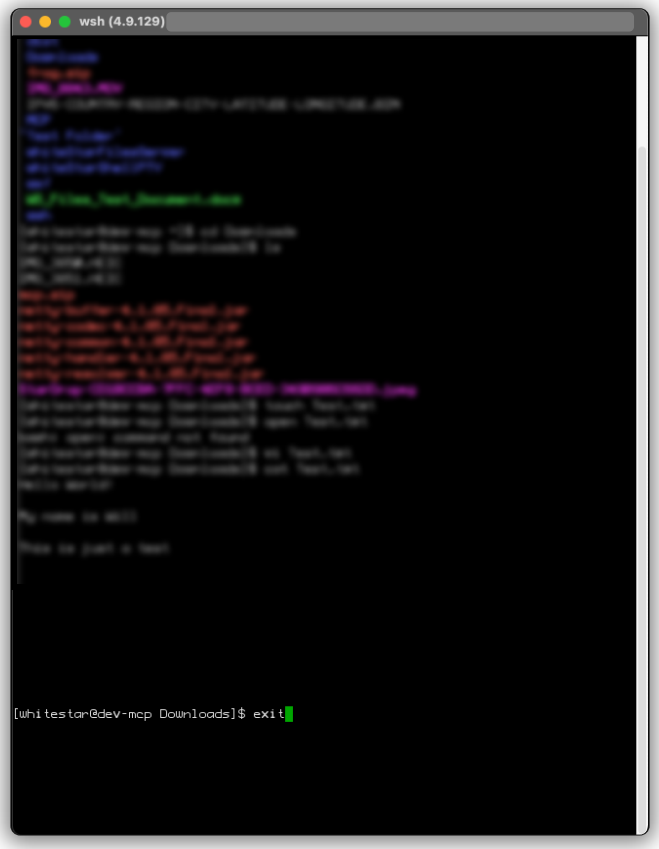

Figure 39

8. Installation of WSH PTY on a Linux System

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

The system administrator will need to run 2 commands, both requiring root privileges to execute.

The **Cockpit software package**[1] must be installed and configured prior to installing the WSH PTY software. The following commands can be issued from the Terminal tab on the Cockpit interface or a terminal shell on the machine.

The first command adds the WhiteStar repository for WSH install files.

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

The second command installs the WSH Cockpit plugin as well as instantiates the WSH service.

```
# sudo dnf install -y wsh-cockpit
```

Once installed, the WhiteStar Shell tab is available on Cockpit (see Figure 40) interface. The administrator may be required to hit **refresh** on their browser if they were already logged in to the cockpit interface in order to display the new WhiteStar Shell tab.

[1] Cockpit (web-based graphical interface for servers). Please visit **https://cockpit-project.org** for more information on how to install and setup Cockpit.

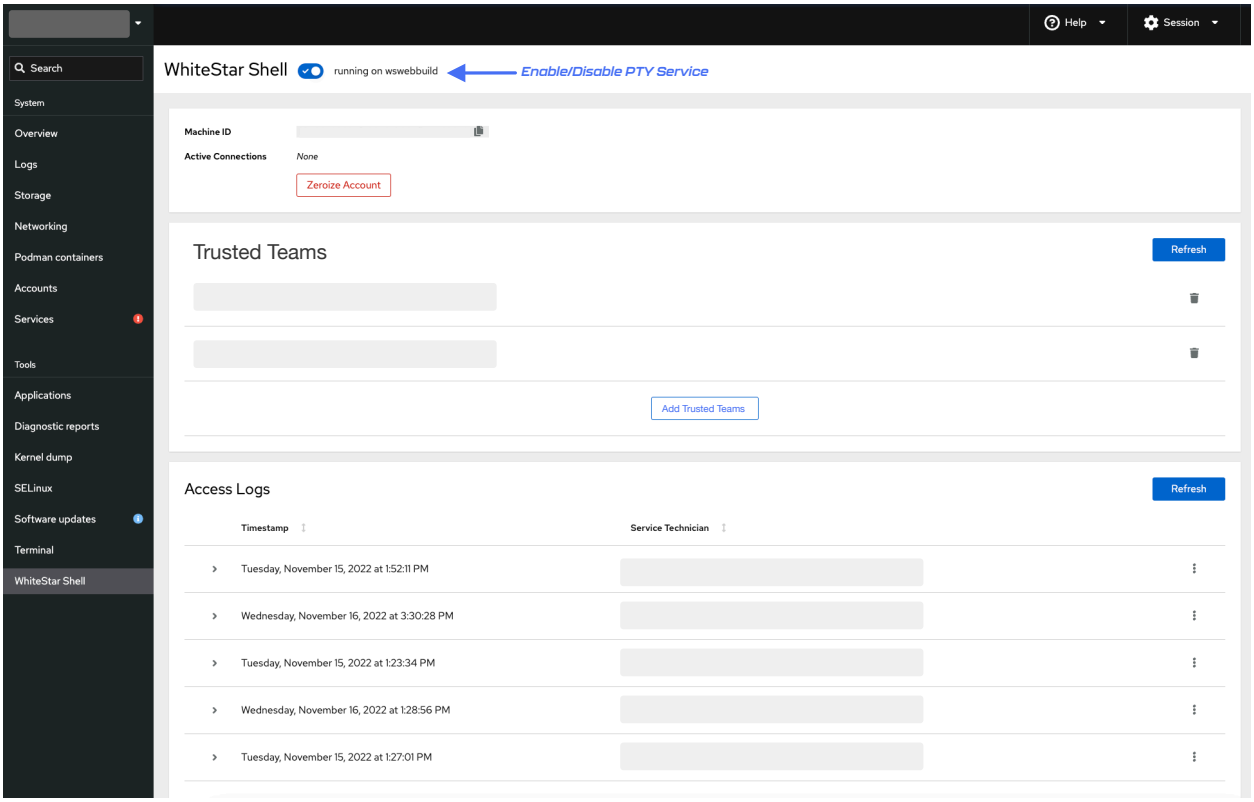

Figure 40

8.1. Configuration and Use of WSH PTY

Once the WSH PTY has been successfully installed, the device administrator can:

- enable and disable the WSH PTY service running on the device,
- view the machine ID of the device which the WSH PTY is installed on,
- maintain the list of trusted teams who can access the device, and finally
- view the log files automatically generated once a trusted support team member accesses the device

8.2. Enabling and Disabling the WSH PTY Service

The WSH PTY service always runs securely on the remote device and only allows connections to trusted teams specifically designated on that device. The service can be kept running at all times, or toggled on and then off for only the time a service technician requires access to the device.

To enable/disable the WSH PTY service:

- Log in to Cockpit on your Linux device
- Click on the WhiteStar Shell Tab (left hand column)
- Click on the toggle button at the very top of the page (see Figure 40 above).

8.3. Viewing the Machine ID of the WSH PTY Device

Each device within the WhiteStar network is referred to by its unique machine ID. To find the machine ID of a particular device (which is necessary to share with the support technician in order for them to access the device via their WSH TTY), do the following:

- Log in to Cockpit on the Linux device
- Click on the WhiteStar Shell Tab (left hand column)
- A the very top of the page, below the WhiteStar Shell toggle (see the black arrow in Figure 26 below) is the machine ID listed (see the blue arrow in Figure 41 below).

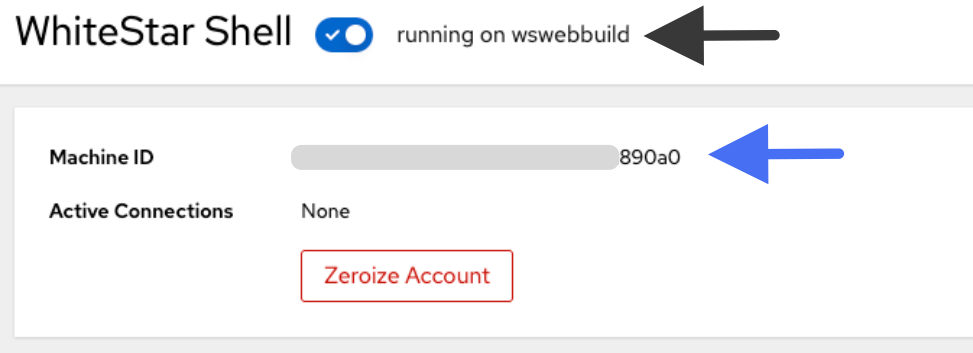

Figure 41

8.4. Zeroizing the WSH PTY interface

If the administrator wants to completely remove the WSH PTY account, and securely delete all log files that have been generated on this device, they can do so by clicking on the "**Zeroize Account**" at the top of the WSH cockpit screen (see Figure 41). If the "**Zeroize Account**" button is pressed, the administrator is asked to confirm the zeroization prior to the action executing (see Figure 42).

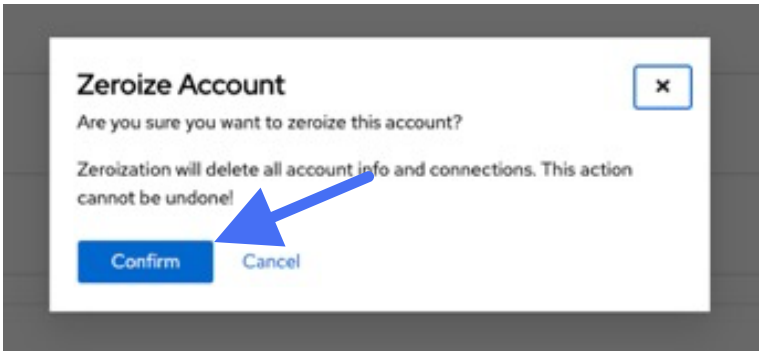

Figure 42

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

In order for a device to be accessed by a WSH TTY client (e.g. a support technician from the company trying to help diagnose an issue), the system administrator of the device must add trusted teams via the Cockpit WSH PTY interface.

To add a trusted team:

- Log in to Cockpit on your Linux device
- Click on the WhiteStar Shell Tab (left hand column)
- Click on the “Add Trusted Team” button in the middle of the page (see Figure 43)

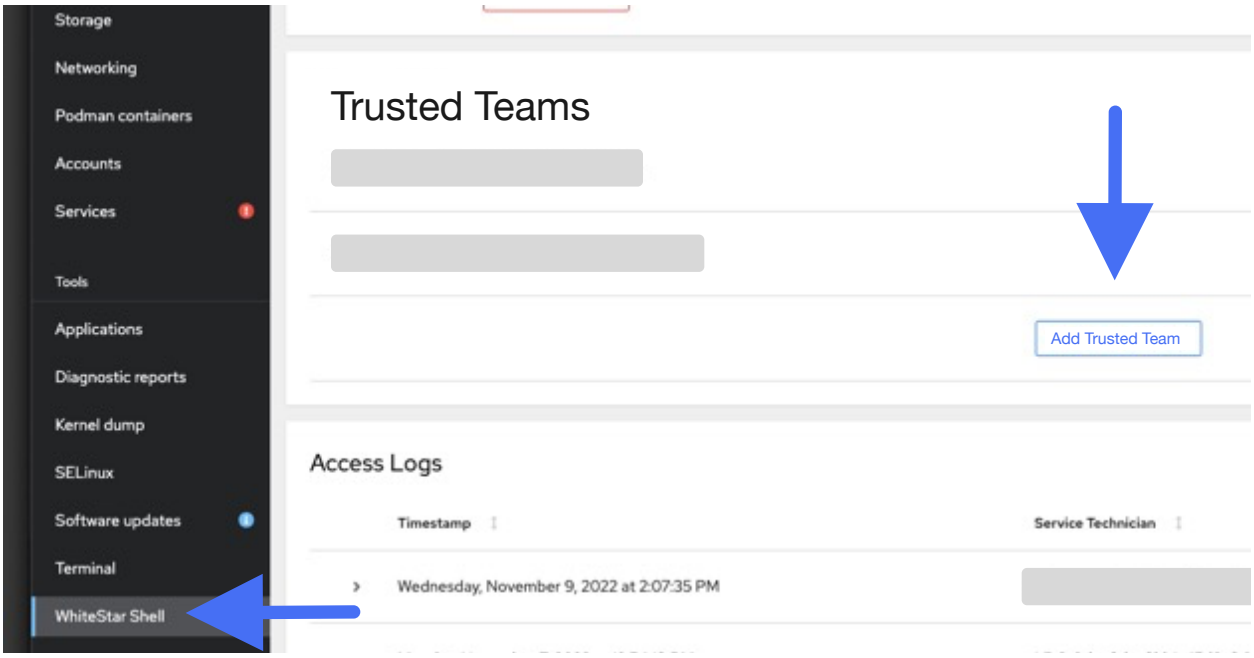

Figure 43

The administrator is presented with a pop-up box (see Figure 44) where they can either select from the White-Listed Trusted Teams in the pre-populated list (blue arrow) or enter the name or ID of the team (provided by your device support organization) in to the search field. Once the appropriate team is selected, hit “**Submit**” to add them to your list. At this point, if the administrator wants to allow the service technician access to the device, they must ensure the WSH PTY service is running on the box (see Enabling and Disabling the WSH PTY Service).

Here you will see only Tags that were made “visible” on the management Dashboard.

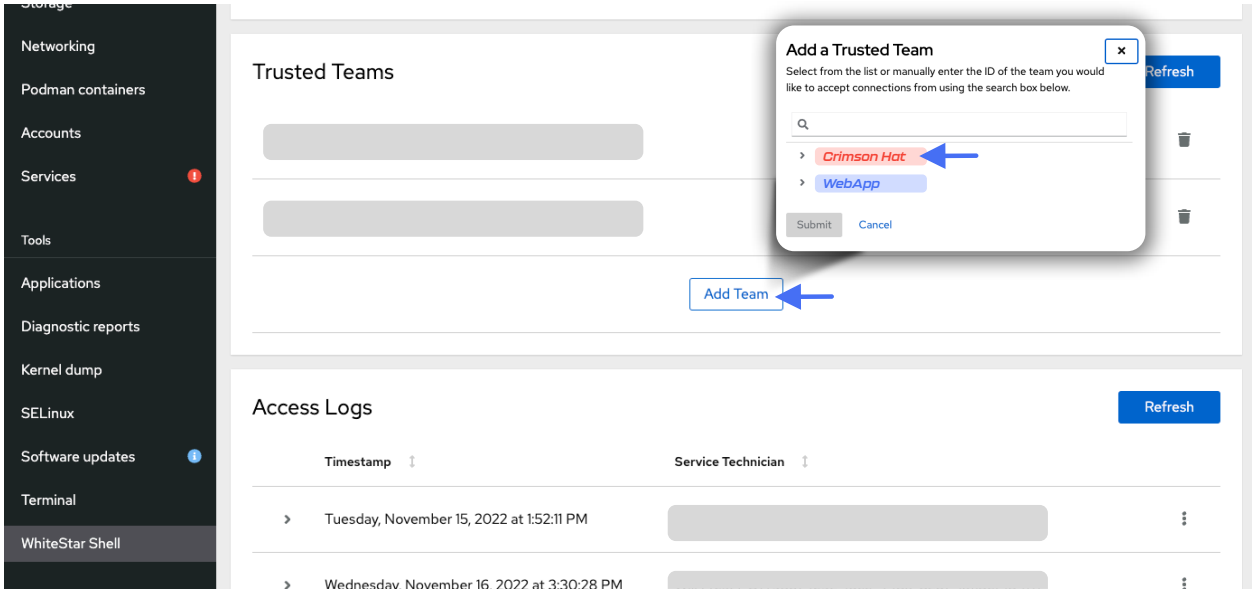

Figure 44

If, at any time, the administrator wants to remove access for a particular trusted team from one of their devices, they need only click on the "garbage can" icon to the right of the team (on that device's cockpit screen) and access is removed for that team.

8.6. Viewing WSH PTY Log Files

Once the service technician connects to a remote device, WSH keeps a complete history of all commands that have been issued for each and every connection session.

These logs are maintained in the "**Access Logs**" section of the WSH cockpit (see Figure 45).

To view a particular log, click on the carrot icon (>) to the left of the log's Timestamp, and scroll up/down through the log to see all of the commands that were entered by the service technician (see Figure 46).

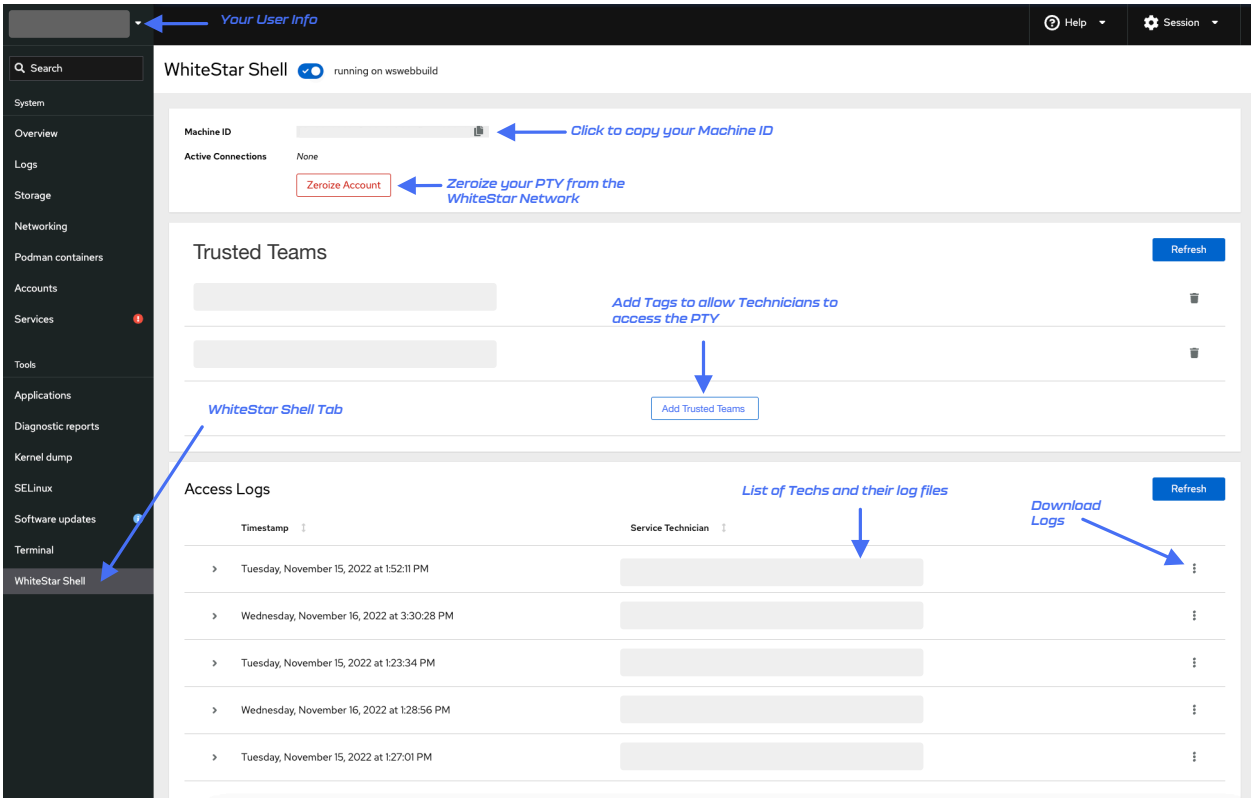

Figure 45

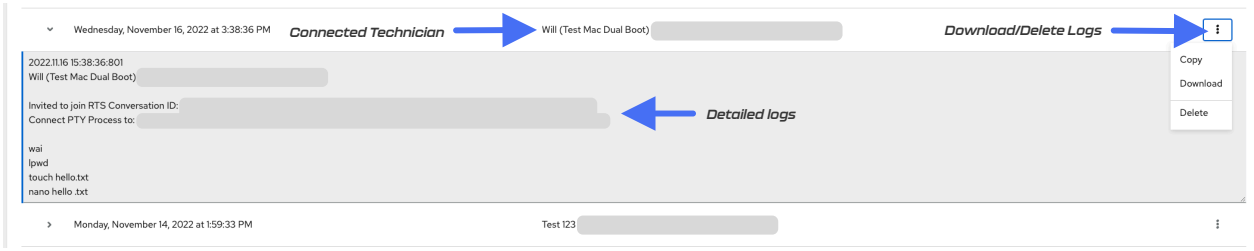

Figure 46

Finally, to Copy, Download, or Delete a particular log, click on the three vertical dots on the far right hand side (for any of the log files) and choose the action that is desired (see Figure 46).

8.7. WhiteStar Shell – Bounding the TTY User

To further enhance security, WhiteStar offers the ability to bound the actions a WSH TTY user can perform when connected to a PTY device. These include such things as limiting the command set the user can execute or restricting which directories the user can navigated to.

Controls are defined and assigned by an administrator (via the administrator's dashboard) to Trusted Team Tags when assigning tags to an individual TTY user (or team). When a TTY user

connects to a PTY device (via one of these bounded Trusted Team Tags), a welcome message is displayed confirming they are using the bounded WhiteStar shell.

While using the WSH, a sub-set of commands is always available to the user:

- **cd**
- **clear**
- **exit**
- **help or ?**
- **history (Unix specific)**
- **sudo (Unix specific)**

Two additional WSH specific commands are also provided:

- **lpath**: lists all allowed and forbidden paths the user can navigate to while connected
- **lsudo**: lists all sudo commands that are allowed (Unix specific)

When connected to a WSH PTY, typing "Help" or "?" displays the list of permissible commands assigned to the Trusted Team Tag. If the TTY user attempts to enter a command not in the list, or change directory to a path that is not permitted, WSH displays an error message indicating that the action is not permissible, and logs this attempt. The administrator also has the ability to force disconnect a user from a system if they exceed a pre-set limit of impermissible commands.

NOTE: users of WSH, when limited by their Tags (as-in, not operating in a superuser mode) will ***not*** have access to "tab completion". This has been done for security purposes.

8.7.1. Setting a Trusted Team Tag's boundary attributes

To set a Trusted Team Tag's boundary attributes, first navigate to the Tags tab on the WS Administrator's Dashboard via the web. If a specific Trusted Team Tag hasn't already been created, see "5.3 Tagging – Providing Access to Customer PTY Devices" above to learn how to create one. Once a Trusted Team Tag is created, click on the Tag under "manage Tags" and the administrator is presented with the ability to assign bounding attributes for that Trusted Tag (see Figure 47).

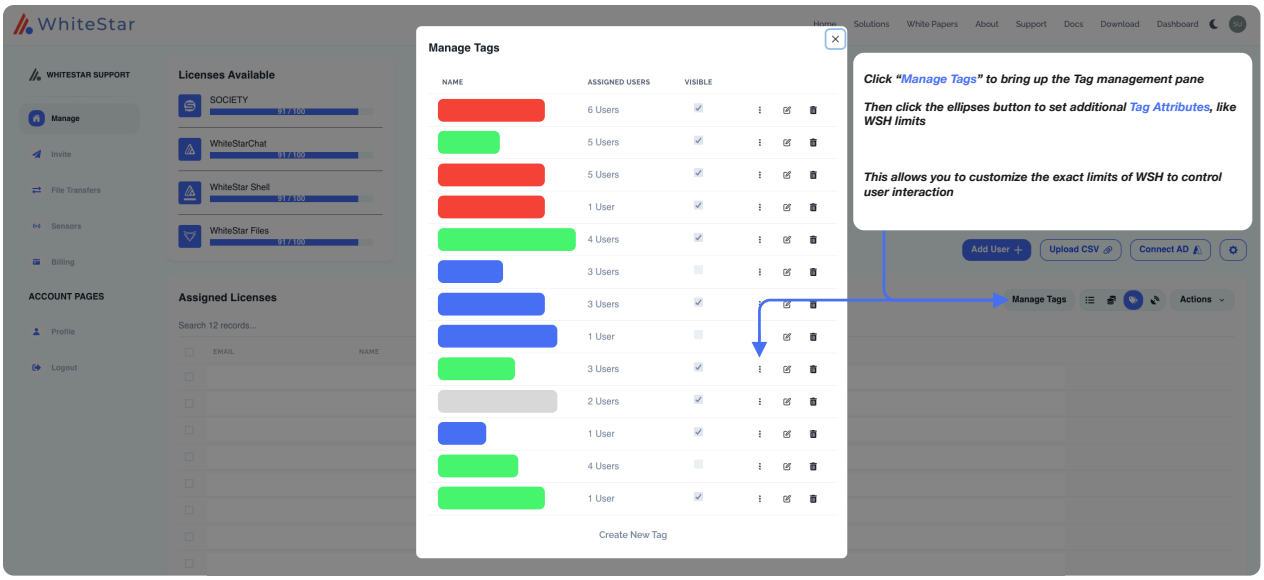

Figure 47

If desired, the administrator can name the Trusted Tag Attribute being created. They then enter the bounding properties of the Trusted Tag Attribute. These boundaries are enforced by any WSH PTY device when a WSH TTY user, with this Trusted Tag assigned to it, connect to it. If a TTY user has more than one Trusted Tag for the same PTY device, WhiteStar provides the ability to prioritize Trusted Tags. The Tag with the highest priority will be the one the WSH PTY uses to apply the boundaries. If Trusted Tags with the same priority are assigned to the same user, and active on the same PTY device, the Tag's boundaries that was created first (determined by a created time stamp) will be enforced. WhiteStar recommends assigning blocks of numbers (100,200,300,400,500…n) rather than sequential numbers (1,2,3,4,5…n) when assigning priorities to allow for additional priorities to be inserted between existing values in

NOTE: In order for many of the Trusted Team Tag attributes to take affect, the admin must first create a Boolean Bounding Key named "enable" (highlighted in green below) and set its value to "on" (true). If this bounding key is not present, WhiteStar's default is "off" (false) for those bounding keys affected by "enable". This allows the admin to set many bounding keys and toggle them on/off for those users who have been assigned the Trusted Team Tag.

The attributes which can be bounded by WhiteStar include:

Bounding Key	Key (short form)	Enable Affected	JSON Type	Definition
allowedcommands	allow	yes	list	Operating system specific commands the TTY user is

				permitted to execute. E.g. “ls” in Unix to list the contents of a directory. If present, **ONLY** these commands are permitted.
allowedpaths	paths	yes	list	The list of directory paths (and below) the TTY user is permitted to view. All other paths will be restricted. If this key is not provided, then the TTY user will be granted access to all directories.
disablewarning	warn	no	boolean	Indicates whether the TTY user is notified of PTY warnings or not (e.g. a filter violation). Default is false (i.e. warnings will be sent to the TTY user)
enablefilter	enable	n/a	boolean	Indicates whether filtering is turned on/off for the specific Trusted Team Tag. All bounding keys affected by enable are ignored if this is set to false. Default is **off** (false).
environmentvariables	env	no	map	Dynamic variables used by a shell and its child processes. E.g. SHELL in Unix which specifies the type of terminal to emulate when running the shell.
forbiddencharacters	forbid	yes	list	Operating system specific characters the TTY user is forbidden from entering on the command line.
getfiles	get	no	boolean	Indicates whether the TTY User is permitted to get (retrieve) files from the PTY device. Default is true. This bounding key, if present, is enforced regardless of the enablefilter setting.
homepath	home	yes	string	The starting directory the TTY user is placed in upon logging in. The user will always have access to this directory and all subdirectories from it.
maximumwarnings	maxwarn	yes	number	The total number of warnings a TTY user is given prior to force exiting the application. This number can be between -1 and n. -1 indicates unlimited warnings.

priority	priority	yes	integer	The priority this Trusted Team Tag is assigned. Used to determine, when a TTY user has multiple Trusted Tags assigned to them, which Trusted Tag to enforce. The larger the number, the higher the priority. Best practice is to separate by at least 100.
sendfiles	send	no	boolean	Indicates whether the TTY user is permitted to send files to the PTY device. Default is true. This bounding key, if present, is enforced regardless of the enablefilter setting.
welcomemessage	welcome	no	string	User defined welcome message displayed to the TTY user upon logging in to the application. This bounding key, if present, is enforced regardless of the enablefilter setting.

When configuring the Trusted Team Tag both the extended and short form of the key variable are accepted (see Figure 48) in the Property name field. Since these are the only keys accepted by WhiteStar Shell, it is highly recommended that the administrator copy and paste these keys to avoid misspelling errors. Entering any other Bounding key (including mis-spelling the keys above) is ignored by the WSH PTY.

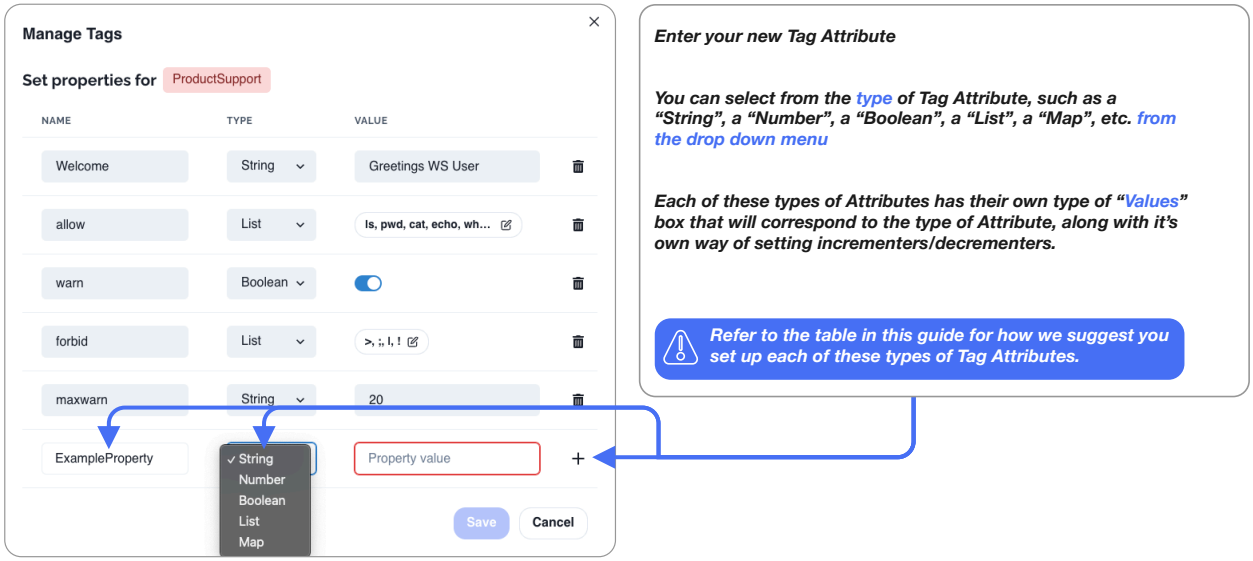

Figure 48

For each Bounding Key, a set of attributes must be provided. For example, an administrator may assign to a Trusted Team Tag the ability to issue the following set of commands: ls, pwd, vi, rm (see Figure 49).

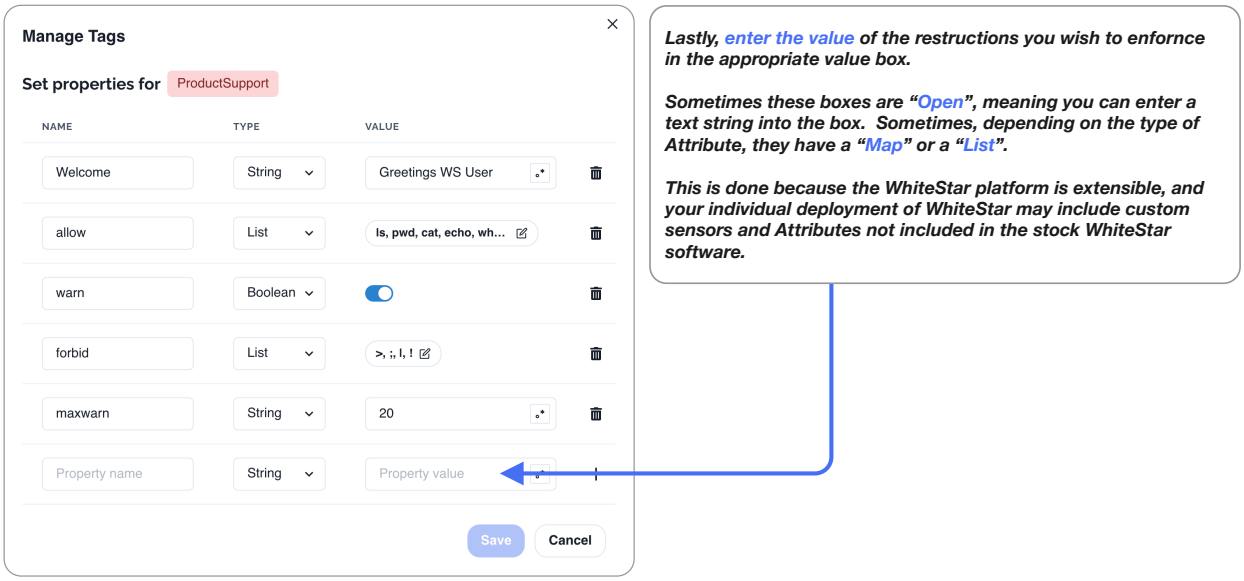

Figure 49

Keep in mind that the administrator of the WSH account is responsible for the Trusted Tags and the boundaries they convey. The owner/operator of the server that the WSH user attaches to will be responsible for setting the expectations of decorum that the WSH administrator should enforce on the users they manage.

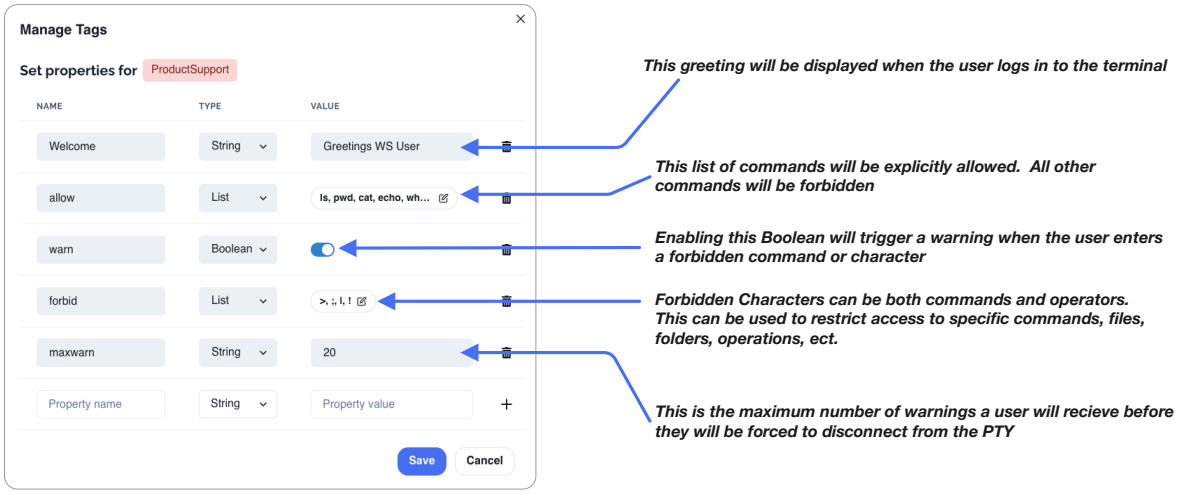

Figure 50

8.7.2. Editing a Trusted Team Tag's boundary attributes

To edit an existing Trusted Team Tag's boundaries, simply click on the "Manage Tags" console from the administrator web page and select the boundaries screen (see Figure 47). Click on

the Trusted Team Tag you want to edit and click in any existing box to edit the values in that box. When done with updates, click “Save” and the updates will be applied (Figure 50).

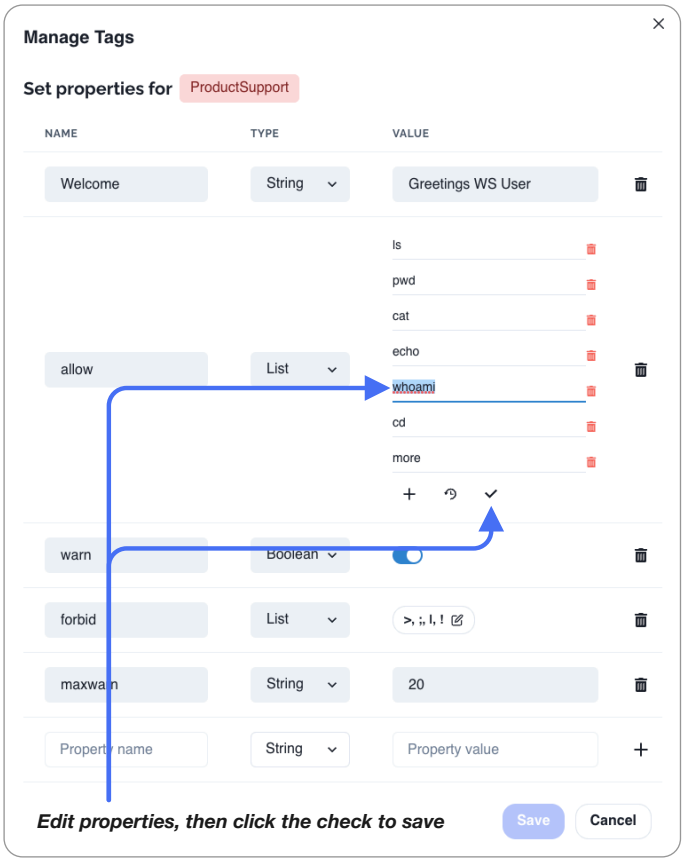

Figure 51

8.7.3. Deleting a Trusted Team Tag’s boundary attributes

To delete an existing Tag’s attributes simply click on the “Manage Tags” console from the administrator web page and select the boundaries screen (see Figure 47). Click the “X” button on the right-hand side of the screen to delete the attribute (see Figure 52). Click “Save” and the updates will be applied.

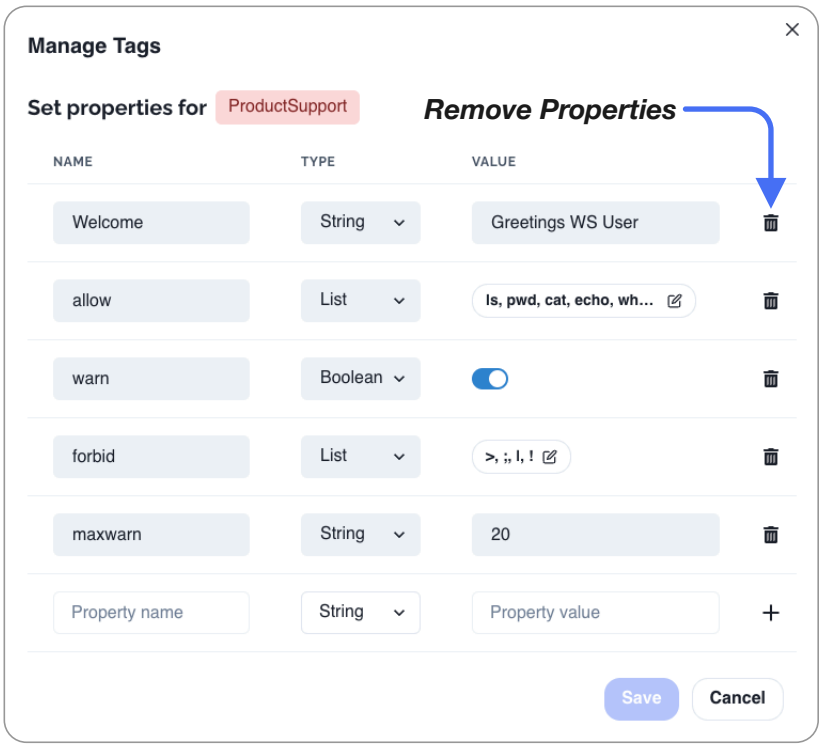

Figure 52

8.8. Maintaining WSH Software

In order to keep the WhiteStar Shell PTY and cockpit plug-in software up to date, the device‘s administrator must issue the following two commands (during their routine maintenance window):

```
# sudo dnf update -y wsh
```

```
# sudo dnf update -y wsh-cockpit
```

These commands automatically check the version of software currently installed to determine if WhiteStar’s software (or any of its dependencies) needs 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*”.

9. Uninstall and Deactivation

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

Windows – Go to the control panel, then add/remove applications, then search for the WhiteStar Shell on the page and locate the application. Then click the ellipses (three dots) on the right-hand side of the screen and 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*/whiteStarShellTTY and delete this directory. Empty the OS trashcan. The application is now fully deleted.

10. FAQ

Q: Can I use the same email for WhiteStar Shell as I do for other WhiteStar applications?

A: Currently all users must have a **unique email address** to use WhiteStar Shell, one that is not associated with any other WhiteStar product.

Q: Why do I need a subscription?

A: WhiteStar bills for the use of our software. In order to use WhiteStar Shell 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 Shell. What should I do?

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

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

A: The first thing an WSH 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 WSH or any WhiteStar tools. If the administrator wants to completely remove the user from the system, they can use the Zerioize 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 (see Figure 53). It will take you to the support portal, where you can send a question or put in a support ticket.

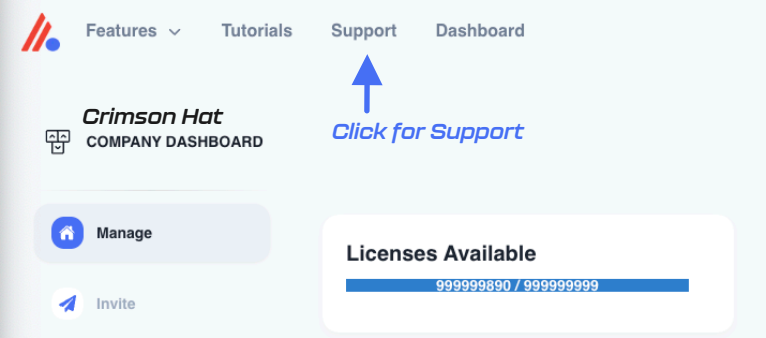

Figure 53

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

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

Q: What is WhiteStar Enterprise Files?

A: Enterprise Files is WhiteStar's file transfer solution which accomplishes encrypted high-speed file transfers, of any size, to and from the WhiteStar Shell TTY and PTY components.

11. Troubleshooting

I cannot connect to a WSH PTY device

If you have successfully started the WSH TTY, and are being denied a connection to a particular WSH PTY device, there are several things to verify:

1. First confirm that your administrator has attached the proper WSH Team Tag, granting access permission to this device, to your user id.
2. Next ensure that the customer has granted access to the WSH Team Tag (the same one your administrator created in #1 above) on the WSH PTY device that is attempting to be accessed.
3. Confirm with the customer that the WSH PTY 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 WSH TTY 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 TTY is stuck trying to "validate" the session. What can I do?

Ensure that the clock on the WSH TTY 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 WSH TTY won't launch

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

The WSH TTY shows a blank screen after connecting and doesn't accept keyboard input

Terminate the current instance of the WSH TTY Shell and restart. If, after restarting, you still cannot interact with the WSH TTY Shell, it may be because there is another technician currently connected to the WSH PTY you attempted to connect to. Check with other team members, who are also permitted to connect to this customer's devices, to ensure they are not currently connected.

The other potential reason you would see this issue is if the WSH PTY 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 PTY is currently on, kill your instance of WhiteStar Shell, and retry your connection.

The WSH TTY 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 technician, 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 technicians, ensure that your WhiteStar account is currently in good standing.

The WSH PTY 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 PTY off and then back on, then reassess whether you see the online devices. Have your remote technician disconnect and reconnect by rebooting their TTY and reconnecting to your PTY.

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.

12. Glossary

ACRONYMN / TERM		Definition
CSV file		Comma separated values file, typically used with Microsoft Excel
Federation 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.
PTY	Pseudo Terminal	The WSH PTY is a service that runs on a remote server that replicates all commands it receives from a user's TTY 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	Enterprise Files	WhiteStar's native anywhere-to-anywhere, always encrypted, unlimited-file-size, platform agnostic file transfer system.
TTY	TeleTypeWriter	The WSH TTY is your local interface with the WSH PTY. It mimics a terminal interface on the server, but is running on your local device.
WSH	WhiteStar Shell	The WhiteStar Shell is the name for the entire PTY/TTY/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 PTY 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 WSH PTY, since WhiteStar never uses group cryptography.
Trinary	Trinary Switch	Having three states

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 app.
Logs	Log Files	A detailed written record of what tasks your computer is currently working on or has completed.
Machine ID		A unique identifier that each machine is assigned. Only one device may ever have this ID, thus it is unique to each individual machine
UUID		Another form of unique identification that can identify a machine, device, or endpoint
Cockpit		Graphical user interface for Linux server management
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.