WS HyperSpace™

Installation and User's Guide

Table of Contents

1. Introduction - What is WhiteStar HyperSpace™?

Businesses need to electronically connect to remote devices and networks in order to exchange highly sensitive information without worrying that the information being exchanged is also being compromised. Illegal appropriation of information 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 legacy means, such as VPNs and Firewalls, which are known to have exploits and vulnerabilities.

Standard remote access solutions require user accounts to be created, complex firewall configurations, group keying, and have inherently slow data rates. 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.

Therefore, there is a need to provide remote access that that is both efficient and secure, preventing exposure to data leaks or hackers; and to do it all at a low cost. WS HyperSpace™ is our solution to the problem. It utilizes full end-to-end encrypted remote connectivity **directly** to and from virtually any device, anywhere in the world, with security natively built in. It runs on our hybrid peer-to-peer WS Network which operates as a “Network as a Service” for secure applications. Equally important, data transfer rates exceed those users typically experience with traditional remote access solutions, yet data is traversing the network in such a way as to be completely impervious to interception.

2. WS HyperSpace™ - Solution Component Overview

WS HyperSpace™ is comprised of **multiple entities:**

Administrator's Dashboard - a web-based console used to manage users and their access to devices an organization wants them to connect to. It provides the interface to grant and revoke access to members of your team - providing them with the proper credentials to connect to remote WS HyperSpace™ Service Agents, WS HyperSpace™ Connection Agents, and WS HyperSpace™ Proxy Agents.

WS HyperSpace™ Federation Agent - a secure quantum resistant application which forms direct peer to peer connections with other WS HyperSpace™ Agents running on remote devices. The WS HyperSpace™ Federation Agent allows seamless secure communications to devices running locally within your intranet or remotely (via the internet) to any device the client has been granted access to. The user can form a personal mesh network by installing the WS Federation Agent on multiple devices (utilizing the same email address) while also forming spoke and hub connections to WS Service, Proxy and Connection Agents.

WS HyperSpace™ Service Agent - a secure service that executes on a device where access is being granted to. This service provides the WS HyperSpace™ user a secure interface between the device and the user's WS Federation, Proxy, and Connection Agent applications. The WS HyperSpace™ Service Agent can be used to connect to other WS Service Agents in order to form a mesh. Depending on the customer's procedures for external access to their devices, administrators may want to keep this service stopped and *only start it when access is required on a particular device*.

WS HyperSpace™ Connection Agent - a secure service that executes on a device providing a hub and spoke connection to WS Service, Proxy, and Federation Agents.

WS HyperSpace™ Proxy Agent - a secure service that executes on a device (typically) co-located with a device the user wants to access (but can't run a WS Agent on). This service provides the WS HyperSpace™ user a secure interface between WS Proxy Agent (running on a co-located device) and the user's Client application. 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 access is required on a particular device*.

2.1. Connection Examples

2.1.1. Forming a Personal Network

Figure 1 illustrates a basic representation of how installing the WS HyperSpace™ Federation Agent on various devices (using the same email address) automatically forms a personal mesh network between these devices – allowing them to seamless interact with each other over the secure WS network, from anywhere in the world.

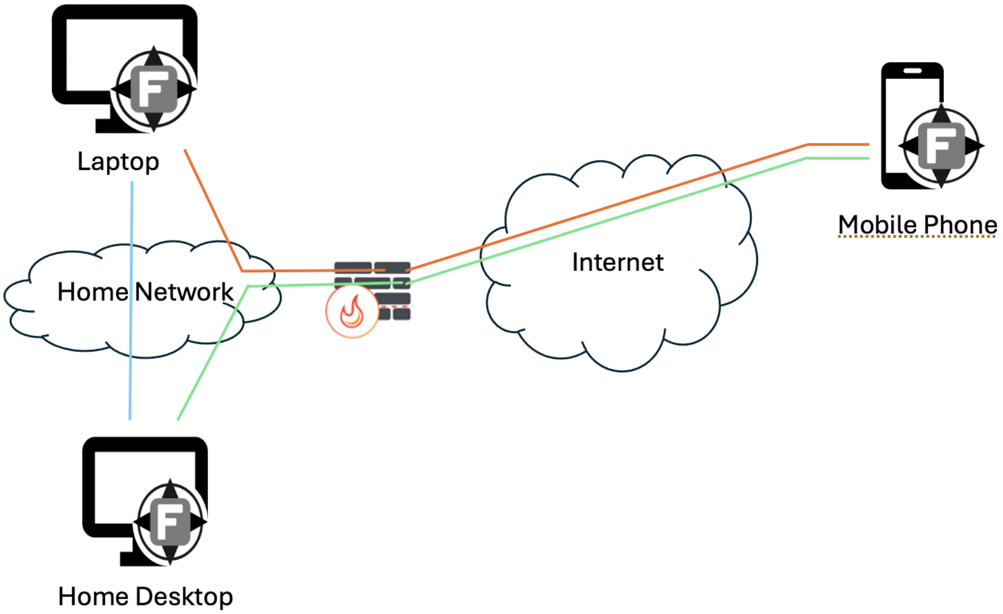


Figure 1

2.1.2. Connecting to Remote Devices running WS HyperSpace™ Service Agent

Figure 2 illustrates a basic representation of how WS HyperSpace™ Federation Agent users connect to WS HyperSpace™ Service Agent devices (both on the same intranet **and** seamlessly through firewalls and the internet). In order for these connections to be made, both the User and the Device they are connecting to, must be assigned the same WS StarTag by the account administrator. Assigning StarTags is discussed later on in this document.

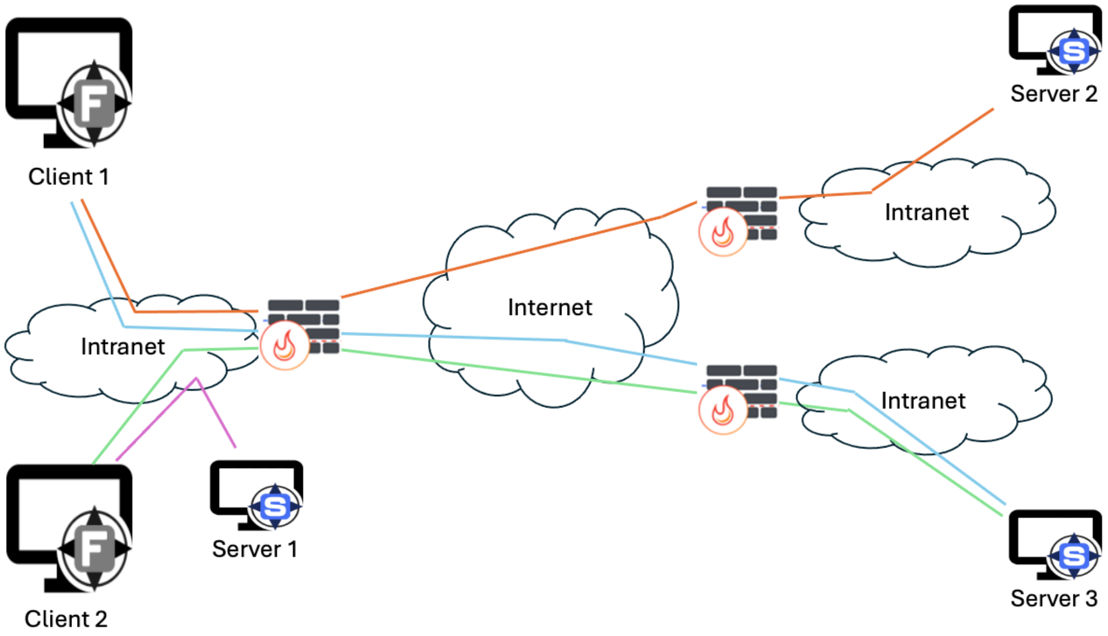


Figure 2

As illustrated above, WS HyperSpace™ Federation Agents can connect to and from devices within their own intranet (Client 2 connecting to Server 1), and to and from devices across the internet (Client 2 connecting to Server 3 and Client 1 connecting to both Server 2 and 3) simultaneously from the same WS HyperSpace™ Federation Agent.

2.1.3. Using WS HyperSpace™ Connection Agent as a Hub

Figure 3 illustrates a basic representation of utilizing the WS HyperSpace™ Connection Agent to connect multiple WS HyperSpace™ Server Agents together – enabling Server Agent to Server Agent communications in a highly efficient manner. The Connection Agent forms a hub and spoke topology thus avoiding the necessity to configure a fully meshed topology between HyperSpace™ Service Agents (and avoiding the performance issues associated with mesh networks in large enterprise environments).

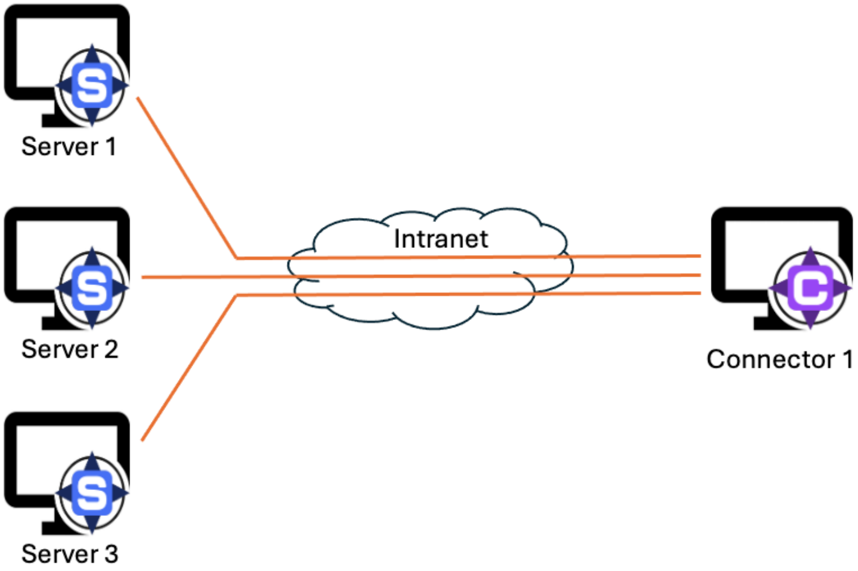


Figure 3

2.1.4. Connecting to a Remote Device via a WS HyperSpace™ Proxy Agent

Figure 4 illustrates a basic representation of utilizing the WS HyperSpace™ Proxy Agent to connect to a remote device that [may be] incapable of running a HyperSpace™ agent itself. It is recommended that Proxy Agents and the devices they are proxying for are as close together in physical proximity as possible to avoid any infiltration of the traffic between the Proxy Agent and that device. The specific example below shows a Federation Agent accessing a legacy Network Attached Storage (NAS) device over the WS network – via the Proxy Agent. While the traffic between the Federation Agent and the Proxy Agent is fully protected, the traffic between the Proxy Agent and NAS device will still be in the clear.

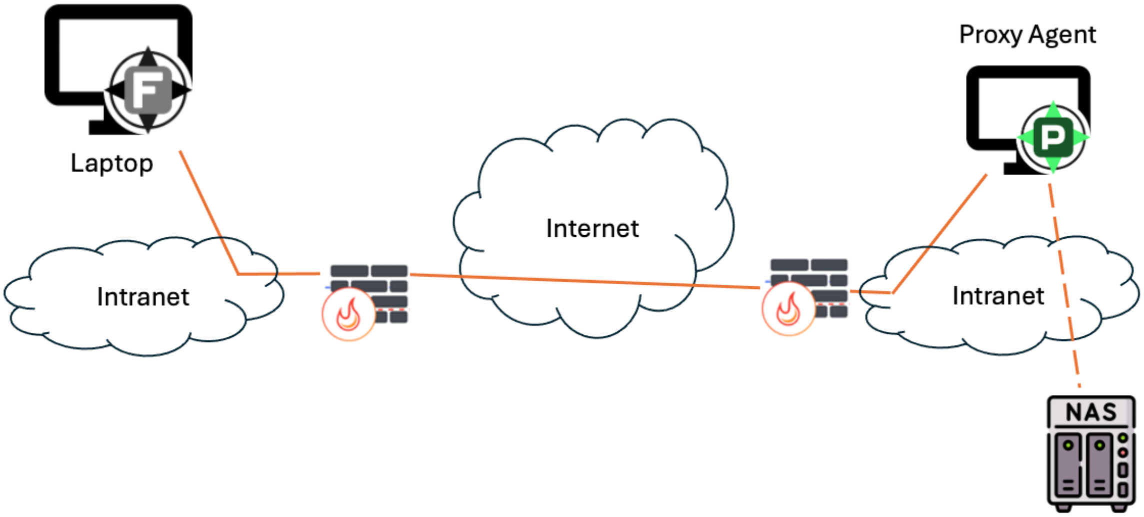


Figure 4

3. Minimum System Requirements

3.1. Software

The following is the minimum Operating System software versions for all WS HyperSpace™ software:

- Windows 10 or higher
- Mac OS 10.15 or higher
- Red Hat Enterprise Linux 8 or higher
- CentOS Stream 8 or higher
- Rocky Linux 8 or higher
- Debian 10 or higher
- Ubuntu 18.04 or higher

3.2. Hardware

The following is the minimum hardware necessary to run WS HyperSpace™ software:

- 2.5 Ghz or faster processor with 2 or more cores (64 bit compatible)
- 8 GB RAM
- 64GB or larger storage device

4. The WS HyperSpace™ Administrator Dashboard

The WS HyperSpace™ Administrator Dashboard is the interface a company uses to add WS HyperSpace™ users to the system, create and assign WS StarTags (which provide access for WS HyperSpace™ Federation Agent users to connect to WS HyperSpace™ Service Agent devices), and maintain the company's profile information. A WS StarTag is the company's "***token***" to gaining access to specific WS HyperSpace™ Service Agent devices and must be assigned to individual WS HyperSpace™ Federation Agent users in order for them to be granted access to a Device.

To access the Administrator Dashboard, a designated company administrator must visit the WhiteStar Communications website at **https://www.whitestar.io** and click the "***Dashboard***" button on the far right side of the menu bar on the landing web page (see Figure 5).

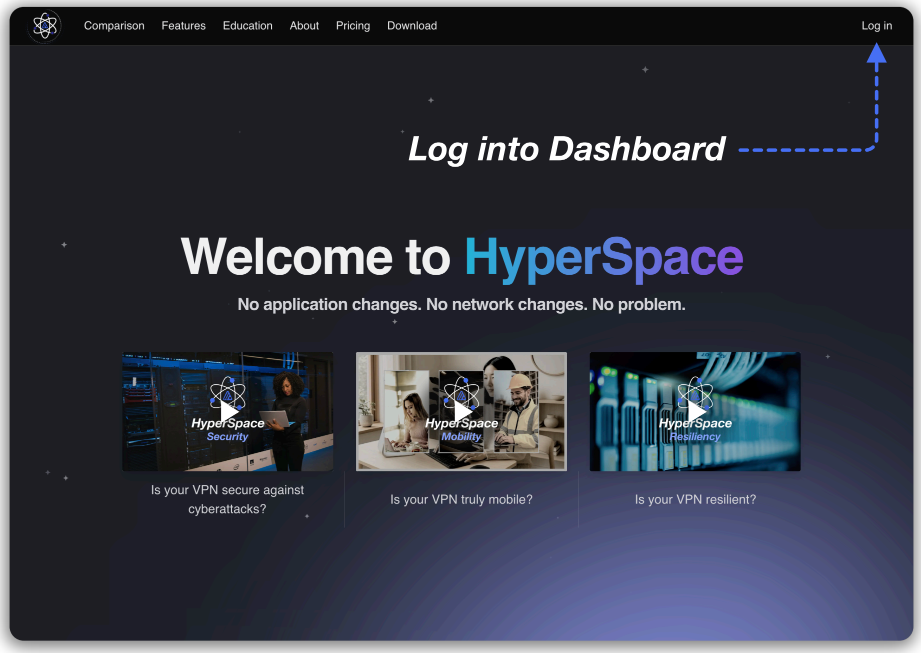
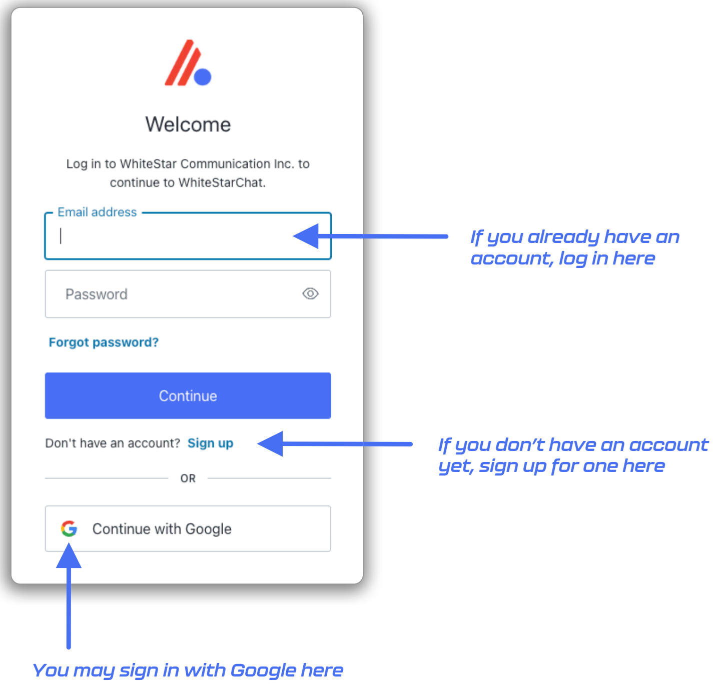


Figure 5

After clicking "***Dashboard***", the administrator is presented a screen prompting them to log in (see Figure 6). If they already have a WS 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)).



Welcome

Log in to WhiteStar Communication Inc. to continue to WhiteStarChat.

If you already have an account, log in here

If you don't have an account yet, sign up for one here

You may sign in with Google here

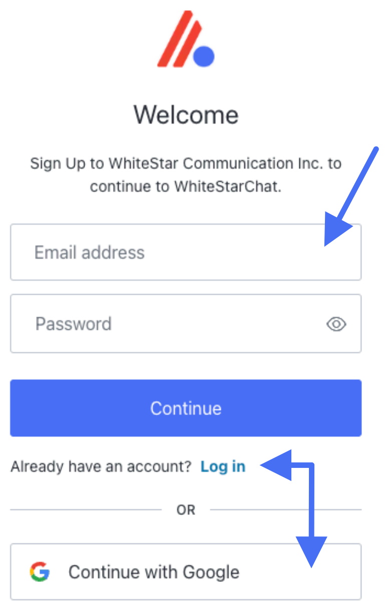
Figure 6

<u>NOTE:</u> 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.

If an account has not been established for the admin, you will need to prior to doing anything else. To obtain an administrator account, click the "***Sign Up***" link on the Admin log in screen (see Figure 6). When signing up for a WS 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 ***<u>strong</u>*** password (see Figure 7). Once the information is entered, click the "***Continue***" box.



Welcome

Sign Up to WhiteStar Communication Inc. to continue to WhiteStarChat.

Email address

Password

Continue

Already have an account? Log in

OR

Continue with Google

Figure 7

A verification email is sent to the address provided in order to verify ownership. Go to your email application and click on the appropriate button to verify your email. If this step is not executed, the administrator account will not be created.

When creating a password for a WS 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.

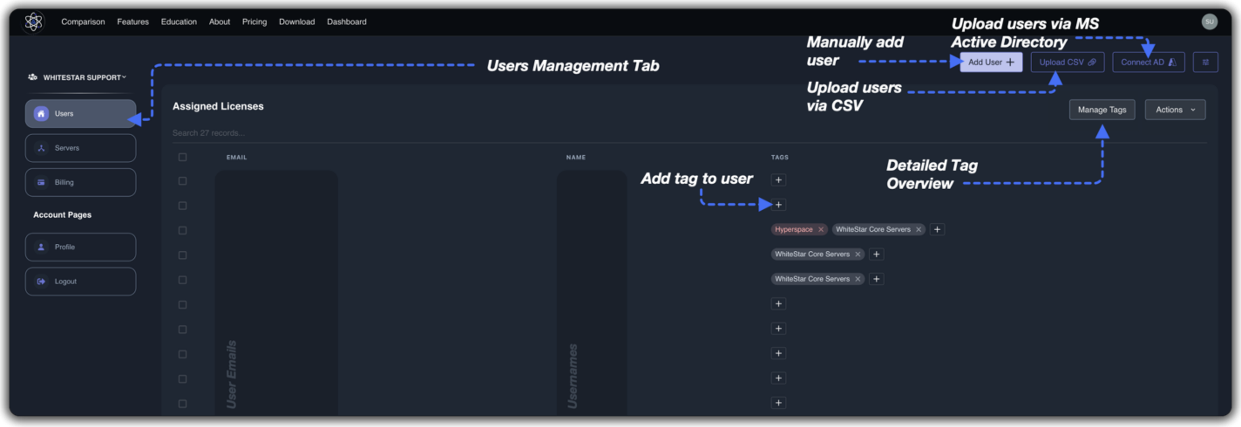
If option #2 is chosen, simple log in with your Google credentials and you will be brought directly to the Administrator dashboard.

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 WS HyperSpace™ password. If you lose your password, you must zeroize, or reset, your WS HyperSpace™ Federation Agent and rebuild your user identity from scratch.

4.1. Administrator Dashboard - Orientation

Once successfully logged in, the administrator sees their dashboard (see Figure 8), which has multiple functions. The lefthand column of the ***Administrator Dashboard*** is used to toggle the main functions of the page: (1) manage users (WS HyperSpace™ users who are utilizing the WhiteStar HyperSpace™ Federation Agent application), (2) Manage Service, Proxy or Connection Agent devices (devices Federation Agent users need to connect to), (3) view billing information, and (4) view company profile information.

The center section of the page provides a summary of the users who have been configured to access WS HyperSpace™. Additionally the administrator is giving the ability to bulk upload or add individual users, assign WS StarTags to users, and assign WS StarTags to servers.



Users Management Tab

Manually add user

Upload users via MS Active Directory

Upload users via CSV

Detailed Tag Overview

Add tag to user

Figure 8

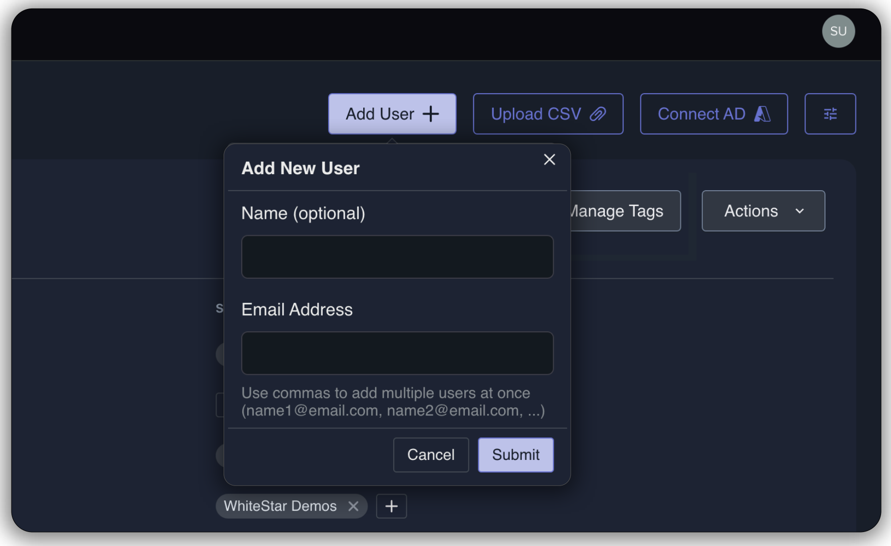
5. Configure/Maintain WS HyperSpace™ via an Administrator Account

5.1. Adding New WS HyperSpace™ 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 8). This allows the administrator to authorize WS HyperSpace™ users to use the WS HyperSpace™ Federation Agent application (by adding their email address to the list of authorized members of an organization). The WS HyperSpace™ users themselves use their email address during the WS HyperSpace™ Federation Agent 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 WS HyperSpace™ users name be entered as well. Once the information is entered, click the "***Submit***" button (see Figure 9).



Use commas to add multiple users at once (name1@email.com, name2@email.com, ...)

Figure 9

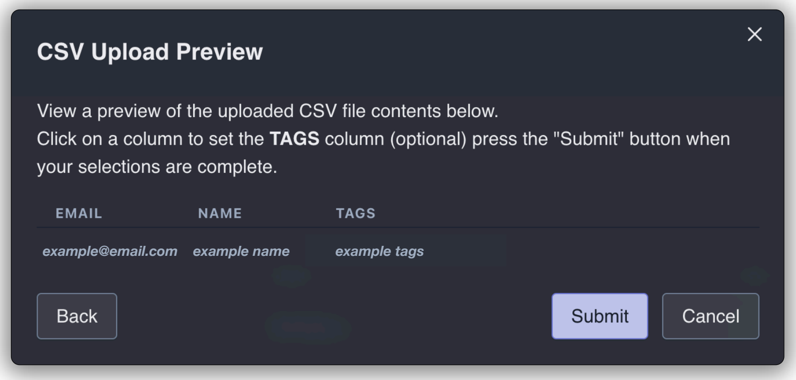
If the administrator wants to bulk upload new WS HyperSpace™ users into the dashboard, there are two ways to achieve this: (1) via upload of a ***CSV file*** or (2) via direct access to your ***Active Directory*** (AD) server.

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 WS HyperSpace™ 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 WS StarTags***. 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 WS StarTags 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 10).



CSV Upload Preview

View a preview of the uploaded CSV file contents below.
Click on a column to set the **TAGS** column (optional) press the "Submit" button when your selections are complete.

EMAIL	NAME	TAGS
example@email.com	*example name*	*example tags*

Figure 10

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

- The top list shows the email addresses that are in the CSV which are new to the system.
- 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.

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.

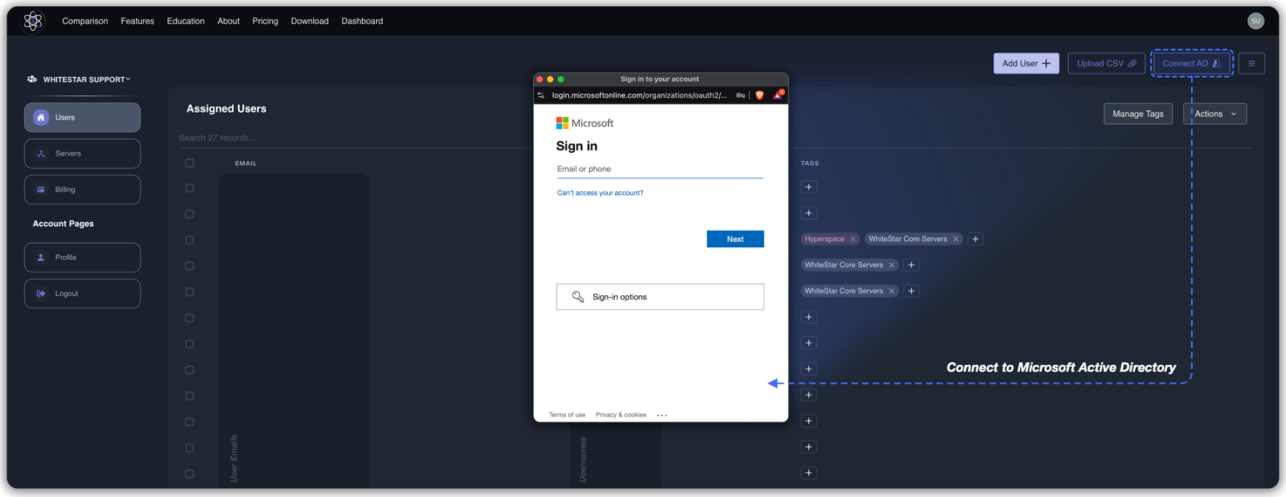


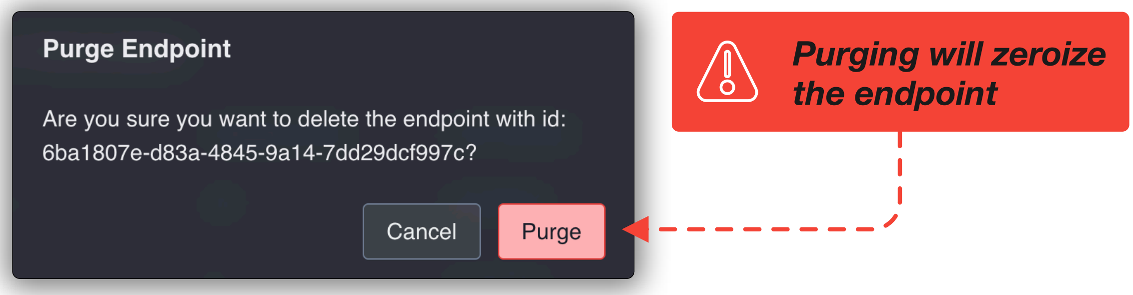
Figure 11

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 WS 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 WS HyperSpace™ Federation Agent data from their device).

If "***Zeroize Selected***" is chosen, a confirmation screen is presented to ensure this is the action the administrator truly wants taken. Understand that any user zeroized will have ALL of their locally stored WS HyperSpace™ Federation Agent 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.



Purge Endpoint

Are you sure you want to delete the endpoint with id: 6ba1807e-d83a-4845-9a14-7dd29dcf997c?

Purging will zeroize the endpoint

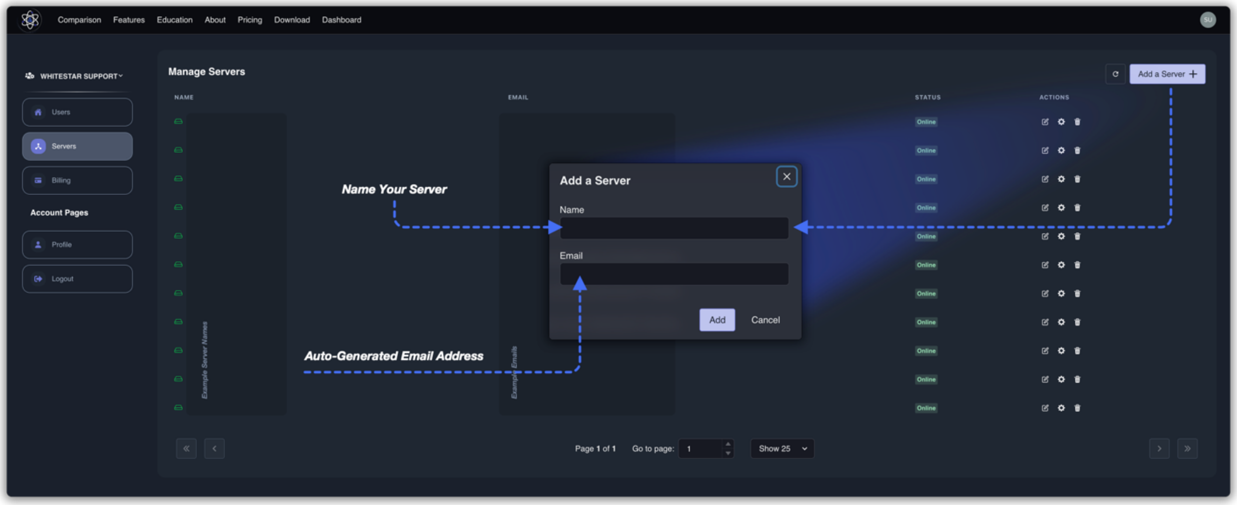
Figure 12

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. Adding a WS HyperSpace™ Server via the Admin Dashboard

Once a WS HyperSpace™ Agent (Service, Proxy or, Connection Agent) has been successfully installed, the device administrator must add it to the list of devices under their control. To do so, log in the administrator's dashboard found at https://hyperspacenetwork.io/dashboard. From there:

- Click on the "**Servers**" button on the left hand column of the web page
- Click on "***Add a Server***" in the upper righthand corner of the screen, which brings up a screen to add this server (see Figure 13).



Name Your Server

Auto-Generated Email Address

Figure 13

The administrator is presented with a screen pop up (See Figure 13) prompting them to enter a free form server name (pick a name to easily identify this machine) plus the synthetic email address generated by the WS HyperSpace™ Agent during installation (see Section 5.4 below).

After clicking "***Add***", your new WS HyperSpace™ Agent is placed in your list of "Servers" controlled by this organization. The administrator is now free to add StarTags to the server in order to allow clients to connect to it.

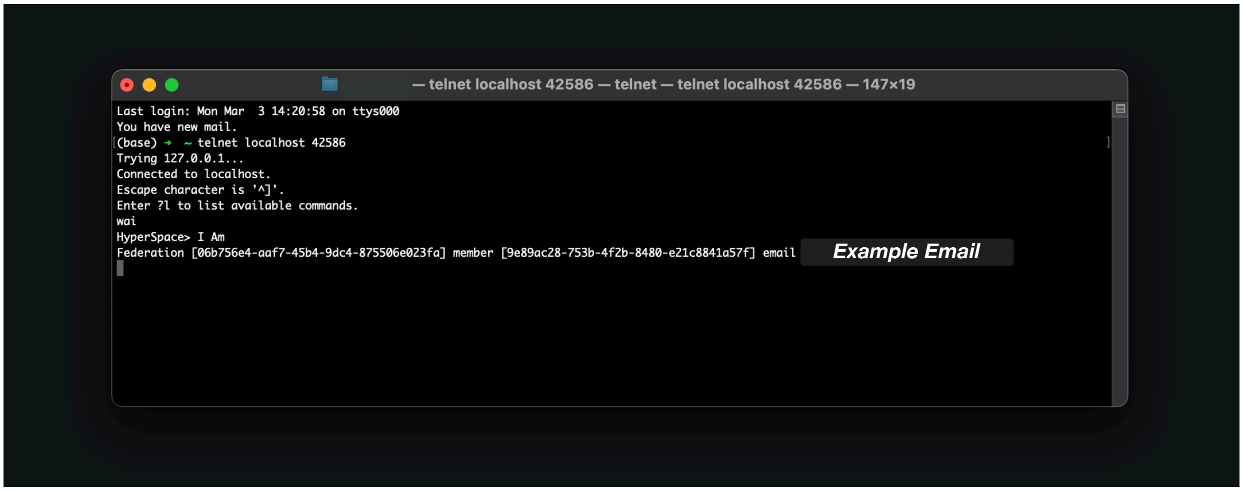
5.4. *Viewing the Unique ID of the WS HyperSpace™ Agent Device*

Each WS HyperSpace™ Agent (Service, Connection, Proxy) within the WS network is referred to by its unique ID (currently its internally generated WhiteStar email address). The administrator will need to enter this email address on the Admin Dashboard, under "Servers", to allow the Admin to claim the server for their organization and grant access to it in order for WS HyperSpace™ Agents to connect to it.

5.4.1. Via the terminal interface

These instructions will be valid for *all* operating systems.

- Open a terminal window on your OS.
- Type ***telnet localhost 42586*** (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.


— telnet localhost 42586 — telnet — telnet localhost 42586 — 147×19

```
Last login: Mon Mar  3 14:20:58 on ttys000
You have new mail.
(base) ➜  ~ telnet localhost 42586
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Enter ?l to list available commands.
wai
HyperSpace> I Am
Federation [06b756e4-aaf7-45b4-9dc4-875506e023fa] member [9e89ac28-753b-4f2b-8480-e21c8841a57f] email  Example Email
```

Figure 14

- 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 “Servers” that get managed by their organization.

5.4.2. Via the GUI interface

- Right click on the CORE green circle on the HyperSpace™ Service Agent GUI (See Figure 15).
- Click on “Show Email Address” from the drop down menu

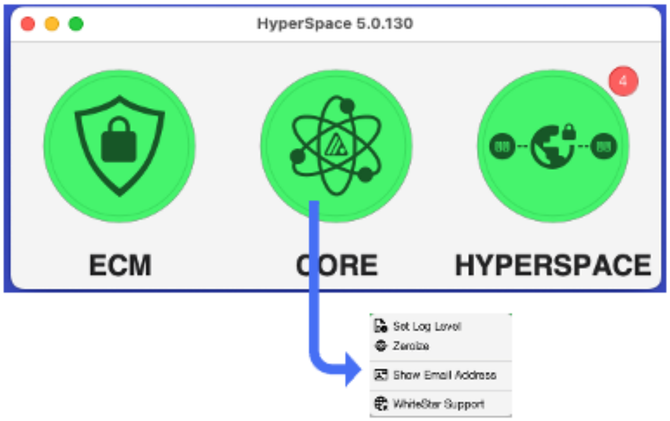


Figure 15

5.5. WS StarTags – Providing Access to other WS HyperSpace™ Agents

Permission to access a WS HyperSpace™ Agent service on another device is granted by unique identifiers referred to as ***WS StarTags*** in the WhiteStar system.

WS StarTags are created on the Administrator Dashboard and assigned to WS HyperSpace™ users either individually or to groups of WS HyperSpace™ users. In order to access a particular Device, it is the customer’s responsibility to log into the admin dashboard, add the Server to their account, create a WS StarTag, and assign the WS StarTag to that server and the user(s) they are granting access to.

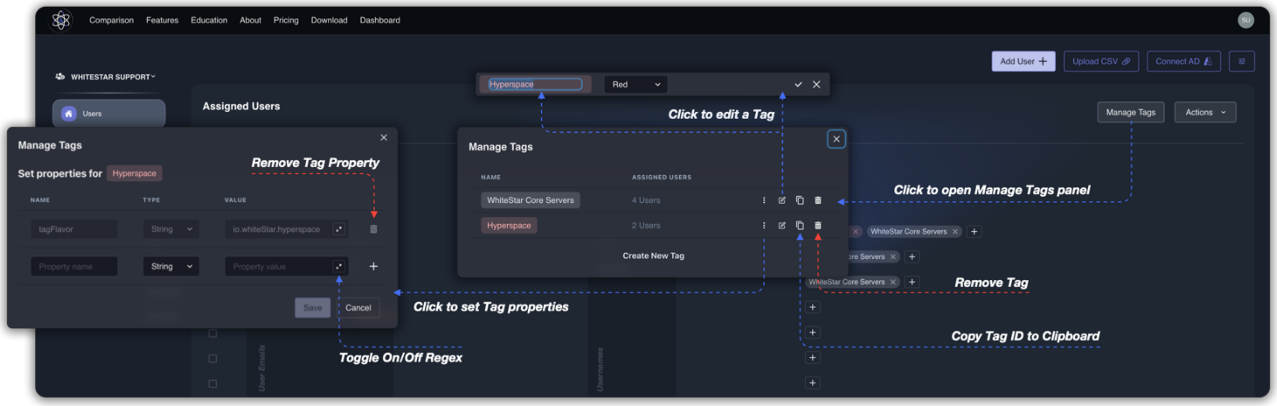


Figure 16

5.5.1. Creating a new WS StarTag

Creating WS StarTags and assigning them to WS HyperSpace™ users is quick and easy. The administrator first logs in to the Administrator dashboard and clicks on "***Users***" in the lefthand column. In the main portion of the screen there is an ***"Assigned Users"*** table that allows you to see the current WS StarTags applied to a given user's account.

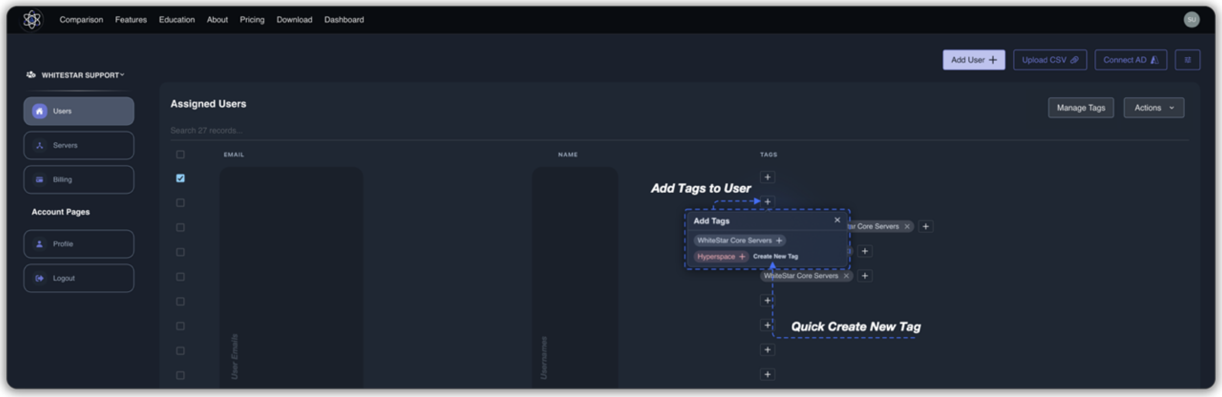
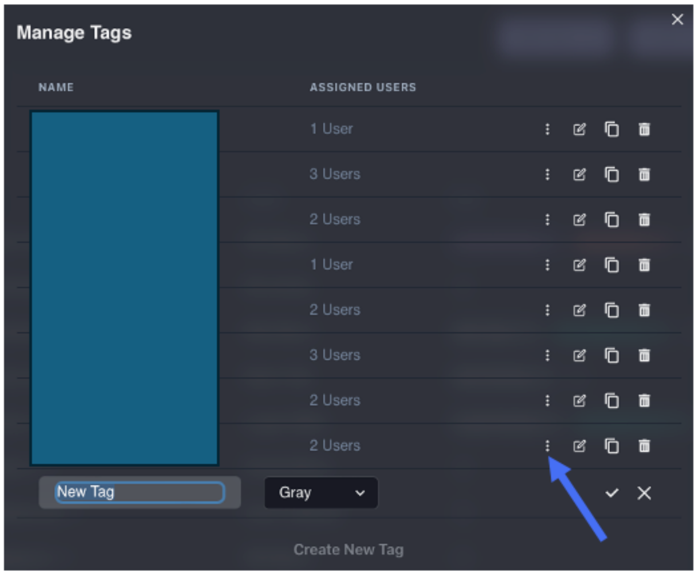


Figure 17

To create a new WS StarTag, click the "***Manage Tags***" button on the top right hand portion of the screen. A "***Manage Tags***" dialog box is presented to the user with the "***Create New Tag***" button at the bottom of that dialog box – click that button. The admin is presented with a free form field to name the new WS StarTag and also given the option to pick a color associated with the tag (to visually identify it on the list of tags). Once done, simply click on the check mark on the right hand side of the line to finish the creation of the StarTag.



NAME	ASSIGNED USERS
[redacted]	1 User
[redacted]	3 Users
[redacted]	2 Users
[redacted]	1 User
[redacted]	2 Users
[redacted]	3 Users
[redacted]	2 Users
[redacted]	2 Users

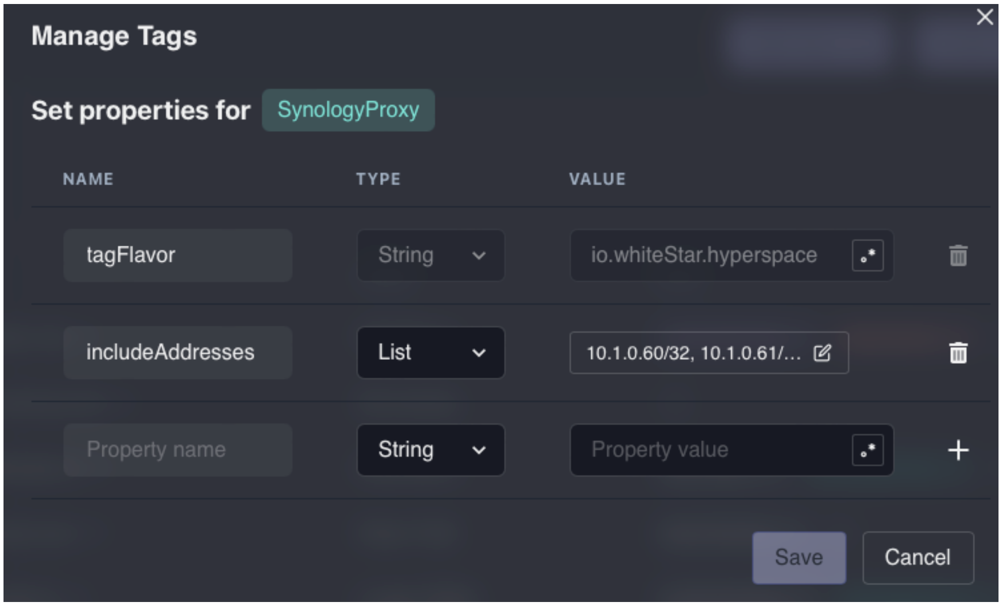
Figure 18

5.5.2. Adding IP Address to HyperSpace™ Proxy Server StarTag

WS applications understand certain "***Properties***" assigned to a WS StarTag, which, when applied to a Server or User cause the WS HyperSpace™ Agent to execute certain special features.

If the case of a WS HyperSpace™ Proxy Server, the admin is responsible for identifying the specific IP address, or range of addresses, a Proxy Agent will be providing access to users that connect through it.

To add additional properties to a WS StarTag, click on the 3 vertical dots to the right of a WS StarTag (see blue arrow in Figure 18). The "***Set properties***" box is presented to the admin. The admin must enter "*includeAddresses*" as the Name of the property, "List" as the Type, and then in the Value field provide the appropriate IP address (or addresses) this proxy will be transmitted traffic to and from. When complete click "Save".



Manage Tags

Set properties for SynologyProxy

NAME	TYPE	VALUE
tagFlavor	String	io.whiteStar.hyperspace
includeAddresses	List	10.1.0.60/32, 10.1.0.61/...
Property name	String	Property value

Figure 19

5.5.3. Assigning a WS StarTag to a User or Server

Once a WS StarTag has been created and (optional) properties have been configured for it, the WS StarTag must now be assigned to Users and Servers the admin wants to connect together.

To add a WS StarTag to a user or server the admin needs to navigate to the "***Servers***" or "***Users***" screen and click the "***Plus***" button in the "**Tags**" column next to the server or user he or she wants to add a WS StarTag to. The admin will be presented with a list of Tags to choose from and simple clicks on the WS StarTag to be assigned. Once assigned both the user and server form a secure network between them thus providing direct access between the two WS HyperSpace™ Agents.

5.5.4. Removing a WS StarTag from a User or Server

Removing a WS StarTag from a user immediately removes their ability to access the WS HyperSpace™ Agents associated with that WS StarTag. Likewise, removal of the user from the admin dashboard *automatically* removes all WS StarTags from their account.

To remove a WS StarTag from either a User or a Server, navigate to the "***Servers***" or "***Users***" screen and simple click on the "X" next to the WS StarTag in the User or Server's row in the table. Access to those WS HyperSpace™ Agents is immediately removed.

5.5.5. Teams – Subdividing Teams

Customers typically only allow "specific" users, or groups of users, to connect to and from one of their devices. The WS HyperSpace™ 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 devices.

Take, for example, an organization with four (4) WS HyperSpace™ users. The administrator may want to grant access to individual users to connect to individual devices or create a small **Trusted Team** of WS HyperSpace™ users permitted to connect to a specific set of devices. They may also want to have a *generic Trusted Team made up of all WS HyperSpace™ users* who can connect to any device. Figure 20 illustrates an administrator who has created three (3) teams [this is done by assigning a **WS StarTag** – or multiple WS StarTags – to their WS HyperSpace™ Federation Agent users]. How to accomplish this is discussed later in this document.

- **Trusted Team #1** (Purple: with 2 WS HyperSpace™ Federation Agent users) has been established to connect to a single "Purple" device at Data Center 1 by both Client users.
- **Trusted Team #2** (Green: with 3 WS HyperSpace™ Federation Agent users) has been established to connect to "Green" 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 connect to any "Green" and "Purple" devices in all Data Centers.
- **Finally, Trusted Team #3** (Red: with only 1 WS HyperSpace™ user) has been established to connect to a single "Red" device in Data Center 3.

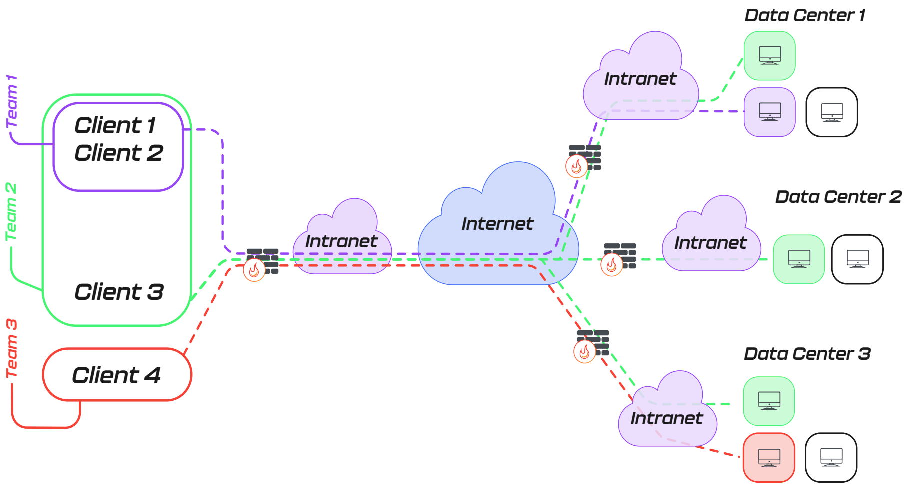


Figure 20

Note: the administrator creates WS StarTags on their **WS Administrator Dashboard** by assigning WS StarTags to their users to delineate which Trusted Team(s) they are a member of. For a customer to grant access to a WS HyperSpace™ Agent device, they must also assign the StarTag to the devices they are granting access to via the same **WS Administrator Dashboard**.

5.6. Accessing/Updating the Administrator Profile

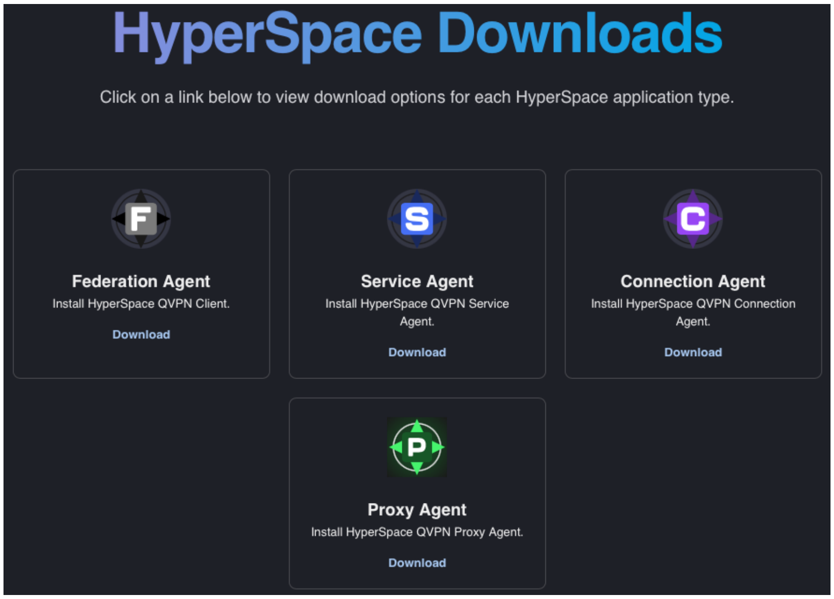
From the main screen of the Dashboard navigate to the left-hand column under "***ACCOUNT PAGES***" and then click on "***Profile***". The administrator will find information about the organization including total licenses purchased, total licenses assigned to users, total licenses claimed by users, etc. 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.

6. Install WS HyperSpace™ Agent (all OS except IOS and macOS 15 and higher)

In order for a WS HyperSpace™ user to connect to another device (also running WS HyperSpace™ Agent software), they will first need to install a WS HyperSpace™ Agent component on both the device they want to connect from and the device they want to connect to. The WS HyperSpace™ Agent components run on Microsoft Windows, Apple macOS (both Intel and Apple Silicon), Apple iPhones, and Linux devices. The following table is used to help determine which agent to install on each device.

HyperSpace™ Agent	Function performed
Federation Agent F	Federation Agents can form mesh networks with each other while also forming spoke and hub connections to Service, Proxy and Connection Agents. This Agent is the one typically installed by end users on their “client” devices.
Service Agent S	Service Agents allow the user to build a spoke and hub connection with Federation, Proxy and Connection Agents. Service Agents can (optionally) form a mesh (using a WS StarTag property) with other Service Agents assigned the same StarTag. This Agent is the one typically installed by end users on their “server” devices.
Connection Agent C	Connection Agents allow the user to build a spoke and hub connection with Federation, Proxy and Connection Agents. This Agent is the one typically installed by end users on a “server” device in order to allow other agents to communicate without forming a mesh.
Proxy Agent P	Proxy Agents allow the user to connect a device to HyperSpace™ that a HyperSpace™ Agent cannot be installed on. Typically the Proxy Agent is installed on another piece of hardware in close proximity to the device that is will “proxy”.

Before proceeding, ensure that the individual performing the installation has the proper privileges on the local device to install software on it. Open a web browser and navigate to the following WhiteStar website: https://hyperspacenetwork.io/download. The user is presented with a web page giving them the option to select which WS HyperSpace™ Agent to download (see Figure 21). Once the Agent type is selected, the user is presented with download links for the operating system they are currently running on. If the proper OS is not selected by default, the user has the option to select the appropriate link for the operating system they want to download and install. Click the proper download button and save the install package.



HyperSpace Downloads

Click on a link below to view download options for each HyperSpace application type.

Federation Agent
Install HyperSpace QVPN Client.

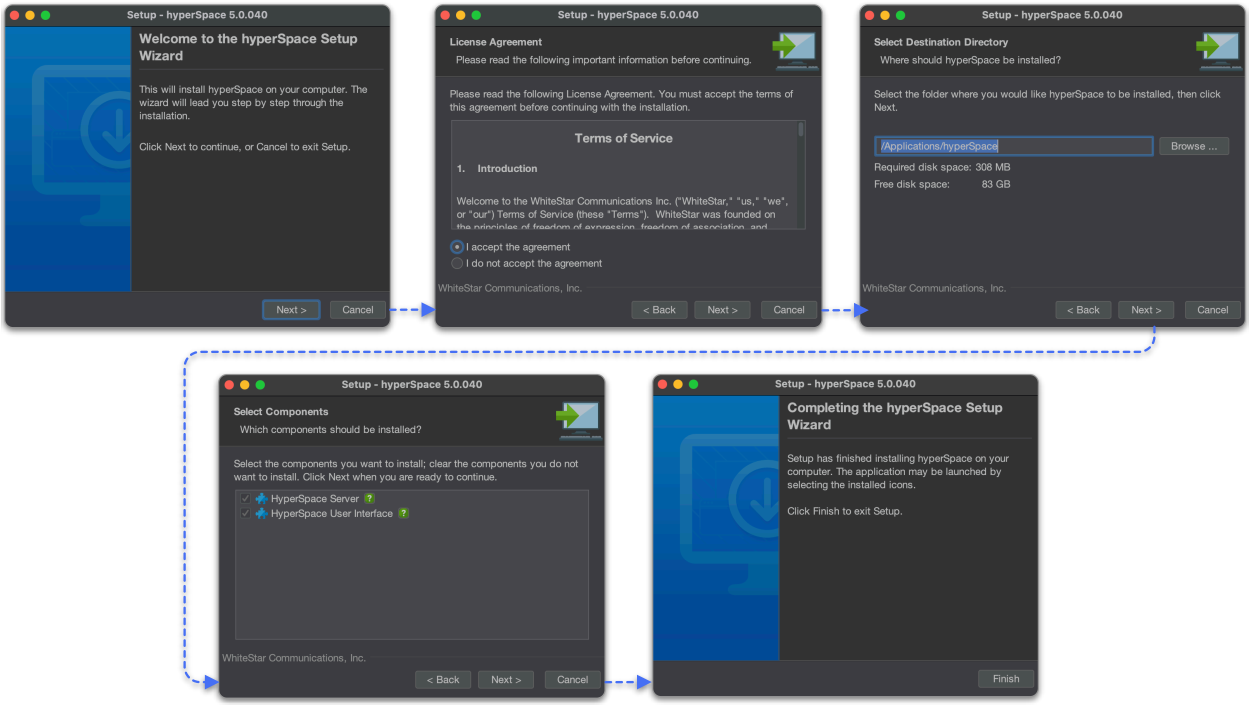
Service Agent
Install HyperSpace QVPN Service Agent.

Connection Agent
Install HyperSpace QVPN Connection Agent.

Proxy Agent
Install HyperSpace QVPN Proxy Agent.

Figure 21

Open the folder where the WS HyperSpace™ installer package was saved. Click on the download package to ***run the installer***. You are brought to the following screen (see Figure 22). 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. Choose the directory for the application to be installed into, and then click the "***Next***" button. Then, click the "***Finish***" button to complete the installation.



Setup - hyperSpace 5.0.040

Welcome to the hyperSpace Setup Wizard

This will install hyperSpace on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.

Setup - hyperSpace 5.0.040

License Agreement
Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Terms of Service

1. Introduction

Welcome to the WhiteStar Communications Inc. ("WhiteStar," "us," "we", or "our") Terms of Service (these "Terms"). WhiteStar was founded on the principles of freedom of expression, freedom of association, and

● I accept the agreement
○ I do not accept the agreement

WhiteStar Communications, Inc.

Setup - hyperSpace 5.0.040

Select Destination Directory
Where should hyperSpace be installed?

Select the folder where you would like hyperSpace to be installed, then click Next.

/Applications/hyperSpace

Required disk space: 308 MB
Free disk space: 83 GB

WhiteStar Communications, Inc.

Setup - hyperSpace 5.0.040

Select Components
Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

☑ HyperSpace Server
☑ HyperSpace User Interface

WhiteStar Communications, Inc.

Setup - hyperSpace 5.0.040

Completing the hyperSpace Setup Wizard

Setup has finished installing hyperSpace on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

Figure 22

6.1. Install WS HyperSpace™ Federation Agent on IOS and Mac OS 15 or higher

In order to install WS HyperSpace™ on either of these operating systems the user needs to install the software from the Apple Store. Open a web browser and navigate to the following WhiteStar website: https://hyperspacenetwork.io/download. Select "***Download***" on the Federation Agent box. Ensure "***Apple Silicon***" is selected and the "Visit the App Store" button is displayed at the bottom of the screen. Clicking that button takes the user to the Apple App store and the WS HyperSpace™ software can be installed in the same fashion all software is installed from their store.

6.2. Setting up a WS HyperSpace™ Federation Agent

The first time the user starts the WS HyperSpace™ Federation Agent they are brought to the registration screen. Enter your name and email address (2x) and click the "***Request Confirmation Code***" button to have a confirmation code send to your email address.

Go to your email client and look for an email from vortex@whitestar-vortex.com with the subject line of "***HyperSpace 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 WS HyperSpace™ Federation Agent installation screen and paste (typically hit **Cntl-V/Cmd-V**) the confirmation code into the appropriate box.

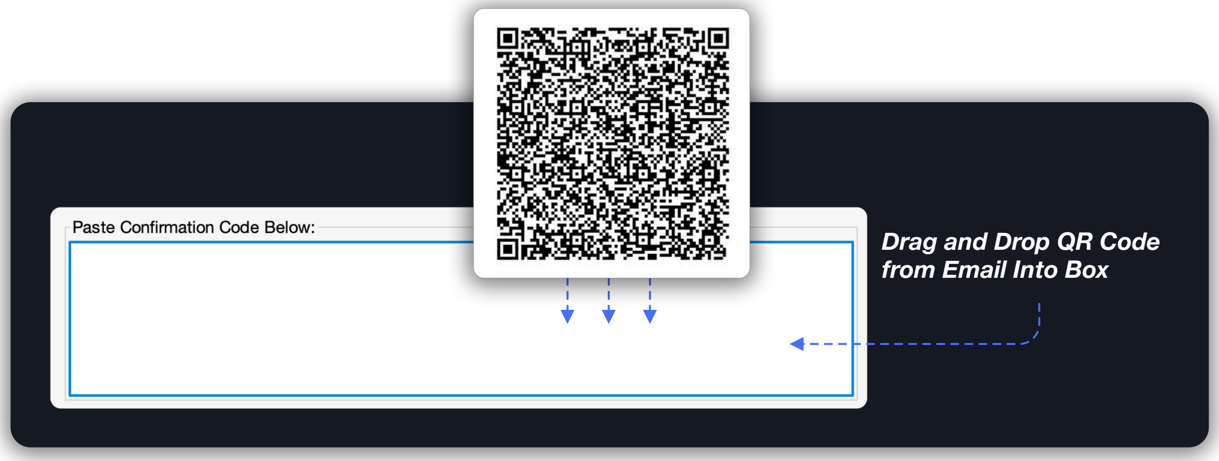

Paste Confirmation Code Below:
Drag and Drop QR Code from Email Into Box

Figure 23

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.

Another option available is clicking the "***Magic Link***" in the email which completes the registration process as well.

Click the "***Finish***" button to complete the installation.

If you already have created an account on WS HyperSpace™, and are returning to the application, you are prompted to log in to the application, and do not need to set your account up a second time.

7. Install WS HyperSpace™ Server Agent

For a WS HyperSpace™ user to connect to a Device (running the WS HyperSpace™ Agent software), an administrator needs to install the WS HyperSpace™ Agent component (Service, Proxy or Connection) on to the machine they want WS HyperSpace™ Federation Agent users to connect to. The WS HyperSpace™ Agent component runs on Microsoft Windows, Apple macOS (both Intel and Apple Silicon), and Linux systems.

7.1. Installation on Linux Server

7.1.1. Installing on Red Hat Enterprise, CentOS or Rocky Linux

Installation of the WS HyperSpace™ Server Agent 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.

HyperSpace™ Agent	Commands to Execute

Service Agent	`# sudo dnf copr enable whitestar/hyperspace`
	`# sudo dnf install -y hyperspace`

Connection Agent	`# sudo dnf copr enable whitestar/connection-agent`
	`# sudo dnf install -y connection-agent`

Proxy Agent	`# sudo dnf copr enable whitestar/proxy-agent`
	`# sudo dnf install -y proxy-agent`

7.1.2. Installing via a .deb file

If installing via the graphical method, double click on the appropriate .deb file that was just downloaded and choose to install it using the default software installer or GDebi. Alternatively, you can use the command line and execute the following command (ensuring you are in the directory the install file was downloaded in to).

HyperSpace™ Agent	Commands to Execute
Service Agent	ARM Processor: `# sudo apt install ./serviceAgent_linux_ARM_<version>.deb`

	X86 Processor: `# sudo apt install ./serviceAgent_linux_X86_<version>.deb`

Connection Agent	ARM Processor:
	`# sudo apt install ./connectionAgent_linux_ARM_<version>.deb`
	
	X86 Processor:
	`# sudo apt install ./connectionAgent_linux_X86_<version>.deb`

Proxy Agent	ARM Processor:
	`# sudo apt install ./proxyAgent_linux_ARM_<version>.deb`
	
	X86 Processor:
	`# sudo apt install ./proxyAgent_linux_X86_<version>.deb`

7.1.3. Installing via a shell script

Open a terminal and navigate to the directory the install file was downloaded in to. Ensure the file has execute permissions and run the script:

HyperSpace™ Agent	Commands to Execute

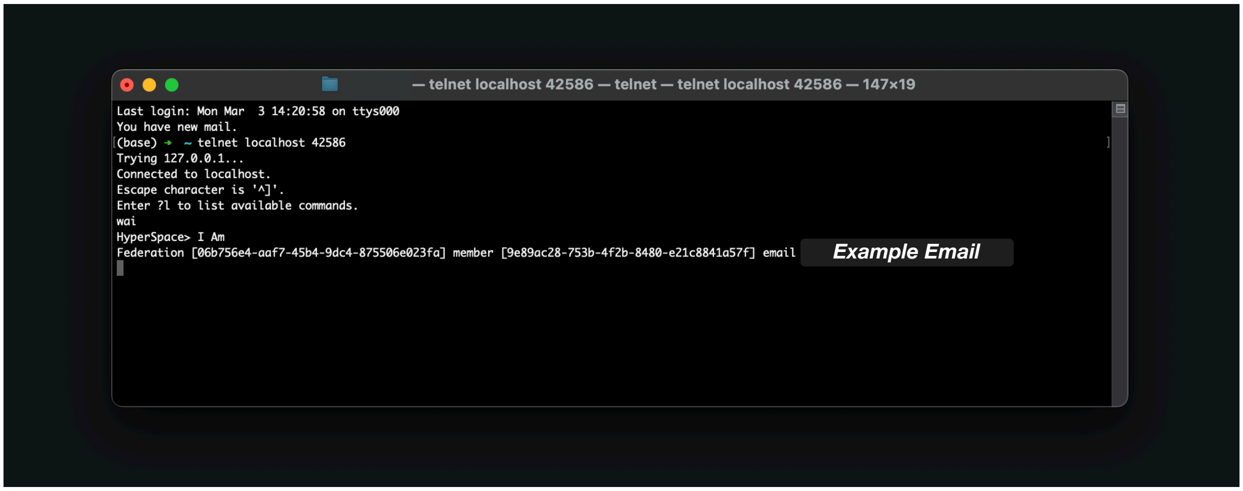
Service Agent	ARM Processor:
	`# sudo bash ./serviceAgent_linux_ARM_<version>.sh`
	
	X86 Processor:
	`# sudo bash ./serviceAgent_linux_X86_<version>.sh`

Connection Agent	ARM Processor:
	`# sudo bash ./connectionAgent_linux_ARM_<version>.sh`
	
	X86 Processor:
	`# sudo bash ./connectionAgent_linux_X86_<version>.sh`

Proxy Agent	ARM Processor:
	`# sudo bash ./proxyAgent_linux_ARM_<version>.sh`
	
	X86 Processor:
	`# sudo bash ./proxyAgent_linux_X86_<version>.sh`

Once the software has been successfully installed, the administrator must obtain the unique Server ID assigned by WhiteStar in order to add it to the list of servers controlled by this organization. In order to obtain this Server ID, execute the following commands:

- Open a terminal on the Linux device
- Telnet to the HyperSpace™ Agent code running by executing the following command "**telnet localhost 42586**"
- 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.



— telnet localhost 42586 — telnet — telnet localhost 42586 — 147×19

```
Last login: Mon Mar  3 14:20:58 on ttys000
You have new mail.
(base) ➜  ~ telnet localhost 42586
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Enter ?l to list available commands.
wai
HyperSpace> I Am
Federation [06b756e4-aaf7-45b4-9dc4-875506e023fa] member [9e89ac28-753b-4f2b-8480-e21c8841a57f] email  Example Email
```

Figure 24

Copy the email address (this is the unique ID) and share this with the administrator so that this server can be added as a Server to the Administrator's dashboard.

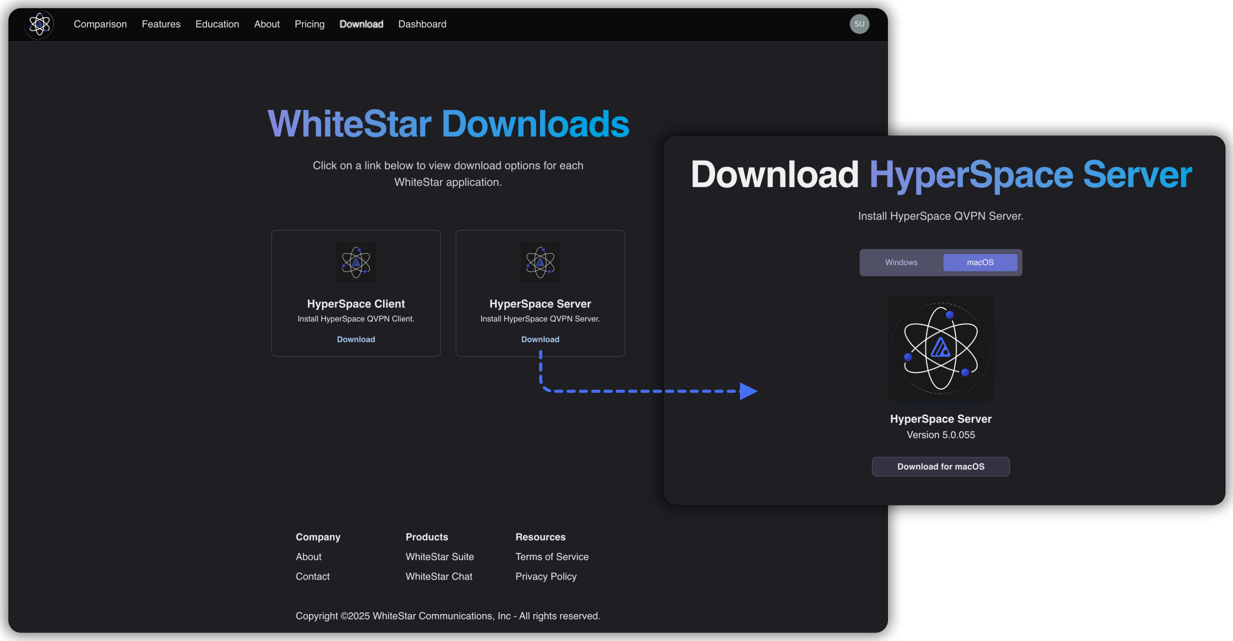
7.2. Installation on Mac OS or Windows

Open a web browser and navigate to the following WhiteStar website: https://hyperspacenetwork.io/download/server. The user is presented with a link to download the WS HyperSpace™ Server Agent 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 WS HyperSpace™ installer package was saved.

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



WhiteStar Downloads

Click on a link below to view download options for each WhiteStar application.

HyperSpace Client
Install HyperSpace QVPN Client.
Download

HyperSpace Server
Install HyperSpace QVPN Server.
Download

Download HyperSpace Server

Install HyperSpace QVPN Server.

HyperSpace Server
Version 5.0.055

Company
About
Contact

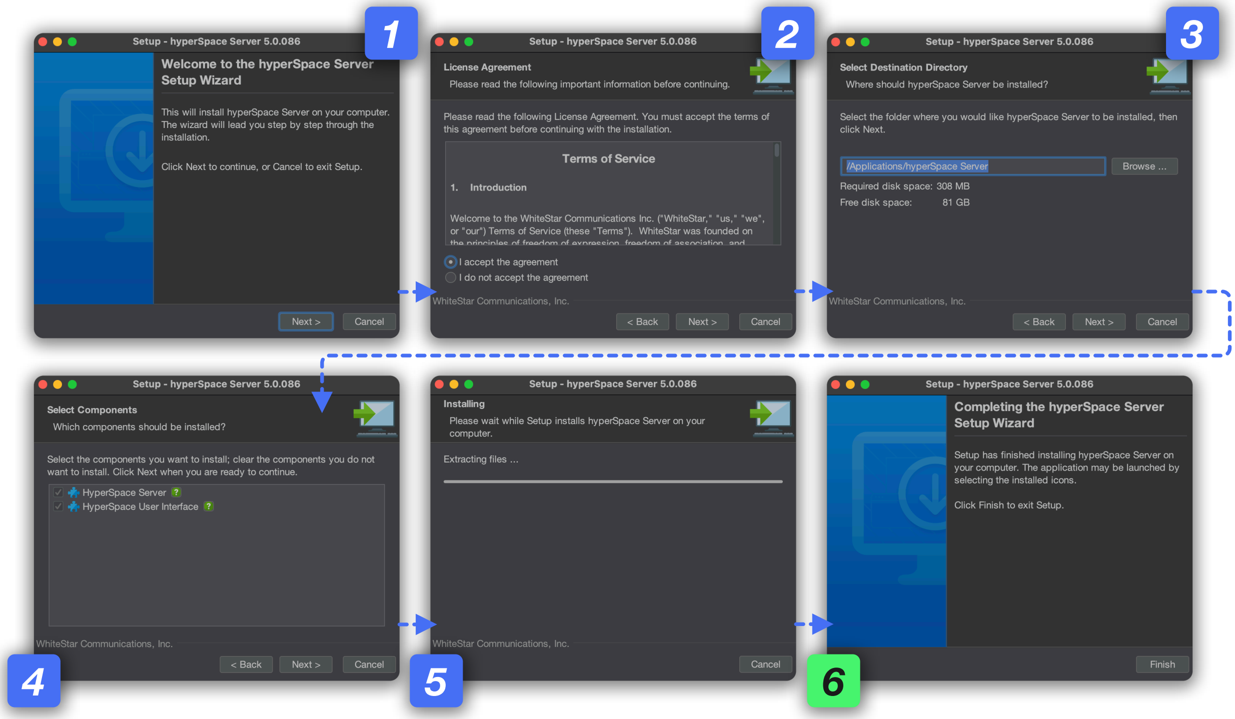
Products
WhiteStar Suite
WhiteStar Chat

Resources
Terms of Service
Privacy Policy

Copyright ©2025 WhiteStar Communications, Inc - All rights reserved.

Figure 25

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



1 Setup - hyperSpace Server 5.0.086

Welcome to the hyperSpace Server Setup Wizard

This will install hyperSpace Server on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.

2 Setup - hyperSpace Server 5.0.086

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Terms of Service

1. Introduction

Welcome to the WhiteStar Communications Inc. ("WhiteStar," "us," "we", or "our") Terms of Service (these "Terms"). WhiteStar was founded on the principles of freedom of expression, freedom of association, and

● I accept the agreement
○ I do not accept the agreement

WhiteStar Communications, Inc.

3 Setup - hyperSpace Server 5.0.086

Select Destination Directory

Where should hyperSpace Server be installed?

Select the folder where you would like hyperSpace Server to be installed, then click Next.

/Applications/hyperSpace Server

Required disk space: 308 MB
Free disk space: 81 GB

WhiteStar Communications, Inc.

4 Setup - hyperSpace Server 5.0.086

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

☑ HyperSpace Server
☑ HyperSpace User Interface

WhiteStar Communications, Inc.

5 Setup - hyperSpace Server 5.0.086

Installing

Please wait while Setup installs hyperSpace Server on your computer.

Extracting files ...

WhiteStar Communications, Inc.

6 Setup - hyperSpace Server 5.0.086

Completing the hyperSpace Server Setup Wizard

Setup has finished installing hyperSpace Server on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

Once installed, the Server application provides a unique Server Identity (See Figure 26) to the individual doing the install. This identity MUST be copied and shared with the administrator who must add it to the list of servers being maintained by this organization. See the section below on how to add a server to the WhiteStar dashboard.

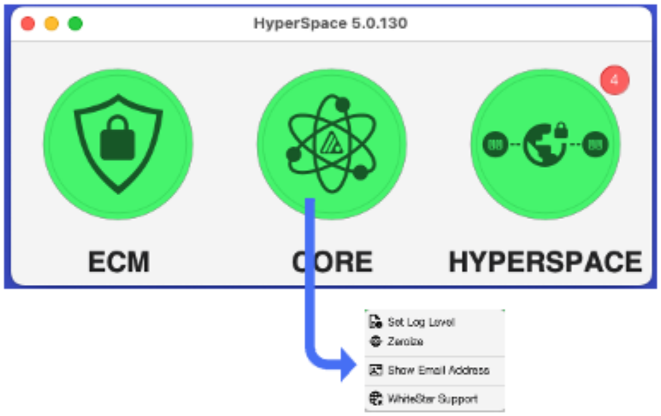


Figure 26

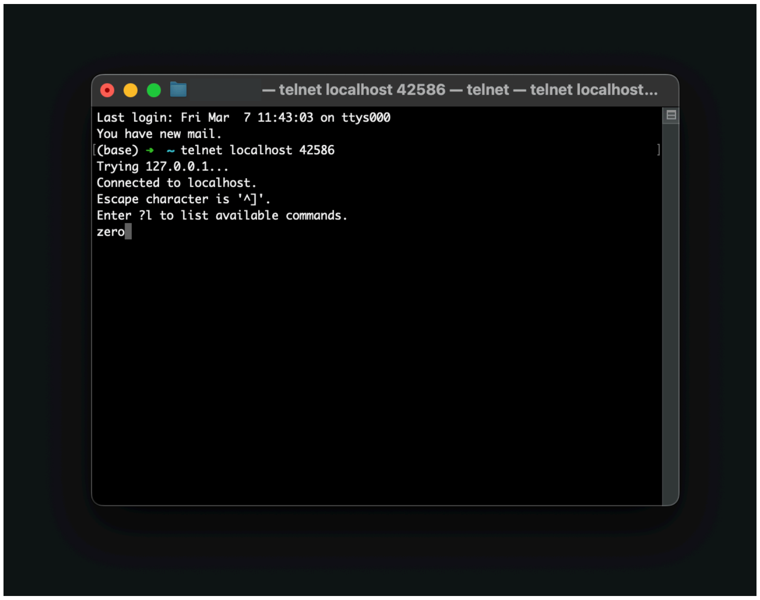
7.3. *Zeroizing the WS HyperSpace™ Server Agent*

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

7.3.1. On a Linux system:

These instructions will be valid for *all* operating systems.

- Open a terminal window on your OS.
- Type ***telnet localhost 42586*** (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")* and hit enter



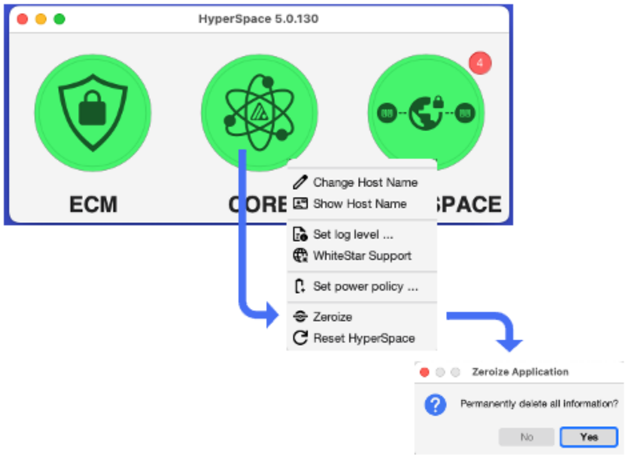
— telnet localhost 42586 — telnet — telnet localhost...

```
Last login: Fri Mar  7 11:43:03 on ttys000
You have new mail.
(base) ➜  ~ telnet localhost 42586
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Enter ?l to list available commands.
zero
```

Figure 27

7.3.2. On a Windows or Mac OS system:

- Right click on the CORE green circle on the HyperSpace™ Agent GUI (See Figure 28).
- Click on “***Zeroize***” from the drop down menu
- Click on “***Yes***” to complete the process

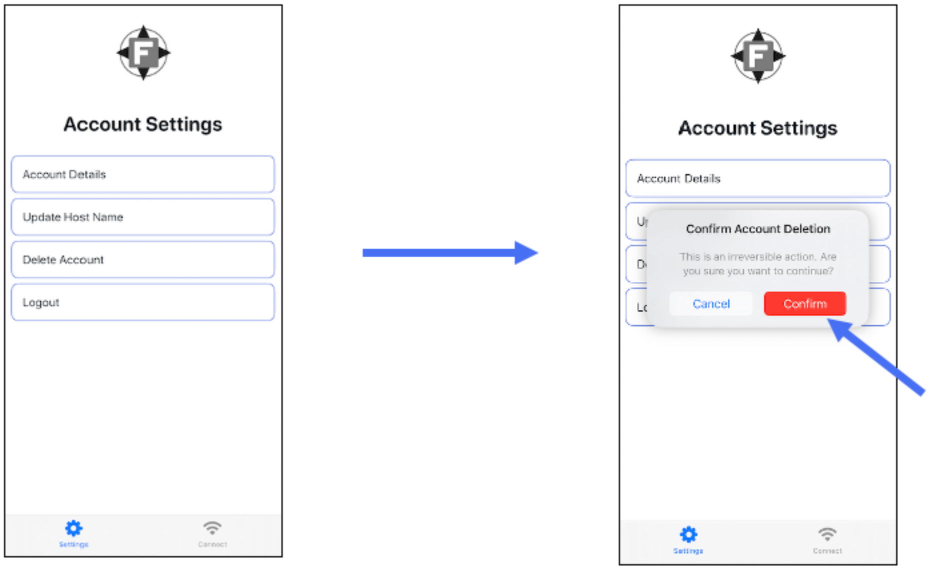


Permanently delete all information?

Figure 28

7.3.3. On an Apple IOS or MAC OS 15 or higher device:

Click the “***Settings***” icon at the bottom left and side of the page, Select “***Delete Account***” and press the “***Confirm***” button to complete the zeroization.



This is an irreversible action. Are you sure you want to continue?

Figure 29

7.4. Firewall Considerations on Linux Servers

If your Linux server is currently running a software firewall service (e.g. firewalld), then additional configuration may be necessary in order for HyperSpace™ Federation Agents to access this device. The following illustrative examples utilize cockpit to enable access of the HyperSpace™ service.

7.4.1. Granting Access to the HyperSpace™ service on your Active Zone

In order by HyperSpace™ to run in a peer to peer fashion with clients accessing the device, the system administrator must add the HyperSpace™ service to the current active firewall zone. To do so, click on the “Networking” tab on the left hand side of the cockpit interface. From there click on the “Edit rules and zones” button on the right hand side of the Firewall entry (see Figure 30).

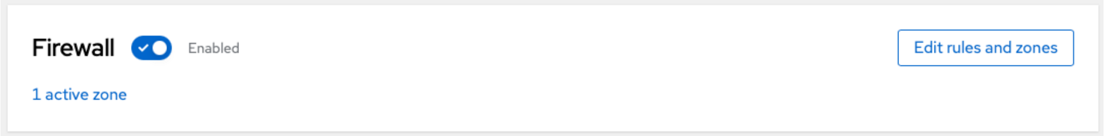
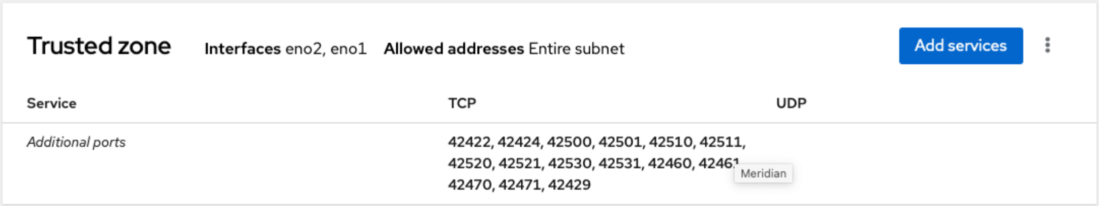


Figure 30

On your current active Zone (e.g. “Trusted” in the example below), click on the “Add Services” button.

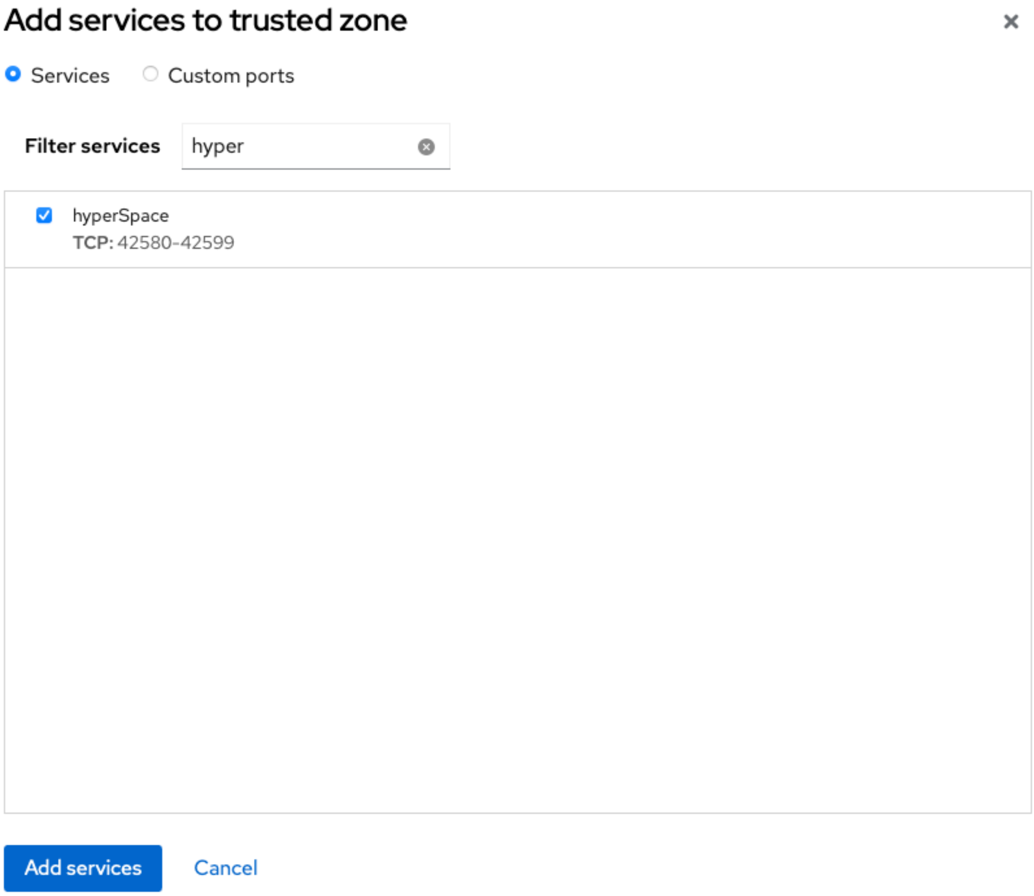


Interfaces eno2, eno1 **Allowed addresses** Entire subnet

Service	TCP	UDP
Additional ports	42422, 42424, 42500, 42501, 42510, 42511, 42520, 42521, 42530, 42531, 42460, 42461 42470, 42471, 42429	

Figure 31

Type in “hyper” in the Filter services box, select “hyperSpace” and click “Add Services” at the bottom to grant permissions (see Figure 32).



● Services ○ Custom ports

Filter services hyper

☑ hyperSpace
TCP: 42580-42599

Figure 32

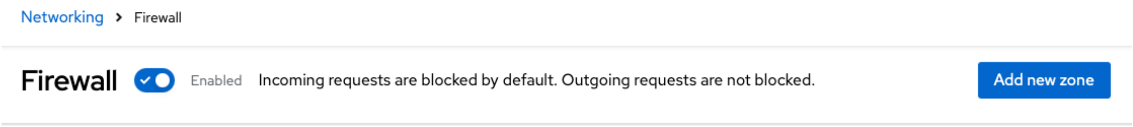
To double check that the service has been added, open a terminal, navigate to the following directory (/etc/firewalld/zones), and ensure that the following linen has been added to your zone xml file:

```
<service name="hyperSpace"/>
```

7.4.2. Granting Services to HyperSpace™’s tunnel

HyperSpace™ creates a tunnel for clients to communicate back and forth with the server. In order for the firewall to allow traffic to flow through the tunnel, services must be granted by the administrator to permit this. To do so, click on the "Networking" tab on the left hand side of the cockpit interface. From there click on the "Edit rules and zones" button on the right hand side of the Firewall entry (see Figure 30).

Next click "Add new zone" at the top of the page (see Figure 33).

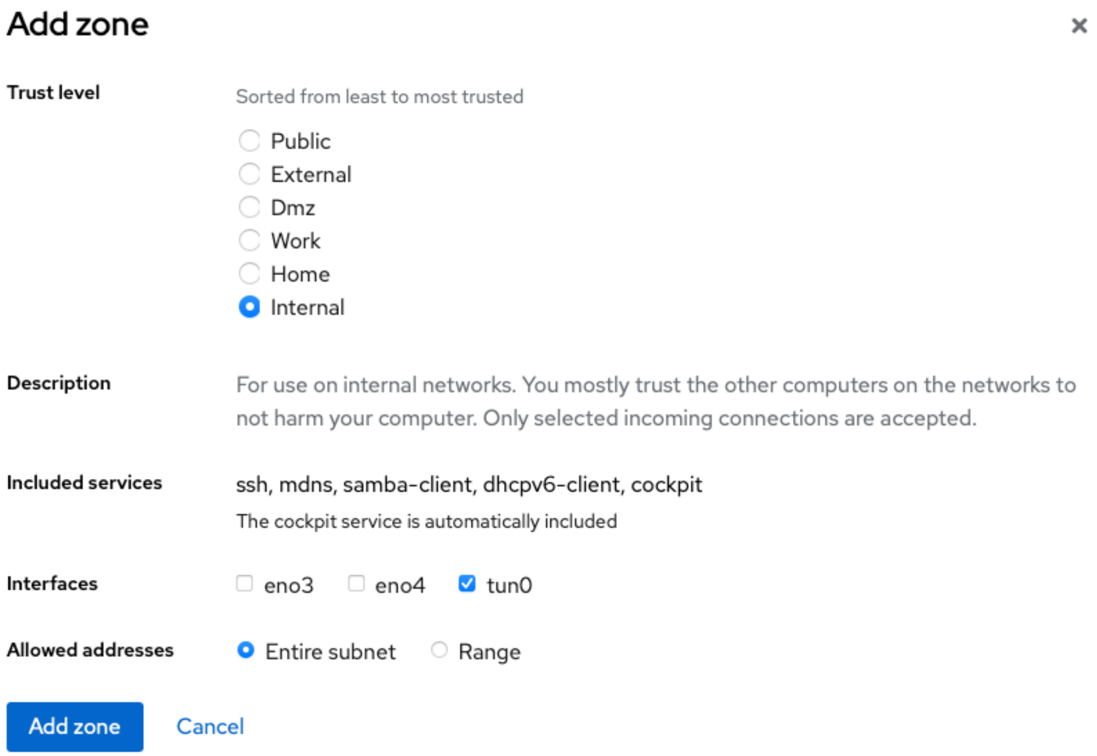


Networking › Firewall

Firewall ● Enabled Incoming requests are blocked by default. Outgoing requests are not blocked.

Figure 33

On the menu provided (see Figure 34), select "Internal" for the "Trust Level" and then select "tun0" on the Interfaces selection list (the tunnel interface created by the HyperSpace™ Service Agent code). Then select "Add zone" in order to make this active.



Add zone

Trust level

Sorted from least to most trusted

○ Public
○ External
○ Dmz
○ Work
○ Home
● Internal

Description For use on internal networks. You mostly trust the other computers on the networks to not harm your computer. Only selected incoming connections are accepted.

Included services ssh, mdns, samba-client, dhcpv6-client, cockpit

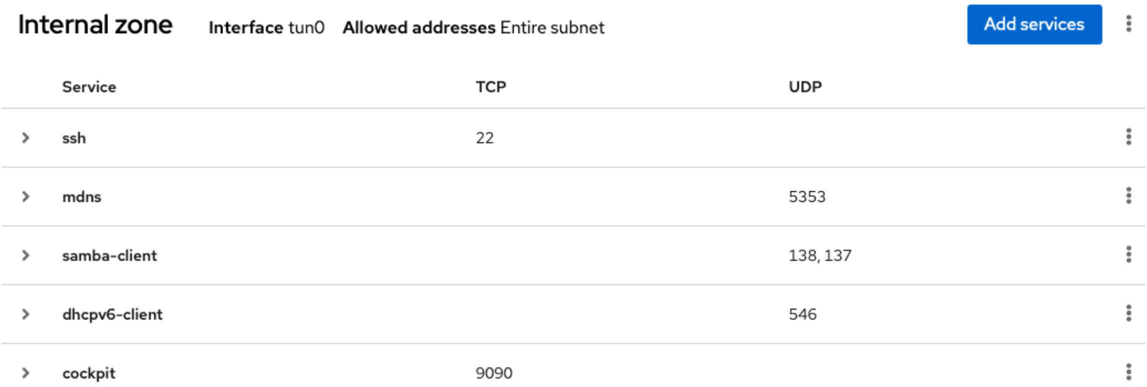
The cockpit service is automatically included

Interfaces □ eno3 □ eno4 ☑ tun0

Allowed addresses ● Entire subnet ○ Range

Figure 34

The zone will be added and the services that can utilize the zone are presented (see Figure 35). If the administrator wants to grant additional services to run over this tunnel, just click the "Add services" button and select from the list provided.



Internal zone **Interface** tun0 **Allowed addresses** Entire subnet

Service	TCP	UDP
ssh	22	
mdns		5353
samba-client		138, 137
dhcpv6-client		546
cockpit	9090	

Figure 35

8. Determine What Devices You are Connected To

Once a user has the WS HyperSpace™ Federation Agent installed and running on their device, they will need to determine the devices they are permitted to access securely via the WhiteStar network.

If the user is part of an Enterprise organization, that group most likely will be allocating WS StarTags and assigning them to both the organization's users and the devices (WS HyperSpace™ Service, Connection, Proxy Agents) they are trying to connect together.

A unique feature of a WS HyperSpace™ Federation Agent is that if the user installs this software on more than one device, utilizing the same email address during initialization on each of their devices, these devices will form a personal secure mesh network between themselves – requiring no interaction from a WS administrator. See Figure 1 for an example of what a Personal Network might look like.

8.1. All Operating Systems including MAC OS (pre Release 15)

To determine the devices you are authorized to connect to, right click on the Green HyperSpace™ circle on the GUI and click on "***Visualize HyperSpace Conduits***" (See Figure 36).

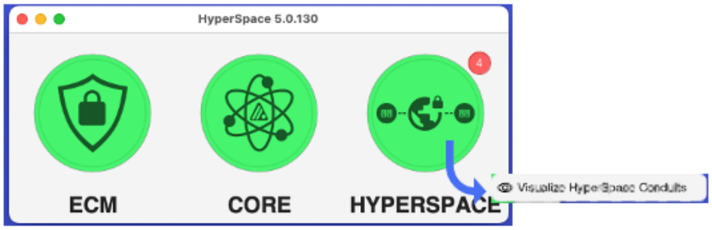
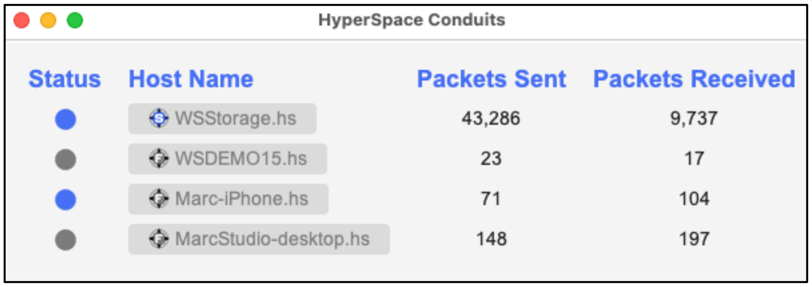


Figure 36

The user is presented with their individual list (See Figure 37). If the connection is active (two way communications are proceeding), either a green dot (peer to peer connection has been formed to that device) or a blue dot (tag switched connect has been formed to that device) will appear under the Status column next to the host name. If a grey dot is present, the user has the permission to connect to that device but it is currently not online (most likely the device is shut off or the WS HyperSpace™ Agent is not currently running on the device).



HyperSpace Conduits

Status	Host Name	Packets Sent	Packets Received
🔵	WSStorage.hs	43,286	9,737
●	WSDEMO15.hs	23	17
🔵	Marc-iPhone.hs	71	104
●	MarcStudio-desktop.hs	148	197

Figure 37

8.2. Apple IOS or MAC OS 15 or higher

To determine the devices you are authorized to connect to, right click or tap on the Green HyperSpace™ circle on the GUI (see Figure 38) and the user is presented with their individual list (see Figure 39).). If the connection is active (two way communications are proceeding), either a green dot (peer to peer connection has been formed to that device) or a blue dot (tag switched connect has been formed to that device) will appear next to the host name. If a grey dot is present, the user has the permission to connect to that device but it is currently not online (most likely the device is shut off or the WS HyperSpace™ Agent is not currently running on the device).

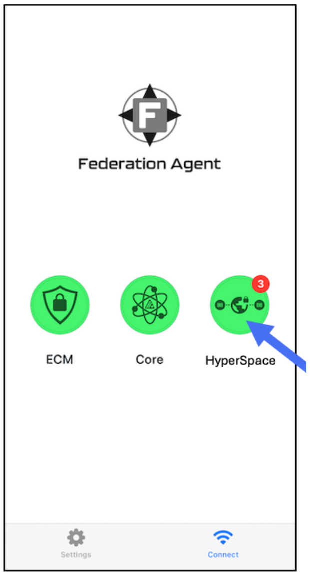
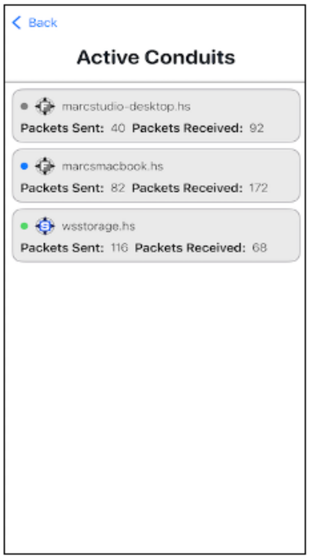


Figure 38



Active Conduits

● marcstudio-desktop.hs
Packets Sent: 40 **Packets Received:** 92

● marcsmacbook.hs
Packets Sent: 82 **Packets Received:** 172

● wsstorage.hs
Packets Sent: 116 **Packets Received:** 68

Figure 39

8.3. Directly Accessing Remote Devices

Once the user has determined which devices they can access, and the conduit between them is active, then the only thing the user needs to do is reference the Host Name associated with that device within any software they are currently utilizing to access remote devices (e.g. remote desktop management, file sharing, etc). To copy the Host Name to your copy buffer (in order to paste it) simply click on the Host Name, or tap it on your screen (See Figure 37 or Figure 39).

9. Maintaining WS HyperSpace™ Agent Software

9.1. Update on Linux Server Red Hat Enterprise, CentOS or Rocky Linux

In order to keep the WS HyperSpace™ Service Agent up to date, the device's administrator must issue the following command (during their routine maintenance window):

HyperSpace™ Agent	Commands to Execute
Service Agent	`# sudo dnf update -y hyperspace`
Connection Agent	`# sudo dnf update -y connection-agent`
Proxy Agent	`# sudo dnf update -y proxy-agent`

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".

9.2. Update on All Other Operating Systems

In order to keep the WS HyperSpace™ Agents 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://hyperspacenetwork.io/download/. The user is presented with a link to download the WS HyperSpace™ Service Agent 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.

10. Creating a Support Case with WhiteStar Support

If the user is experiencing issues with the WS HyperSpace™ Agent application, it may be necessary to create a support ticket to have the issue addressed.

Navigate to the WhiteStar home page (https://www.whitestar.io), click on the *Support* link from the main menu bar, and select *Help Portal*. From there you can create a ticket to get your issues addressed.

11. FAQ

Q: What is the WS Network?

A: The WS 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 WS HyperSpace™. What should I do?

A: WS applications never save your password on your device or to an external repository. If a WS HyperSpace™ Federation Agent user cannot remember their password they must fully delete, and then reinstall, the WS HyperSpace™ Federation Agent software.

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

A: The first thing a WS HyperSpace™ administrator must do is deactivate the license, via the WS Administrator dashboard, that is associated with this user. This will disable the user from accessing WS HyperSpace™ or any WS 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 WS 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.

Q: Why do I need a WS StarTag to connect to a device?

A: WS StarTags are unique identifiers, created by your organization's administrator, to identify an individual user, or team of users, within the support organization. This StarTag 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 WS HyperSpace™ Service Agent device. A StarTag asserts (to your customer) that your company and users are a trustworthy entity capable of accessing their devices. Any attempt to connect to a device without the correct StarTag in place results in a failed connection attempt.

Q: Why does WS HyperSpace™ generate an email address during setup?

A: The email address generated synthetically during initial setup of your WS HyperSpace™ Service Agent contains your server's Federation ID, which is used to help identify the server on the WS HyperSpace™ 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 WS HyperSpace™ Service Agent as a "Server" on your Dashboard. You will need a Tag to control access permissions on the device, however.

Merely adding the "Server" to your Dashboard does not also allow users to access that WS HyperSpace™ Service Agent. 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 "Server"?

A: The term "Server" 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 "Servers" because they could be any kind of device - in the case of WS HyperSpace™ this primarily refers to servers – but within WhiteStar a "Server" 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 WS HyperSpace™ Service Agent, the command "**Zero**" will cause the server to Zeroize, and the WS HyperSpace™ Federation Agent contains a zeroize command on the right click menu. Zeroization removes all of the locally stored information from WS HyperSpace™, deleting the user account, password and any connections that the user has, effectively resetting the program to "zero".

12. Troubleshooting

I cannot connect to a WS HyperSpace™ Service Agent device

If you have successfully started the WS HyperSpace™ Federation Agent, and are being denied a connection to a particular WS HyperSpace™ Service Agent device, there are several things to verify:

1. First confirm that your administrator has attached the proper WS HyperSpace™ StarTag, granting access permission to this device, to your user id.
2. Next ensure that the customer has granted access to the WS HyperSpace™ StarTag (the same one your administrator created in #1 above) on the WS HyperSpace™ Service Agent device that is attempting to be accessed.
3. Confirm with the customer that the WS HyperSpace™ Service Agent 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 WS HyperSpace™ Federation Agent 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 WS HyperSpace™ Federation Agent device is set correctly. WS 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 WS HyperSpace™ Federation Agent won't launch

Make sure that there are no instances of the WS HyperSpace™ Federation Agent currently running in the background. Only one instance of the WS HyperSpace™ Federation Agent is permitted to be running on a particular device.

The WS HyperSpace™ Federation Agent shows a blank screen after connecting and doesn't accept keyboard input

Terminate the current instance of the WS HyperSpace™ Federation Agent Shell and restart. If, after restarting, you still cannot interact with the WS HyperSpace™ Federation Agent Shell, it may be because there is another user currently connected to the WS HyperSpace™ Service Agent you attempted to connect to. Check with other team members, who are also permitted to connect to this Devices, to ensure they are not currently connected.

The other potential reason you would see this issue is if the WS HyperSpace™ Service Agent 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 WS HyperSpace™ Service Agent 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.

13. 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 WS 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	WS HyperSpace™ Service for Remote Transfers	The WS HyperSpace™ Service Agent 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, WS HyperSpace™	WhiteStar's native anywhere-to-anywhere, always encrypted, unlimited-file-size, platform agnostic file transfer system.
Client	WS HyperSpace™ local Client, WS HyperSpace™ Federation Agent	The WS HyperSpace™ Federation Agent is your local interface with the WS HyperSpace™ Service Agent. 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 WS HyperSpace™ Federation Agent also shows batch-send progress during the transfer process.
Zeroize		Zeroization permanently deletes not only your Endpoint and Federation ID from the WS 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 WS 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 WS HyperSpace™ Service Agent, since WhiteStar never uses group cryptography.
Trinary	Trinary Switch	Having three states
StarTag	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 WS 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.
Edge-to-Edge		A communication model where data is securely transmitted between two boundary points (edges) within a network, typically from one device or system edge to another, ensuring controlled flow without exposing intermediate pathways.

Peer-to-Peer	P2P	A decentralized network architecture where devices, or "peers," communicate directly with each other without relying on centralized servers, enabling efficient data exchange and collaboration.
Hybrid Peer-to-Peer	HP2P	Similar to a pure P2P network, a HP2P network is largely decentralized, but with centralized services to provide utilities on an ad hoc, on demand basis to devices within the network.
End-to-End	E2E	A security and communication principle where data is encrypted and maintained from the originating source to the final destination, ensuring that only the endpoints can access or interpret the transmitted information.
Conduit	HyperSpace™ Conduit	A secure, controlled channel or pathway used to transmit data between systems or network segments, often encapsulating traffic to protect it from external interference or unauthorized access.
Crypto-Tag-Switching	CTS, Tag-Switching	A method of dynamically routing encrypted data packets by attaching cryptographic tags, allowing secure, efficient switching and forwarding within a network without exposing sensitive routing information.
Autonomic Synchronizer	AS, Synchronizer	An intelligent system component that automatically manages and maintains synchronization of data or configurations across distributed devices or nodes, operating without manual intervention to ensure consistency and reliability.
Replicator		A WS network facility to help individual devices communicate at scale.
Core	WhiteStar Core	The centralized services provided to help scale the WS Network, and to provide useful services needed for reliable and secure networking.