WhiteStar HyperSpace

Quantum VPN Solution

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 WhiteStar 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 Overview

WS HyperSpace is comprised of **three parts:**

Administrator's Dashboard - a web-based console used to manage access to your devices plus granting and revoking access to members of your team (providing them with the proper credentials to connect to remote WS HyperSpace servers).

WS HyperSpace Client - a secure quantum VPN application that interfaces directly with the WS HyperSpace Server service running on remote devices. The WS HyperSpace Client allows transparent access to devices running locally within your intranet or remotely (via the internet) to any device the client has been granted access to. Once a connection is no longer required, the user simply exits from the WS HyperSpace Client application and all secure network connections are torn down automatically.

WS HyperSpace Server - 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 Server device and the user's Client application. The WS HyperSpace Server can be started and stopped, as needed, providing the Server device administrators the ability to enable/disable remote WS HyperSpace 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 access is required on a particular device*.

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

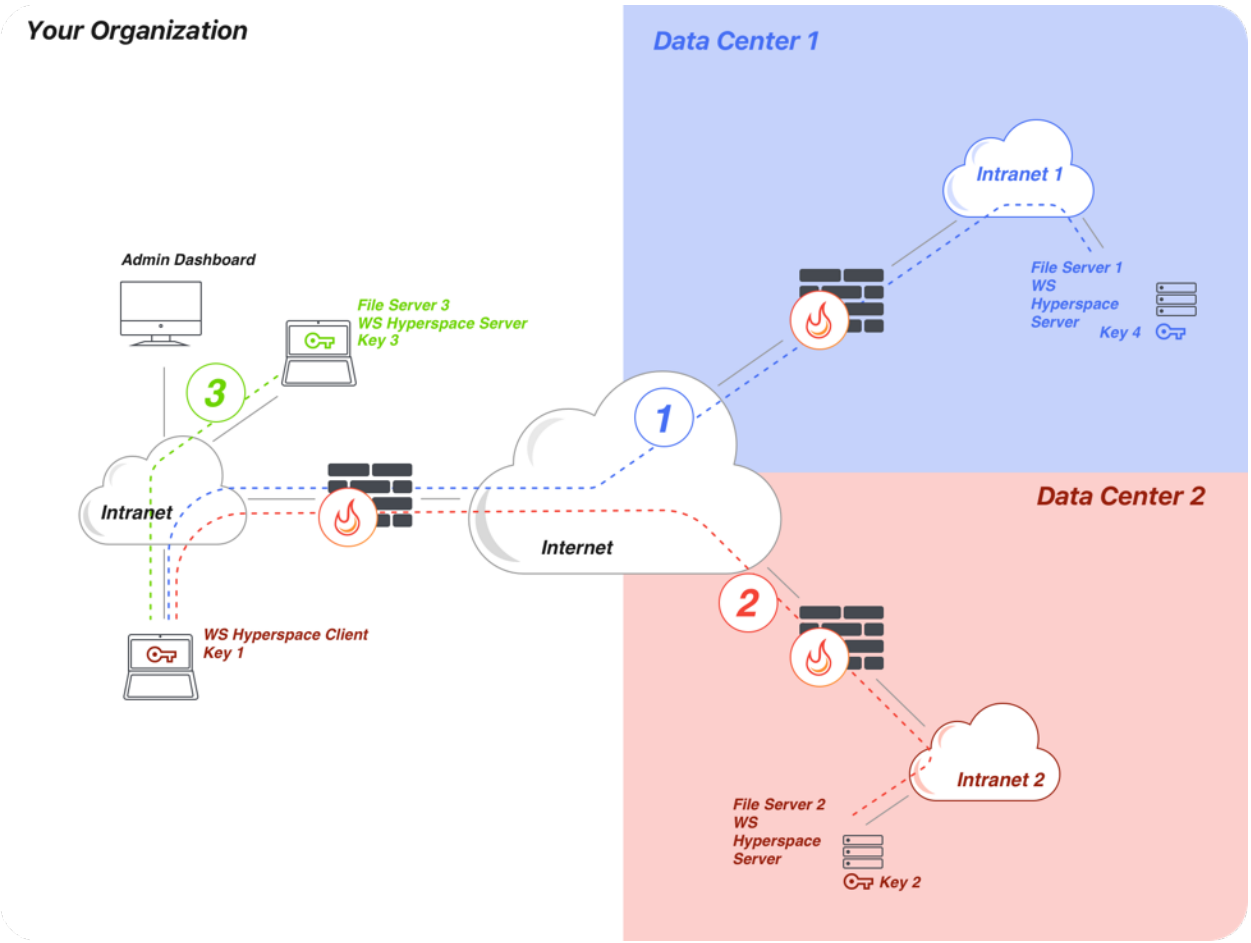

Figure 1

As illustrated above, the WS HyperSpace client can connect to and from devices within its own intranet (#3), and to and from devices across the internet to itself (#1 and #2),– simultaneously all from the same WS HyperSpace client.

2.1. Teams – Subdividing Teams

Customers typically only allow "specific" users, or groups of users, to connect to and from one of their server 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 server 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 server devices or create a small **Trusted Team** of WS HyperSpace users permitted to connect to a specific set of server devices. They may also want to have a *generic Trusted Team made up of all WS HyperSpace users* who can connect to any Server device. Figure 2 illustrates an administrator who has created three (3) teams [this is done by assigning a **WhiteStar Trusted Team Tag** – or multiple Trusted Team

Tags – to their WS HyperSpace Client users]. How to accomplish this is discussed later in this document.

- **Trusted Team #1** (Purple: with 2 WS HyperSpace Client users) has been established to connect to a single "Purple" server device at Data Center 1 by both Client users.
- **Trusted Team #2** (Green: with 3 WS HyperSpace Client users) has been established to connect to "Green" server devices at all 3 Data Centers. Note that Client #'s 1 and 2 are members of both Team #1 and #2 and therefore can connect and 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" server device in Data Center 3.

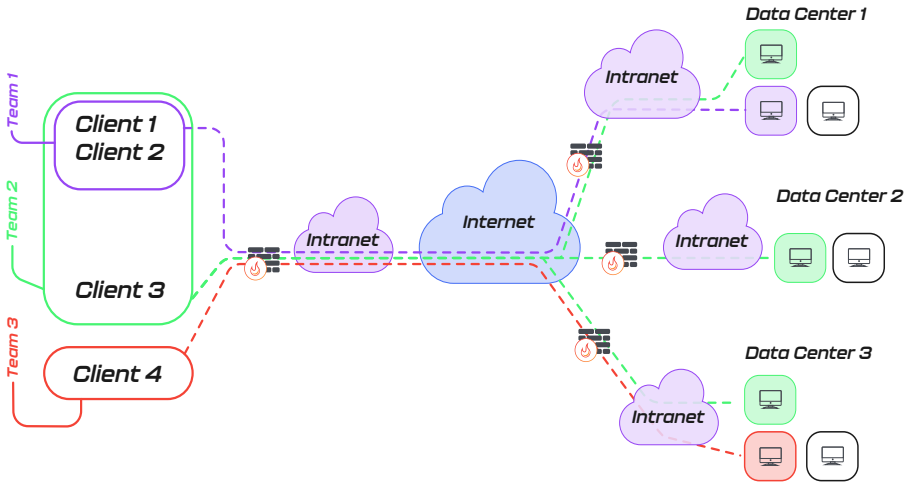

Figure 2

Note: the administrator creates Trusted Teams Tags on their **WhiteStar Administrator Dashboard** by assigning WhiteStar Trusted Team Tags to their users to delineate which Trusted Team(s) they are a member of. For a customer to grant access to a WS HyperSpace Server device, they must also assign the Trusted Team Tag to the Servers they are granting access to via the same **WhiteStar Administrator Dashboard**.

3. Minimum System Requirements

3.1. Software

3.1.1. WS HyperSpace Client

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

3.1.2. WS HyperSpace Server

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

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

3.2. Hardware – WS HyperSpace Client

Operating System	Minimum Requirements
Windows OS	• 2.5 Ghz or faster processor with 2 or more cores (64 bit compatible) • 8 GB RAM • 64GB or larger storage device
MAC OS *	• 2.5 Ghz or faster processor with 2 or more cores (64 bit compatible) • 8 GB RAM • 64GB or larger storage device
Linux flavors	• 2.5 Ghz or faster processor with 2 or more cores (64 bit compatible) • 8 GB RAM • 64GB or larger storage device

* *Both* X86 and Apple Silicon where applicable

4. The WhiteStar HyperSpace Administrator Dashboard

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

To access the Administrator Dashboard, a designated company administrator must visit the WhiteStar Communications website at **https://www.whitestar.io** and click the "***Dashboard***" button on the far right side of the menu bar on the landing web page (see Figure 3).

Figure 3

After clicking "***Dashboard***", the administrator is presented a screen prompting them to log in (see Figure 4). If they already have a WhiteStar administrator account, they can enter their email address and password information and hit "***Continue***", or they can click on "***Continue with Google***" to use Sign in with Google (Google Single Sign On (SSO)). If an account has not been established for the admin, they can sign up by clicking the "***Sign Up***" link on the screen. For additional details on obtaining an administrator's account, please refer to section 5 below.

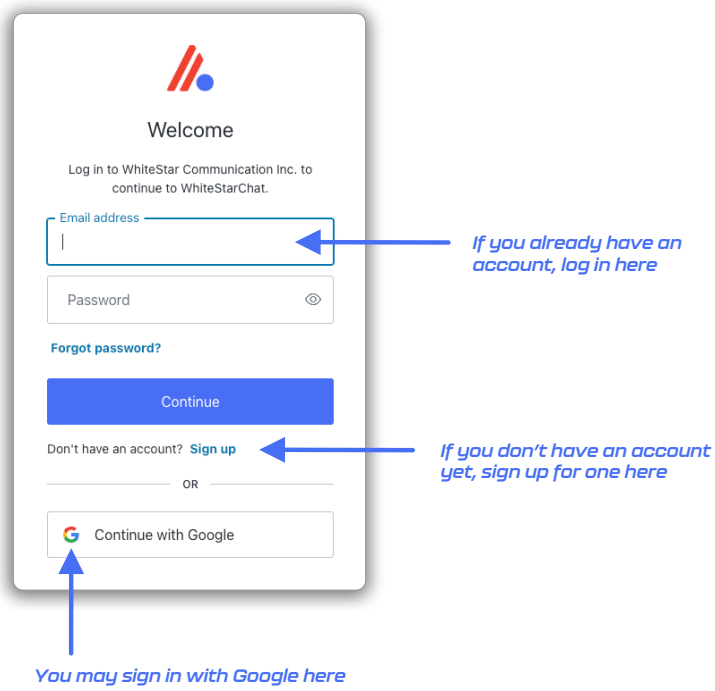

Figure 4

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

4.1. Administrator Dashboard - Orientation

Once successfully logged in, the administrator sees their dashboard (see Figure 5), which has multiple functions. The lefthand column of the ***Administrator Dashboard*** is used to toggle the main functions of the page: (1) manage users (WS HyperSpace users who are utilizing the WhiteStar HyperSpace Client application), (2) Manage Servers (devices users need to connect to), (3) view billing information, and (4) view company profile information.

The middle section of the page provides a summary of the users who have been configured to access WhiteStar HyperSpace. Additionally the administrator is giving the ability to bulk upload or add individual users, assign Trusted Team Tags to users, and assign Trusted Team Tags to servers.

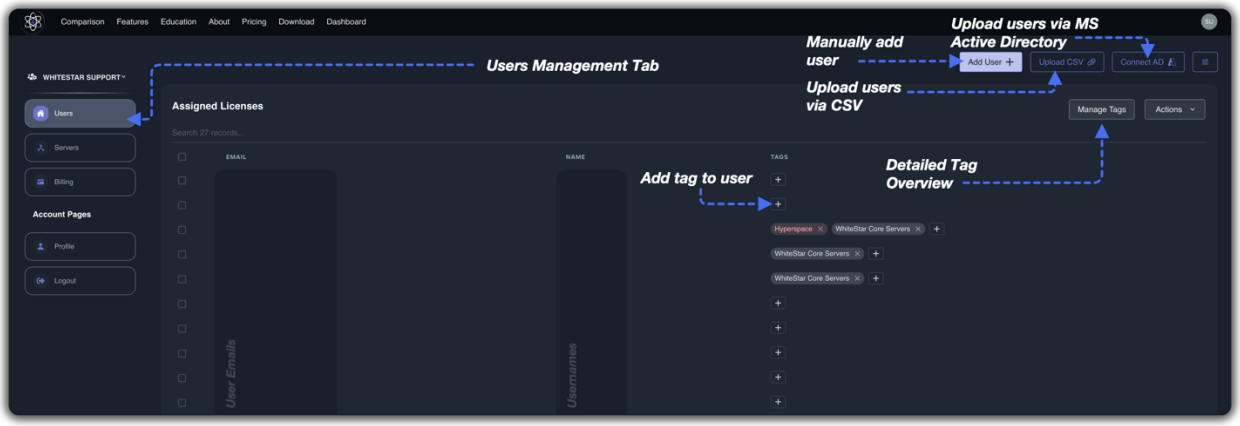

Figure 5

5. Signing up for an Administrator Account

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

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

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

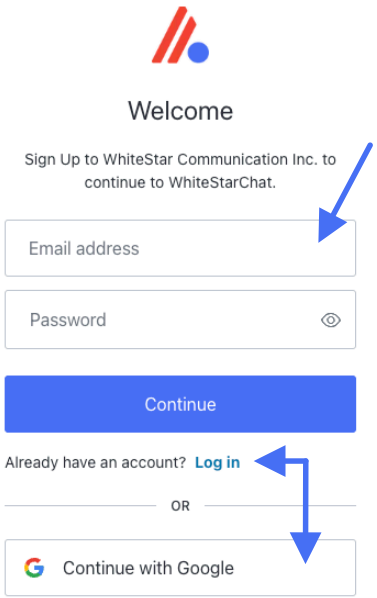

Figure 6

A verification email is sent to the address provided in order to verify ownership. 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 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 WS HyperSpace password. If you lose your password, you must zeroize, or reset, your WS HyperSpace Client and rebuild your user identity from scratch.

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 5). This allows the administrator to authorize WS HyperSpace users to use the WS HyperSpace Client 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 Client installation process to activate this license.

After clicking on "***Add User***" in the main screen, the "***Add New User***" screen is presented to the admin. The only required field on this panel is the email address, but it is highly recommended that the WS HyperSpace users name be entered as well. Once the information is entered, click the "***Submit***" button (see Figure 7).

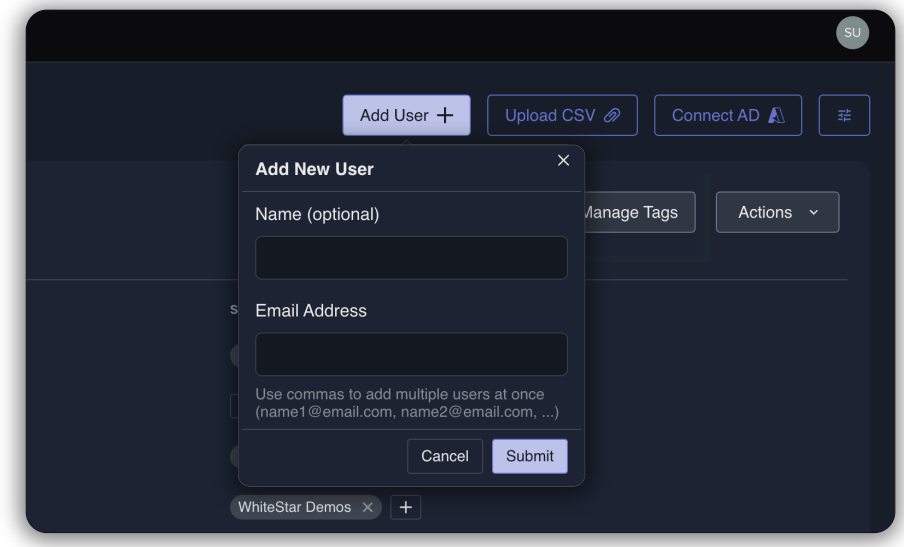

Figure 7

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 Trusted Team Tags***. Current column assignments can be seen in the first row of the preview table.

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

corresponding columns, the user may press **"*Submit*"** to continue the bulk license assignment (see Figure 8).

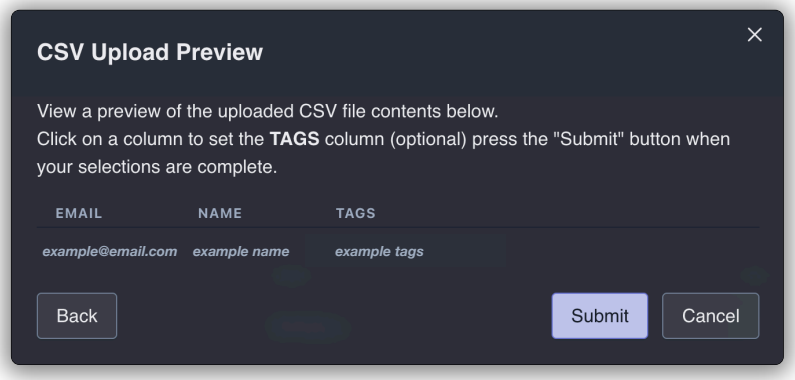

Figure 8

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.

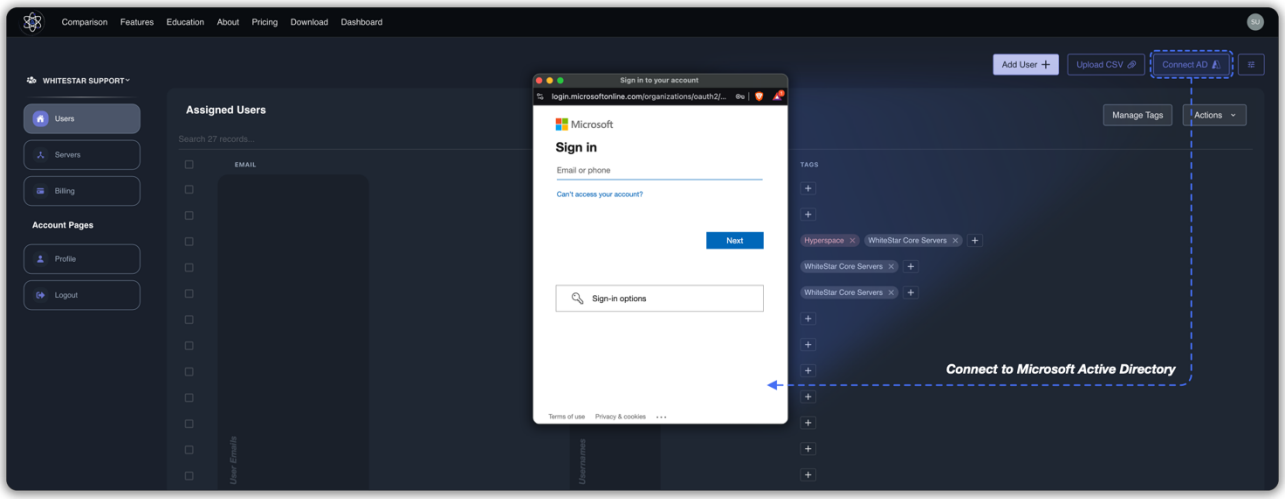

Figure 9

5.2. Removing a User from the System

If the administrator needs to remove a user from your organization (and zeroize the information on their device), they must log into the WhiteStar Administrator dashboard, click on "***Manage***" in the lefthand column, and then click the check box next to the user(s) they wish to delete/zeroize. The administrator must then click on the "***Actions***" button and selects either "***Remove Selected***" (to delete the user from the system and free up their license) or "***Zeroize Selected***" (to delete the user from the system, free up their license, and delete all the WS HyperSpace Client 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 Client information, and any network connection information, ***deleted permanently***.

Zeroization cannot be undone, but the administrator can always set up a new account for that user if needed.

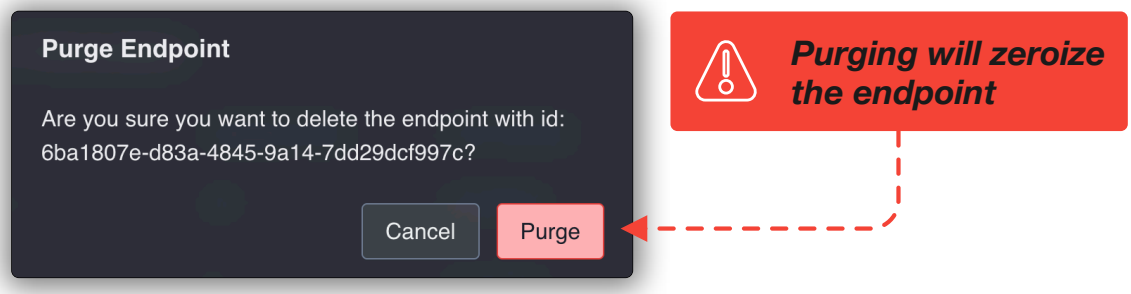

Figure 10

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. Trusted Team Tags – Providing Access to Server Devices

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

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

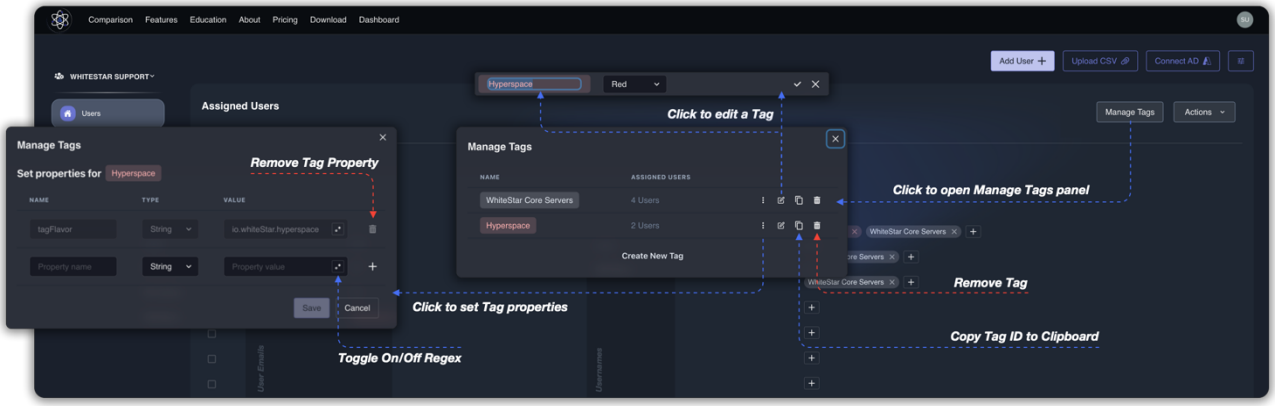

Figure 11

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

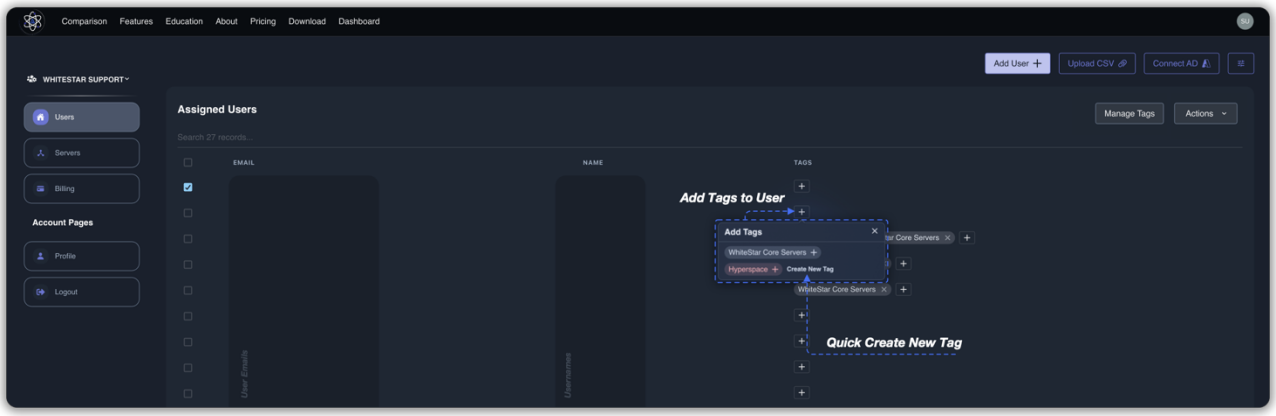

Figure 12

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

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

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

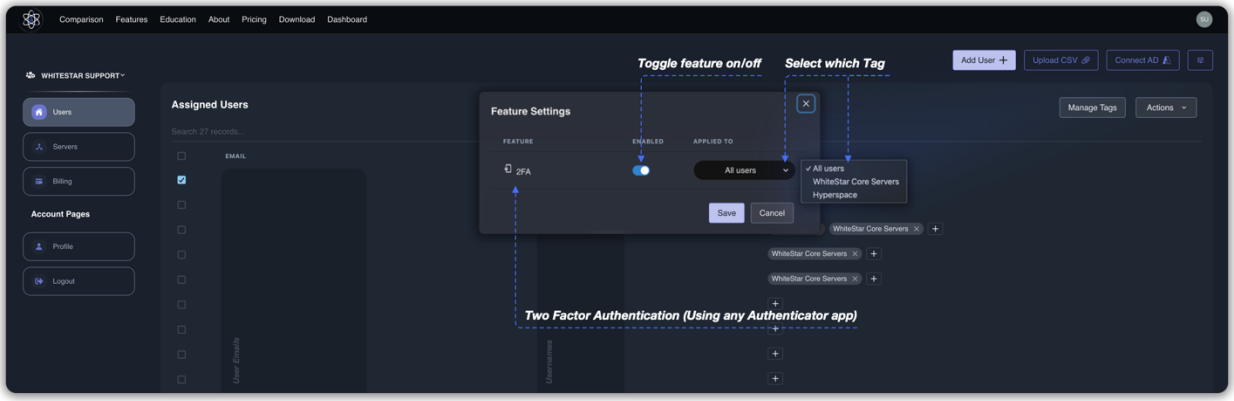

Figure 13

As shown in Figure 13, you can access Feature Tags from the manage portal on the Dashboard near the righthand side of the screen. This will bring up the Feature Tags available to you as an administrator. You can apply these to a Tag and enable and disable the feature if needed. ***We***

suggest creating a specific Tag for each Feature, which you can then apply selectively to the Federations you manage (for example, creating a 2FA Tag that can be applied to certain Federations who you believe need to have multi-factor authentication.)

5.4. 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. Installation of WS HyperSpace Client

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

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

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

Open the folder where the WS HyperSpace installer package was saved. Click on the download package to ***run the installer***. You are brought to the following screen. 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.

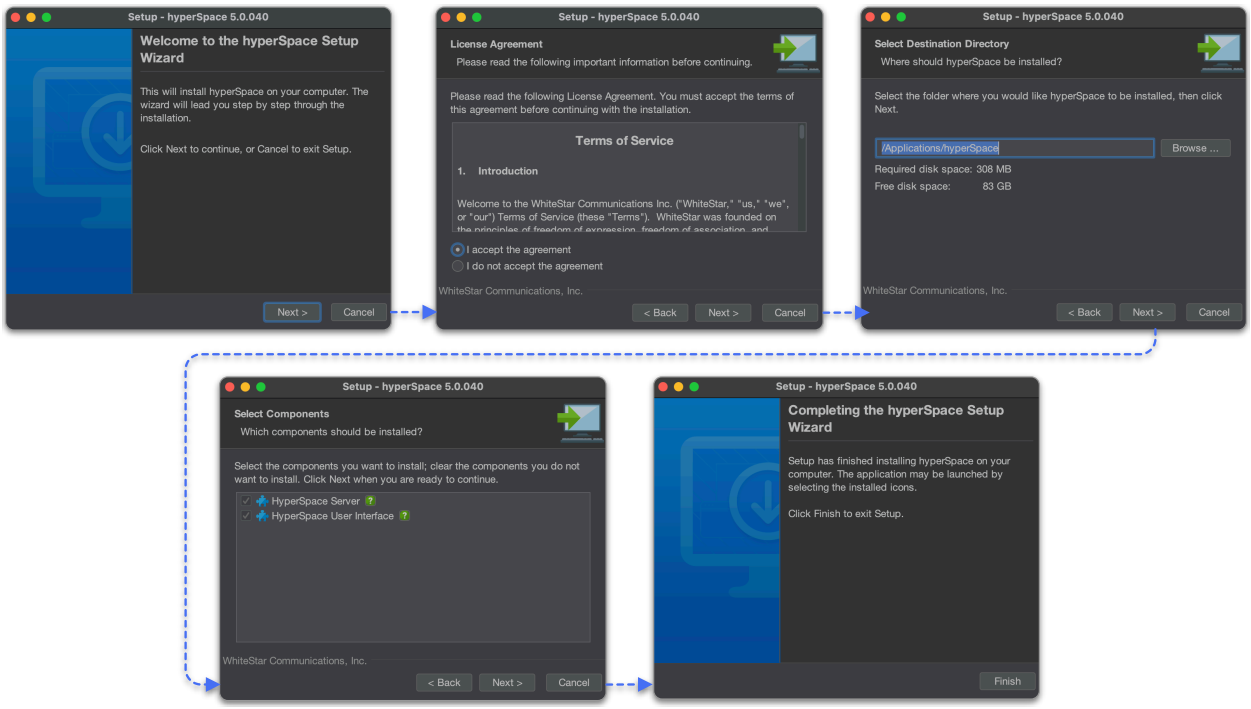

Figure 14

The first time the user starts the WS HyperSpace Client program they are brought to the registration screen. 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.

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

Go to your email client and look for an email from vortex@whitestar-vortex.com with the subject line of "***WhiteStar Validation Code***" (check your spam folder if you don't see the email within 2-3 minutes). Open the email and copy the **entire** confirmation code (including the single quotes) from the email into the copy buffer (typically highlight the entire code and hit **Cntl-C/Cmd-C**). Go back to the WS HyperSpace Client installation screen and paste (typically hit **Cntl-V/Cmd-V**) the confirmation code into the appropriate box.

Figure 15

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.

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

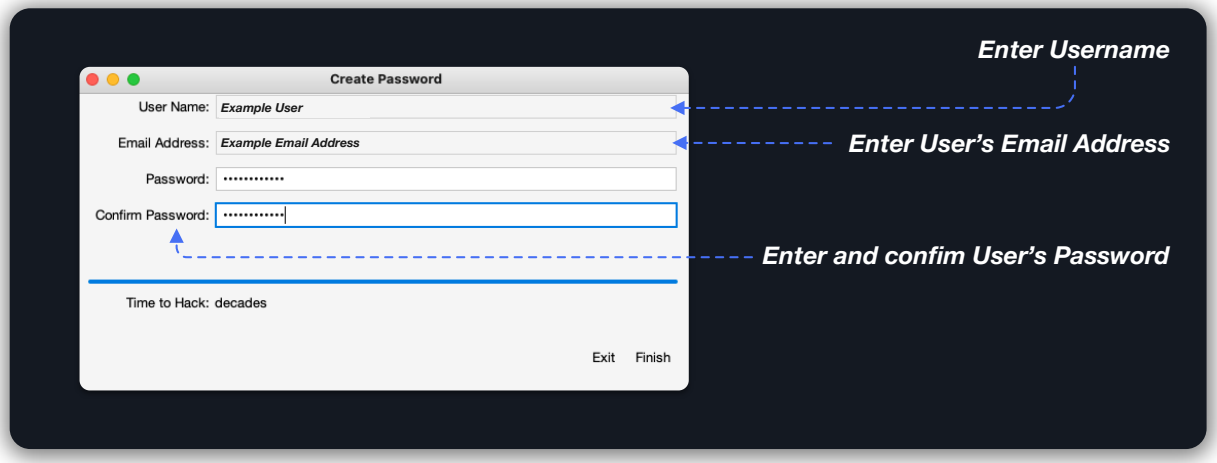

Figure 16

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

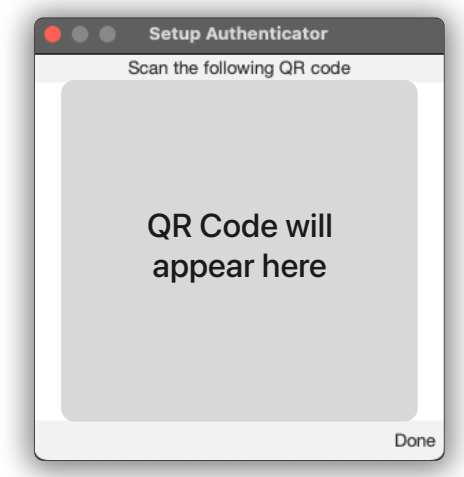

Figure 17

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 16).

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

7. Running the WS HyperSpace Client

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

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

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

The user is prompted to enter their password and are brought to the main WS HyperSpace Client screen. Both the left and right panes display the file system of the current device you are running the client on.

7.1. Changing your Password

To change your password, right click on the Core icon. Then click "***Change Password***".

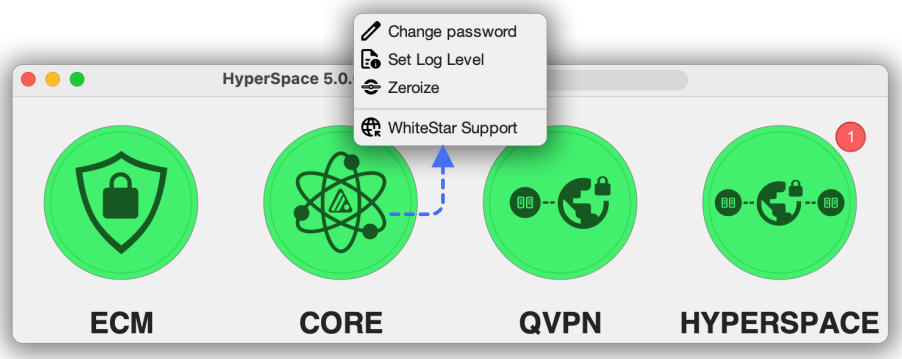

Figure 18

Enter your new password, and confirm the same new password in the second input box. Once successfully entered twice, click "***Change***" for it to take effect.

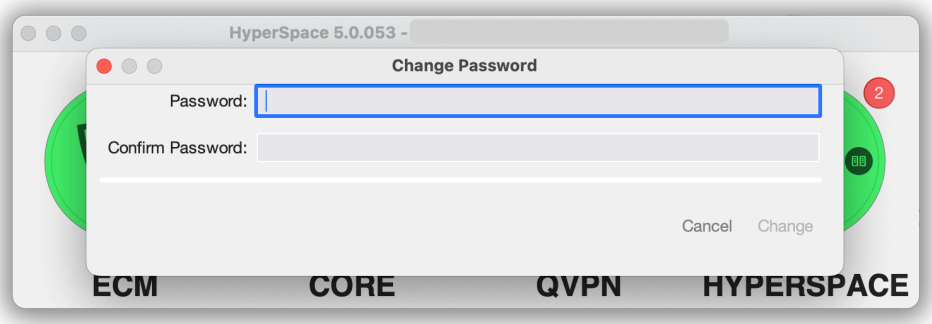

Figure 19

The next time the user logs in, they will be required to use the new password.

7.2. Setting the Log Level

If the user experiences issues with the HyperSpace application, WhiteStar may ask to gather diagnostic data to assist in debugging the issue. The system logs diagnostic data to various degrees from "No Logging" at all to "All" Diagnostic records. The WhiteStar support person will instruct you on what level to set your logging to.

To change your Log Level, right click on the Core icon. Then click "***Set Log Level***" (See Figure 18). Choose the appropriate level from the drop down menu and then click on "***OK***" for it to take effect.

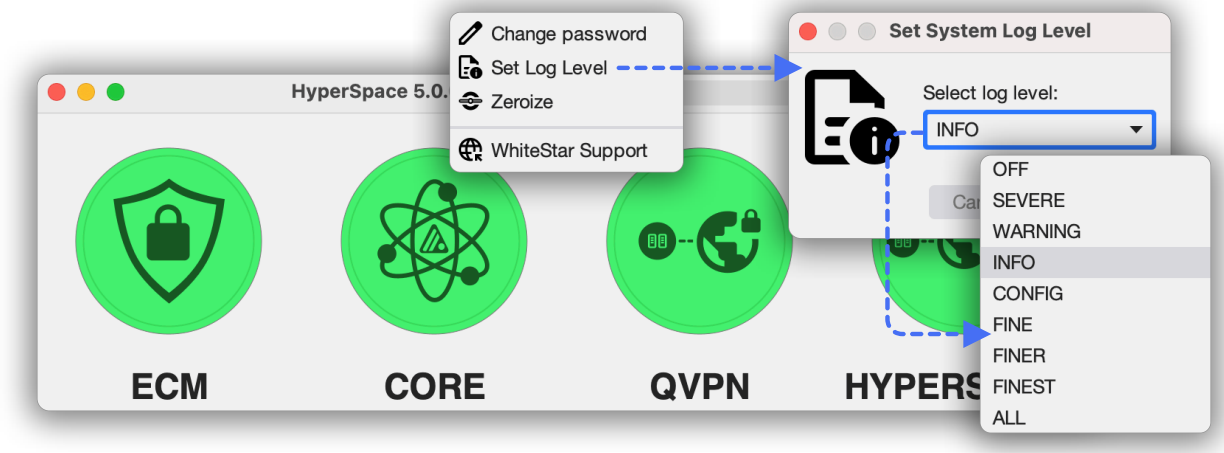

Figure 20

7.3. Zeroizing your Application

If the user wants to completely remove their WS HyperSpace account, and securely delete all information that have been generated on this device, they do so by clicking on the "***Zeroize***" in the right click menu (See Figure 18).

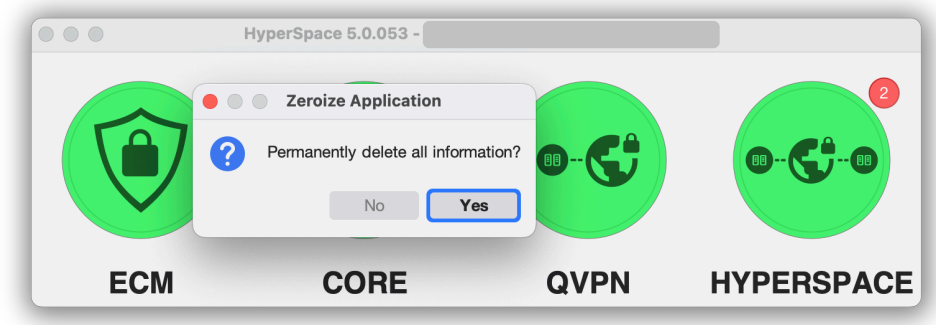

Figure 21

Once clicked, the user is asked to confirm this action, prior to proceeding.

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

7.4. Creating a Support Case with WhiteStar Support

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

To change your Log Level, right click on the Core icon. Then click "***WhiteStar Support***" (See Figure 18). This will bring you to a web page where you can create a support ticket for the issue you are experiencing.

8. Installation / Configuration of WS HyperSpace Server

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

8.1. Installation on Linux Server

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

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

```
# sudo dnf copr enable whitestar/hyperspace

# sudo dnf install -y hyperspace
```

Once the server 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 Server 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.

Figure 22

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

8.2. 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 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

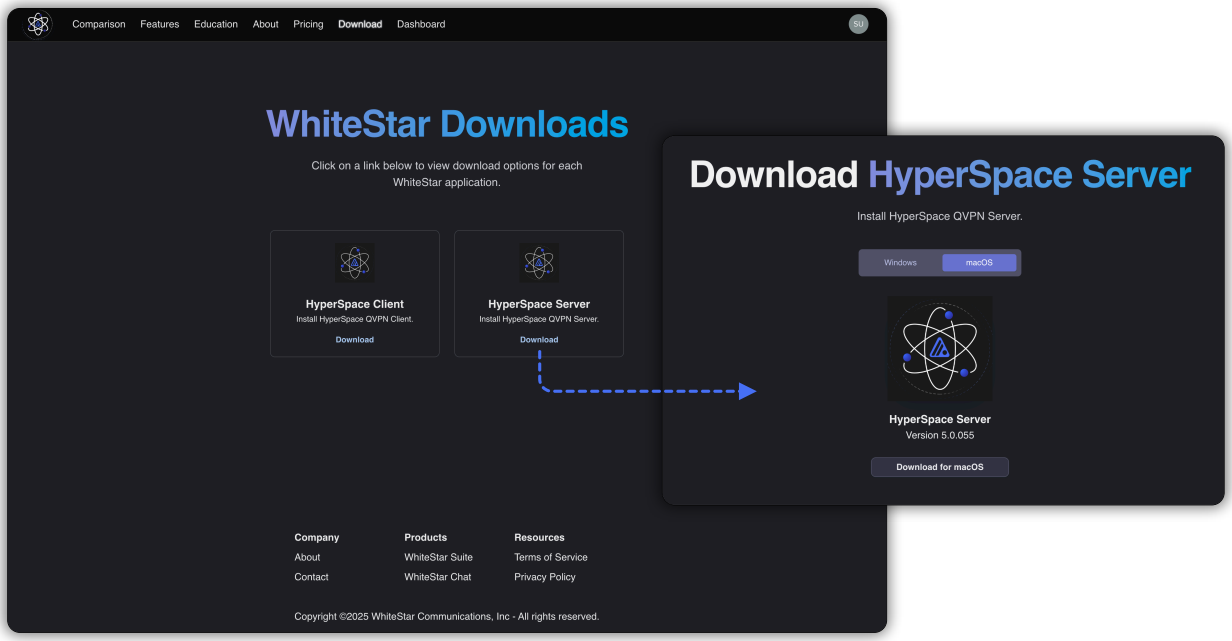

Figure 23

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

Once installed, the Server application provides a unique Server Identity (See Figure 24) 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.

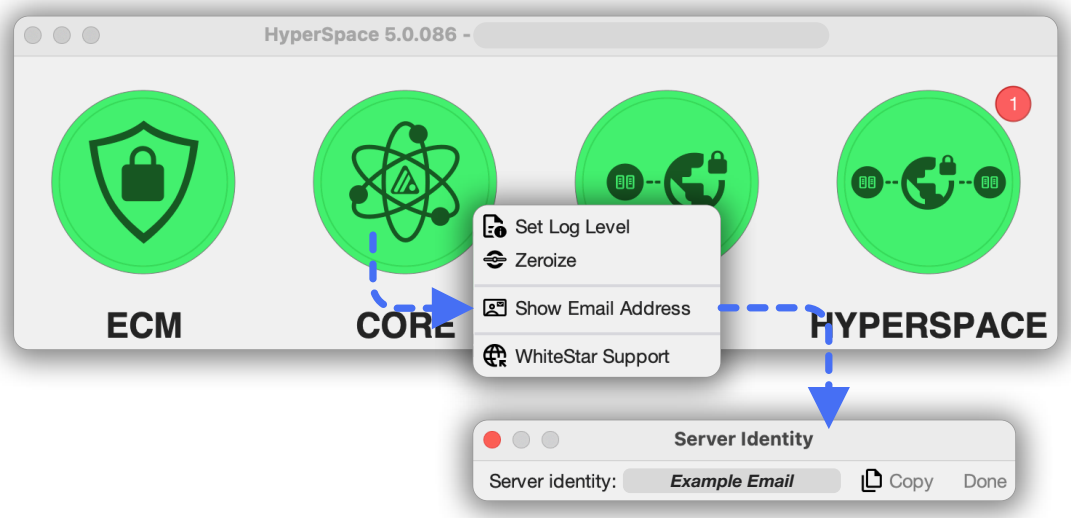

Figure 24

8.3. Adding a Server via the WS HyperSpace Dashboard

Once the WS HyperSpace Server has been successfully installed, the device administrator must add it to the list of devices under their control. To do so, log in the administrators 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 25).

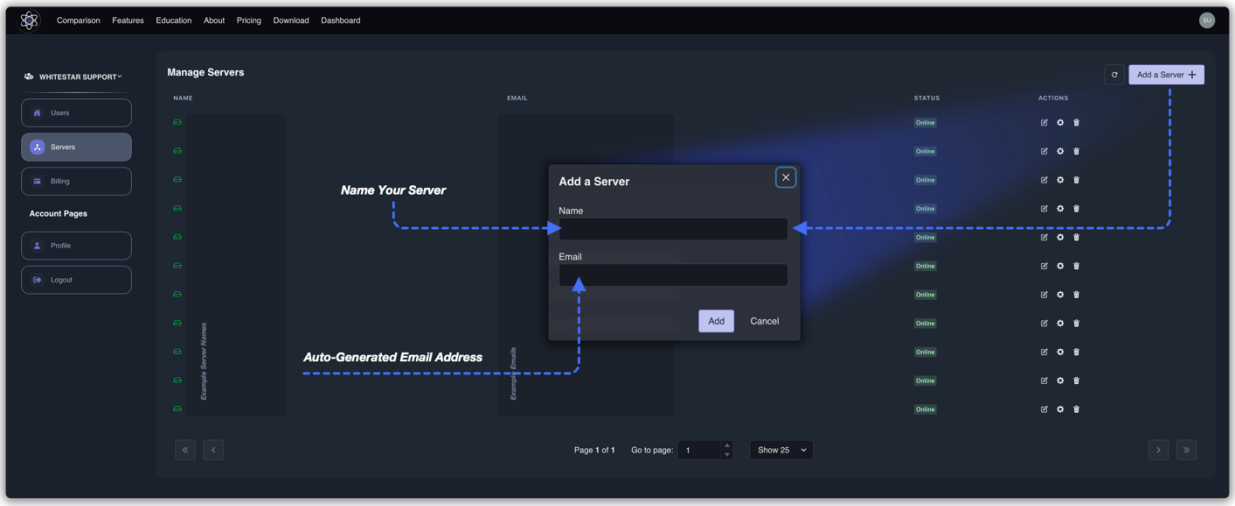

Figure 25

The administrator is presented with a screen pop up (See Figure 25). The administrator is prompted 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 Server during installation (see Section 8.3 above).

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

8.4. Starting and Stopping the WS HyperSpace Server Service

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

To start/stop the WS HyperSpace Server service:

- Log in to the device the WS HyperSpace Server has been installed on

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

- Start: sudo /Applications/hyperSpace\ Client/hyperSpaceService start
- Stop: sudo /Applications/hyperSpace\ Client/hyperSpaceService stop

8.5. Viewing the Unique ID of the WS HyperSpace Server Device

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

8.5.1. On Linux Server

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

Figure 26

- 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.

8.5.2. On a Windows or Mac

- Right click on the CORE green circle on the HyperSpace Server GUI (See Figure 27).

- Click on “Show Email Address” from the drop down menu

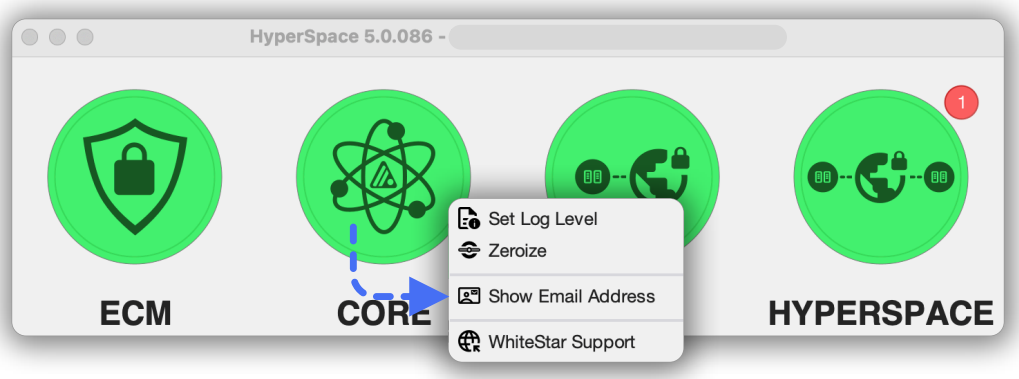

Figure 27

8.6. Zeroizing the WS HyperSpace Server interface

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

8.6.1. On a Linux system:

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

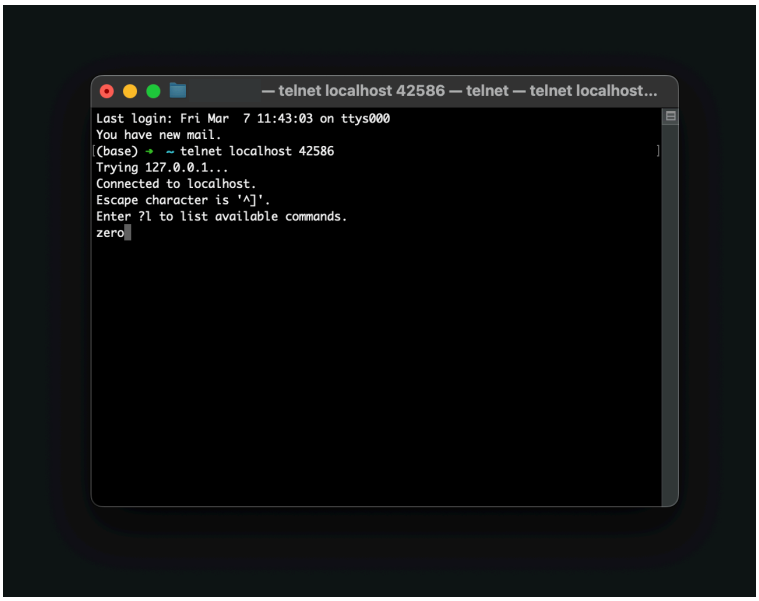

Figure 28

8.6.2. On a Windows or Mac OS system:

- Right click on the CORE green circle on the HyperSpace Server GUI (See Figure 27).
- Click on "***Zeroize***" from the drop down menu

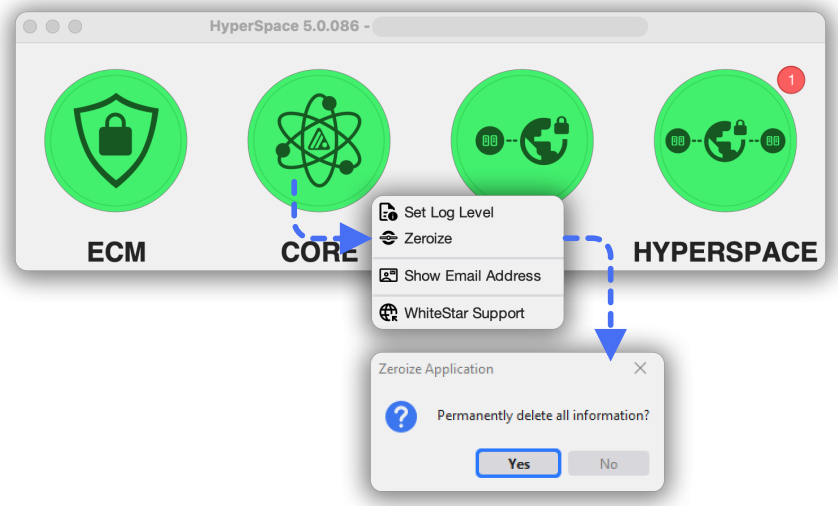

Figure 29

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

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

To add a trusted team tag:

- Log in to the Admin Dashboard (from the WhiteStar web page: https://www.whitestar.io)
- Click “Servers” on the lefthand side of the screen, which displays all devices that have been claimed by your organization
- Find the “Server” you wish to grant a Trusted Team Tag to, and click on the ***pencil icon*** on the righthand side of the screen to manage that “Server’s” options
- There is a ***“+”*** button at the top of the page which will allow you to add a previously defined Trusted Team Tag to the server device

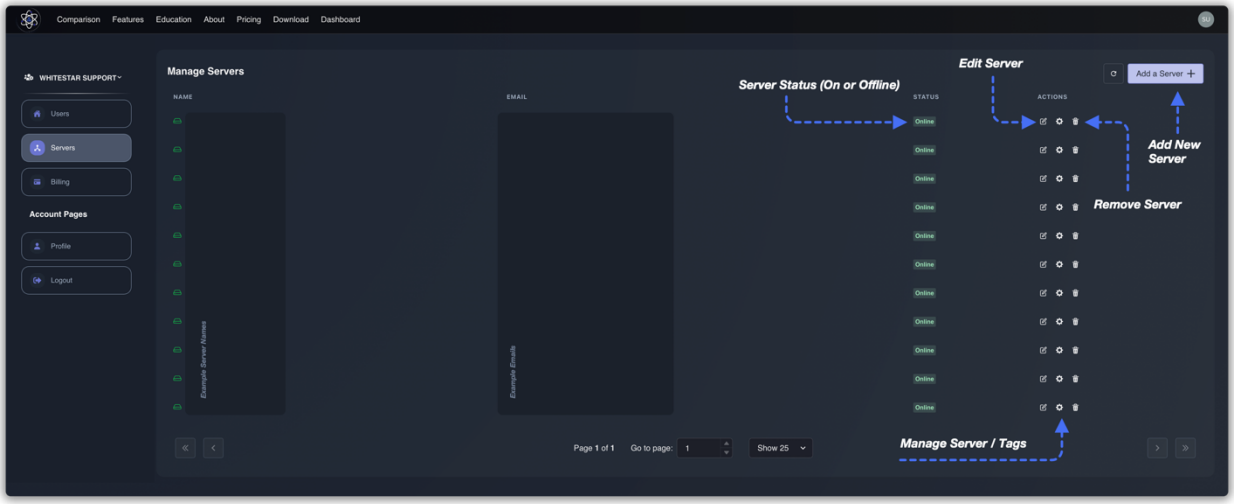

Figure 30

Users who have this Trusted Team Tag assigned to them ***will now be able to access this device***

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

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

8.8. 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 clients to access this device. The following illustrative examples utilize cockpit to enable access of the HyperSpace service.

8.8.1. 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 31).

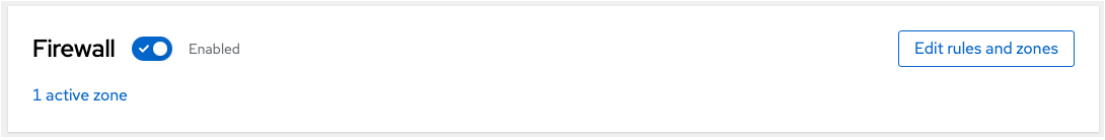

Figure 31

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

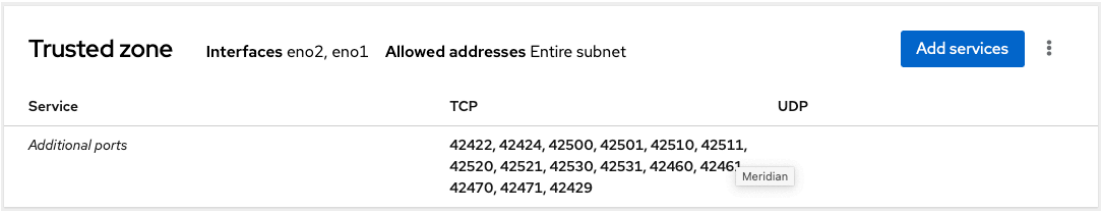

Figure 32

Type in "hyper" in the Filter services box, select "hyperSpace" and click "Add Services" at the bottom to grant permissions (see Figure 33).

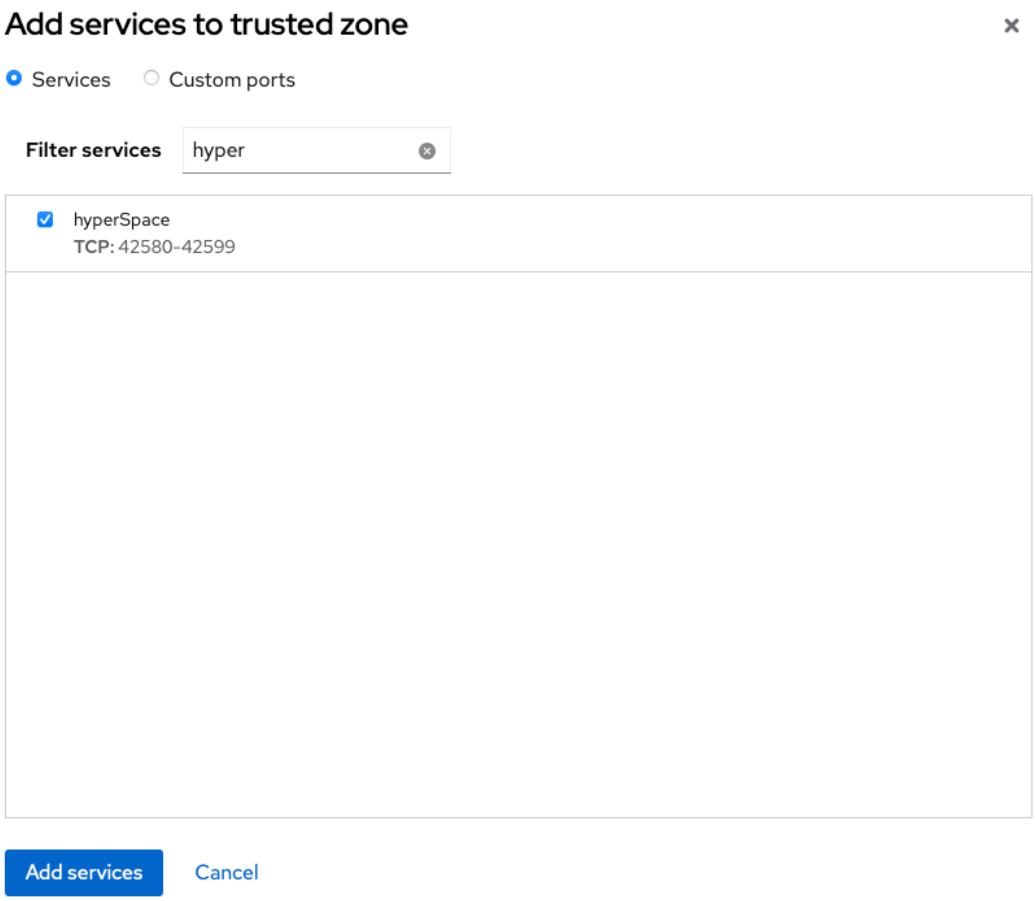

Figure 33

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"/>

8.8.2. 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 31).

Next click "Add new zone" at the top of the page (see Figure 34).

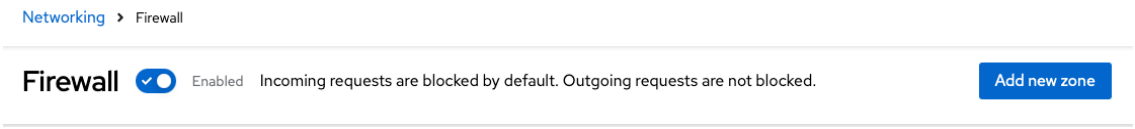

Figure 34

On the menu provided (see Figure 35), select “Internal” for the “Trust Level” and then select “tun0” on the Interfaces selection list (the tunnel interface created by the HyperSpace Server code). Then select “Add zone” in order to make this active.

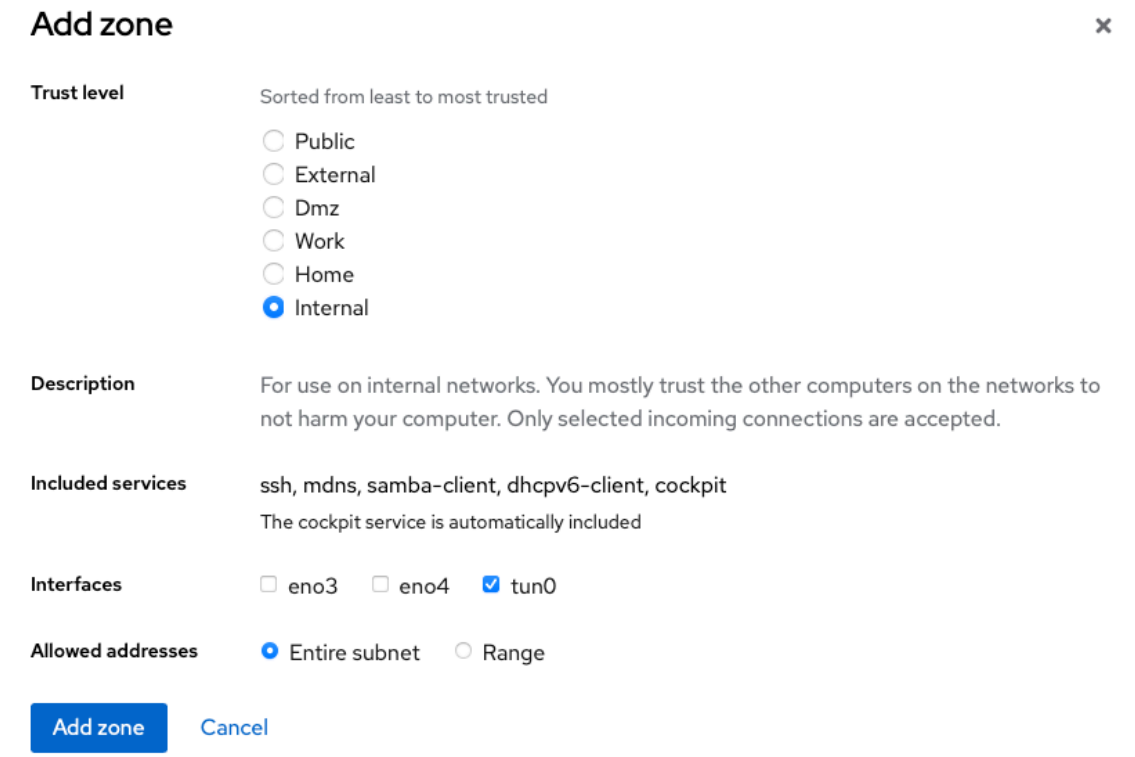

Figure 35

The zone will be added and the services that can utilize the zone are presented (see Figure 36). 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.

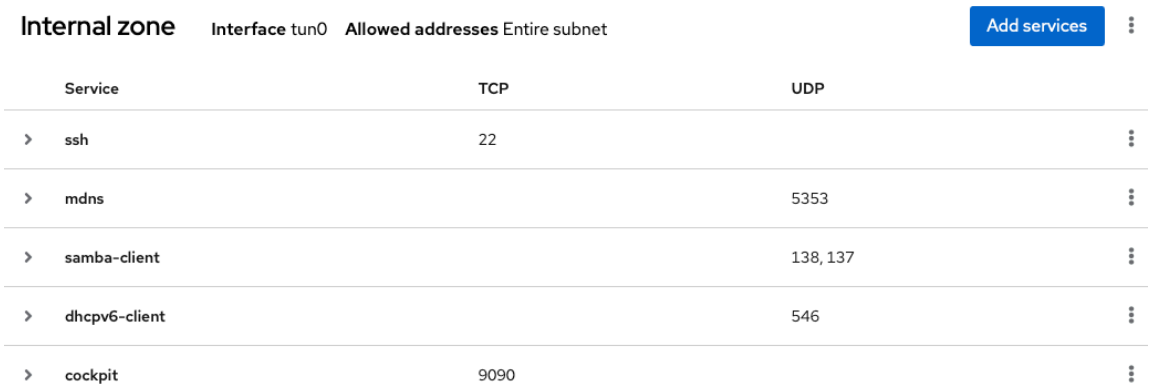

Figure 36

8.9. Configuring a Windows Server for HyperSpace

8.9.1. Installing the Routing Software

On your Windows Server machine, launch the Windows Server Manager

Click on ***Dashboard*** in the left hand column

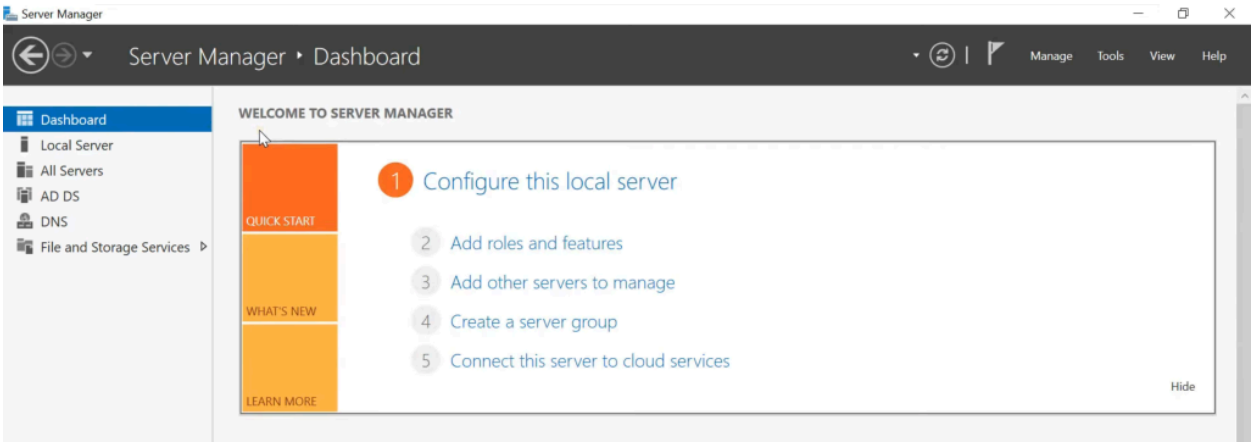

Figure 37

Click on "***Add Roles and Features***" (#2) in Figure 37, the following Wizard is presented to the user

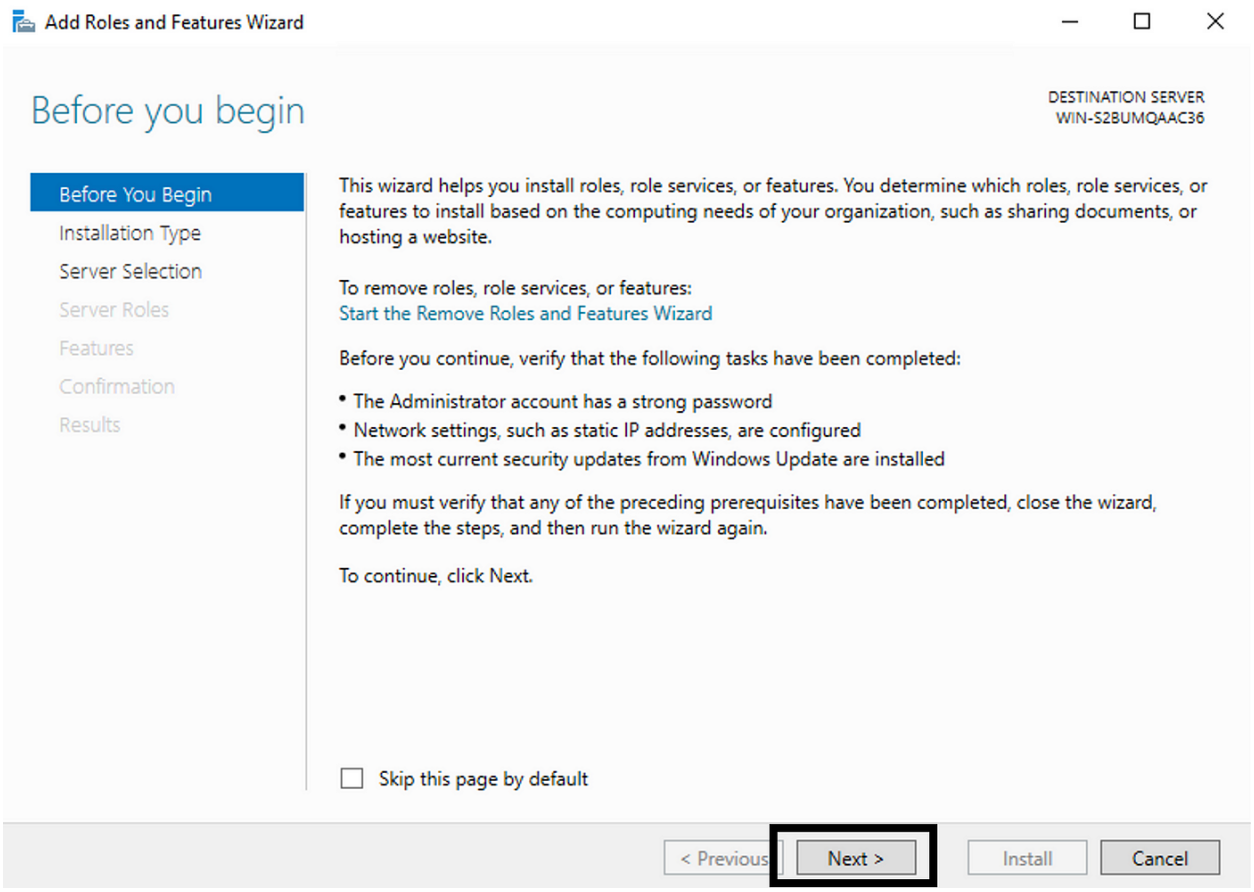

Figure 38

Click "***Next***" to begin.

Click on "***Role-based feature-based installation***" and then click "***Next***".

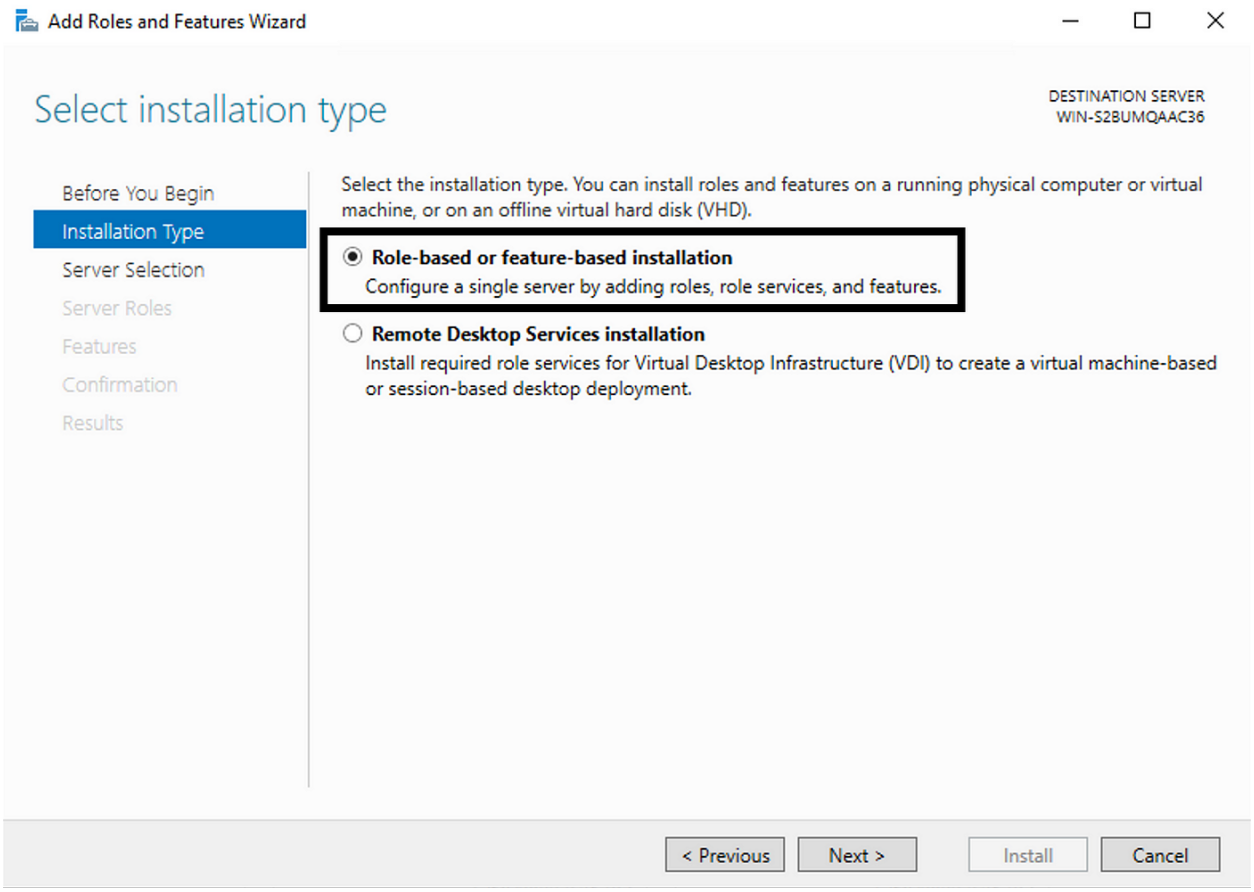

Figure 39

On "***Select destination server***", click "**Select a server from the server pool**" and select the server you are currently running on in the list presented, then click "***Next***".

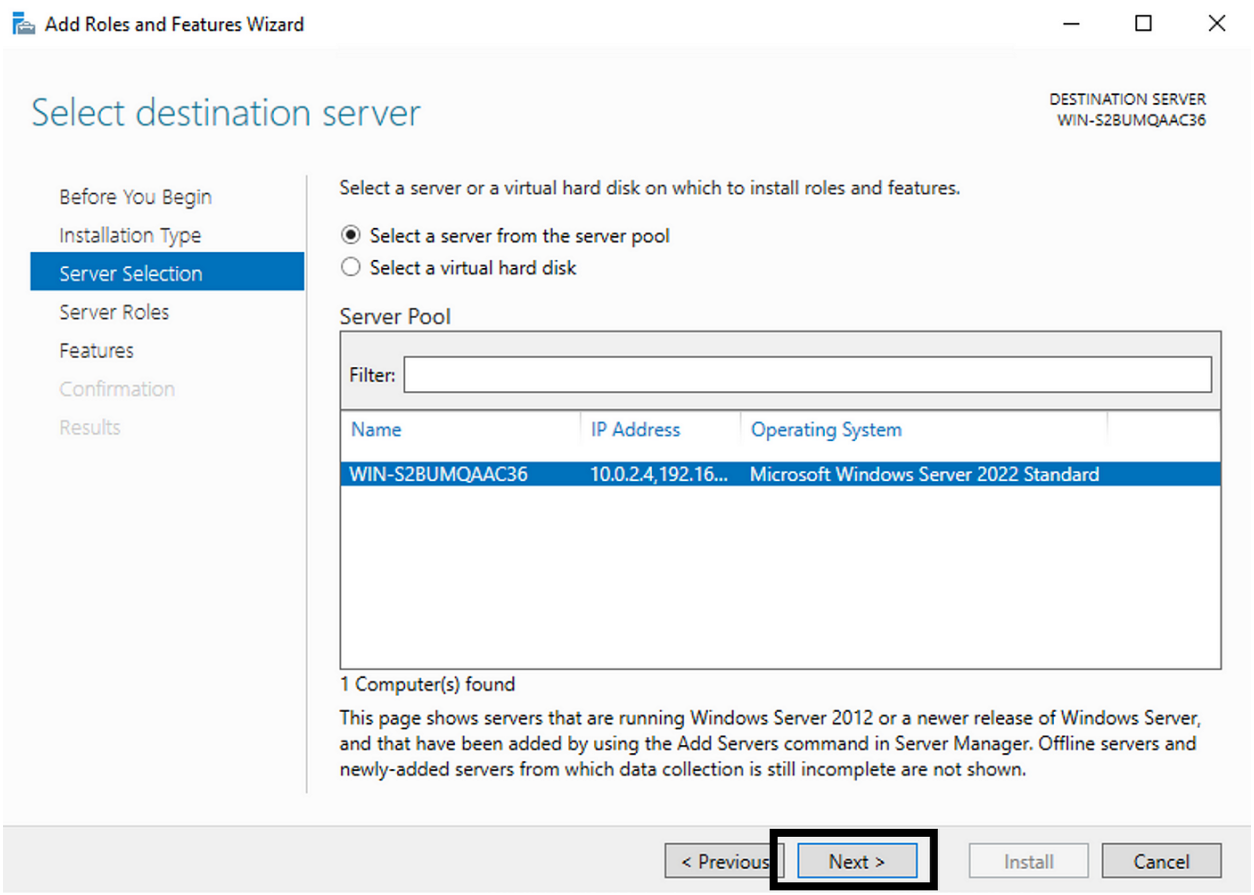

Figure 40

On "***Select server roles***" select "***Remote Access***" from the list of Roles and click "***Next***".

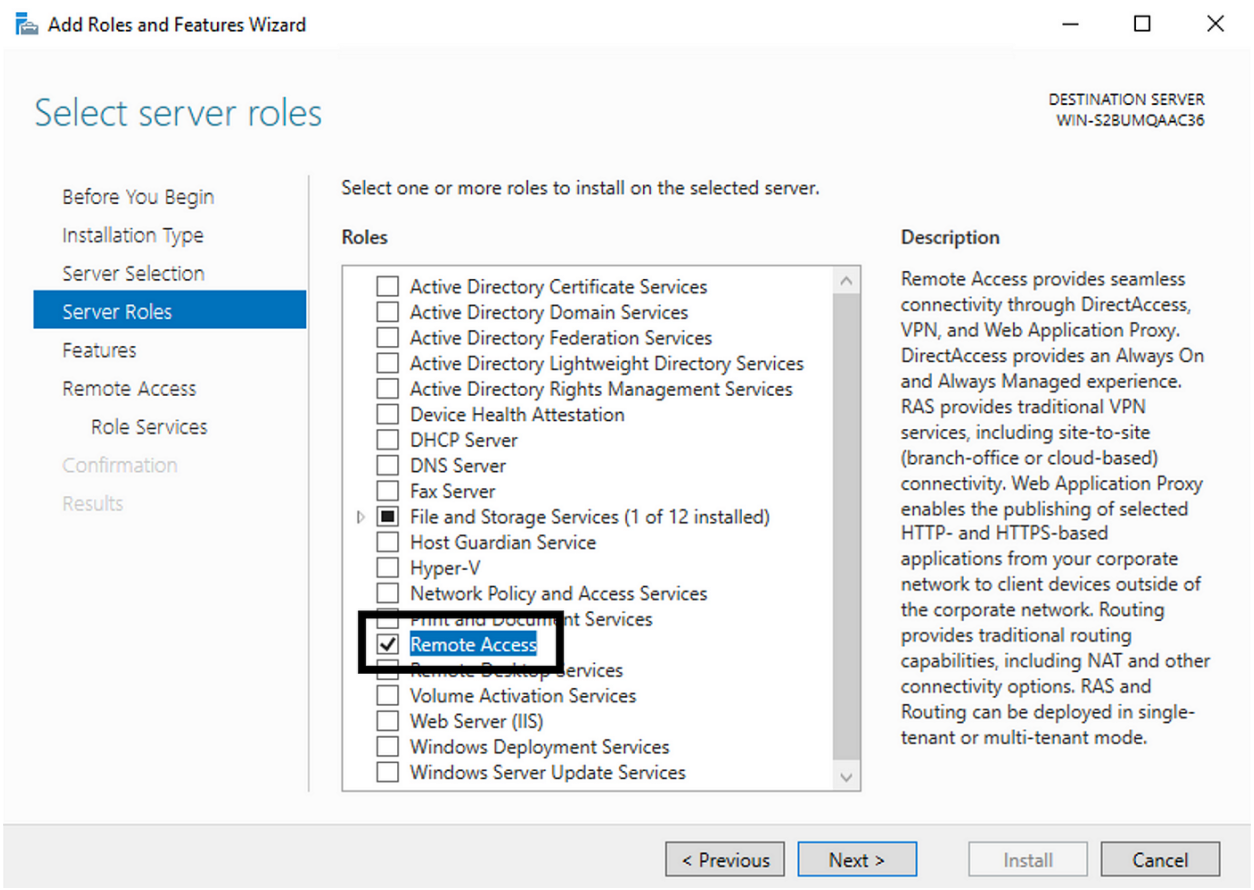

Figure 41

On "***Select Features***" for that Role, take the default settings that are selected by Microsoft and click "***Next***".

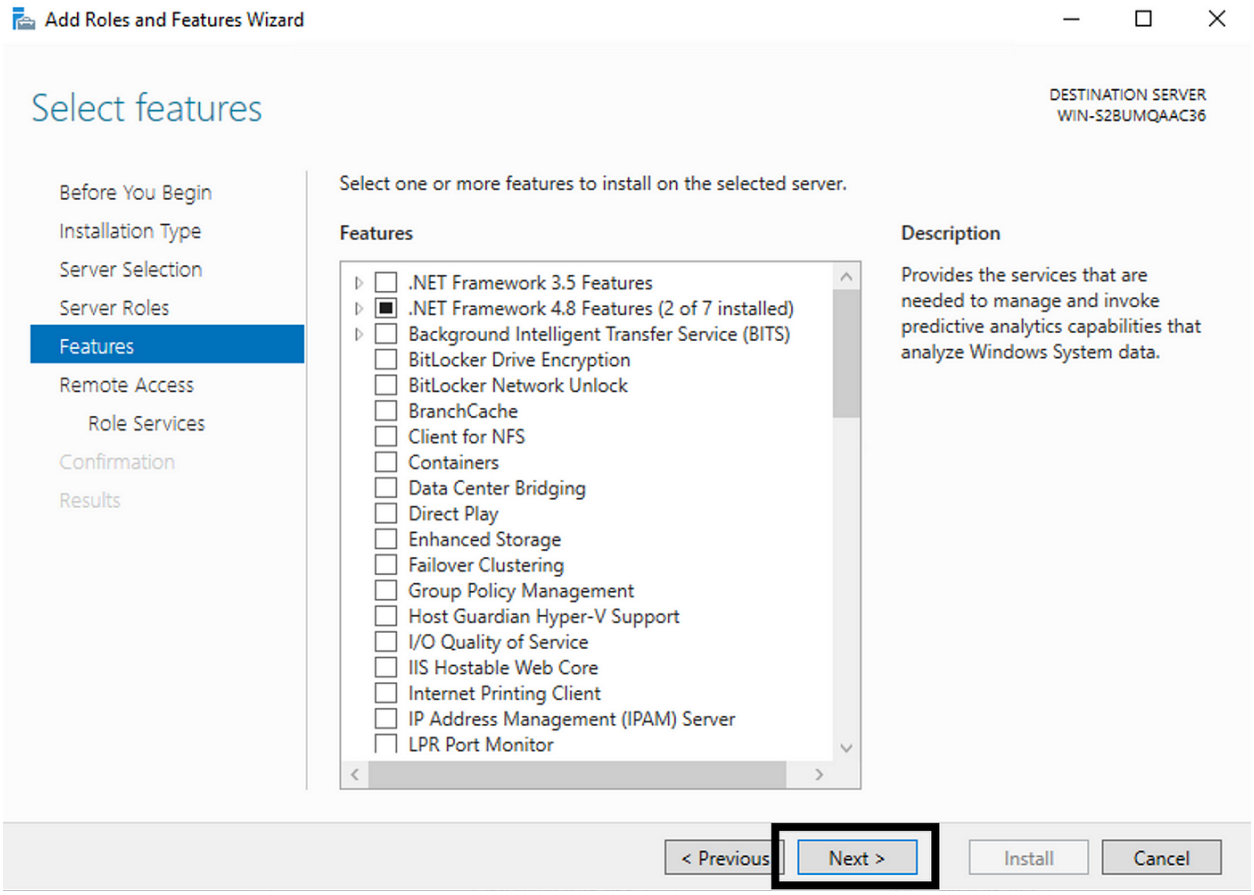

Figure 42

On "***Remote Access***" click "Next" to get to "***Role Services***".

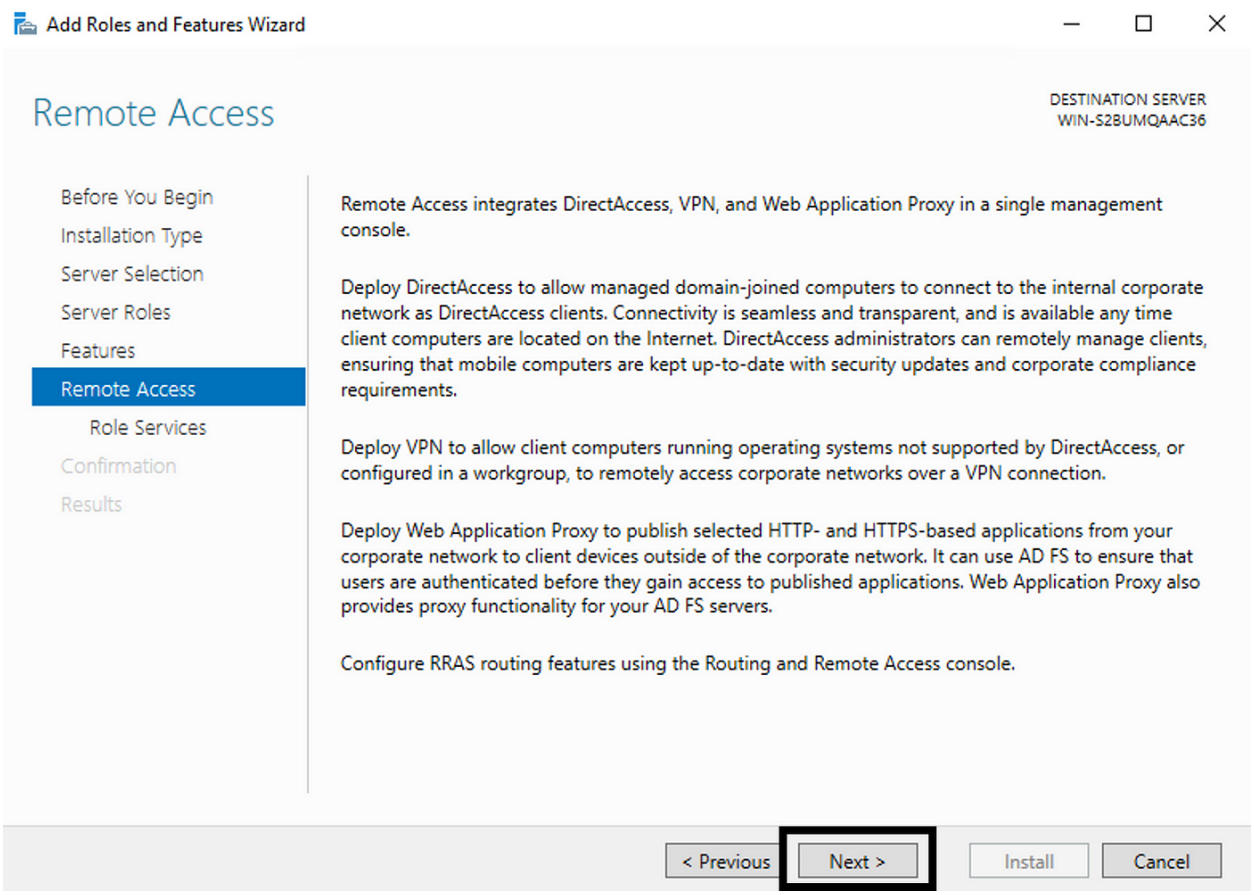

Figure 43

Click "***Routing***". "**Direct Access VPN (RAS)"** will also get selected by the wizard and can't be de-selected. Click on "***Next***".

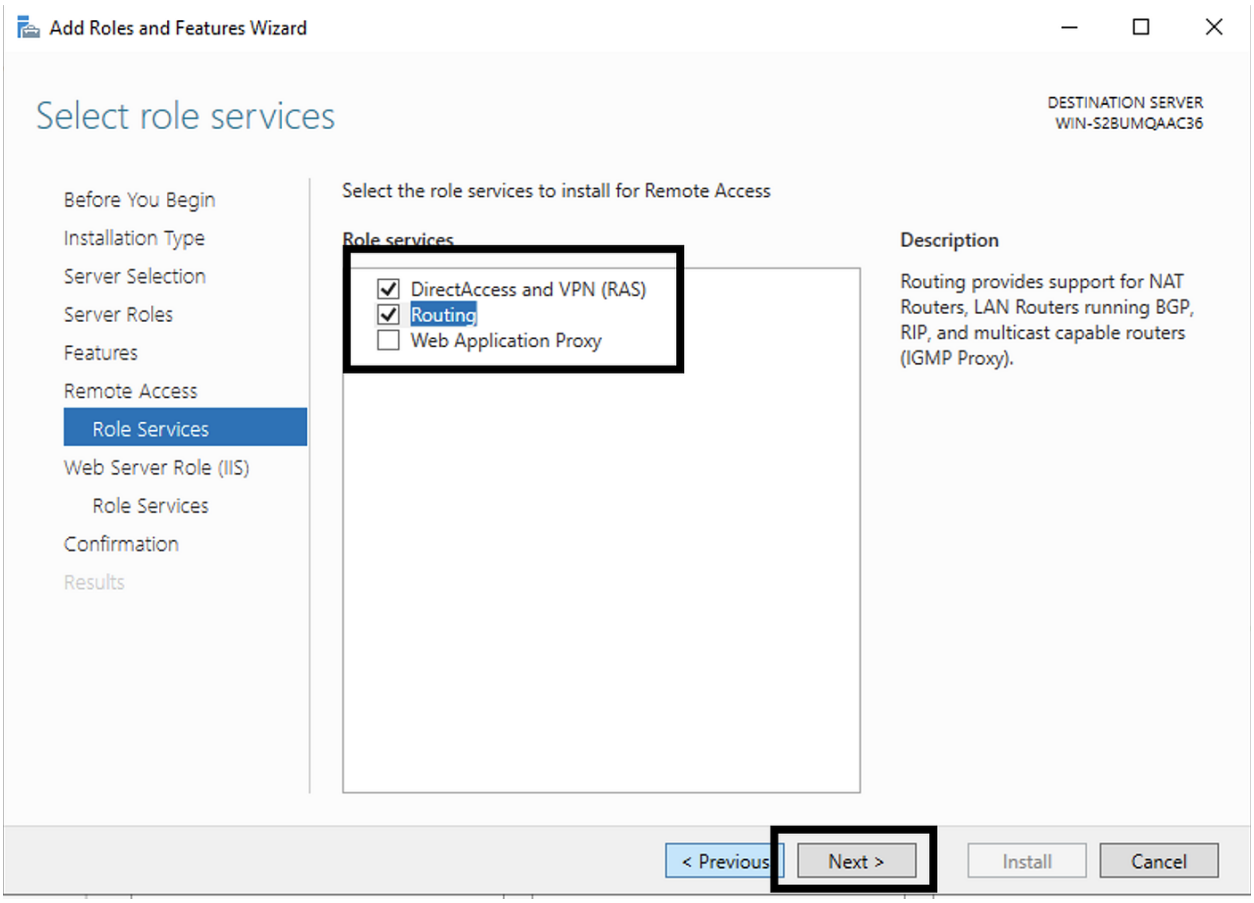

Figure 44

A Wizard will pop up. Click on "***Include Management Tools***" and then click "***Add Features***"

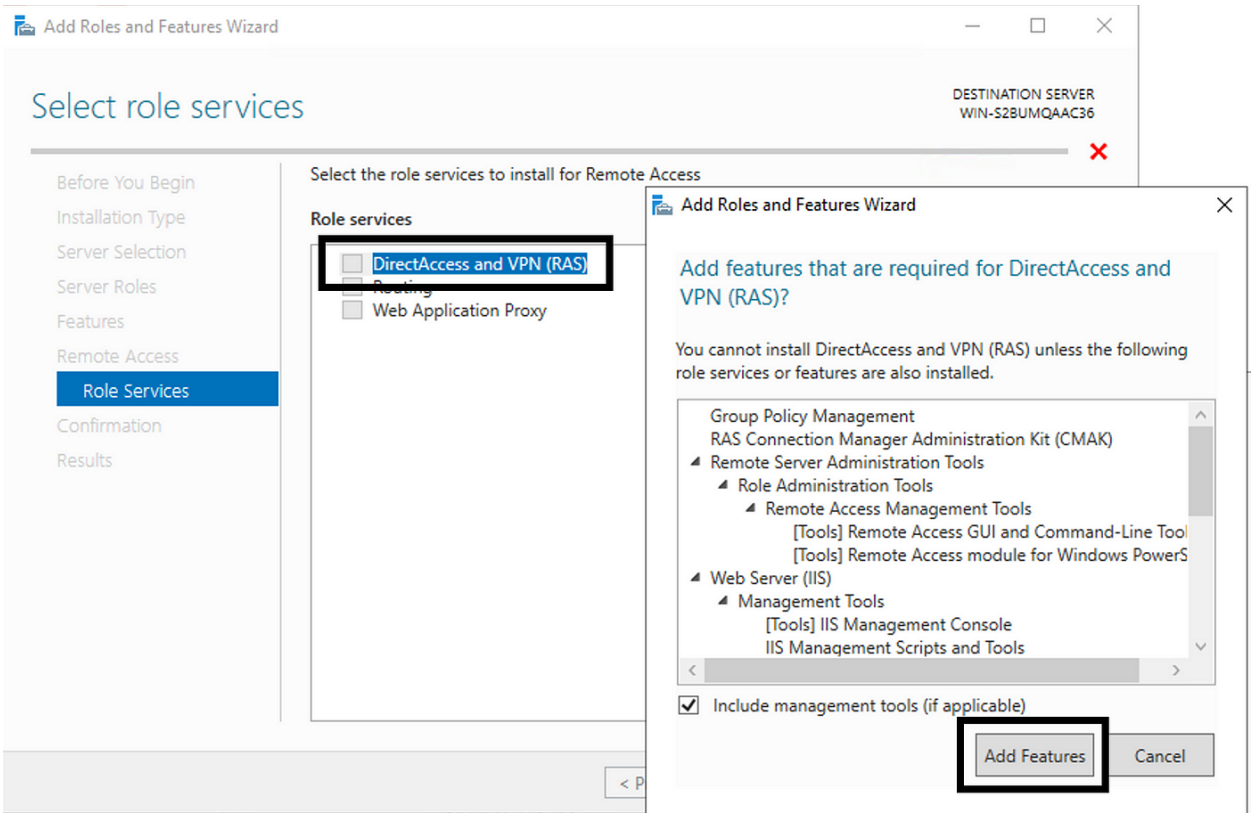

Figure 45

On "***Web Server Role***" click "***Next***".

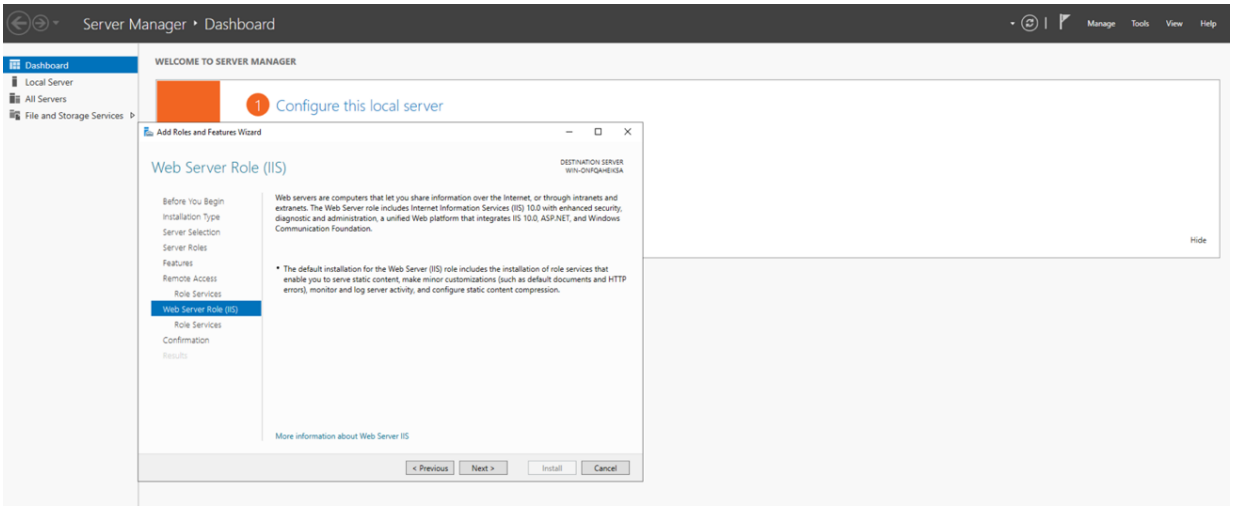

Figure 46

Keep the default Role Services and click "***Next***".

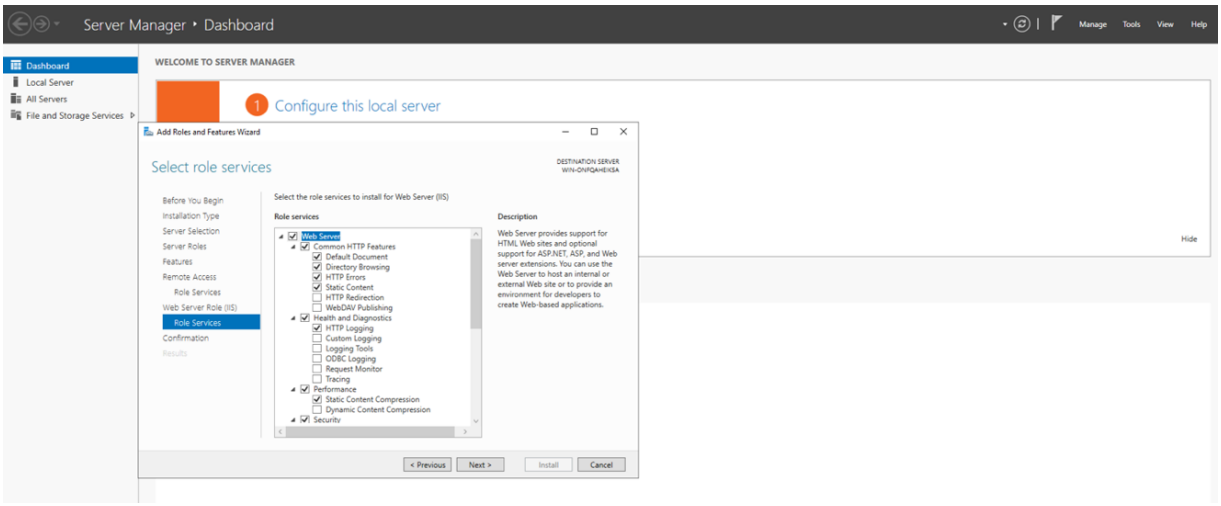

Figure 47

Click "***Install***". A "***Starting installation***" progress bar will appear at the top. Wait for it to complete.

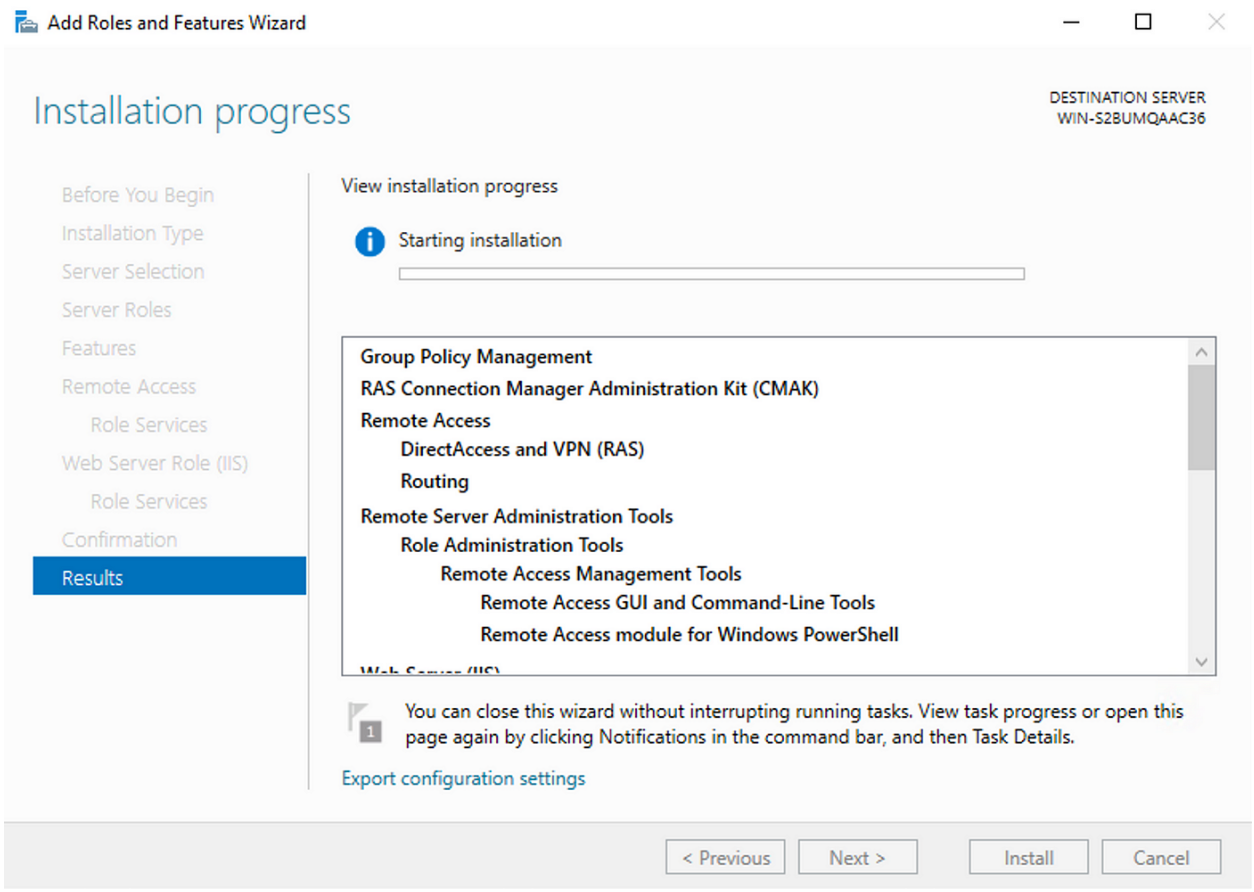

Figure 48

After the progress bar completes, click "***Close***".

8.9.2. Configure the Routing Software

From the Server Manager Dashboard, Go to the top menu bar and click "***Tools***" in the upper right-hand corner to configure the router.

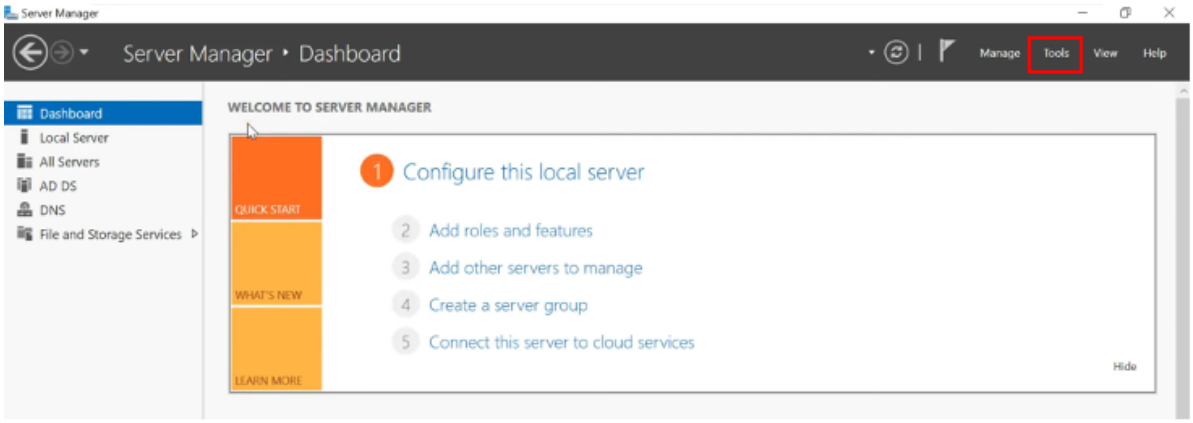

Figure 49

Click "***Routing and Remote Access***"

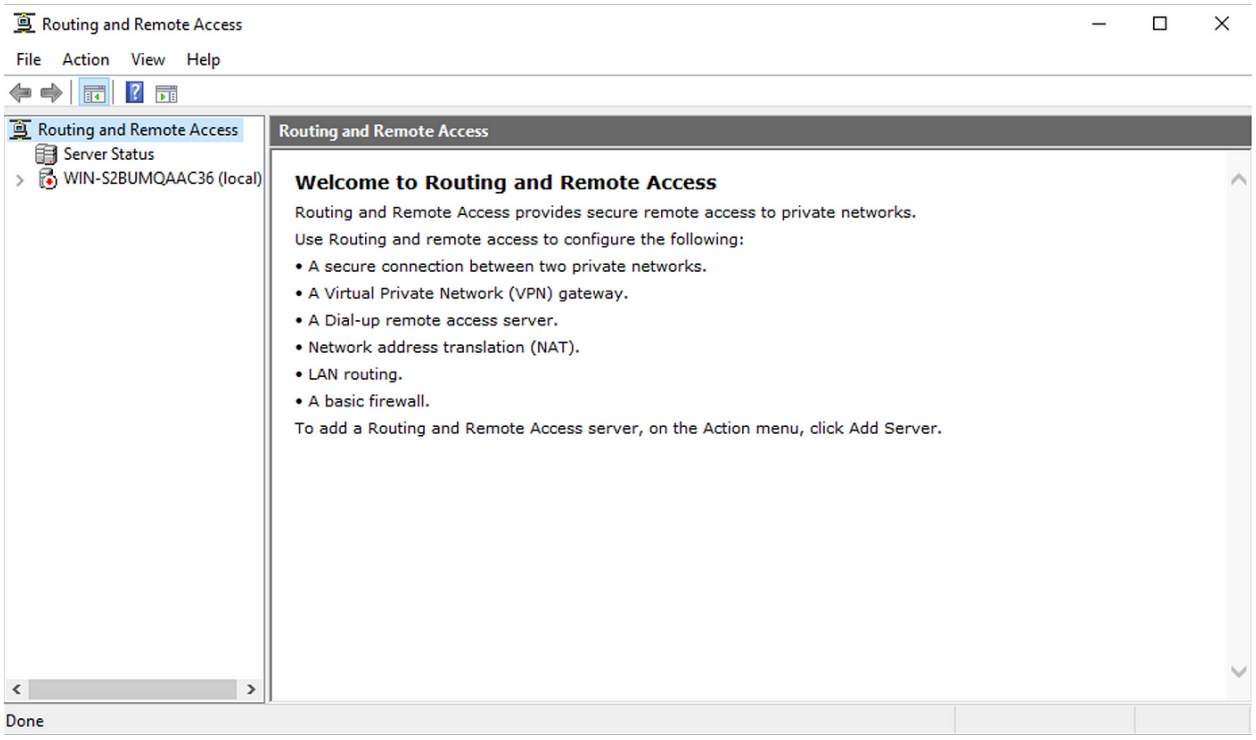

Figure 50

In the left hand column, select the current server and then ***Right click*** on the Server Name and select "***Configure and Enable routing and Remote Access***" from the drop down menu.

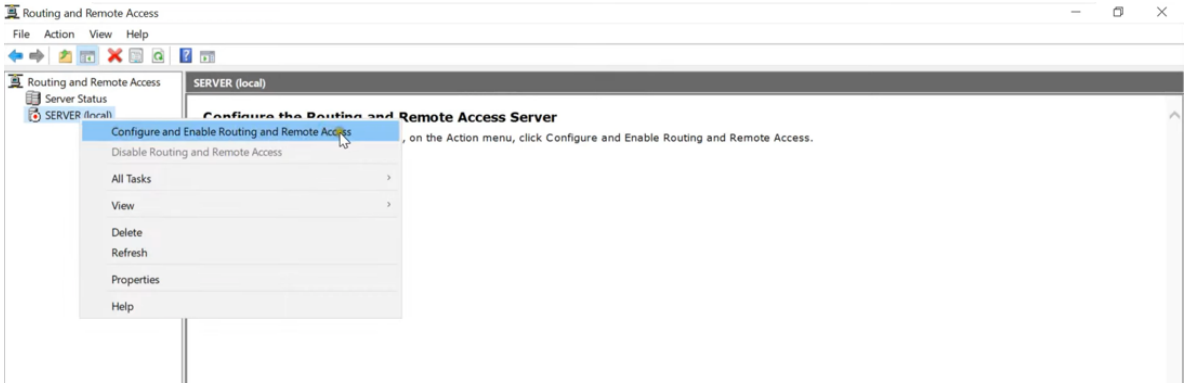

Figure 51

Click "***Next***" on the first screen.

Select "***Custom Configuration***" and then click "***Next***".

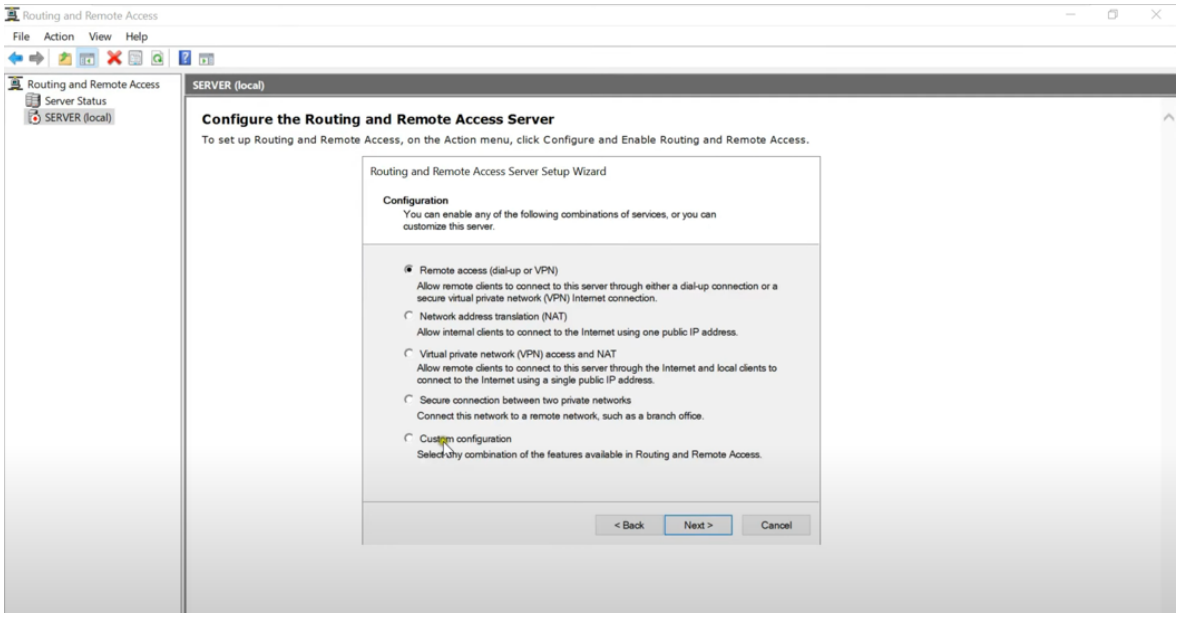

Figure 52

Select "***LAN Routing***" and click "***Next***".

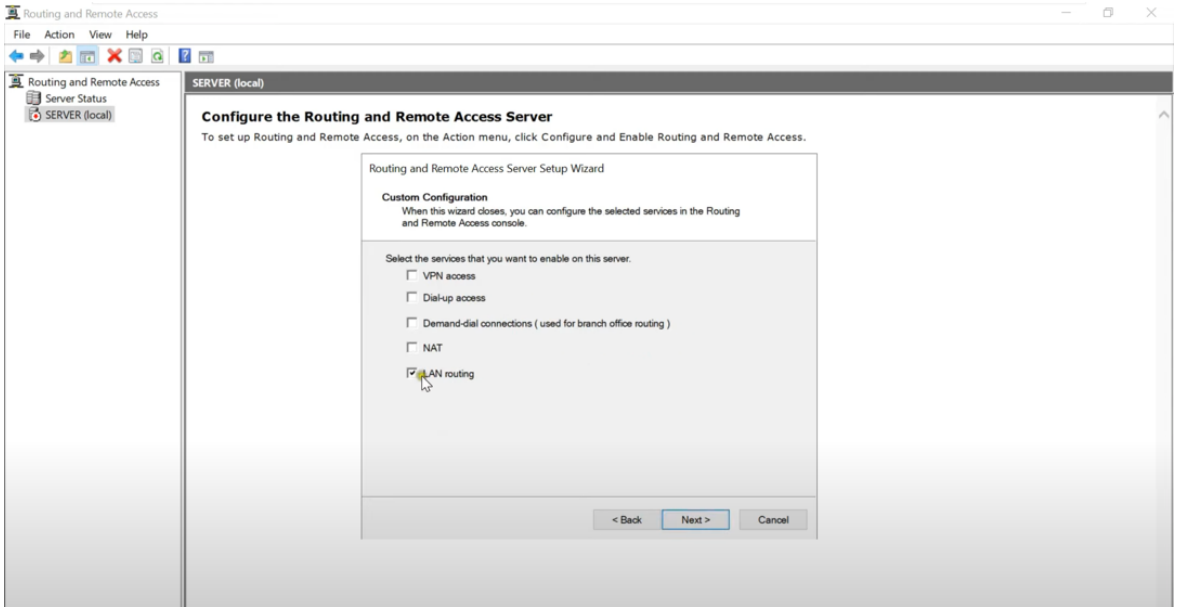

Figure 53

Finally click "***Finish***".

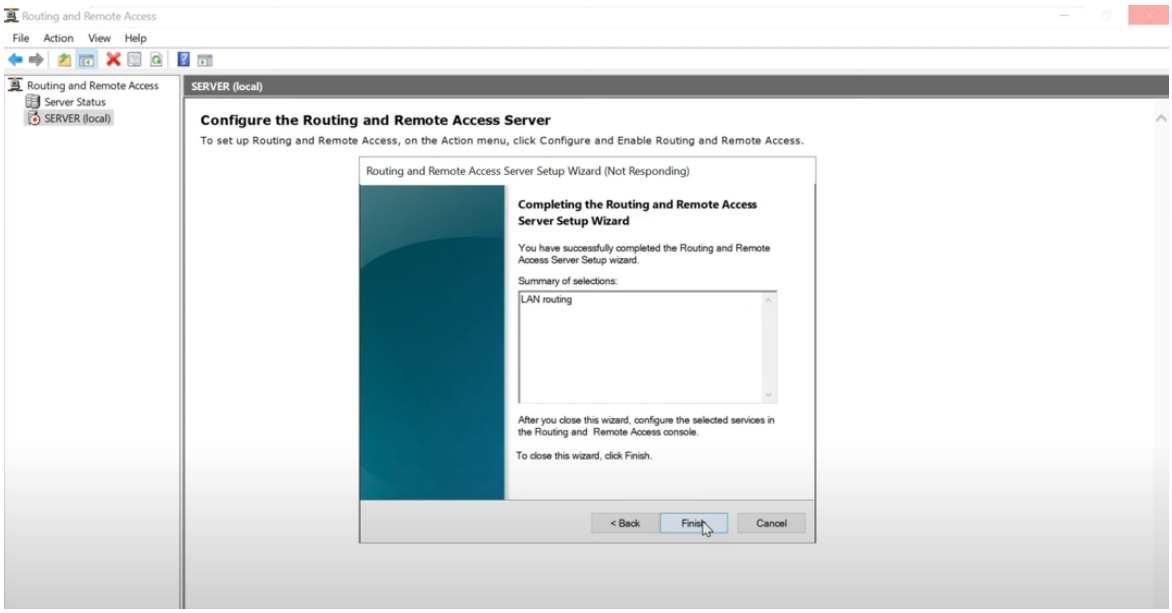

Figure 54

If you see an warning message, click "**OK**" as this Server is *not* being configuring to provide VPN service, and this warning is not applicable.

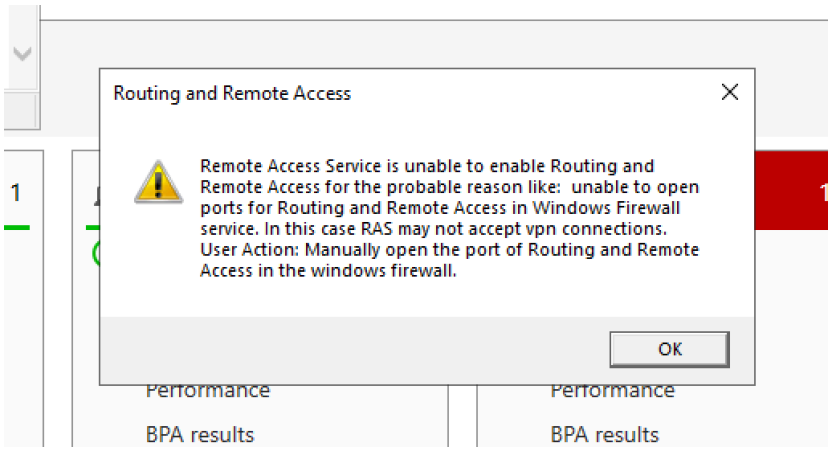

Figure 55

When prompted, Click "***Start service***" to start the service.

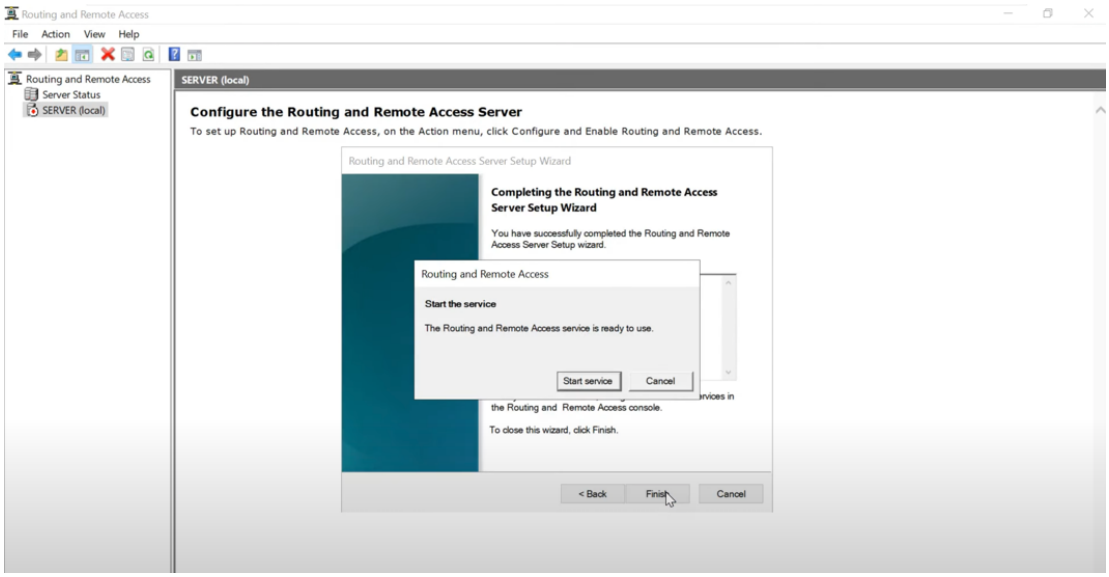

Figure 56

Routing is now installed and configured.

8.10. Maintaining WS HyperSpace Server Software

8.10.1. Update on Linux Server

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

```
# sudo dnf update -y hyperspace
```

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

8.10.2. Update on Mac OS or Windows

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

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

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

9. Uninstall and Deactivation

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

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

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

10. FAQ

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 HyperSpace. What should I do?

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

A: The first thing a WS HyperSpace 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 WS HyperSpace or any WhiteStar tools. If the administrator wants to completely remove the user from the system, they can use the Zeroize feature available to them in the dashboard.

Q: How can I contact customer support?

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

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

A: WhiteStar Trusted Team Tags are unique identifiers, created by your organization's administrator, to identify an individual user, or team of users, within the support organization. This Trusted Team Tag is then used by a customer to grant access to a device within their network – thus permitting **only** that user, or team, the ability to connect to their WS HyperSpace Server device. A Trusted Team Tag asserts (to your customer) that your company

and users are a trustworthy entities capable of accessing their devices. Any attempt to connect to a device without the correct Trusted Team Tag in place results in a failed connection attempt.

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

A: The email address generated synthetically during initial setup of your WS HyperSpace server 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 server 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 server. Keep in mind, only once a Tag is added to the server can anyone with that Tag access the server, and only users with that Tag may access the server. Servers can have multiple Tags with multiple permission sets (IE: one Tag allows access to the top levels of a file directory, whereas another Tag may only allow access to a restricted subfolder and not allow the user to "go higher" in the directory tree).

Q: What's a "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 server, the command "**Zero**" will cause the server to Zeroize, and the WS HyperSpace client 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".

11. Troubleshooting

I cannot connect to a WS HyperSpace Server device

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

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

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

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

The WS HyperSpace Client won't launch

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

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

Terminate the current instance of the WS HyperSpace Client Shell and restart. If, after restarting, you still cannot interact with the WS HyperSpace Client Shell, it may be because there is another user currently connected to the WS HyperSpace Server you attempted to

connect to. Check with other team members, who are also permitted to connect to this Server devices, to ensure they are not currently connected.

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

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

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

I cannot add more members to my WhiteStar dashboard

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

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

12. Glossary

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

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