

Orchid Fusion VMS Installation Guide

23.12 — Last update: 1 March 2024

IPConfigure

Table of Contents

About the Orchid Fusion VMS Installation Guide	4
Working in Windows.....	5
Installing Orchid Fusion VMS in Windows	6
How to Edit a Configuration File in Windows	10
How to Manage the Orchid Fusion VMS Services in Windows	12
Uninstalling Orchid Fusion VMS for Windows	14
Working in Ubuntu 16.04 to 22.04	15
Installing Orchid Fusion VMS on Ubuntu 16.04 to 22.04	16
How to Edit a Configuration File in Ubuntu 16.04 to 22.04	26
How to Manage the Orchid Fusion VMS Services Through the Command Line	29
Uninstalling Orchid Fusion VMS in Ubuntu 16.04 to 22.04	31
Working in Red Hat	32
Installing Orchid Fusion VMS in Red Hat Enterprise Linux 7	33
How to Edit a Configuration File in Red Hat	35
How to Manage the Orchid Fusion VMS Services in Red Hat.....	38
Post-Installation Steps in Red Hat.....	40
Uninstalling the Orchid Fusion VMS Package in Red Hat.....	41
Installation Support Topics	42
Orchid Fusion VMS Configuration Settings	43
Orchid Fusion VMS and Java	52
Orchid Fusion VMS Firewall/Ports Configuration	54
Enabling Google Authentication	56
Enabling Active Directory	58
Enabling Azure Active Directory	61
Detailed Steps for Configuring Azure Active Directory	63
Enabling FreeIPA Authentication	74
Enabling Single Sign-On with SAML	76
Modify the Fusion Configuration File	77
Configuring an Identity Provider	79
Identity Provider: Google Workspace.....	81
Identity Provider: Microsoft Entra ID (formerly Azure AD)	83
Identity Provider: Auth0	86
Identity Provider: Ping	89
Assigning Permissions to SAML Users	91
Enabling External Cloud Storage	93
Orchid Fusion VMS APPs	95
Creating a Superuser	97
Linux Tips & Tricks	99

Important Directories and Files	100
---------------------------------------	-----

About the Orchid Fusion VMS Installation Guide

The Orchid Fusion VMS Installation Guide is designed for IPConfigure dealers, integrators, or system administrators who are tasked with software installation. In addition to installation instructions, this guide provides assistance with editing configuration files, working with the Orchid Fusion VMS services, and uninstalling the Orchid Fusion VMS software.

This guide covers Orchid Fusion VMS installation and configuration topics for the following operating systems:

- Windows
- Ubuntu 16.04 to 22.04 (LTS versions) (Refer to Ubuntu 16.04 LTS)
- Red Hat Enterprise Linux 7 and 8, 64-bit (Refer to Red Hat Enterprise Linux 7)
- CentOS 7 and 8 (Refer to Red Hat Enterprise Linux 7)
- Debian Jessie (Refer to Ubuntu 16.04 LTS)
- Raspbian Jessie (Refer to Ubuntu 16.04 LTS)

This guide also includes general, helpful information in the *Installation Support Topics* section.

✿ Downgrading the Orchid Fusion VMS software is not supported.

✿ As of version 21.9, Orchid Fusion VMS no longer provides installers for Ubuntu 14.04.

✿ You may notice that there are very few mentions of Orchid Hybrid VMS in this guide (even though the Orchid Fusion VMS User Guide and Admin Guide cover both Fusion and Hybrid). Since Orchid Hybrid VMS is a managed system, IPConfigure will perform the Hybrid installation and the configuration that is required for some special features.

Working in Windows

IPConfigure distributes a single Windows installer that is valid for all 64-bit versions of Windows 7 and up, as well as 64-bit Windows Server 2008 R2 and up.

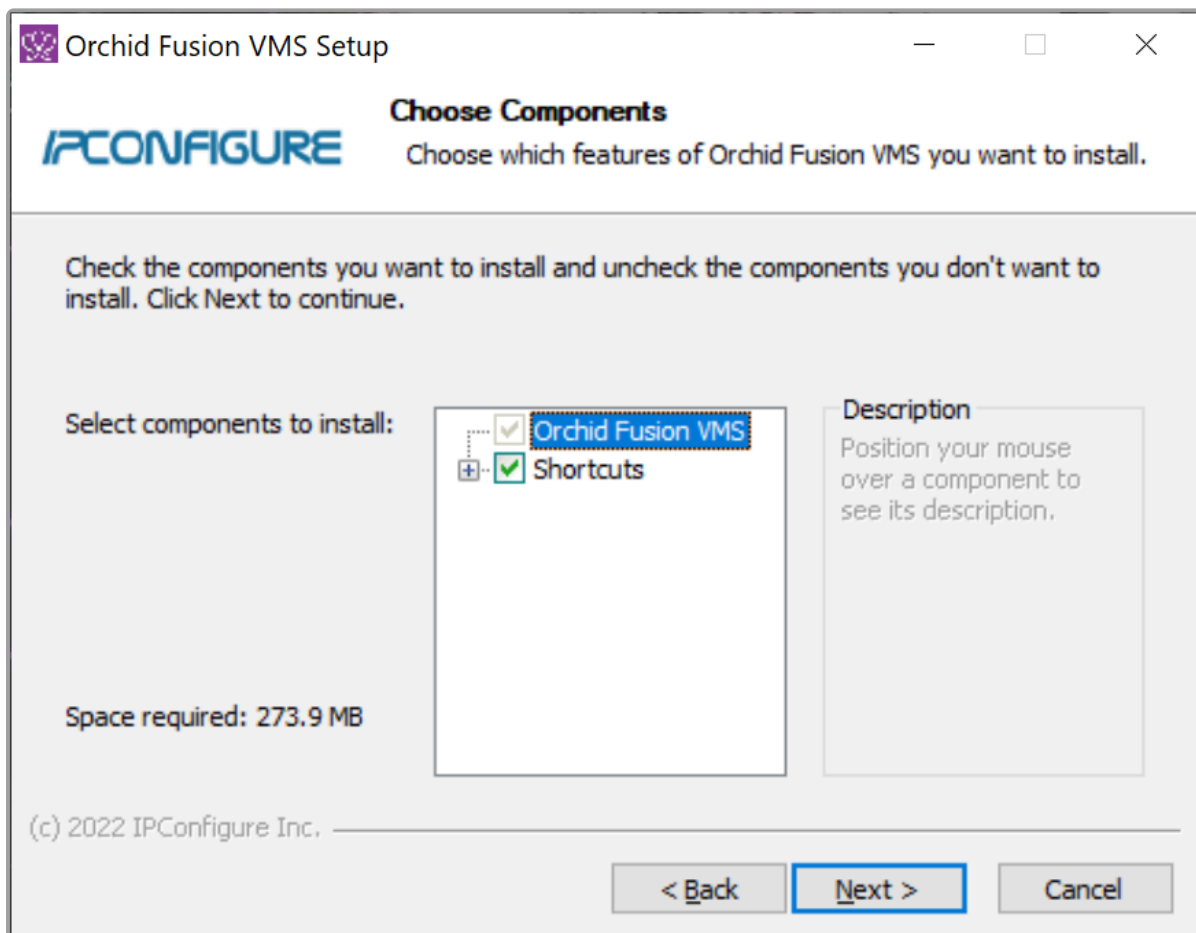
✿ Orchid Fusion VMS can only be installed on a 64-bit operating system; it is not compatible with 32-bit operating systems.

✿ You must sign in to the computer as a user with administrative privileges.

✿ If you are performing an upgrade of your Orchid Fusion VMS, you should check to make sure that all of the registered Orchid Recorders are running, at minimum, Orchid version 2.8.0. (You will receive a warning message during the installation if this is not the case.)

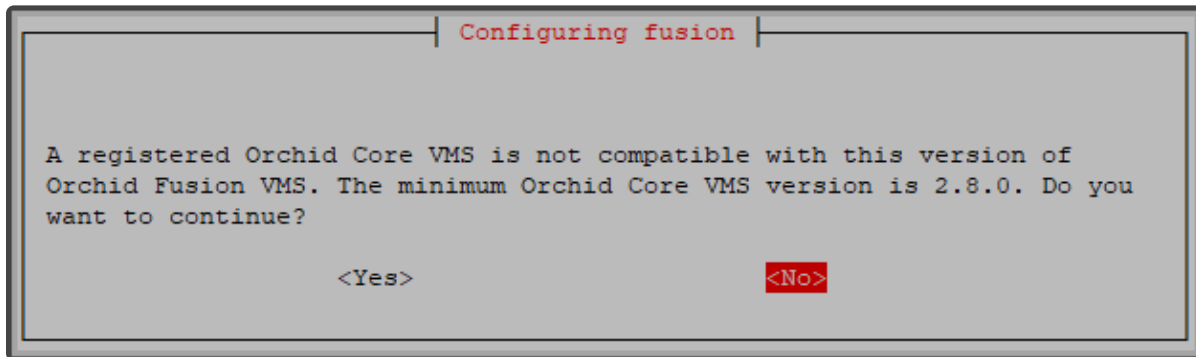
Installing Orchid Fusion VMS in Windows

1. Download the Orchid Fusion VMS executable file. You can find the latest version of the Orchid Fusion VMS on IPConfigure's website at <http://www.ipconfigure.com/download>.
2. Open the Orchid Fusion VMS executable file. You will be asked to allow the installer to make changes to your computer. Click **Yes** to allow the installer to open.
3. Before proceeding with the installation, close all other applications, then click **Next** to continue.
4. You will be asked to accept the End-User License Agreement. After reading the agreement, click the **I Agree** button to accept it.
5. You will be asked to select the components you want to install. *Orchid Fusion* and *Shortcuts* will already be checked.

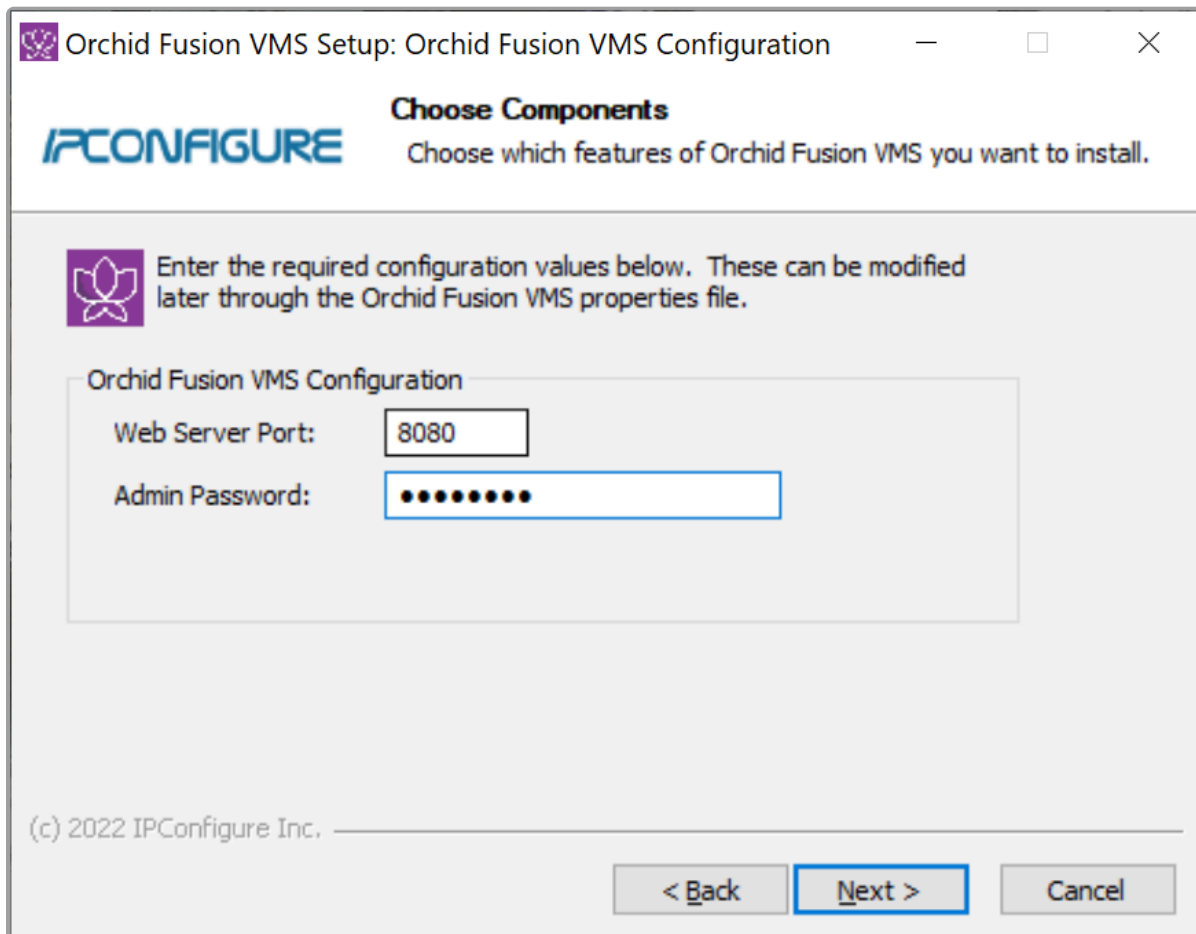


- **Orchid Fusion VMS:** This is the Orchid Fusion VMS application.
 - **Orchid Fusion VMS Rclone Service:** This service (although not pictured here) is installed automatically. Orchid Fusion VMS uses this service to enable exporting *Library* files to an external cloud storage location, if configured to do so.
 - **Shortcuts:** This installs shortcuts on the computer to open the Orchid Fusion VMS user interface in a web browser.
6. Click the **Next** button to proceed with the installation for all selected components.

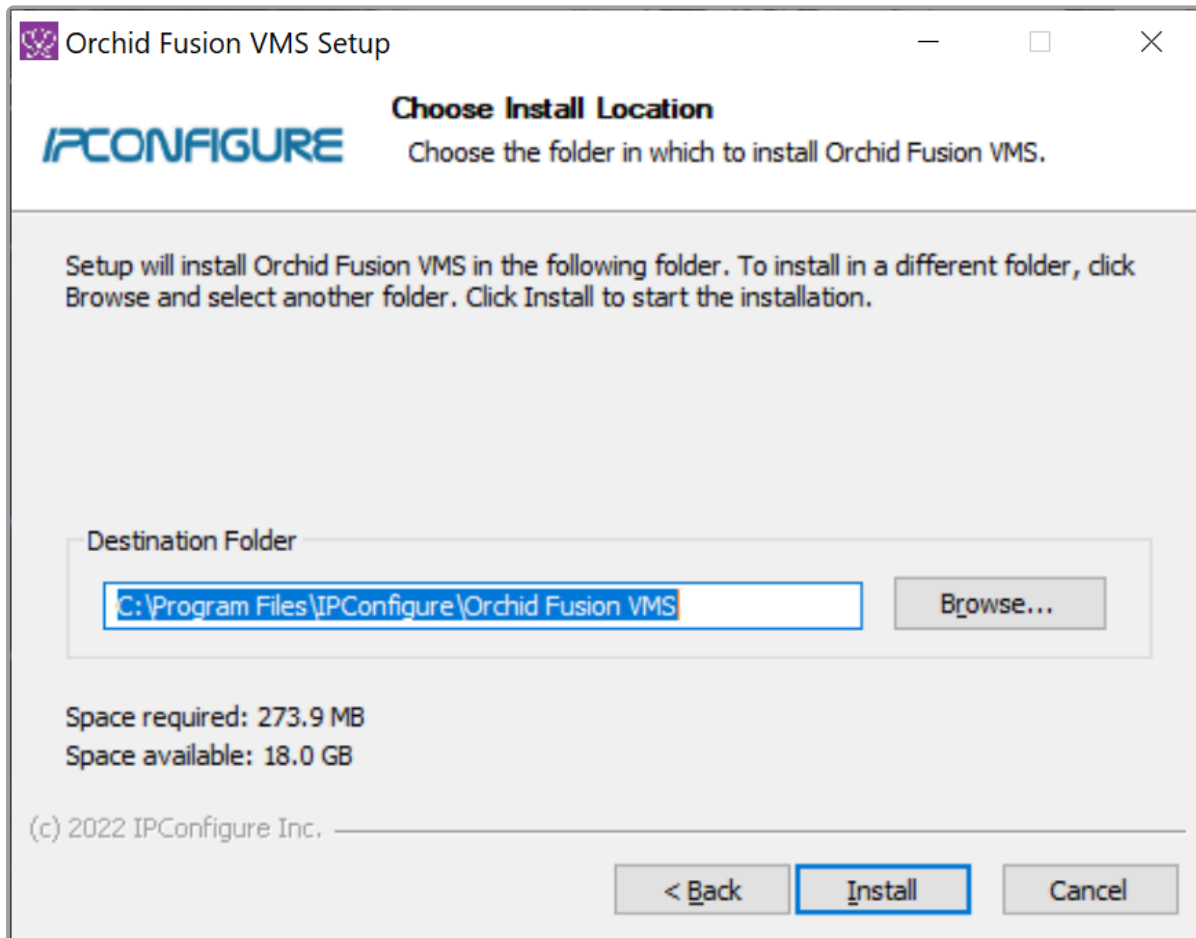
7. If you are performing an upgrade, and any of the registered servers have an Orchid version number older than 2.8.0, you will receive a warning message similar to the one pictured below.



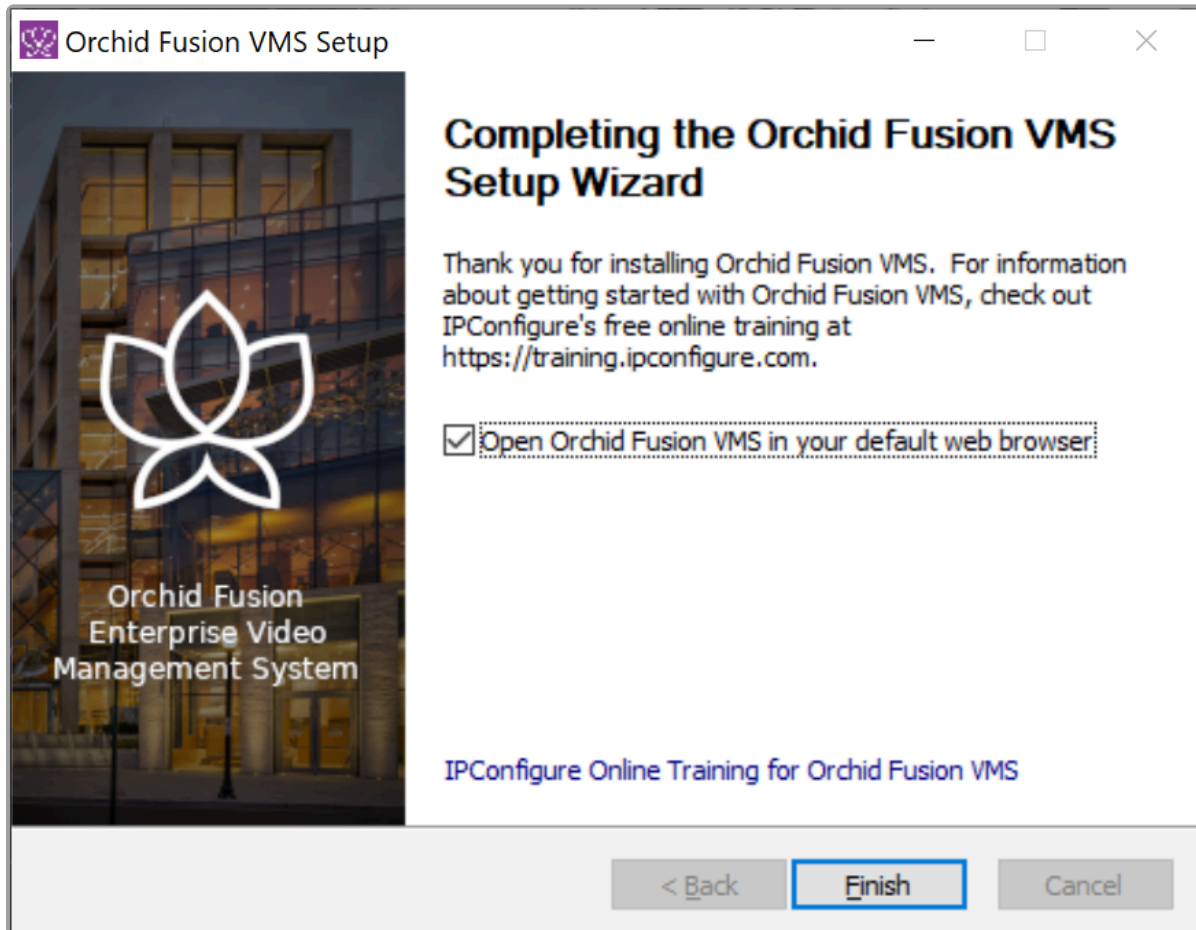
- You will need to upgrade older Orchid Recorders before they will work in this new version of Orchid Fusion VMS.
 - Click the **OK** button to acknowledge this warning. The software installation will begin. (Proceed to step 12.)
8. If this is a first-time installation, the installer will ask you to set the Web Server Port and the Admin Password.



- By default, the web server port is set to port 8080 (recommended for most installations). Update the port number only if Orchid Fusion VMS needs to use a port other than 8080.
 - Enter the password you would like to set for the default admin account in the *Admin Password* field.
9. Click the **Next** button to continue.
 10. The installer will ask you to confirm the installation folder. By default this is *C:\Program Files\IPConfigure\Orchid Fusion VMS* and does not need to be changed. However, the installation directory can be updated, if needed.



11. Click the **Install** button to proceed with the installation. The installation will complete automatically without any additional prompts. This process may take a few minutes.
12. Once the installer says "Completing" at the top of the window, mark the *Open Orchid Fusion...* checkbox if you want to open Orchid Fusion VMS in your default web browser upon exit.



13. Click the **Finish** button to close the installer. Orchid Fusion VMS will automatically open in the computer's default web browser (if so marked). (For more details on signing in, please refer to the *Enabling ...* topics included in the [Installation Support Topics](#) section, and the *Sign In* topic in the [Orchid Fusion VMS Administrator Guide](#).)

How to Edit a Configuration File in Windows

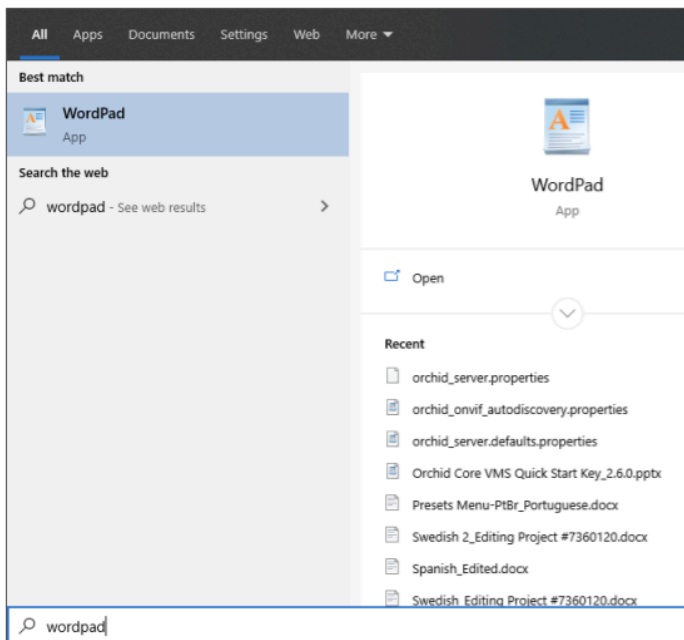
The default location for the Orchid Fusion VMS configuration file in Windows is:

- *C:\Program Files\IPConfigure\Orchid Fusion VMS\conf\fusion.properties*
 - Stores all of the Orchid Fusion VMS default settings and can be used to update things like the Orchid Fusion VMS port number, manually update the admin password, etc.

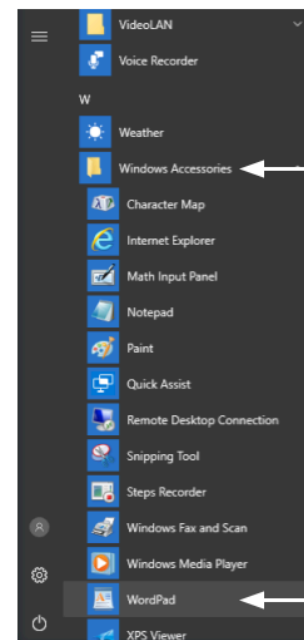
Refer to the [Installation Support Topics](#) section for a list of available properties.

✿ In order to edit the Orchid Fusion VMS configuration file, you will need to be signed in as a user with administrative privileges.

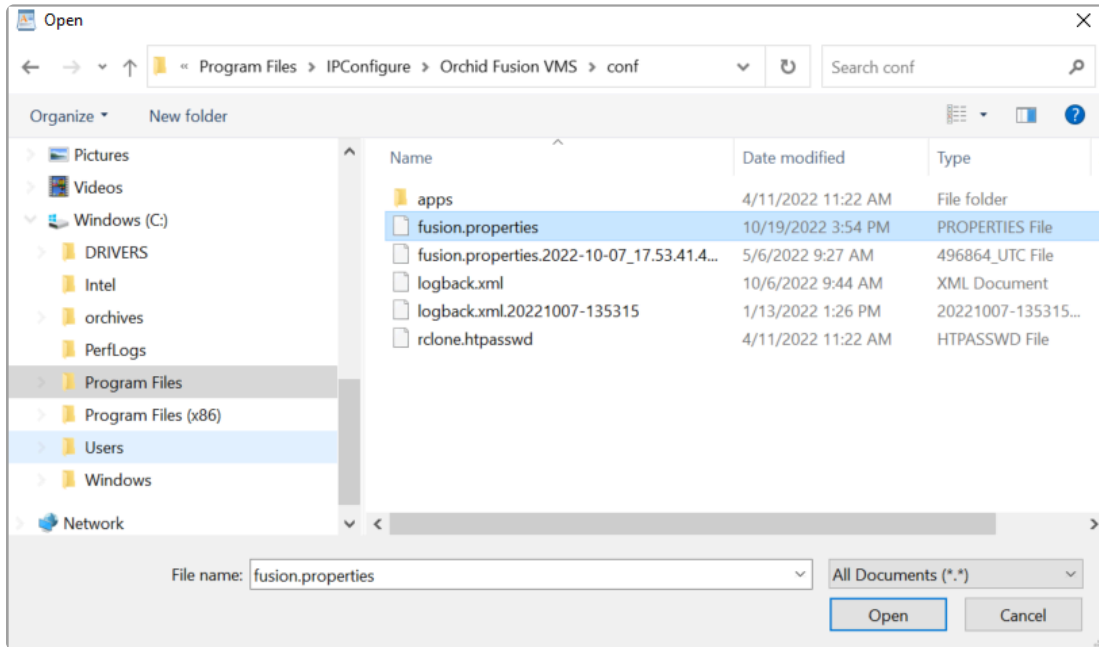
1. Open the Windows Start Menu and type **Wordpad** into the search bar, or go to *Windows Accessories*, then select *WordPad*.



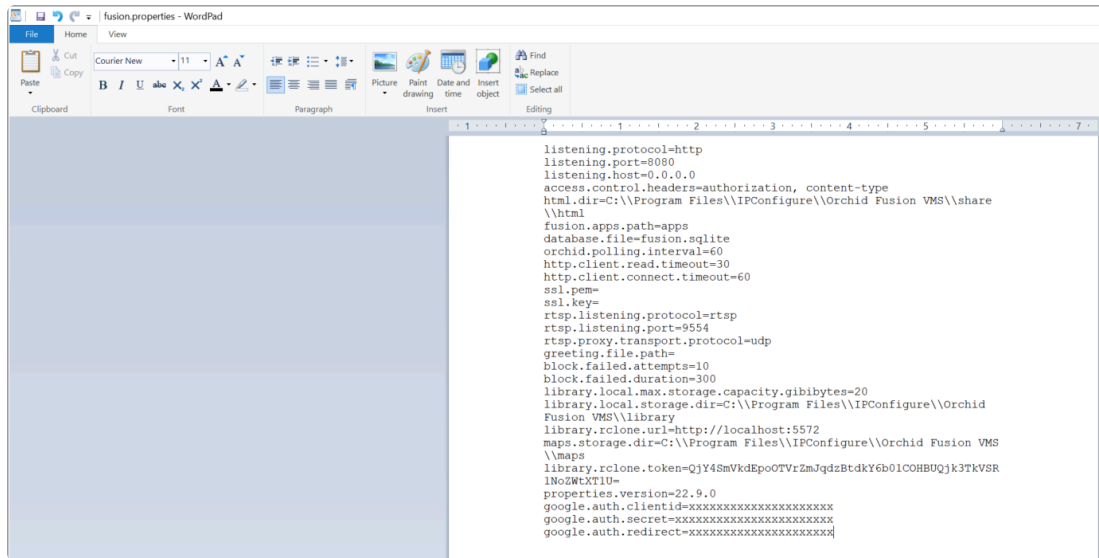
- OR -



2. Right click on the **WordPad** icon and click Run as administrator.
3. Click the **Yes** button to let WordPad make changes to the computer.
4. Select **File/Open**, then navigate to the *fusion.properties* file. (If no files appear, ensure the *All Documents* option is selected.)



5. Select the file and click the *Open* button.
6. The file will open in WordPad. Make setting changes as necessary.



7. When you are ready to save the file, select *File/Save* to save the configuration file.
8. You must [restart](#) the Orchid Fusion VMS service in Windows to implement the new settings.

✿ Some of the Orchid Recorder configuration settings can be edited from within the Orchid Fusion VMS user interface. (This is done using the *Advanced Settings* feature which is explained in the [Orchid Fusion VMS Administrator Guide](#).) To edit the Orchid Recorder configuration file using standard text editors in Windows, please refer to the [Orchid Recorder Installation Guide](#).

How to Manage the Orchid Fusion VMS Services in Windows

The following services are used by Orchid Fusion VMS in Windows. If you need to check the status, start, or stop the service, you can do this through the *Services Manager* whenever necessary.

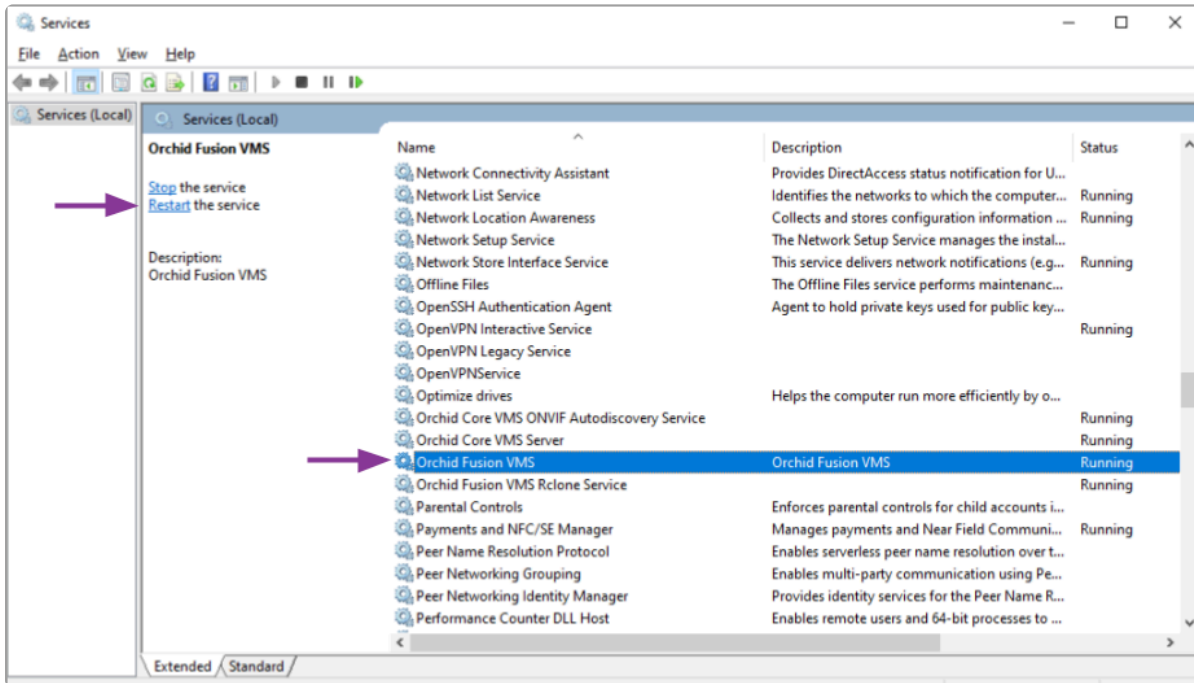
- **Orchid Fusion VMS:** This service supports the Orchid Fusion VMS server that manages registered Orchid Recorders and provides access to video from those servers.
 - You will need to restart this service whenever a change has been made to the Orchid Fusion VMS configuration file.
- **Orchid Fusion VMS Rclone Service:** This service supports Fusion's ability to export video files to an external cloud storage location, via the Rclone open-source library.
 - You will need to restart this service if you re-run the Rclone executable.



You must be signed into the computer as a user with administrative privileges in order to use the *Services Manager*.

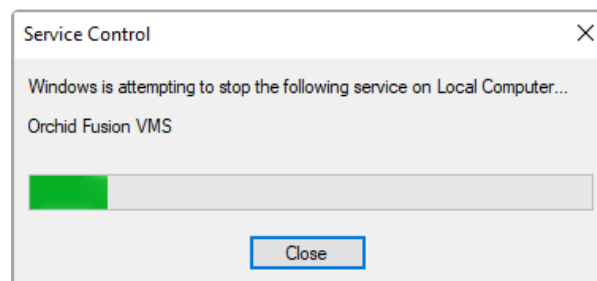
To manage the Orchid Fusion VMS service:

1. Open the Windows Start Menu and type *Services* into the search bar, or go to *Windows Administrative Tools*.
2. Click the **Services** icon to open the *Services Manager*. The *Services Manager* will display a list of all the services setup in Windows.



3. Scroll through the list and click on the service you need to work on: the *Orchid Fusion VMS* service or the *Orchid Fusion VMS Rclone Service*. (Notice that the status of the service will appear in the *Status* column.)
4. Click the **Restart the service** button/link (at the left of the list of services) to restart the service. (Click the **Stop the service** link if you need to stop the service.)

A status window will appear to show the progress of the restart. Once the service has restarted successfully, the software will return to the *Services Manager* window; the *Status* column will indicate that the service is *Running*.



Uninstalling Orchid Fusion VMS for Windows

To remove the Orchid Fusion VMS software, follow the steps below. (This will remove all files installed and created by Orchid Fusion VMS.)

1. To uninstall Orchid Fusion VMS, locate the uninstall file on the computer. The default location for this file is *C:\Program Files\IPConfigure\Orchid Fusion VMS\uninstall.exe*.
2. Double-click on the uninstall file.
3. Click the **Yes** button to allow the application to make changes to the computer.
4. Click the ***Uninstall*** button to proceed with the uninstall process. This may take a moment.
5. Once the uninstall is complete, click the ***Close*** button to exit.

Working in Ubuntu 16.04 to 22.04

IPConfigure distributes Orchid Fusion VMS for Ubuntu through debian package files (.deb files). The recommended method for installing the package file is through GDebi Package installer. GDebi can be used either through command line, or through the Graphical User Interface (GUI).

The installation instructions provided for Ubuntu 16.04 LTS also apply to Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Debian Jessie and Raspbian Jessie. Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, and Ubuntu 22.04 will use the same installation package file. Debian Jessie and Raspbian Jessie will each have a different installation package file.

* Orchid Fusion VMS can only be installed on a 64-bit operating system. If you are currently running a 32-bit operating system, the installer will return an “Architecture not supported” error and Orchid Fusion VMS installation will fail.

* You must sign in to the computer as a user with “root” or “sudo” privileges.

* If you are performing an upgrade of your Orchid Fusion VMS, you should check to make sure that all of the registered Orchid Recorders are running, at minimum, Orchid version 2.8.0. (You will receive a warning message during the installation if this is not the case.)

* Ubuntu 14.04 is no longer supported. The 16.04 installer cannot be used to install Fusion on a system running Ubuntu 14.04.

Installing Orchid Fusion VMS on Ubuntu 16.04 to 22.04

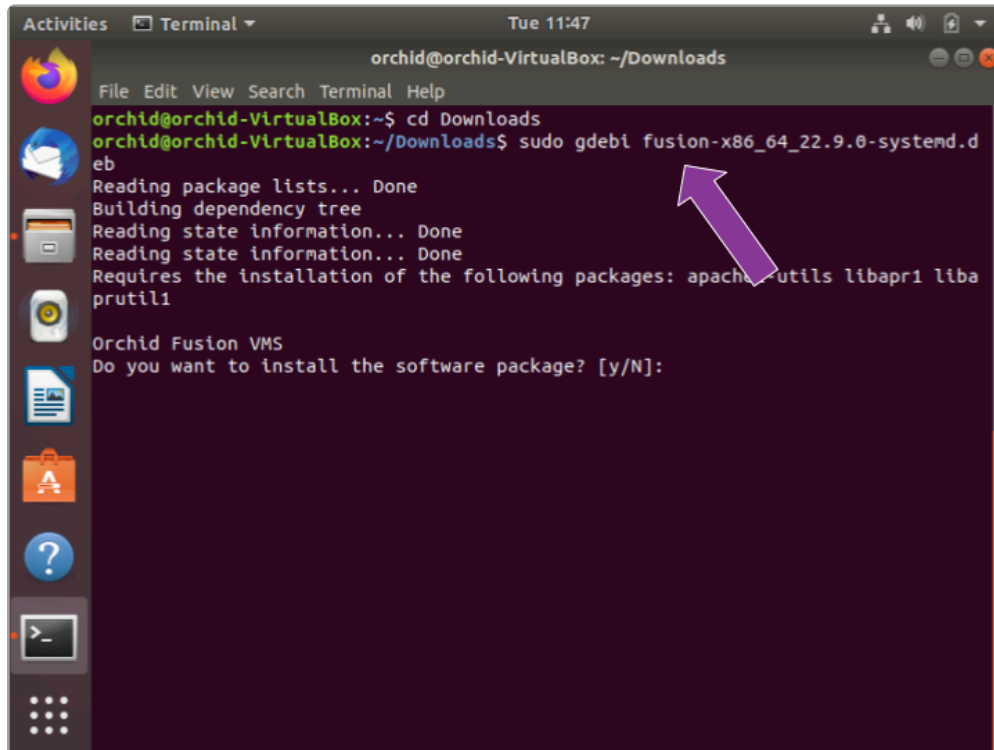
There are a couple of steps you will need to perform to prepare to install Orchid Fusion VMS.

1. Download the Fusion .deb file. You can find the latest version of Orchid Fusion VMS (for Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Debian Jessie, and Raspbian Jessie) on IPConfigure's website at <http://www.ipconfigure.com/download>.
2. Once you've downloaded the Orchid Fusion VMS installation package, decide whether you want to perform the installation via the Command Line or the GUI.

Installing through the Command Line (Ubuntu Server):

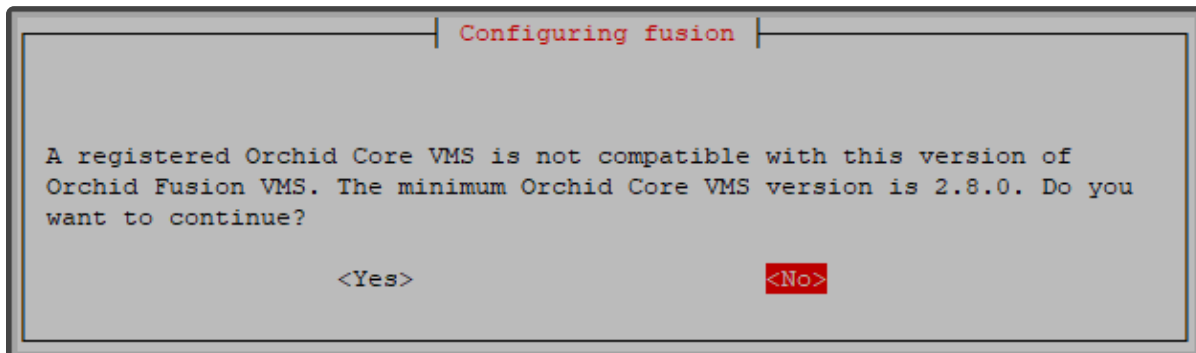
* If you are performing an upgrade of your Orchid Fusion VMS, you should check to make sure that all of the registered Orchid Recorders are running, at minimum, Orchid version 2.8.0. (You will receive a warning message during the installation if this is not the case.) In addition, you should install the Orchid Fusion VMS upgrade using the command line.

1. Open the *Terminal* program (**CTRL+ALT+T**) and navigate to the directory where you downloaded the Orchid Fusion VMS installation package. (The package is probably stored in the *Downloads* folder.)
2. Unless GDebi has been installed manually, it will need to be installed. Type the following command:
`sudo apt-get install gdebi`. Then press **Enter**.
It may take a few minutes for GDebi to install, depending on the speed of your system.
3. The GDebi command can now be used to install the Orchid Fusion VMS debian package. The syntax is `sudo gdebi (package-name).deb`, where *package-name* is the complete filename of the Orchid Fusion VMS installation package that you downloaded. For example, if the name of the package is *fusion-x86_64_22.9.0-systemd.deb*, type the following command: `sudo gdebi fusion-x86_64_22.9.0-systemd.deb`. Then press **Enter**.



```
orchid@orchid-VirtualBox: ~/Downloads
File Edit View Search Terminal Help
orchid@orchid-VirtualBox:~$ cd Downloads
orchid@orchid-VirtualBox:~/Downloads$ sudo gdebi fusion-x86_64_22.9.0-systemd.d
eb
Reading package lists... Done
Building dependency tree
Reading state information... Done
Reading state information... Done
Requires the installation of the following packages: apache-utils libapr1 liba
prutil1
Orchid Fusion VMS
Do you want to install the software package? [y/N]:
```

4. You will be asked if you want to install the software. Respond by pressing **Y** and **Enter**.
- If you are performing an upgrade of your Orchid Fusion VMS, the installer will check the Orchid version numbers on each of the registered Orchid Recorders. If any of the registered servers have an Orchid version number older than 2.8.0, you will receive a warning message similar to the one pictured here.



- Orchid Fusion VMS Setup will ask if you want to continue with the installation. IPConfigure recommends that you select **No**, and upgrade any Orchid Recorders that don't meet the minimum version requirement. When all of your Orchid Recorder upgrades are complete, return to step 3 to install the new Orchid Fusion VMS.
5. You will be asked to accept the End User License Agreement. After reading the agreement, press the **Tab** key, then the **Enter** key to accept it.
 6. You will then be asked to accept the agreement in a separate prompt. Use the **Left Arrow** key to select **Yes**, and press **Enter** to accept it.
 7. The installer will then ask for the web server port number to use for Orchid Fusion VMS.

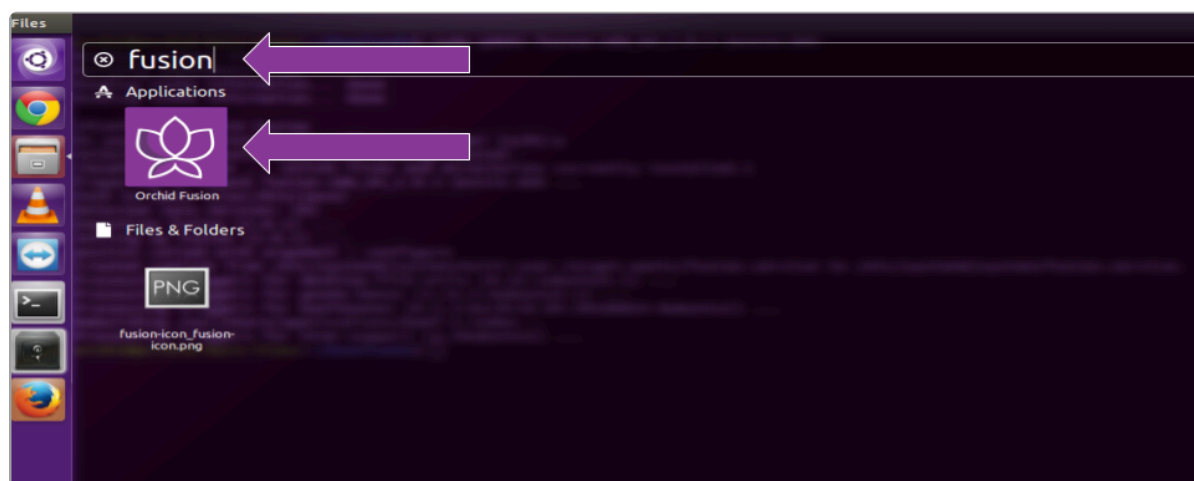
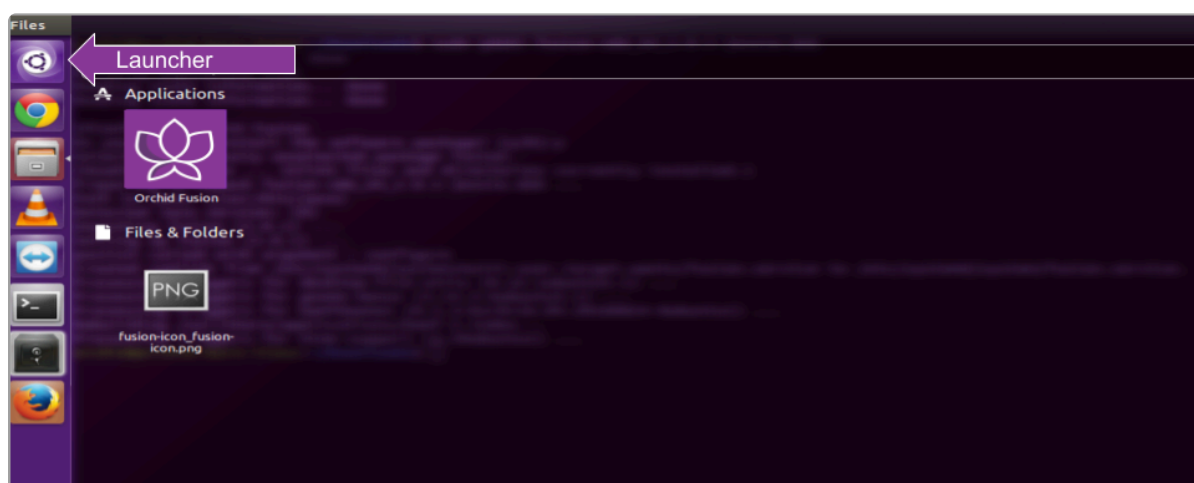
By default, it is set to port 8080 (which is the recommended port for most installations). If Orchid Fusion VMS needs to use a different port, update the port then press the **Enter** key.

8. Enter the password you would like to set for the default admin account, then press the **Enter** key.

The installation will complete automatically without any additional prompts. This process may take a few minutes. The Orchid Fusion VMS service starts automatically once the package installation is done, after which you can access the Orchid Fusion VMS user interface in your web browser. (For more details on signing in, please refer to the *Enabling...* topics included in the [Installation Support Topics](#) section, and the *Sign In* topic in the [Orchid Fusion VMS Administrator Guide](#).)

You may automatically launch a browser to Orchid Fusion VMS using the link installed on your server:

- Click on the **Launcher** icon in the top left corner of the screen. Then type *fusion* in the search box, and click the **Orchid Fusion** icon listed under *Applications*.



- Or, you can click the **Applications** icon (in your favorites or the lower-left corner of the

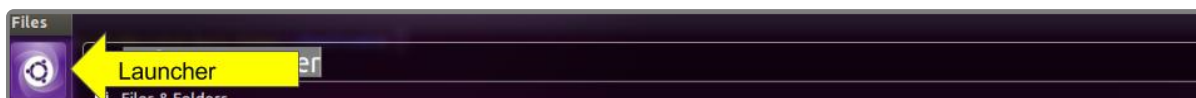
screen), then click on the *Orchid Fusion* icon.

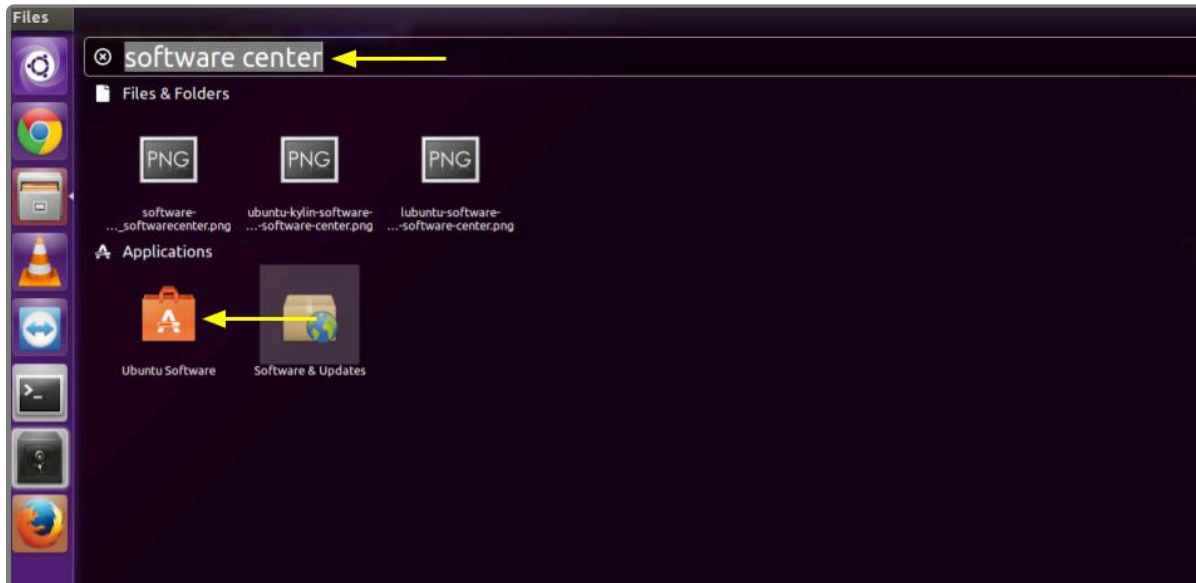


Installing through the GUI (Ubuntu Desktop):

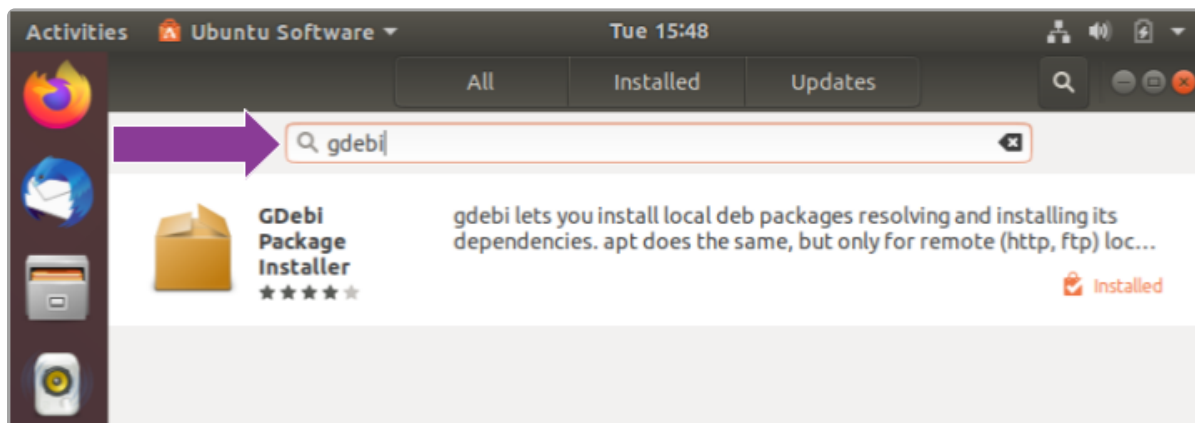
* If you are performing an upgrade of your Orchid Fusion VMS, you should perform the upgrade using the command line.

1. First, we'll need to open the *Ubuntu Software Center*. Here are a couple of ways to do this.
 - a. Click on the *Launcher* icon in the top left corner of the screen. Then type *Software Center* in the search box, and click the *Ubuntu Software Center* icon listed under *Applications*.
 - b. Click the *Applications* icon (in your Favorites list, or in the lower-left corner of the screen). Then click on the *Ubuntu Software Center* icon.

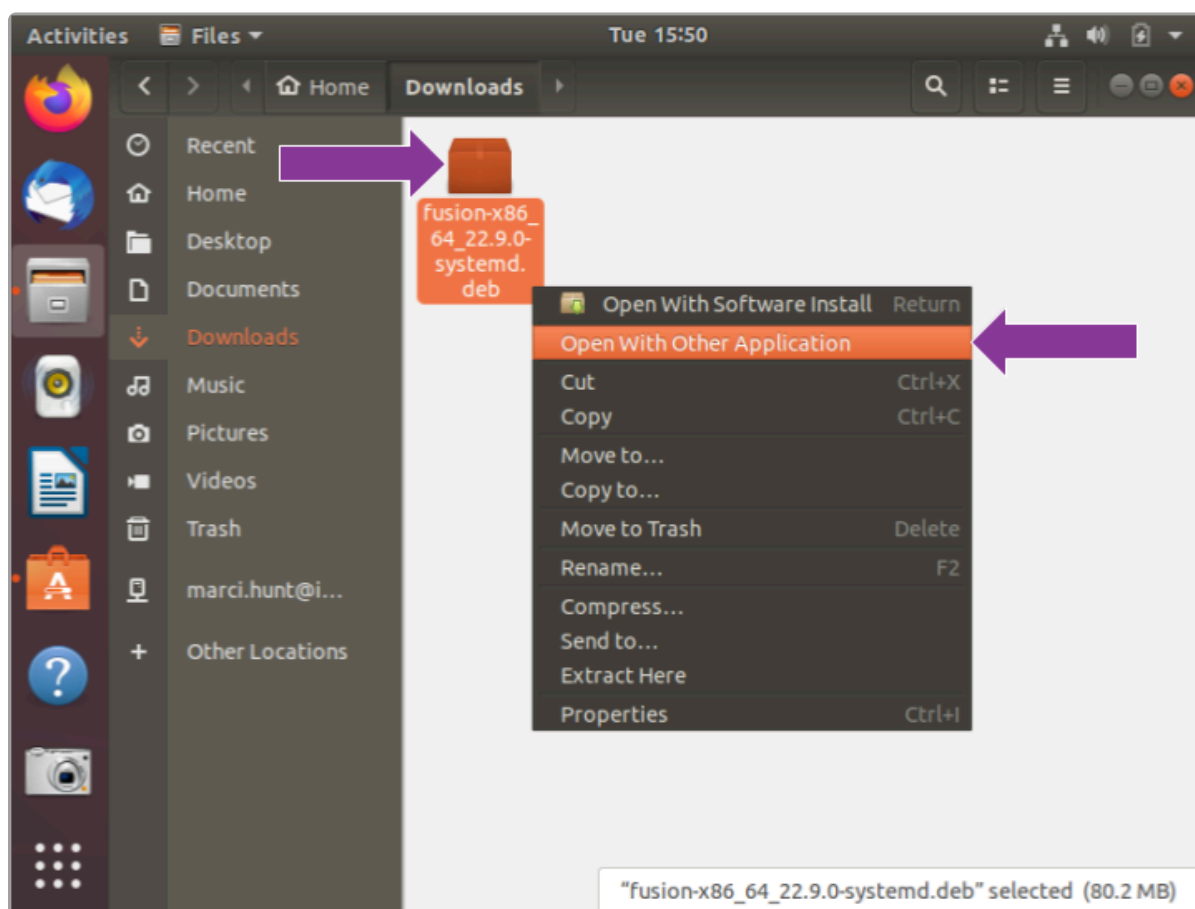


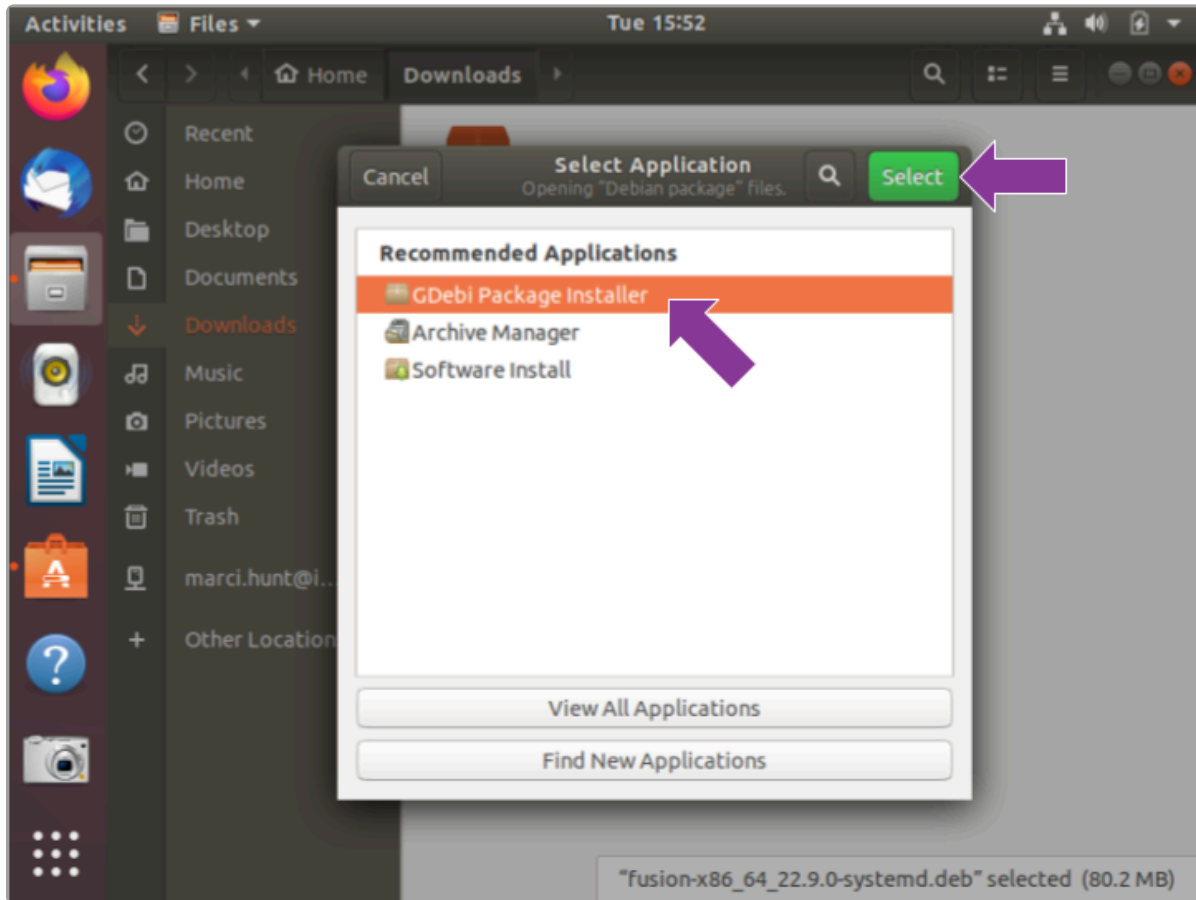


2. In the Software Center search bar (below), type *gdebi*.

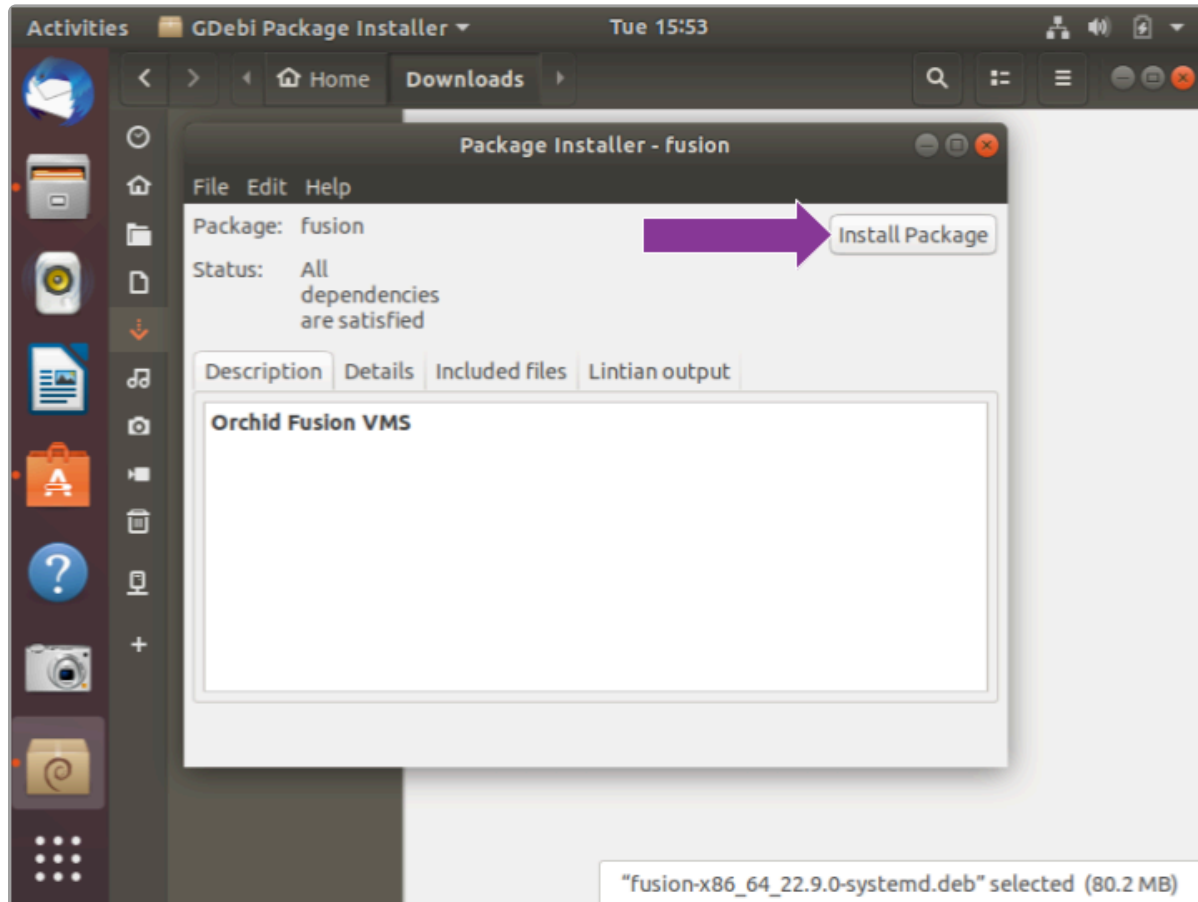


3. Select *GDebi Package Installer (gdebi)*, and then click the *Install* button.
4. After GDebi has finished installing, click the *Files* icon to open the *Files Explorer*, then navigate to the folder storing your Orchid Fusion VMS package (.deb file). (The package is probably stored in the *Downloads* folder.)
5. Right-click on the Orchid Fusion VMS package, select *Open With Other Application*, then select the *GDebi Package Installer* option.

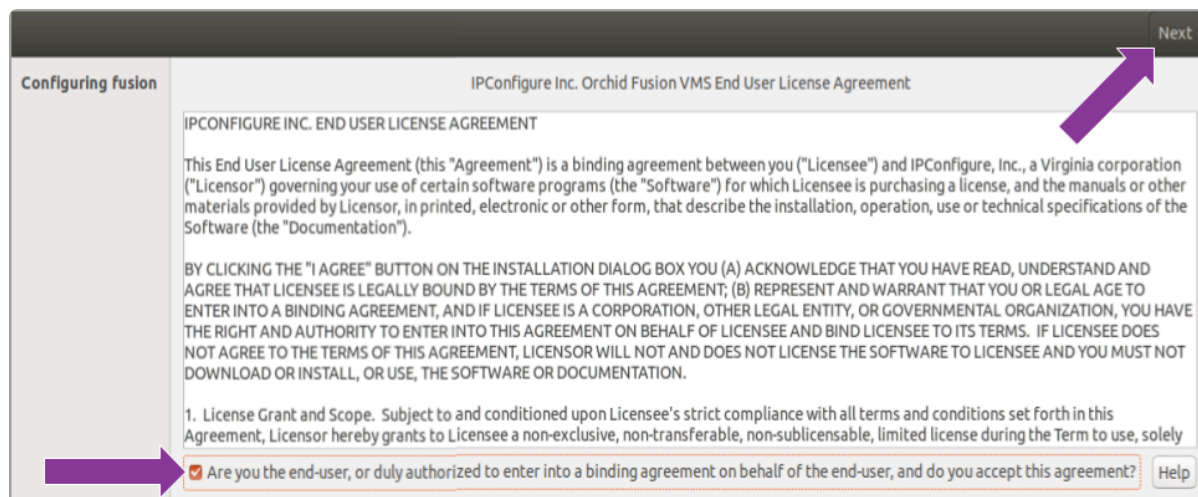




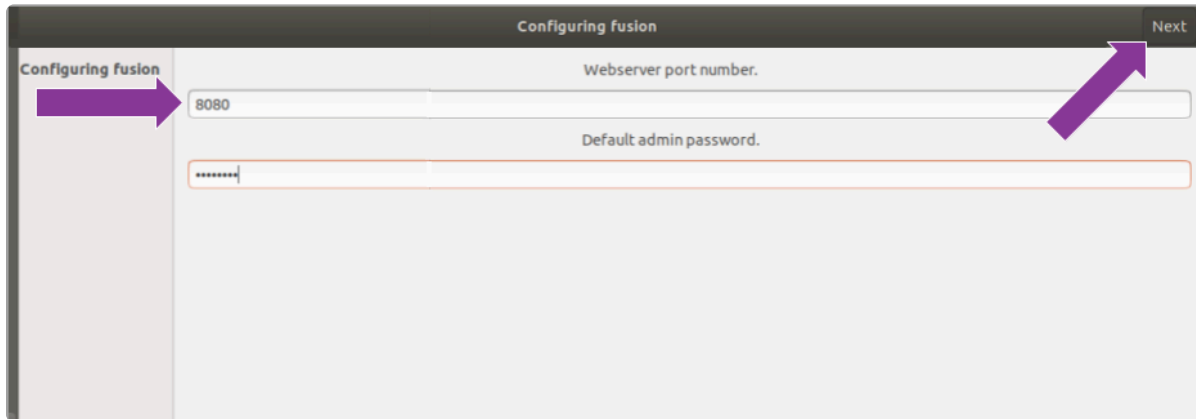
6. Once the GDebi package installer loads, click the ***Install Package*** button in the top right-hand corner of the window. (You may be asked to enter the administrator password.)



7. You will be asked to accept the End User License Agreement. After you read the agreement, mark the *Do you accept this agreement* checkbox and click the **Forward** button, or mark the *Are you the end user* checkbox and click the **Next** button.



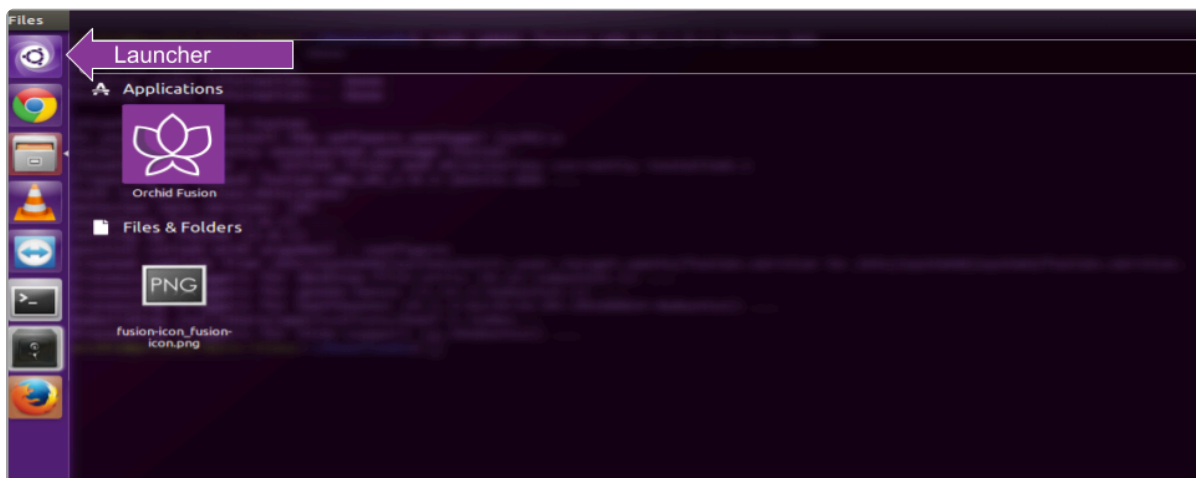
8. The installer will ask you to set the web server port and default admin password:
- By default, the web server port is set to port 8080, which is recommended for most installations. Update the port number only if Orchid Fusion VMS needs to use a port other than 8080.
 - Enter the password you would like to set for the default admin account.

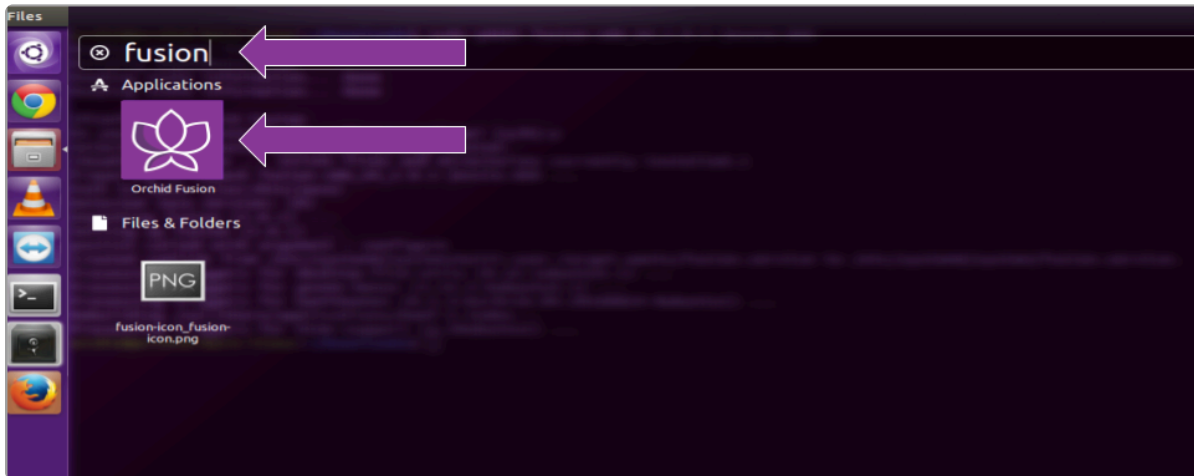


9. When finished, click the **Forward** or the **Next** button.
The installation will complete automatically without any additional prompts. This may take a few minutes.
10. Once the package installer displays an “Installation Finished” message at the top of the screen, click the **Close** button to close the installer and complete the installation. The Orchid Fusion VMS service will start automatically once the package installation is done, after which you can access the Orchid Fusion VMS user interface in your web browser. (For more details on signing in, please refer to the *Enabling...* topics included in the [Installation Support Topics](#) section, and the *Sign In* topic in the [Orchid Fusion VMS Administrator Guide](#).)

You can automatically launch a browser to Orchid Fusion VMS using the link installed on your server:

- Click on the **Launcher** icon in the top left corner of the screen. Then type *fusion* in the search box, and click the **Orchid Fusion** icon listed under *Applications*.





- Or, you can click the *Applications* icon (in your favorites or the lower-left corner of the screen), then click on the *Orchid Fusion* icon.



How to Edit a Configuration File in Ubuntu 16.04 to 22.04

If it becomes necessary, you can edit the Orchid Fusion VMS configuration file using standard text editors in Linux. This section will describe two methods for editing the configuration files: using the Command Line and using the Graphical User Interface (GUI).

✿ In order to edit text files as the root user, you will need administrator access to the computer on which Orchid Fusion VMS is installed.

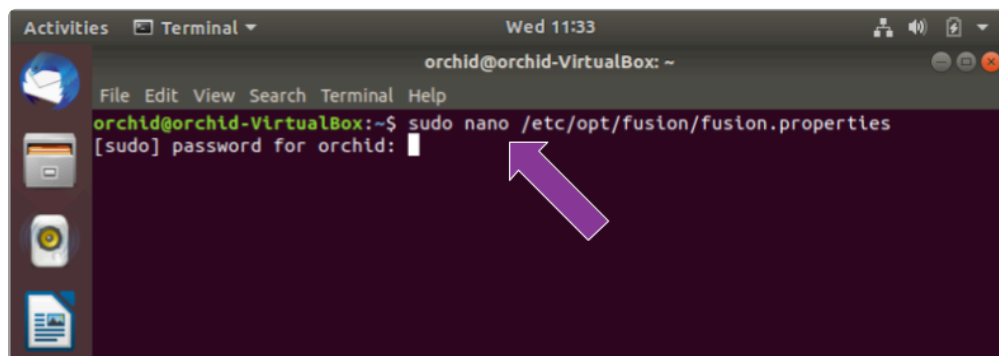
The default location for the Orchid Fusion VMS configuration file in Linux is:

- `/etc/opt/fusion/fusion.properties`
 - Stores all of the Orchid Fusion VMS settings and can be used to update things like the Orchid Fusion VMS port number, manually update the admin password, etc.

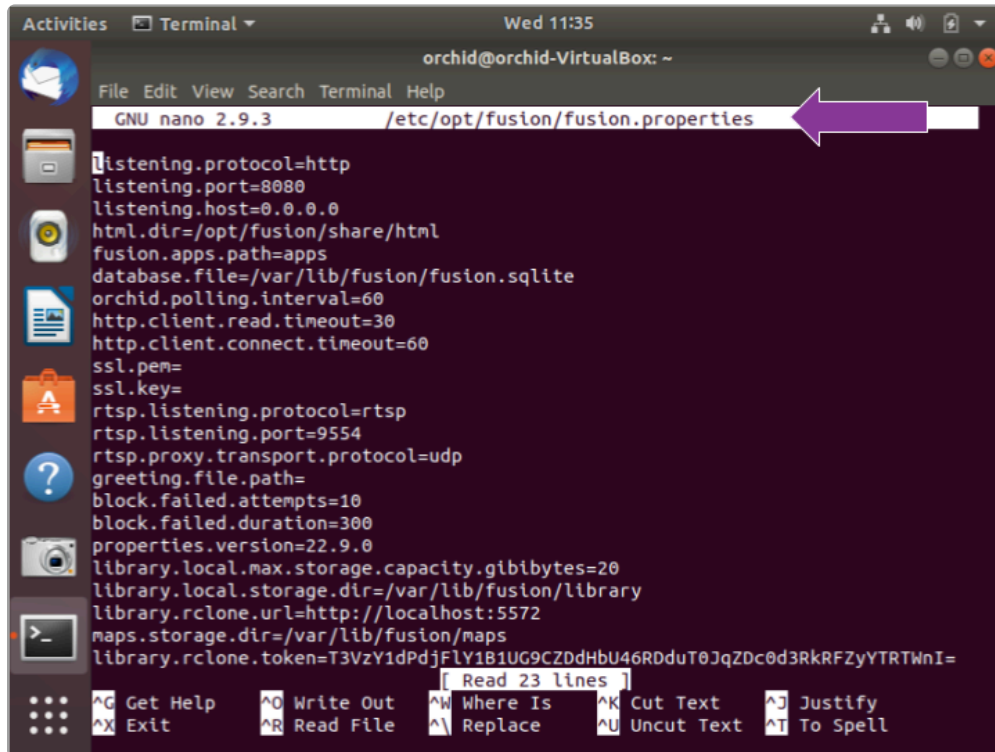
Refer to the [Installation Support Topics](#) section for a list of available properties.

Editing Configuration Files Through the Command Line:

1. Open the *Terminal* program (**CTRL+ALT+T**) and open the Orchid Fusion VMS configuration file in the nano text editor by typing the following command: `sudo nano /etc/opt/fusion/fusion.properties`. Then press **Enter**.



2. After running that command, you will be prompted to enter the *[sudo] password* for your user. Type the password used to sign in to your computer, then press **Enter**. The configuration file will open.

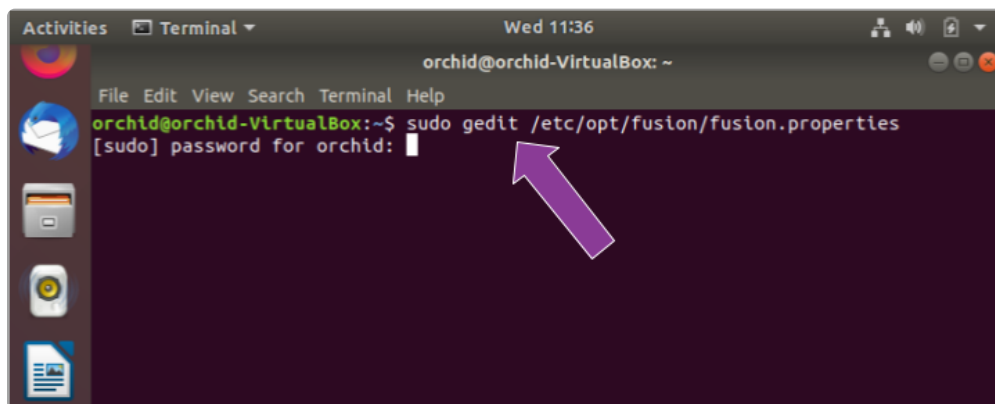


```
GNU nano 2.9.3 /etc/opt/fusion/fusion.properties
listening.protocol=http
listening.port=8080
listening.host=0.0.0.0
html.dir=/opt/fusion/share/html
fusion.apps.path=apps
database.file=/var/lib/fusion/fusion.sqlite
orchid.polling.interval=60
http.client.read.timeout=30
http.client.connect.timeout=60
ssl.pem=
ssl.key=
rtsp.listening.protocol=rtsp
rtsp.listening.port=9554
rtsp.proxy.transport.protocol=udp
greeting.file.path=
block.failed.attempts=10
block.failed.duration=300
properties.version=22.9.0
library.local.max.storage.capacity.gibibytes=20
library.local.storage.dir=/var/lib/fusion/library
library.rclone.url=http://localhost:5572
maps.storage.dir=/var/lib/fusion/maps
library.rclone.token=T3VzY1dPdJFLY1B1UG9CZDdHbU46RDduT0JqZDc0d3RkRFZyYTRTWnI=
[ Read 23 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File  ^A Replace   ^U Uncut Text ^T To Spell
```

3. Use the arrow keys to move the cursor around the screen and update any default settings. You may also add new settings to the end of the file.
4. When you are ready to save the file, click **CTRL+X** on the keyboard, then type **Y** to save the file and close the text editor. If you do not want to save the file, type **N** (instead of **Y**) after typing **CTRL+X**.
5. Restart the Orchid Fusion VMS service in Linux to implement the new settings.

Editing Configuration Files Through the GUI:

1. Open the *Terminal* program (**CTRL+ALT+T**) and open Orchid Fusion VMS's configuration file by typing the following command: `sudo gedit /etc/opt/fusion/fusion.properties`. Then press **Enter**.

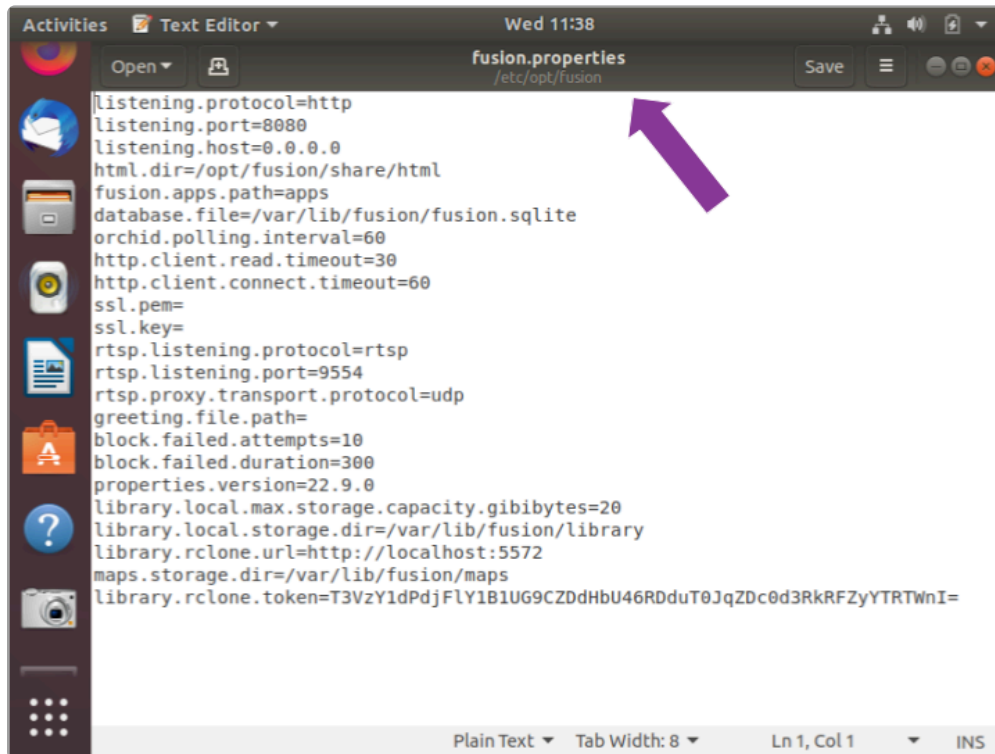


```
orchid@orchid-VirtualBox: ~
File Edit View Search Terminal Help
orchid@orchid-VirtualBox:~$ sudo gedit /etc/opt/fusion/fusion.properties
[sudo] password for orchid: 
```

2. After running that command, you will be prompted to enter your password to perform administrative tasks. Type the same password you use to sign in to your computer, then

press **Enter**.

3. A text editor will open in a new window allowing you to edit the configuration file. Update default settings as needed. You may also add new settings to the end of the file.



4. When you are ready to save the file, click **File/Save**.
5. [Restart](#) the Orchid Fusion VMS service in Linux to implement the new settings.

✿ Some of the Orchid Recorder configuration settings can be edited from within the Orchid Fusion VMS user interface. (This is done using the *Advanced Settings* feature which is explained in the [Orchid Fusion VMS Administrator Guide](#).) To edit the Orchid Recorder configuration file using standard text editors in Linux, please refer to the [Orchid Recorder Installation Guide](#).

How to Manage the Orchid Fusion VMS Services Through the Command Line

The following services are used by Orchid Fusion VMS in Linux. If you need to check the status, start, or stop the service, you can do this from the command line.

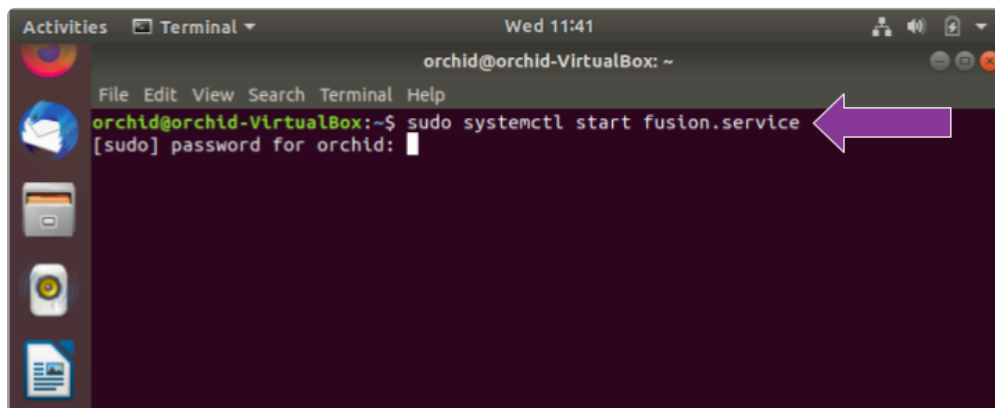
- **Fusion:** This service supports the Orchid Fusion VMS server that manages registered Orchid Recorders and provides access to video from those servers.
 - You will need to restart this service whenever a change has been made to the Orchid Fusion VMS configuration file.
- **Fusion_Rclone:** This service supports Fusion's ability to export video files to an external cloud storage location, via the Rclone open-source library.
 - You will need to restart this service if you re-run the Rclone executable.

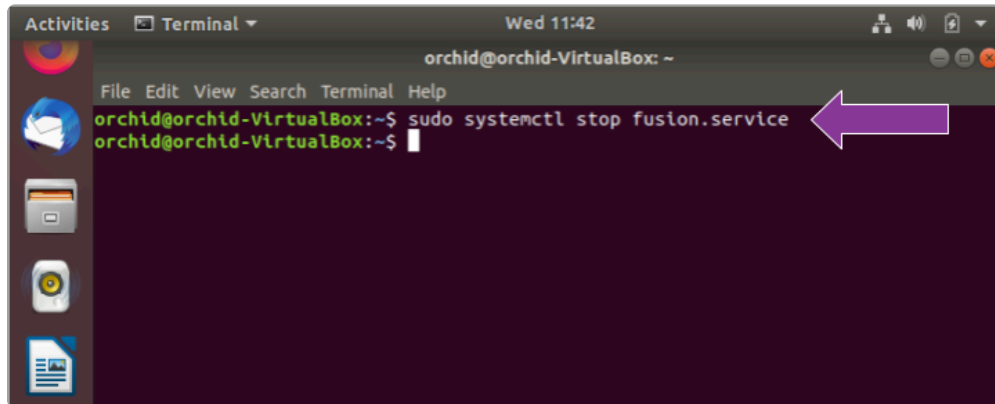
Tip

- After you've configured your Orchid Fusion VMS properties and started the service, you should check the service status to verify Orchid Fusion VMS is running.

To manage the Orchid Fusion VMS service from the command line:

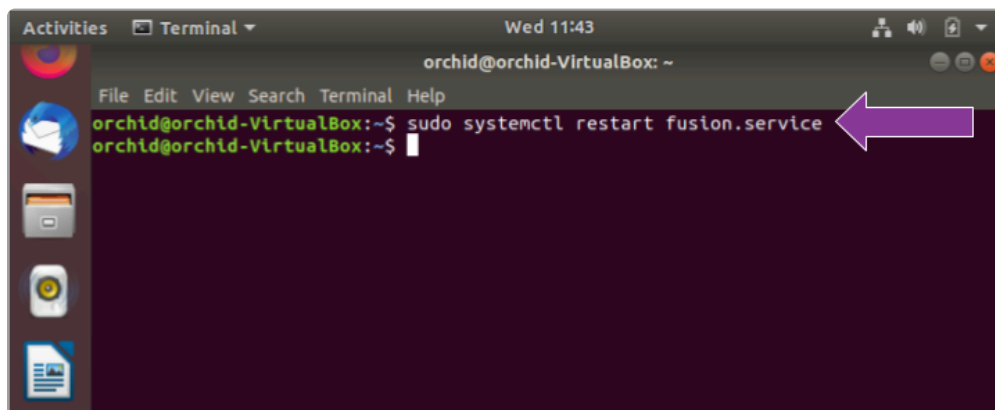
1. Open the *Terminal* program (**CTRL+ALT+T**).
2. Type the following command: `sudo systemctl (command) fusion.service`, where the *command* is *start*, *stop*, *restart*, or *status*. Then press *Enter*.





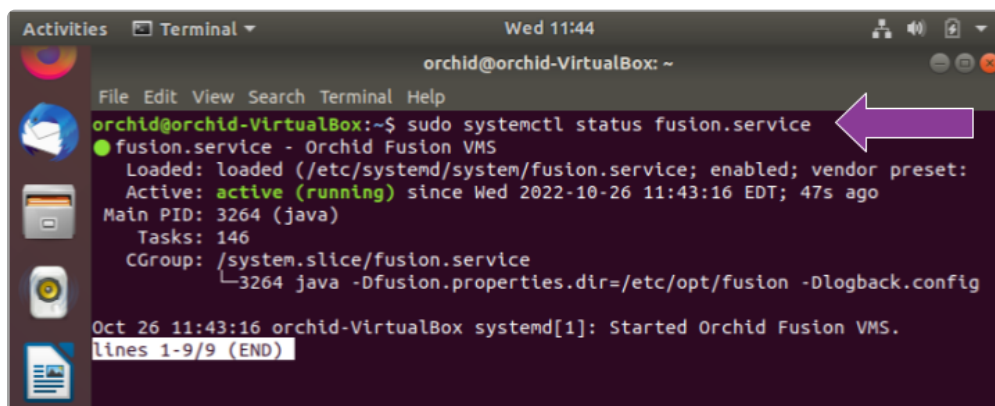
A terminal window titled 'Wed 11:42' and 'orchid@orchid-VirtualBox: ~'. The command 'sudo systemctl stop fusion.service' is entered and executed. A purple arrow points to the command. The terminal output shows the command was successful.

```
orchid@orchid-VirtualBox:~$ sudo systemctl stop fusion.service
orchid@orchid-VirtualBox:~$
```



A terminal window titled 'Wed 11:43' and 'orchid@orchid-VirtualBox: ~'. The command 'sudo systemctl restart fusion.service' is entered and executed. A purple arrow points to the command. The terminal output shows the command was successful.

```
orchid@orchid-VirtualBox:~$ sudo systemctl restart fusion.service
orchid@orchid-VirtualBox:~$
```



A terminal window titled 'Wed 11:44' and 'orchid@orchid-VirtualBox: ~'. The command 'sudo systemctl status fusion.service' is entered and executed. A purple arrow points to the command. The terminal output shows the service is active (running).

```
orchid@orchid-VirtualBox:~$ sudo systemctl status fusion.service
● fusion.service - Orchid Fusion VMS
   Loaded: loaded (/etc/systemd/system/fusion.service; enabled; vendor preset:
   Active: active (running) since Wed 2022-10-26 11:43:16 EDT; 47s ago
     Main PID: 3264 (java)
        Tasks: 146
      CGroup: /system.slice/fusion.service
              └─3264 java -Dfusion.properties.dir=/etc/opt/fusion -Dlogback.config

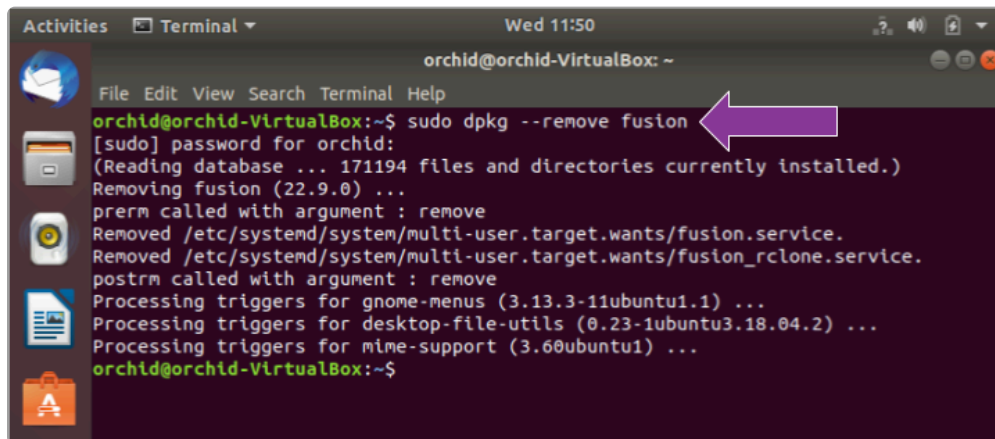
Oct 26 11:43:16 orchid-VirtualBox systemd[1]: Started Orchid Fusion VMS.
lines 1-9/9 (END)
```

* The set of commands above will only manage the Fusion server service. If you need to manage the Fusion_Rclone service, replace `fusion.service` with `fusion_rclone.service` in the command line.

Uninstalling Orchid Fusion VMS in Ubuntu 16.04 to 22.04

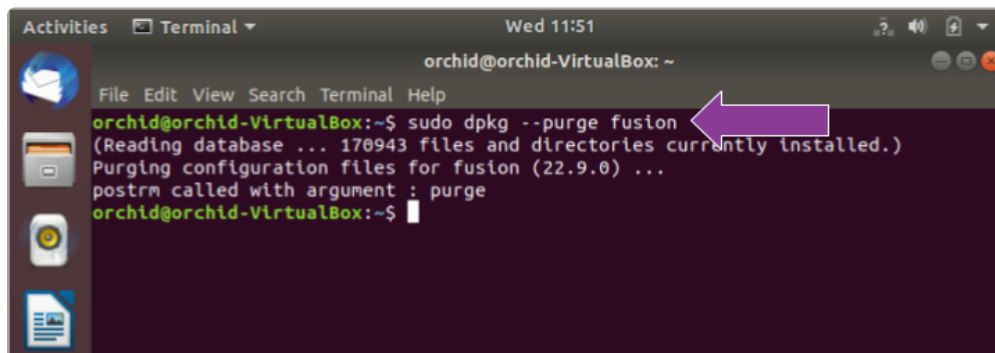
There are a couple of options for removing the Orchid Fusion VMS software. The *Remove* command will uninstall all files installed and created by Orchid Fusion VMS except the configuration files and the database. The *Purge* command will uninstall all files installed and created by Orchid Fusion VMS.

1. Open the *Terminal* program (*CTRL+ALT+T*).
2. To uninstall Orchid Fusion VMS, use either step 3 or step 4 below.
3. To uninstall Orchid Fusion VMS (while keeping the configuration files and the database), type the following command: `sudo dpkg --remove fusion`. Enter the password when prompted to do so, then press *Enter*.



```
Activities Terminal Wed 11:50
orchid@orchid-VirtualBox: ~
File Edit View Search Terminal Help
orchid@orchid-VirtualBox:~$ sudo dpkg --remove fusion
[sudo] password for orchid:
(Reading database ... 171194 files and directories currently installed.)
Removing fusion (22.9.0) ...
prerm called with argument : remove
Removed /etc/systemd/system/multi-user.target.wants/fusion.service.
Removed /etc/systemd/system/multi-user.target.wants/fusion_rclone.service.
postrm called with argument : remove
Processing triggers for gnome-menus (3.13.3-11ubuntu1.1) ...
Processing triggers for desktop-file-utils (0.23-1ubuntu3.18.04.2) ...
Processing triggers for mime-support (3.60ubuntu1) ...
orchid@orchid-VirtualBox:~$
```

4. To uninstall all of the Orchid Fusion VMS files, type the following command: `sudo dpkg --purge fusion`. Enter the password when prompted to do so, then press *Enter*.



```
Activities Terminal Wed 11:51
orchid@orchid-VirtualBox: ~
File Edit View Search Terminal Help
orchid@orchid-VirtualBox:~$ sudo dpkg --purge fusion
(Reading database ... 170943 files and directories currently installed.)
Purging configuration files for fusion (22.9.0) ...
postrm called with argument : purge
orchid@orchid-VirtualBox:~$
```

Working in Red Hat

IPConfigure distributes Orchid Fusion VMS for Red Hat using an .rpm file. Use this file to install Orchid Fusion VMS on systems running Red Hat Enterprise Linux versions 7 and 8, and CentOS versions 7 and 8.

* You must sign in to the computer as a user with “root” access.

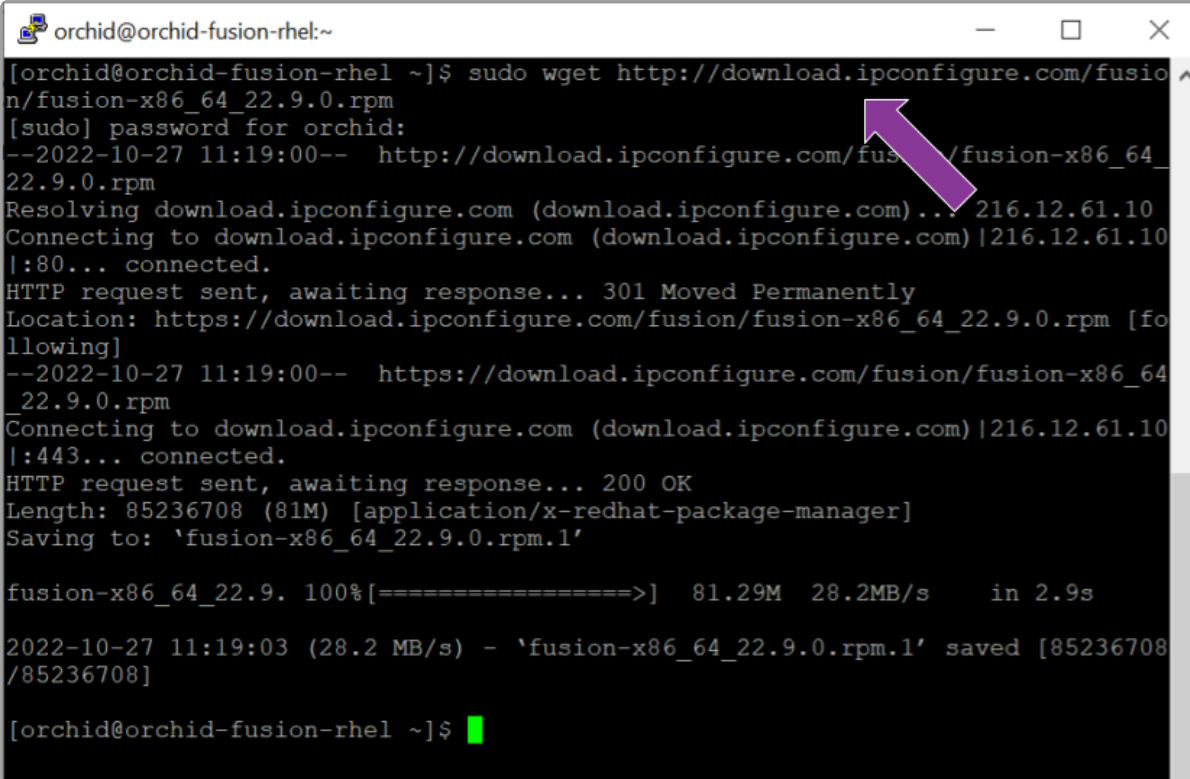
* If you are performing an upgrade of your Orchid Fusion VMS, you should check to make sure that all of the registered Orchid Recorders are running, at minimum, Orchid version 2.8.0. (You will receive a warning message during the installation if this is not the case.)

Installing Orchid Fusion VMS in Red Hat Enterprise Linux 7

The following installation instructions provided for Red Hat Enterprise Linux 7 also apply to Red Hat Enterprise Linux 8, CentOS 7, and CentOS 8.

Installing Orchid Fusion VMS in RedHat

1. To obtain the Orchid Fusion VMS installation package (.rpm file), do either of the following:
 - Use a web browser to obtain the file from the IPConfigure web site.
 - Type the following command at the *Terminal* screen: `sudo wget http://download.ipconfigure.com/fusion/fusion-x86_64_VERSION.rpm`, where *VERSION* is the software version number. Then press *Enter*.



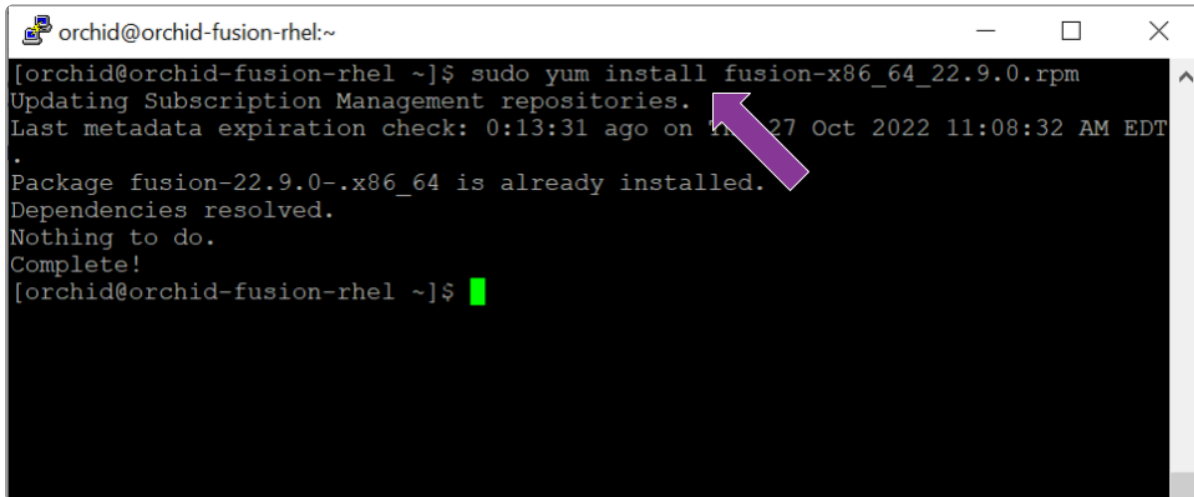
```
orchid@orchid-fusion-rhel:~$ sudo wget http://download.ipconfigure.com/fusion-x86_64_22.9.0.rpm
[sudo] password for orchid:
--2022-10-27 11:19:00-- http://download.ipconfigure.com/fusion-x86_64_22.9.0.rpm
Resolving download.ipconfigure.com (download.ipconfigure.com)... 216.12.61.10
Connecting to download.ipconfigure.com (download.ipconfigure.com)|216.12.61.10|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://download.ipconfigure.com/fusion/fusion-x86_64_22.9.0.rpm [following]
--2022-10-27 11:19:00-- https://download.ipconfigure.com/fusion/fusion-x86_64_22.9.0.rpm
Connecting to download.ipconfigure.com (download.ipconfigure.com)|216.12.61.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 85236708 (81M) [application/x-redhat-package-manager]
Saving to: 'fusion-x86_64_22.9.0.rpm.1'

fusion-x86_64_22.9. 100%[=====>] 81.29M 28.2MB/s in 2.9s

2022-10-27 11:19:03 (28.2 MB/s) - 'fusion-x86_64_22.9.0.rpm.1' saved [85236708/85236708]

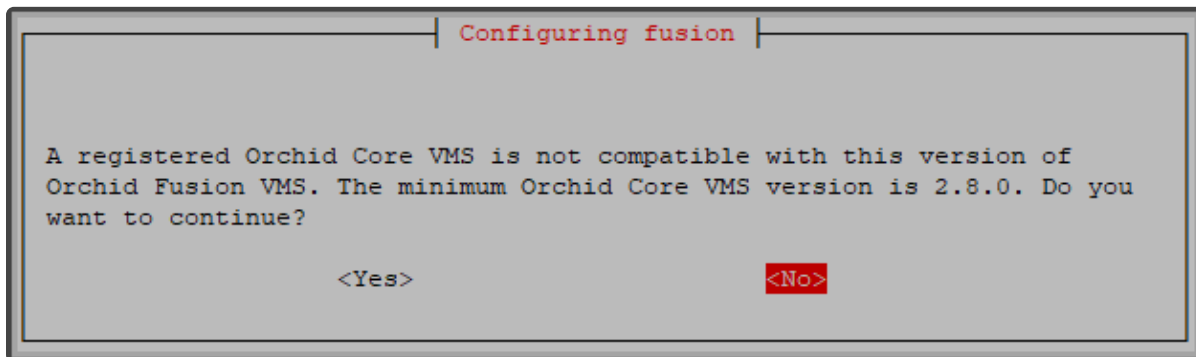
orchid@orchid-fusion-rhel ~]$
```

2. Install Orchid Fusion VMS by typing the following command: `sudo yum install fusion-x86_64_VERSION.rpm`, where *VERSION* is the software version number. Then press *Enter*.



```
orchid@orchid-fusion-rhel:~  
[orchid@orchid-fusion-rhel ~]$ sudo yum install fusion-x86_64_22.9.0.rpm  
Updating Subscription Management repositories.  
Last metadata expiration check: 0:13:31 ago on Mon 27 Oct 2022 11:08:32 AM EDT  
.  
Package fusion-22.9.0-.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[orchid@orchid-fusion-rhel ~]$
```

- If you are performing an upgrade of your Orchid Fusion VMS, the installer will check the Orchid version numbers on each of the registered Orchid Recorders. If any of the registered servers have an Orchid version number older than 2.8.0, you will receive a warning message similar to the one pictured here.



Orchid Fusion VMS Setup will ask if you want to continue with the installation. IPConfigure recommends that you select **No**, and upgrade any Orchid Recorders that don't meet the minimum version requirement. When all of your Orchid Recorder upgrades are complete, return to step 2 to install the new Orchid Fusion VMS.

This will install all necessary files for Orchid Fusion VMS and the Orchid Fusion VMS services. By default, the services will *not* be started. (For details on working with the services, please refer to the [How to Manage the Orchid Fusion VMS Services](#) section.)

3. Press the **Y** key and **Enter** to accept the EULA, or **N** to decline.
4. **After the installation is complete, you must set the admin password in the configuration file. (Refer to the next section for details.)**

How to Edit a Configuration File in Red Hat

Orchid Fusion VMS uses a configuration file to store all of the system settings. This file may be edited to revise settings such as the Orchid Fusion VMS port number, the admin password, etc. Right after installation, you **must** set the admin password in the configuration file before you run the software. You can edit the Orchid Fusion VMS configuration file using your favorite text editor. (If you don't have a favorite, try nano.)



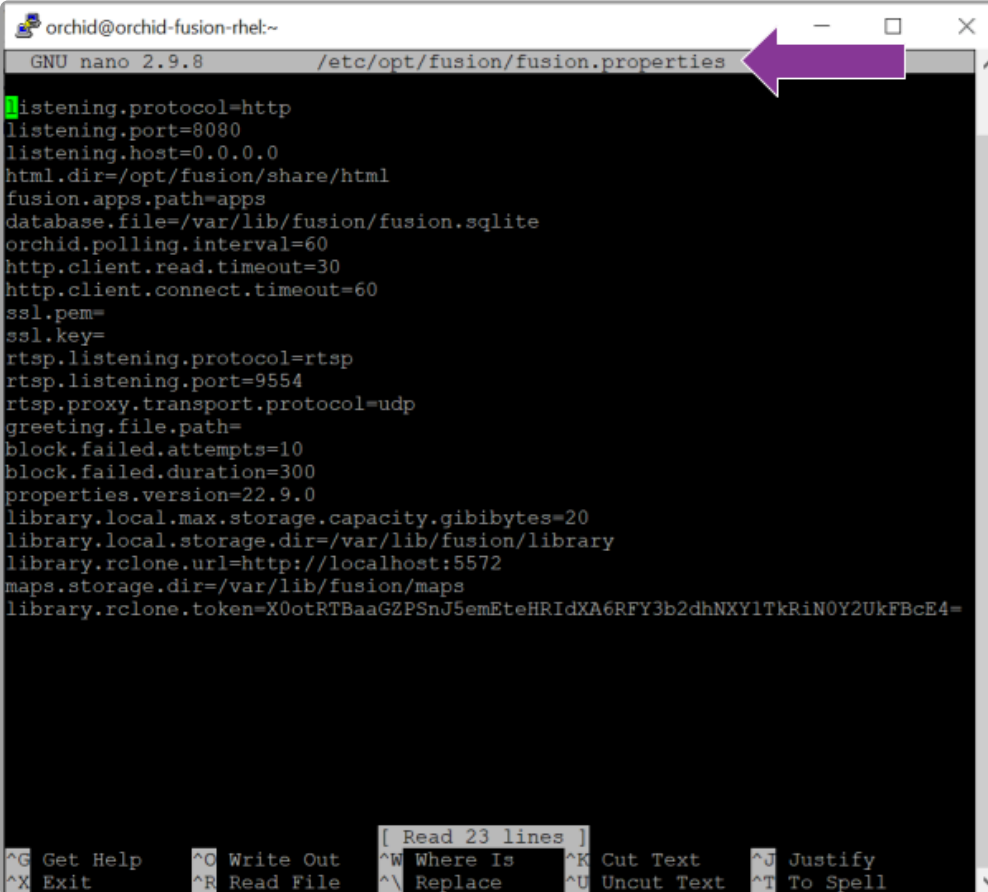
You must sign in to the computer as a user with “root” access.

The default location for the Orchid Fusion VMS configuration file in Linux is:

- `/etc/opt/fusion/fusion.properties`

Refer to the [Installation Support Topics](#) section for a list of available properties.

1. Open the *Terminal* program (**CTRL+ALT+T**).
2. Open the Orchid Fusion VMS configuration file in the nano text editor by typing the following command: `sudo nano /etc/opt/fusion/fusion.properties`. Then press **Enter**.

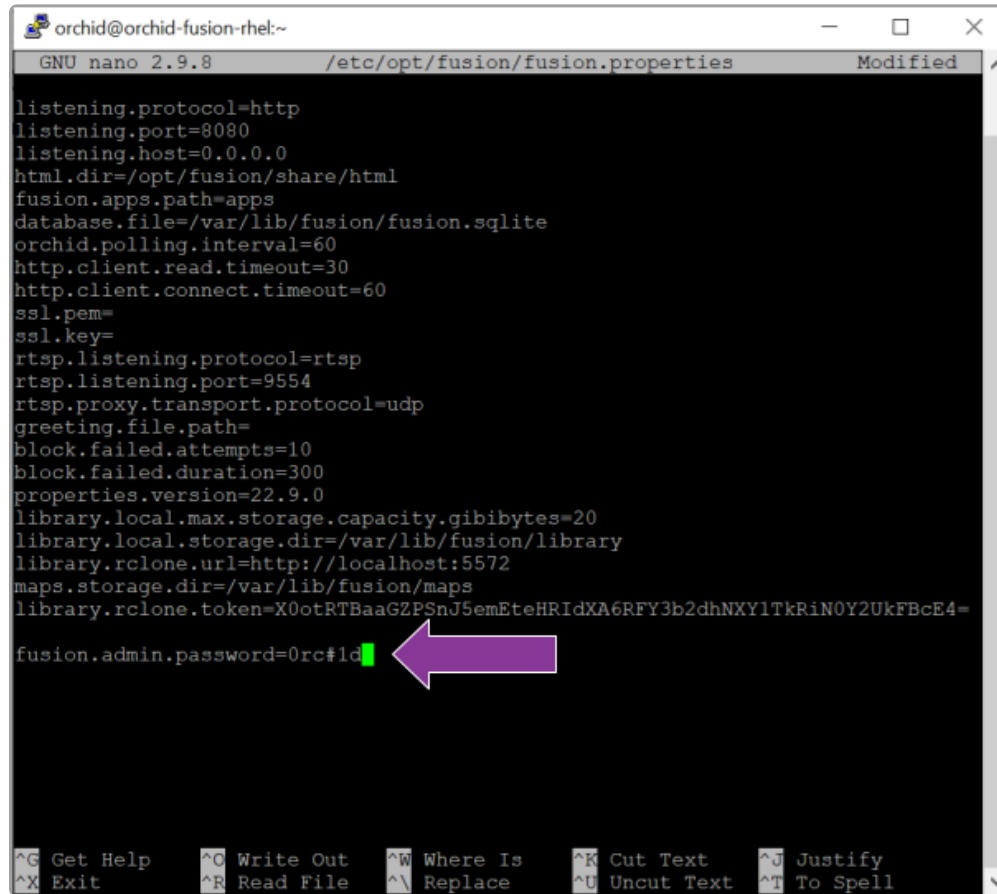


```
orchid@orchid-fusion-rhel:~  
GNU nano 2.9.8 /etc/opt/fusion/fusion.properties  
listening.protocol=http  
listening.port=8080  
listening.host=0.0.0.0  
html.dir=/opt/fusion/share/html  
fusion.apps.path=apps  
database.file=/var/lib/fusion/fusion.sqlite  
orchid.polling.interval=60  
http.client.read.timeout=30  
http.client.connect.timeout=60  
ssl.pem=  
ssl.key=  
rtsp.listening.protocol=rtsp  
rtsp.listening.port=9554  
rtsp.proxy.transport.protocol=udp  
greeting.file.path=  
block.failed.attempts=10  
block.failed.duration=300  
properties.version=22.9.0  
library.local.max.storage.capacity.gibibytes=20  
library.local.storage.dir=/var/lib/fusion/library  
library.rclone.url=http://localhost:5572  
maps.storage.dir=/var/lib/fusion/maps  
library.rclone.token=X0otRTBaaGZPSnJ5emEteHRIdXA6RFY3b2dhNXY1TkRiN0Y2UkFBcE4=  
  
[ Read 23 lines ]  
^G Get Help  ^C Write Out  ^W Where Is  ^K Cut Text   ^J Justify  
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell
```

3. Scroll down to review or set the Orchid Fusion VMS admin password (below). It will take effect only when Orchid Fusion VMS is started for the first time [typically meaning that the Orchid Fusion VMS database (at `/var/lib/fusion/fusion.sqlite`) does not exist when Orchid Fusion VMS starts].

fusion.admin.password

Sets the admin password used upon first sign in. After the first sign in, the admin password can be changed via the user interface.



```
orchid@orchid-fusion-rhel:~  
GNU nano 2.9.8 /etc/opt/fusion/fusion.properties Modified  
listening.protocol=http  
listening.port=8080  
listening.host=0.0.0.0  
html.dir=/opt/fusion/share/html  
fusion.apps.path=apps  
database.file=/var/lib/fusion/fusion.sqlite  
orchid.polling.interval=60  
http.client.read.timeout=30  
http.client.connect.timeout=60  
ssl.pem=  
ssl.key=  
rtsp.listening.protocol=rtsp  
rtsp.listening.port=9554  
rtsp.proxy.transport.protocol=udp  
greeting.file.path=  
block.failed.attempts=10  
block.failed.duration=300  
properties.version=22.9.0  
library.local.max.storage.capacity.gibibytes=20  
library.local.storage.dir=/var/lib/fusion/library  
library.rclone.url=http://localhost:5572  
maps.storage.dir=/var/lib/fusion/maps  
library.rclone.token=X0otRTBaaGZPSnJ5emEteHRIdXA6RFY3b2dhNXYlTkRiN0Y2UkFBcE4=  
fusion.admin.password=0rc#1d  
  
^G Get Help  ^C Write Out  ^W Where Is  ^K Cut Text   ^J Justify  
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell
```

4. Review or edit the remainder of the parameters as needed.
5. Start or [Restart](#) the Orchid Fusion VMS service to implement the new settings.

✿ Some of the Orchid Recorder configuration settings can be edited from within the Orchid Fusion VMS user interface. (This is done using the *Advanced Settings* feature which is explained in the [Orchid Fusion VMS Administrator Guide](#).) To edit the Orchid configuration file using standard text editors in Linux, please refer to the [Orchid Recorder Installation Guide](#).

How to Manage the Orchid Fusion VMS Services in Red Hat

The following services are used by Orchid Fusion VMS in Red Hat. If you need to enable, check the status, start, or stop the services, you can do this from the command line.

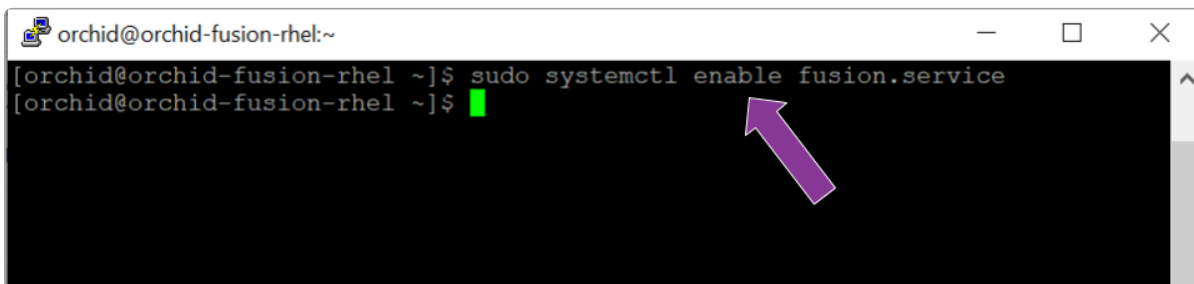
- **Fusion:** This service supports the Orchid Fusion VMS server that manages registered Orchid Recorders and provides access to video from those servers.
 - You will need to restart this service whenever a change has been made to the Orchid Fusion VMS configuration file.
- **Fusion_Rclone:** This service supports Fusion's ability to export video files to an external cloud storage location, via the Rclone open-source library.
 - You will need to restart this service if you re-run the Rclone executable.

Tips

- In Red Hat, you have to enable both of the Orchid Fusion VMS services. This will allow the services to automatically start on bootup and restart in the case of failure.
- After you start the services, you should configure the firewall.
- After you've configured your Orchid Fusion VMS properties and started the service, you should check the service status to verify Orchid Fusion VMS is running.

To manage the Orchid Fusion VMS service:

1. Type the following command: `sudo systemctl (command) fusion.service`, where the *command* is *enable*, *start*, *stop*, or *status*. Then press **Enter**.

A terminal window titled 'orchid@orchid-fusion-rhel:~' with standard window controls. It shows the command 'sudo systemctl enable fusion.service' being entered and executed. A green cursor is at the end of the second line. A purple arrow points to the 'enable' part of the command.

```
orchid@orchid-fusion-rhel:~  
[orchid@orchid-fusion-rhel ~]$ sudo systemctl enable fusion.service  
[orchid@orchid-fusion-rhel ~]$
```

```
orchid@orchid-fusion-rhel:~  
[orchid@orchid-fusion-rhel ~]$ sudo systemctl start fusion.service  
[sudo] password for orchid:  
[orchid@orchid-fusion-rhel ~]$
```

```
orchid@orchid-fusion-rhel:~  
[orchid@orchid-fusion-rhel ~]$ sudo systemctl stop fusion.service  
[orchid@orchid-fusion-rhel ~]$
```

```
orchid@orchid-fusion-rhel:~  
[orchid@orchid-fusion-rhel ~]$ sudo systemctl status fusion.service  
● fusion.service - Orchid Fusion VMS  
   Loaded: loaded (/etc/systemd/system/fusion.service; enabled; vendor preset: enabled)  
   Active: failed (exit-code) since Thu 2022-10-27 11:37:36 EDT; 1min 1s ago  
     Process: 1484744 ExecStart=/opt/fusion/bin/fusion (code=exited, status=143)  
    Main PID: 1484744 (code=exited, status=143)  
  
Oct 27 10:18:34 orchid-fusion-rhel systemd[1]: Started Orchid Fusion VMS.  
Oct 27 10:18:37 orchid-fusion-rhel fusion[1484744]: (java:1484744): GStreamer:  
Oct 27 10:18:37 orchid-fusion-rhel fusion[1484744]: (java:1484744): GStreamer:  
Oct 27 11:37:35 orchid-fusion-rhel systemd[1]: Stopping Orchid Fusion VMS...  
Oct 27 11:37:36 orchid-fusion-rhel systemd[1]: fusion.service: Main process e  
Oct 27 11:37:36 orchid-fusion-rhel systemd[1]: fusion.service: Failed with re  
Oct 27 11:37:36 orchid-fusion-rhel systemd[1]: Stopped Orchid Fusion VMS.  
lines 1-13/13 (END)
```

* The set of commands above will only manage the Fusion server service. If you need to manage the Fusion_Rclone service, replace `fusion.service` with `fusion_rclone.service`.

Post-Installation Steps in Red Hat

Configure the Firewall

By default, the *firewalld* service will block access to Orchid Fusion VMS. Refer to the [Installation Support Topics](#) for a list of the ports used by Orchid Fusion VMS, and consult your RHEL 7 documentation for configuring *firewalld*. The following example will open default ports used by Orchid Fusion VMS, but you should understand the security implications of modifying your firewall settings before proceeding.

```
sudo firewall-cmd --zone=public --add-port=8080/tcp --permanent
sudo firewall-cmd --zone=public --add-port=9554/tcp --permanent
sudo firewall-cmd --zone=public --add-port=40000-50000/udp --permanent
sudo firewall-cmd --reload
```

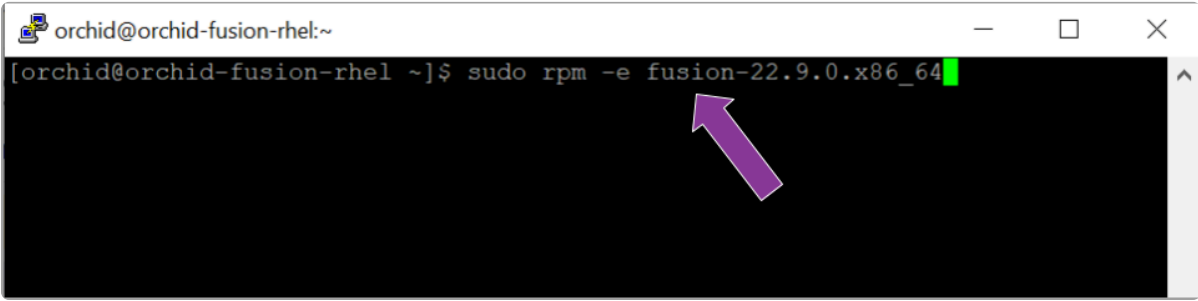
How to Sign In to Orchid Fusion VMS in Red Hat

Sign in to Orchid Fusion VMS using a web browser pointed to your server's IP address at the port specified in the configuration file (default is 8080). Unless changed during the configuration process, the default sign in credentials are *admin* and *password*. (For more details on signing in, please refer to the *Enabling...* topics included in the [Installation Support Topics](#) section, and the *Sign In* topic in the [Orchid Fusion VMS Administrator Guide](#).)

Uninstalling the Orchid Fusion VMS Package in Red Hat

1. To remove the Orchid Fusion VMS package, type the following command: `sudo rpm -e fusion-version.x86_64`, where `version` is the software version number. Then press **Enter**.

(This will remove all files installed and created by Orchid Fusion VMS.)

A terminal window titled 'orchid@orchid-fusion-rhel:~' with standard window controls. The command prompt shows '[orchid@orchid-fusion-rhel ~]\$ sudo rpm -e fusion-22.9.0.x86_64' with a green cursor at the end. A purple arrow points to the package name 'fusion-22.9.0.x86_64' in the command.

```
orchid@orchid-fusion-rhel:~  
[orchid@orchid-fusion-rhel ~]$ sudo rpm -e fusion-22.9.0.x86_64
```

Installation Support Topics

As you work with Orchid Fusion VMS, you may encounter issues that are not typical of daily operation and should be addressed by an advanced user. Please review these topics if you need extra help. For in-depth explanations and additional topics, we encourage you to check our [Knowledge Base](#).

Orchid Fusion VMS Configuration Settings

Orchid Fusion VMS uses a configuration file (*fusion.properties*) and a logging file (*logback.xml*). These files contain settings that don't change on a regular basis, and are reserved for those with administrator access. If a change to the configuration settings is required, please refer to the appropriate section (such as *Working in Windows* or *Working in Ubuntu 16.04*) earlier in this *Installation Guide*.

Orchid Fusion VMS's configuration settings are included below.

Web Server Settings

listening.protocol

Possible values include **http** and **https**. (The *ssl.pem* and *ssl.key* also need to be set. See *SSL Properties*, which is described later in this topic.)

listening.port

Port number of the web server.

html.dir

Root path to the Orchid Fusion VMS HTML files.

listening.host

Listening address (0.0.0.0 binds to all network interfaces).

SSL Properties

ssl.pem

Full path to the PEM encoded TLS certificate file.

ssl.key

Full path to the PEM encoded RSA key.

Database Settings

database.file

The sqlite database file.

Fusion Server Settings

orchid.polling.interval

Number of seconds between Orchid Recorder data sync.

fusion.admin.password

Updates the admin password (removed from the file after parsed).

fusion.(username).enabled

This allows for the creation of a new user. (Set this to **True** and set the password property below to create a new user. Set this to **False** to delete a Fusion user.)

fusion.(username).password

This may be used to reset the password of any user, or to create a new user (when combined with the *enabled* property above).

fusion.(username).superuser

This allows for the promotion of any user to superuser status. (Set this to **True** to create a new superuser. Set this to **False** to revoke superuser status.)

pages.orchids.size

Sets the number of Orchid Recorders that will be displayed per page (on the *Servers* screen). The default is 10.

fusion.temp.storage.dir

This sets the location in which temporary media files (related to library export and the motion alerts feature) will be stored. The default locations are listed below.

- (Linux) **fusion.temp.storage.dir** = **/var/spool/ipconfigure/fusion**
- (Windows) **fusion.temp.storage.dir** = **C:\Windows\Temp\ipconfigure\fusion**



The temporary media files related to library export were previously stored in **library.local.storage.dir**. Beginning in Fusion version 22.9, these files will be stored in the locations listed above. System administrators may need to adjust the properties file for this migration.

fusion.public.url

This setting may be used to set a custom, public URL for the Fusion server.

- This setting is *optional* for systems not configured for SAML. This public URL will be displayed in *Notification* emails. In prior versions, the *Notification* emails displayed an IP address (which was not always helpful in identifying the source of the problem).
- This setting is *required* if you are configuring your system for Single Sign-On with SAML.

inactivity.threshold.minutes

This setting may be used to automatically log a user out of the system after a set number of minutes of inactivity. Enter a number greater than zero to set the number of minutes of inactivity that the system will allow. (After that number of minutes expires, the software will log the user out of the system.) Enter zero to disable this setting. (Default: 0.)

Library Settings

library.local.max.capacity.gibibyte

This represents the maximum capacity that the *Library* (local Fusion storage) will be able to hold. Value must be a whole number.

library.local.storage.dir

This is the file path to the local directory for *Library* exports.

- (Linux) library.local.storage.dir = /var/lib/fusion/library
- (Windows) library.local.storage.dir = windows-install-dir/library

library.export.threads

The maximum number of threads used by the pool to execute *Library* export requests. (Default: 100)

library.export.http.client.read.timeout

The maximum time (in seconds) that the *Library* export HTTP client will wait for a response from Orchid when performing a *Library* export. (Default: 180)

library.export.http.client.connect.timeout

The maximum time (in seconds) that the *Library* export HTTP client will wait to establish a connection to Orchid when performing a *Library* export. (Default: 60)

library.export.signing.disabled

This setting allows you to disable the digital signature that will be applied to all *Library* exports. When set to **True**, *Library* exports will not be digitally signed. (Default: False)

library.rclone.remote

This is the name of your Rclone *remote*. (This is required if you want to export *Library* items to an external cloud storage service.)

library.rclone.url

This is the url through which Fusion and Rclone communicate. (This property is set by the installer and should *not* be changed.)

library.rclone.token

This is how Fusion authenticates to the Rclone service. (This property is set by the installer and should *not* be changed.)



For additional instructions on enabling the use of an external cloud storage system, please refer to the [Enabling External Cloud Storage](#) section.

Motion Alert Template Setting

Orchid Fusion VMS now offers the ability to use a custom email template when sending *Motion Alert* emails. After you create the template, modify the Fusion configuration file with the property below (so Fusion will be able to find the template).

`motion.alerter.email.template`

This is the file path to the custom template for the *Motion Alert* emails. This path must be an *absolute* path to the custom template. For example:

- (Linux) `motion.alerter.email.template = </etc/opt/fusion/motion-alert-template.txt.tmpl>`
- (Windows) `motion.alerter.email.template = <C:\\Program Files\\IPConfigure\\Fusion\\template.txt.tmpl>`

RTSP Proxy Server Settings

`rtsp.listening.protocol`

Options are as follows:

- `rtsp`
Default – Orchid Fusion VMS UI will access the streams via UDP.
- `rtspt`
Orchid Fusion VMS UI will access the streams via TCP-interleaved.
- `rtspS`
Orchid Fusion VMS UI will access the streams via UDP SRTP. (Secure — `ssl.pem` and `ssl.key` must be set)
- `rtspst`
Orchid Fusion VMS UI will access the streams via TCP-interleaved TLS. (Secure tcp — `ssl.pem` and `ssl.key` must be set)

`rtsp.listening.port`

The port the rtsp proxy listens on (default 9554)

`rtsp.proxy.transport.protocol`

This is the RTSP transport protocol between Orchid Fusion VMS and Orchid Recorder. Options are:

- `udp`
Default
- `tcp`
- `http`
(http only works with target Orchid Recorders running rtsp)

`rtsp.session.cleanup.period`

Time (in seconds) to periodically check for inactive sessions. Default is 2 seconds.

rtsp.server.backlog

The maximum number of queued requests for the server. Default is 50.

rtsp.max.threads

The maximum number of threads used by the pool to handle client requests. A value of 0 will use the pool mainloop; a value of -1 will use an unlimited number of threads. The default is 100.

rtsp.max.sessions

The maximum allowed number of sessions. A value of 0 allows an unlimited number of sessions. Default is 128.

rtsp.port.range.min

Sets the minimum RTP port range. A value of 0 will disable the minimum setting (meaning the server may use any available port). Default is 0. If this is set to 0 (disabled), the **rtsp.port.range.max** will also be disabled.

rtsp.port.range.max

Sets the maximum RTP port range. A value of 0 will disable the maximum setting (meaning the server may use any available port). Default is 0. If this is set to 0 (disabled), the **rtsp.port.range.min** will also be disabled.

Sign In Options

Orchid Fusion VMS offers multiple ways to sign in. Important information regarding the configuration file is included below.

✿ For more detailed instructions on enabling alternative sign in methods, please refer to the following sections: * [Enabling Google Authentication](#) * [Enabling Active Directory](#) * [Enabling Azure Active Directory](#) * [Enabling FreeIPA Authentication](#) * [Enabling Single Sign-On with SAML](#) *

Google Authentication

Enabling Google sign-in requires Google credentials for Orchid Fusion VMS. These are generated by Google. To create these credentials through Google, please visit <https://console.cloud.google.com/apis/credentials>.

✿ Beginning with version 22.9, Orchid Fusion/Hybrid VMS upgraded to Google OAuth2 sign-in. This replaced Google's legacy sign-in (which they [discontinued](#) in

2023). For information on formatting your system for this new sign-in method, please refer to the [Enabling Google Authentication](#) article in our Knowledge Base.

google.auth.clientid

This property is required for Google sign in. (For example: `google.auth.clientid=<your client id>`)

google.auth.secret

This property is required for Google sign in. (For example: `google.auth.secret=<your client secret>`)

google.auth.redirect

This property is required for Google sign in. (For example: `google.auth.redirect=<your redirect url>`)

Active Directory

To use Active Directory authentication, you must already have an Active Directory server with at least one Active Directory group with one Active Directory user. The following properties will also need to be configured, as noted.

authentication.active.directory.servers

This command identifies the active directory server. If there are more than one, use a comma to separate multiple server addresses.

authentication.active.directory.admin.groups

This property was previously required to initialize admin access and provides a comma-separated list of groups for each domain. This property is now optional. You may use the Orchid Fusion VMS user interface to add Active Directory Administrator groups.

authentication.active.directory.referral.mode

This property allows authentication to follow references to another server. Values include **follow** (the default), **ignore**, and **throw**.

Azure Active Directory

To use Azure Active Directory authentication, you must create an Azure Active Directory App. (Please refer to Microsoft documentation for the most up-to-date instructions.). The following properties will also need to be configured, as noted.

authentication.azure.active.directory.clientid

This property provides the Application ID assigned to your App when you registered it with Azure Active Directory.

authentication.azure.active.directory.clientsecret

This property provides the application secret that you saved after creating it in the Azure Portal.

authentication.azure.active.directory.endpoint

This property provides the Microsoft OAuth 2.0 Authorize Endpoint assigned to your App when you registered it with Azure Active Directory.

authentication.azure.active.directory.domain

This property defines the domain associated with this Azure Active Directory instance. This can be anything, but in most cases should match the domain into which users are logging in. For example, for users logging in as *<Users>@ipconfigure.com*, the appropriate domain setting would be *ipconfigure.com*.

FreeIPA Authentication

To use FreeIPA authentication, you must already have a FreeIPA server with at least one FreeIPA group with one user. The following properties will also need to be configured, as noted.

authentication.freeipa.servers

This property provides a list of authentication domains from FreeIPA.

authentication.freeipa.(domain).userdn

This property sets the base domain name used when authenticating a FreeIPA user. (This is an advanced FreeIPA option that will only need to be defined if the users are located somewhere other than the domains defined in the property above.)

All LDAP Authenticators (Active Directory, FreeIPA)

Orchid Fusion VMS uses the LDAP protocol to communicate with both Active Directory and FreeIPA servers. You may need to define the property below (as noted).

authentication.domain.alias

This property provides a list of alternate domain names for servers registered with Active Directory or FreeIPA. (This is an advanced setting that will only be needed if the users are signing in to an “alias” domain for Active Directory or FreeIPA.)

Single Sign-On Settings

Beginning in version 23.12, Orchid Fusion VMS supports Single Sign-On using SAML. SAML works with a variety of identity providers (IdPs); Fusion has been tested with each of the following:

- Google Workspace

- Microsoft Entra ID (Formerly Azure AD)
- Auth0
- Ping

Additional configuration is required for Single Sign-On to work. Important information regarding the configuration file is included below.



For more detailed instructions on enabling SAML and the different IdPs, please refer to the following section and all of its subsections: [Enabling Single Sign-On with SAML](#).

Single Sign-On Using SAML

To use SAML for Single Sign-On, there are multiple properties that need to be configured. These include common configuration settings and individual provider settings. The common settings are used to configure the Fusion side of Single Sign-On. The individual provider settings are specific to each provider that is used. Since Fusion can handle multiple IdPs (up to five), the individual provider settings will need to be set for each of the IdPs in use.

Common Settings (Required)

`fusion.public.url`

This setting is required for SAML configuration, but it may already exist in your configuration file. (Please see *Fusion Server Settings* earlier in this section for more [details](#).)

`saml.common.setting.domain`

This property represents your domain name which will be used to configure permissions. (For example: `saml.common.setting.domain=ipcsite.com`) Please refer to the [SAML Permission Group](#) section of the *Orchid Fusion/Hybrid VMS Administrator Guide* for details on setting up *Permission Groups*.

Common Settings (Optional)

The following settings are for advanced users. These settings are not required for SAML setup, but may be useful in your application.

`saml.common.setting.keystore.path`

Use this property if you need to specify where you want the system-generated keystore file to be. This defaults to the same path as the *fusion.properties* file.

`saml.common.setting.keystore.password`

Use this property if you need to specify a password for the keystore file. This defaults to "changeit".

saml.common.setting.privatekey.password

Use this property if you need to specify a private key to the keystore file. This defaults to “changeit”.

saml.common.setting.max.auth.life

Use this property if you need to set a max authorization life. This may be helpful in cases where the IdP is configured for token lifespans greater than 31536000 seconds. This defaults to 31536000 seconds.

Individual Provider Settings (Required)

Reminder: This set of properties must be configured for each IdP that is used.

saml.provider.<provider key>.common.name

This setting identifies the IdP by its common/commercial name, such as *Auth0*, *Ping*, or *Microsoft Entra ID*. (For example: `saml.provider.samlclient1.common.name=Auth0`)

saml.provider.<provider key>.idp.metadata.filename

This setting provides the name of the IdP’s XML metadata file that you have (or will) download from the IdP during setup. (For example: `saml.provider.samlclient1.idp.metadata.filename=ap-auth0-metadata.xml`)

saml.provider.<provider key>.attr.key.name

This is the key used by the IdP to identify a user. (For example:

`saml.provider.samlclient1.attr.key.name=name`) This value must match the IdP’s SAML attribute configuration for the user name.

saml.provider.<provider key>.attr.key.group

This is the key used by the IdP to identify a user group. (For example:

`saml.provider.samlclient1.attr.key.group=group`) This value must match the IdP’s SAML attribute configuration for the group.

Individual Provider Settings (Optional)

The following setting is for advanced users. This setting is not required for SAML setup, but may be useful in your application.

saml.provider.<provider key>.sign.logout

Use this property if your IdP requires logout to be signed. If this is the case, set this to *True*. This property defaults to *False*.

Orchid Fusion VMS and Java

Java Requirement for Orchid Fusion VMS

Beginning with version 23.6, Orchid Fusion VMS requires Java 17. This will be bundled with all of the supported operating systems, and will be installed automatically.

How to Edit the Java Options File in Linux

Orchid Fusion VMS contains a Java Options file that may be used for additional system configuration. If it becomes necessary, you can edit the Java Options file using a standard text editor in Linux. This section will describe how to edit the Java Options file from the command line.

✿ This file should only be modified by a knowledgeable administrator.

✿ In order to edit a text file as the root user, you will need administrator access to the computer on which Orchid Fusion VMS is installed.

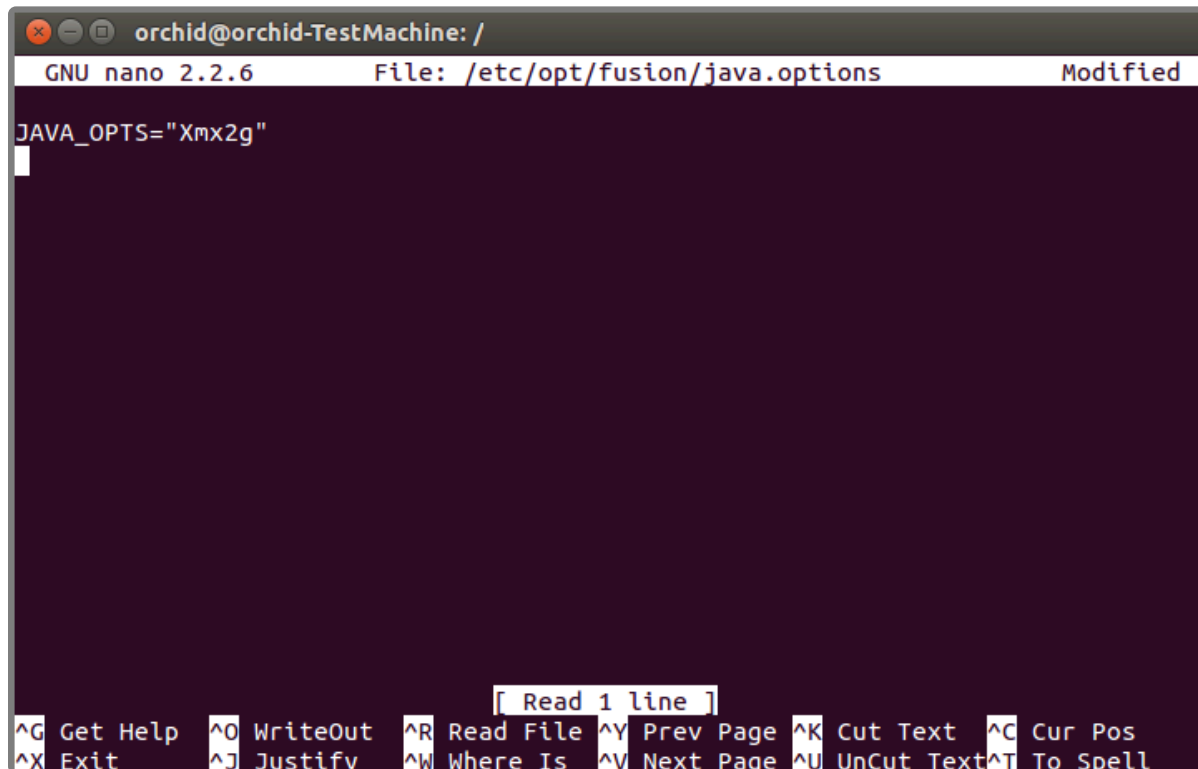
The default location for the Java Options file in Linux is:

- `/etc/opt/fusion/java.options`
 - This file contains the variable `JAVA_OPTS`. By default, this variable is empty, but experienced administrators may use this variable to set Java/JVM related parameters.

Editing the Java Options File from the Command Line:

1. Open the *Terminal* program (**CTRL+ALT+T**).
2. Open the Java Options file in a text editor (such as nano) by typing the following command: `sudo nano /etc/opt/fusion/java.options`. Then press **Enter**.

The file will open to display one variable: `JAVA_OPTS`. This variable will initially be blank, but may be modified to define one or more settings. In the example below, the variable is modified to `-Xmx2g` (which sets the JVM maximum heap size to 2 gibibytes).



```
orchid@orchid-TestMachine: /
GNU nano 2.2.6      File: /etc/opt/fusion/java.options      Modified
JAVA_OPTS="Xmx2g"
[ Read 1 line ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

3. Modify the Java Options file as needed.
4. When you are ready to save the file, click **CTRL+X** on the keyboard, then type **Y** to save the file and close the text editor. If you do not want to save the file, type **N** (instead of **Y**) after typing **CTRL+X**.
5. Restart the Orchid Fusion service in Linux to implement the new settings. (If you need extra help, refer back to the *How to Manage the Orchid Fusion VMS Service* section that corresponds to the operating system you are using.)
6. Once the restart is complete, you can sign into Orchid Fusion VMS.

Orchid Fusion VMS Firewall/Ports Configuration

This topic describes all of the network ports used by Orchid Fusion VMS and which configuration properties allow you to change each port.

Required External Ports

This port is *required* to access Orchid Fusion VMS in any configuration.

- Web server TCP port
 - Default: **8080**
 - Configuration property: **listening.port** (number between 1 and 65535.)

Optional External Ports

Orchid Fusion VMS's RTSP server ports may be configured with the optional parameters below. The RTSP server is not used by the Orchid Recorder or Orchid Fusion VMS user interfaces, but may be used by certain third-party integrations or other applications.

- RTSP TCP port
 - Default: **9554**
 - Configuration property: **rtsp.listening.port** (number between 1 and 65535)
- RTP UDP port range
 - Defaults: **0** (any port)
 - Configuration properties:
 - **rtsp.port.range.min** (number between 1 and 65535)
 - **rtsp.port.range.max** (number between 1 and 65535)

RTSP Configuration Properties

The following two settings are related to Orchid Fusion VMS's Proxy mode (which provides a workaround when the Orchid Recorder is not directly accessible to your web browser).

- **rtsp.listening.protocol**
Options are as follows:
 - **rtsp**
Default – Orchid Fusion VMS UI will access the streams via UDP.
 - **rtspt**
Orchid Fusion VMS UI will access the streams via TCP-interleaved.
 - **rtsp**

Orchid Fusion VMS UI will access the streams via UDP SRTP. (Secure — ssl.pem and ssl.key must be set)

- **rtspst**

Orchid Fusion VMS UI will access the streams via TCP-interleaved TLS. (Secure tcp — ssl.pem and ssl.key must be set)

- **rtsp.proxy.transport.protocol**

This is the RTSP transport protocol between Orchid Fusion VMS and Orchid Recorder.

Options are:

- **udp**

Default

- **tcp**

- **http**

(http only works with target Orchid Recorders running rtsp)

Enabling Google Authentication

Orchid Fusion VMS offers multiple ways to sign in. By performing some configuration work on the front end, your Orchid Fusion VMS users will be able to sign in with their existing Google credentials.

* If you are using Orchid Hybrid VMS, remember that it is a managed system. IPConfigure Support staff will need to configure the system to use Google authentication.

* These instructions were updated for Orchid Fusion VMS version 22.9 to reflect the new requirements for Google OAuth2 sign-in.

Creating the Google Credentials

The first step in enabling Google authentication is to create an *OAuth client ID* that Orchid Fusion VMS will use to identify itself with Google OAuth servers.

1. Navigate and sign in to <https://console.cloud.google.com>.
2. Select **APIs & Services**.
3. Click **Credentials**.
4. Click **Create Credentials** and select **OAuth Client ID**.
5. Select **Web application**.
6. Set the name to *Fusion*.
7. Enter the URL for your instance of Fusion under Authorized Javascript origins.
8. Enter *https://<servername>:<port>/redirect.html* under Authorized redirect URIs.
9. Click **Create**. When the credentials are created, copy the client ID, the client secret, and the redirect URI. (You will need these for your Fusion configuration file.)

Creating Users in Orchid Fusion VMS

Orchid Fusion VMS users now need to be associated with Google accounts. For each user that would like to sign in using a Google account, create or modify their Orchid Fusion VMS account and specify their Google account in the email address field. For more information, please refer to the *Creating and Managing Users* section in the [Orchid Fusion VMS Administrator Guide](#).

Modifying the Configuration File

! Prior to version 22.9.0, Google Authentication was previously configured using the property `google.auth.clientid`. Note the updated property names below.

To finish up, you will need to modify the Orchid Fusion VMS configuration file and then restart Orchid Fusion VMS. For help with the steps below, please refer back to the *Installation* section that corresponds to the operating system in which you are working.

1. Add (or modify) the following line in your Orchid Fusion VMS configuration file:
 - `authentication.google.oauth.clientid=<your client ID>`
 - Replace `<your client ID>` with the client ID that you copied from Google.
2. Add (or modify) the following line in your Orchid Fusion VMS configuration file:
 - `authentication.google.oauth.secret=<your secret>`
 - Replace `<your secret>` with the secret that you copied from Google.
3. Add (or modify) the following line in your Orchid Fusion VMS configuration file:
 - `authentication.google.oauth.redirect=<your redirect url>`
 - Replace `<your redirect url>` with the redirect url that you copied from Google.
4. Restart the Orchid Fusion VMS service.

* If you're using Chrome, it may be necessary to restart Chrome if the user is currently signed into the browser and having trouble with the Google credentials.

Enabling Active Directory

Orchid Fusion VMS offers multiple ways to sign in. By performing some configuration work on the front end, your Orchid Fusion VMS users will be able to sign in with their existing Active Directory credentials.

* If you are using Orchid Hybrid VMS, remember that it is a managed system. IPConfigure Support staff will need to configure the system to use Active Directory authentication.

Prerequisites

To configure Orchid Fusion VMS to work with Active Directory, you will need to have an Active Directory server that:

- Is reachable from your Orchid Fusion VMS server.
- Contains at least one Active Directory user who is a member of at least one Active Directory group.

Modifying the Configuration File

There are several properties in the Orchid Fusion VMS configuration file that will need to be modified in order for Active Directory authentication to work.

* For extra help with the steps below, please refer back to the *Installation* section that corresponds to the operating system in which you are working.

1. Set the following properties in the Orchid Fusion VMS configuration file:

- `authentication.active.directory.servers=`
`<domain1>|ldap(s)://<domainServerAddress1>,<domain2>|`
`ldap(s)://<domainServerAddress2>`
- `authentication.active.directory.admin.groups= <domain>\\<group> (Optional)`
- `authentication.active.directory.referral.mode=follow`

Here is an example enabling the domain *malibu.beach* with server address 192.168.105.46, and an Active Directory group called *FusionAdmins* that will be given administrator access in Orchid Fusion VMS.

- `authentication.active.directory.servers=malibu.beach|ldap://192.168.105.46`
- `authentication.active.directory.admin.groups= malibu.beach\\FusionAdmins (Optional)`

- `authentication.active.directory.referral.mode=follow`

✿ The `authentication.active.directory.admin.groups` property is now optional. Instead of modifying this property in the configuration file, you may add Active Directory Admin groups using the Orchid Fusion VMS user interface. Please refer to the *Add a Permission Group for Active Directory* section of the [Orchid Fusion VMS Administrator Guide](#) for more details.

✿ `<domainServerAddress>` may be a DNS name or IP address and may be prefixed with either `ldap://` or `ldaps://` to specify the protocol.

2. After modifications to the configuration file are complete, restart the Orchid Fusion VMS service, then sign in to Orchid Fusion VMS.

Refer to the *Add a Permission Group for Active Directory* section of the [Orchid Fusion VMS Administrator Guide](#) for instructions on setting Active Directory groups.

Troubleshooting

If your administrator Active Directory user is unable to sign in, but you believe the mappings have been configured correctly, check the *fusion.log* file on the Orchid Fusion VMS server found in the following locations:

- `C:\Program Files\IPConfigure\Orchid Fusion VMS\logs\fusion.log` (Windows)
- `/var/logs/fusion/fusion.log` (Linux)

During server startup, the list of the configured Orchid Fusion VMS administrator Active Directory mappings are logged. So using the previous example, you would see a line in the file that looks like this:

```
14:33:46.804 [main] INFO c.i.f.i.Init03ActiveDirectoryAdminGroupsInitializer - Administrator active directory groups: malibu.beach| |FusionAdmins
```

Also, a failed sign in attempt will show the list of Active Directory groups of which the user is a member. So using the previous example, you would see a line in the file that looks like this:

```
14:32:48.888 [XNIO-1 task-21] INFO c.i.f.u.a.ActiveDirectoryAuthenticator - Active directory user: nofusionaccess@malibu.beach successfully authenticated with domain: malibu.beach server address: 192.168.105.46 but failed to authenticate with Fusion because the user is not a member of any active directory groups authorized by Fusion.
```

`nofusionaccess@malibu.beach` is a member of active directory domain:

malibu.beach groups:

malibu.beach\\Developers

malibu.beach\\Domain Users

Fusion has authorized domain: malibu.beach groups:

Enabling Azure Active Directory

Orchid Fusion VMS allows Azure Active Directory authentication. By performing some configuration work on the front end, your Orchid Fusion VMS users will be able to sign in with their existing Azure Active Directory credentials.

* If you are using Orchid Hybrid VMS, remember that it is a managed system. IPConfigure Support staff will need to configure the system to use Azure Active Directory authentication.

Prerequisites

To configure Orchid Fusion VMS to work with Azure Active Directory, you will need to have an Azure Active Directory server that:

- Is reachable from your Orchid Fusion VMS server.
- Contains at least one Azure Active Directory user who is a member of at least one Azure Active Directory group.

Create an Azure Active Directory Application

Follow the steps below to create an Azure Active Directory App. For a more detailed look at this process, please refer to the next [topic](#). (Please refer to Microsoft documentation for the most up-to-date instructions.)

- Log into the Azure Active Directory portal
 - https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview
- Register an Azure Active Directory “App”
 - Manage – “App registrations” – click “New registration”
 - Enter name
 - Select “Single tenant”
 - Select “Client Application (Web, iOS, Android, Desktop+Devices)”
 - App registrations – – click “Authentication”
 - “Add a platform” – select “Web”
 - Enter the Fusion redirect URI: /redirect.html
 - App registrations – – “API permissions”
 - Add Microsoft Graph Directory.Read.All (Delegated)
 - Admin consent – Microsoft Graph Directory.Read.All
 - App registrations – – “Certificates & secrets”
 - Click “New client secret” – copy and save secret value

Modifying the Configuration File

There are several properties in the Orchid Fusion VMS configuration file that will need to be modified in order for Azure Active Directory authentication to work.

✿ For extra help with the steps below, please refer back to the *Installation* section that corresponds to the operating system in which you are working.

1. Set the following properties in the Orchid Fusion VMS configuration file:
 - `authentication.azure.active.directory.clientid=<applicationid>`
 - Replace `<applicationid>` with the Application ID assigned to your App when you registered it with Azure Active Directory.
 - `authentication.azure.active.directory.clientsecret=<secretvalue>`
 - Replace `<secretvalue>` with the secret value you saved after creating it in the Azure portal.
 - `authentication.azure.active.directory.endpoint=https://login.microsoftonline.com/tenant/oauth2/authorize`
 - Replace `tenant` with the OAuth 2.0 Authorization Endpoint assigned to your App when you registered it with Azure Active Directory.
 - `authentication.azure.active.directory.domain=</domain>`
 - Typically, you will replace `</domain>` with the domain into which users are signing in.
2. After modifications to the configuration file are complete, restart the Orchid Fusion VMS service, then sign in to Orchid Fusion VMS.

Refer to the *Add a Permission Group for Azure Active Directory* section of the [Orchid Fusion VMS Administrator Guide](#) for instructions on setting Permission Groups for Azure Active Directory groups.

Detailed Steps for Configuring Azure Active Directory

This section provides a quick walk-through of configuring Azure Active Directory (free tier) (for enabling Azure Active Directory-based authentication in Orchid Fusion VMS). Specifically this section will guide you through the following:

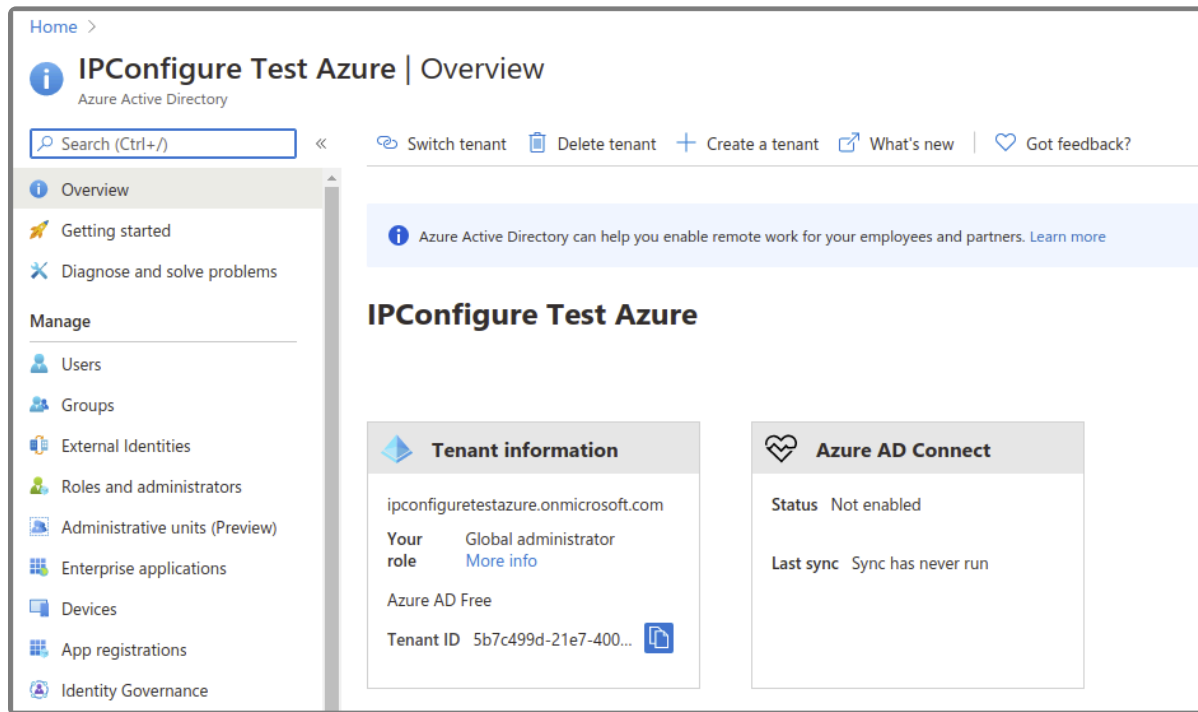
- Creating a free Microsoft Account (if needed)
- Creating an Azure Active Directory user
- Creating an Azure Active Directory group
- Registering an Azure Active Directory app



Please be aware that screenshots and descriptions of the Microsoft Azure AD web interface are current as of June, 2020, but may be changed by Microsoft at any time.

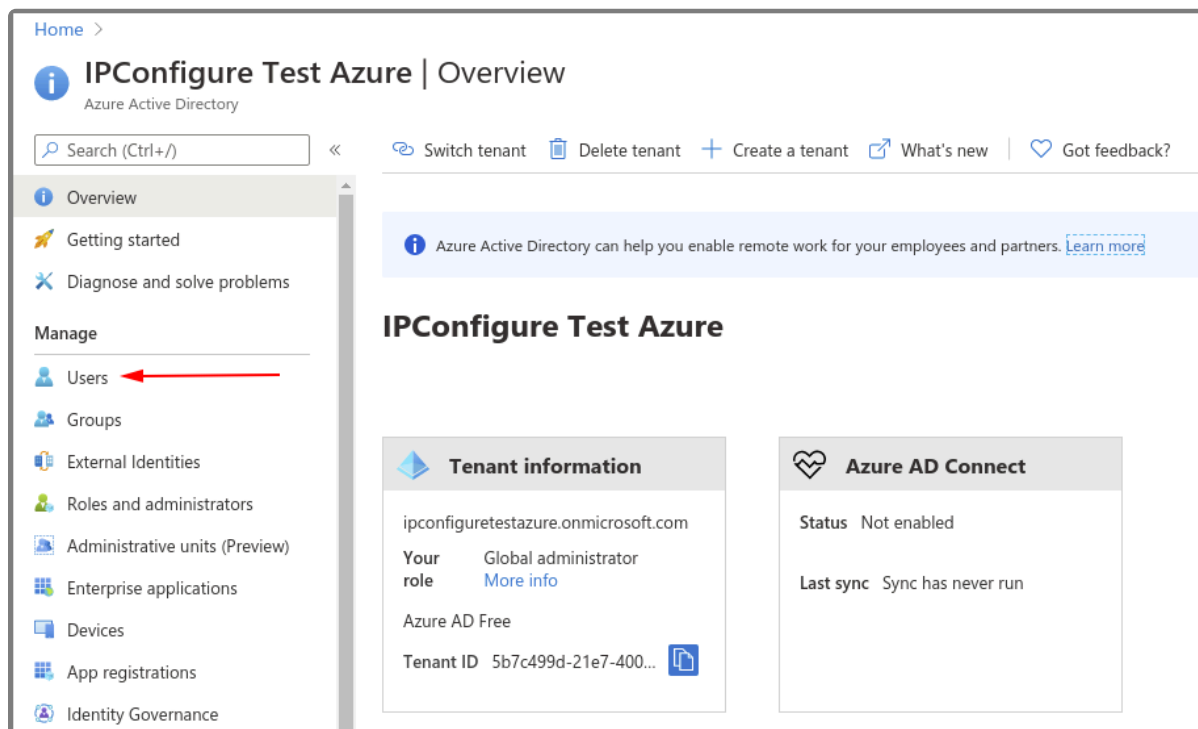
Microsoft Azure Active Directory Account Setup and Portal Login

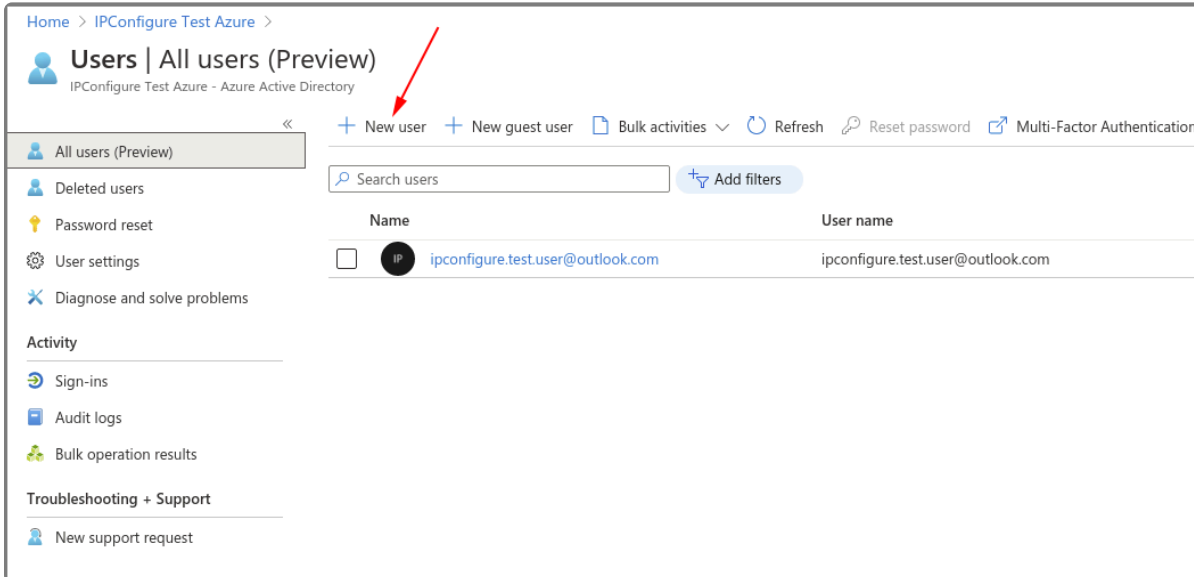
1. If you do not have a Microsoft account, create a free account here:
<https://account.microsoft.com/account>
2. Log into the Azure Active Directory (free tier) portal using your Microsoft account:
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview



Create an Azure Active Directory User

1. Enter a name for the user in the *User name* field. (This is a short name that you use to sign in, like *TJones* @ ipconfigure.com.)
2. Enter the formal (long) name for the user in the *Name* field (like *Tom Jones*).





Home > IPConfigure Test Azure >

Users | All users (Preview)
IPConfigure Test Azure - Azure Active Directory


« + New user + New guest user Bulk activities Refresh Reset password Multi-Factor Authentication

All users (Preview) Deleted users Password reset User settings Diagnose and solve problems

Activity Sign-ins Audit logs Bulk operation results

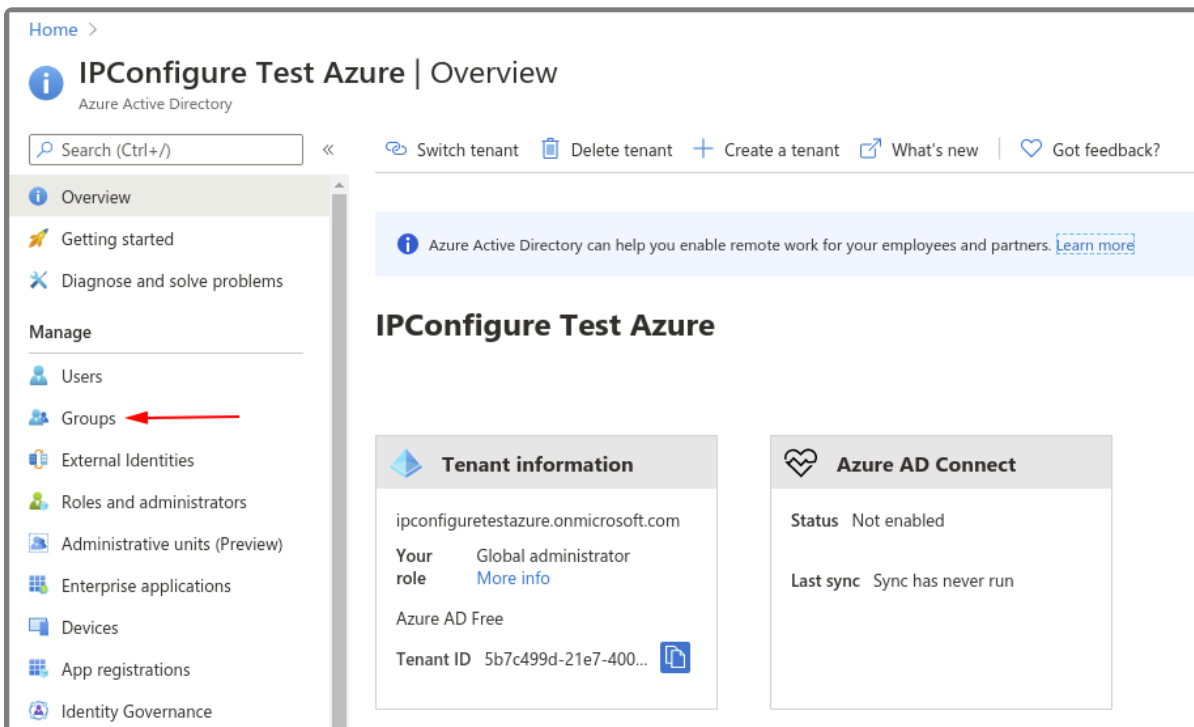
Troubleshooting + Support New support request

Search users Add filters

Name	User name
<input type="checkbox"/>  ipconfigure.test.user@outlook.com	ipconfigure.test.user@outlook.com

Create an Azure Active Directory Group

1. You will need to create at least one Azure Active Directory Group with at least one member.
 - a. Select a type from the *Group type* drop-down.
 - b. Enter a name for the group in the *Group name* field.
 - c. Select group members by clicking on the *Members* link.



Home >

IPConfigure Test Azure | Overview
Azure Active Directory

Search (Ctrl+/) « Switch tenant Delete tenant + Create a tenant What's new Got feedback?

Overview Getting started Diagnose and solve problems

Manage Users **Groups** External Identities Roles and administrators Administrative units (Preview) Enterprise applications Devices App registrations Identity Governance


IPConfigure Test Azure

Tenant information

ipconfiguretestazure.onmicrosoft.com

Your role Global administrator [More info](#)

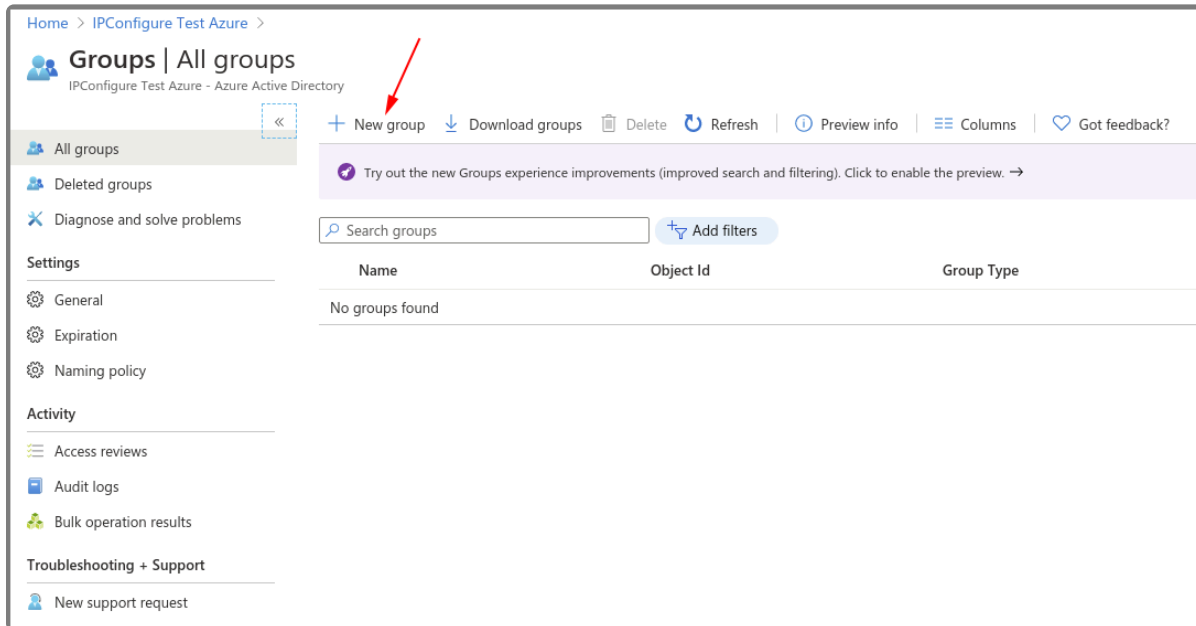
Azure AD Free

Tenant ID 5b7c499d-21e7-400... 

Azure AD Connect

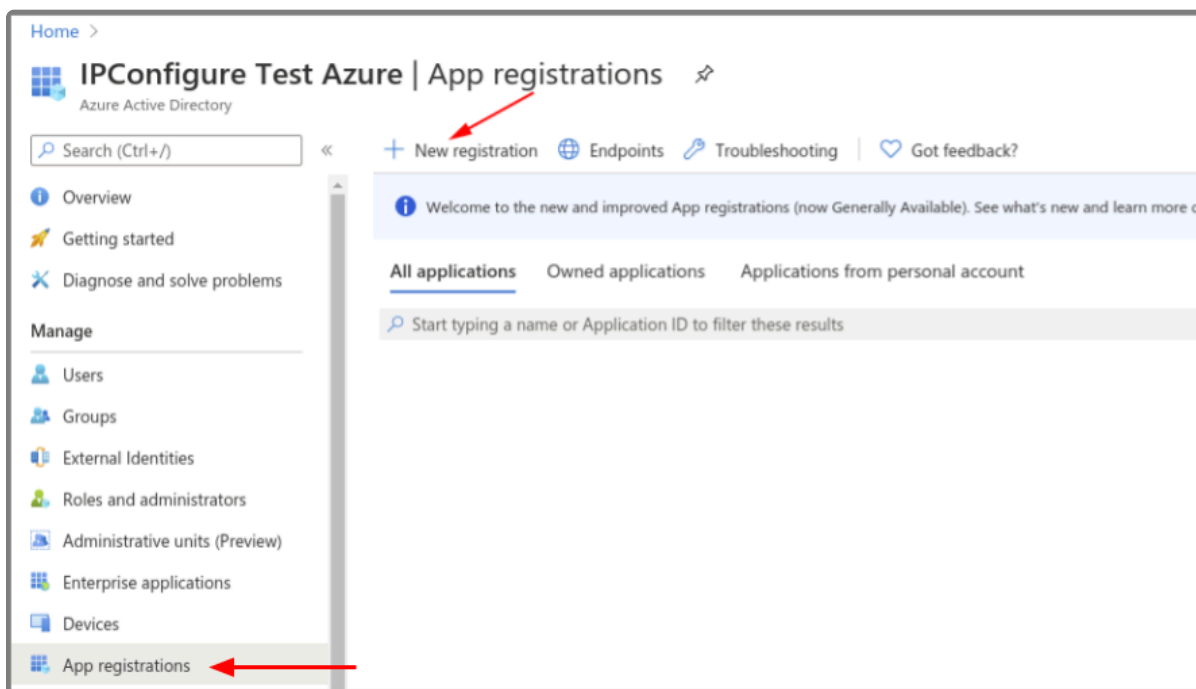
Status Not enabled

Last sync Sync has never run



Register an Azure Active Directory App

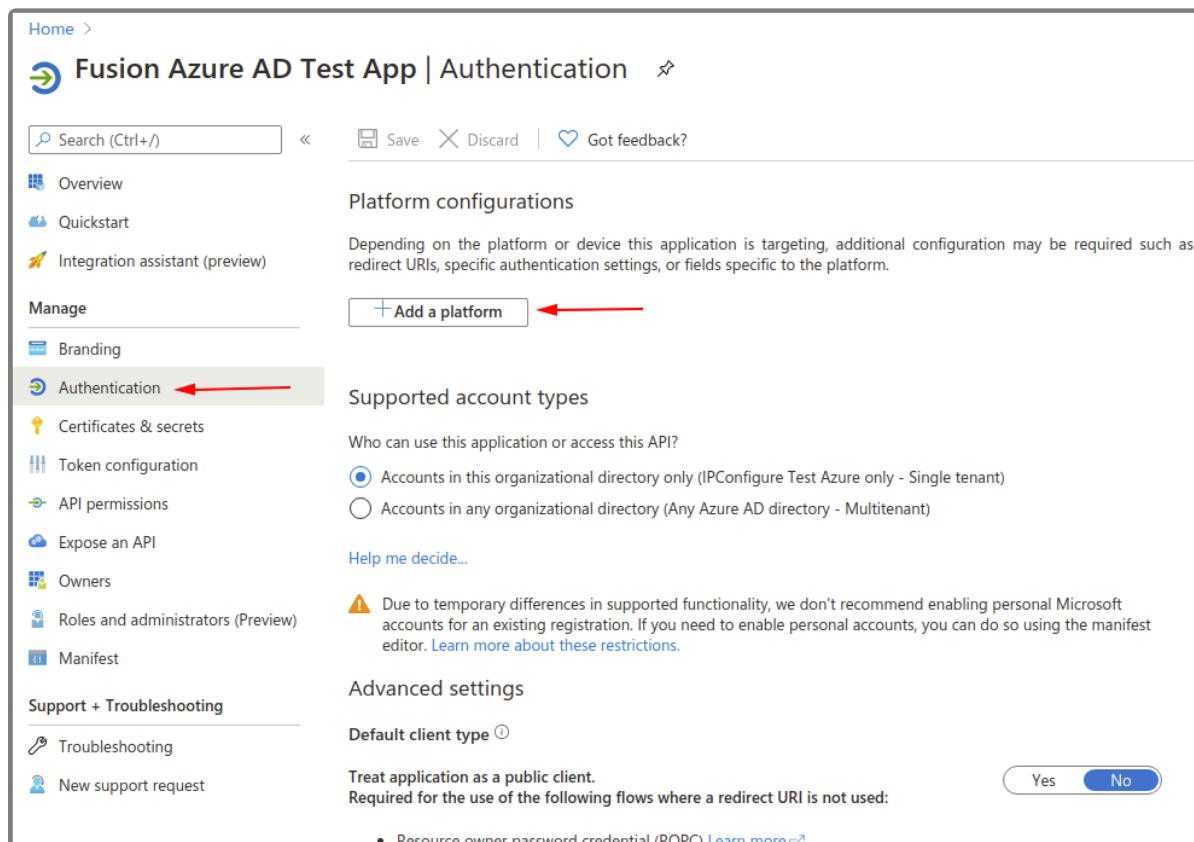
1. To register a New app, be sure to set the following:
 - a. Enter the user-facing display name for this application in the *Name* field.
 - b. Select the *Single Tenant* option under *Supported Account Types*.
 - c. Select the *Client Application* option under *Platform Configuration*.

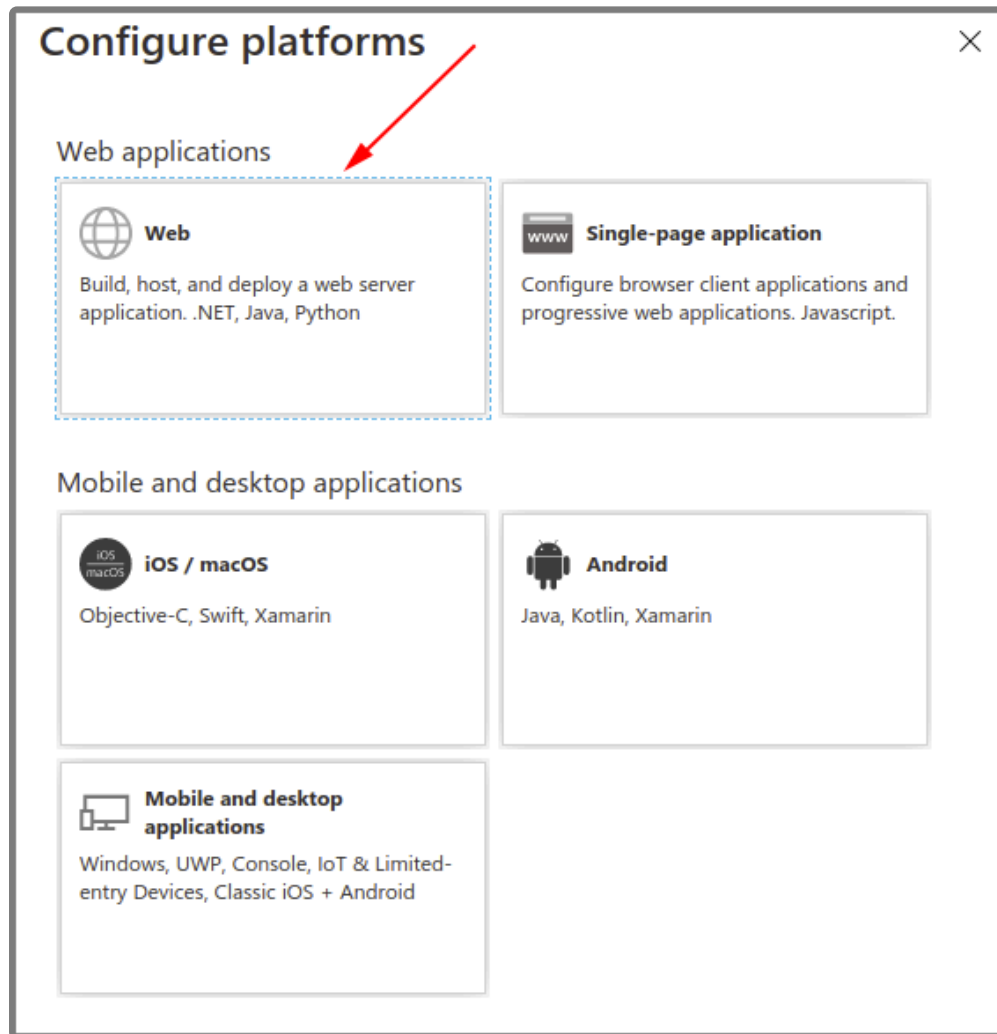


Azure AD App – Authentication – Add a Web Platform

1. Go to *Authentication*, then select *Add a platform*.

- a. Select the *Web* type application.
- b. Enter the Fusion redirect URL: *http(s)://<fusion-url>/redirect.html* in the *Redirect URIs* field (where <fusion-url> is the URL for your Fusion server).





Configure Web

[All platforms](#)[Quickstart](#)[Docs](#)

Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

✓

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Checking Access tokens and ID tokens is recommended only if the application has a single-page architecture (SPA), has no back-end components, does not use the latest version of MSAL.js with auth code flow, or it invokes a web API via JavaScript. ID Token is needed for ASP.NET Core Web Apps. [Learn more about the implicit grant flow](#)

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens☐ ID tokens

Azure AD App – API Permissions

1. Go to *API permissions*, then select *Add a permission*.
 - a. Select the *Microsoft Graph*.
 - b. Select the *Directory.Read.All* delegated permission.

Copyright © 2024 IPConfigure

Page 69 of 100

Home > Fusion Azure AD Test App | API permissions

Search (Ctrl+/) « Refresh

Overview
Quickstart
Integration assistant (preview)

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- Owners
- Roles and administrators (Preview)
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for IPConfigure Test Azure

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

Request API permissions

Select an API

Microsoft APIs

APIs my organization uses

My APIs

Commonly used Microsoft APIs



Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Service Management

Programmatic access to much of the functionality available through the Azure portal



Office 365 Management APIs

Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

Request API permissions

< All APIs

Microsoft Graph
<https://graph.microsoft.com/>
[Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Directory.Read.All

Permission

Admin consent required

▼ Directory (1)

<input checked="" type="checkbox"/>	Directory.Read.All Read directory data	Yes
-------------------------------------	---	-----

2. Select *Grant admin consent* for your application.

Home >

Fusion Azure AD Test App | API permissions

Search (Ctrl+/) << Refresh

[Overview](#)
[Quickstart](#)
[Integration assistant \(preview\)](#)

Manage

[Branding](#)
[Authentication](#)
[Certificates & secrets](#)
[Token configuration](#)
[API permissions](#)
[Expose an API](#)
[Owners](#)
[Roles and administrators \(Preview\)](#)
[Manifest](#)

Support + Troubleshooting

[Troubleshooting](#)
[New support request](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the all the permissions the application needs. [Learn more about permissions and consent](#)

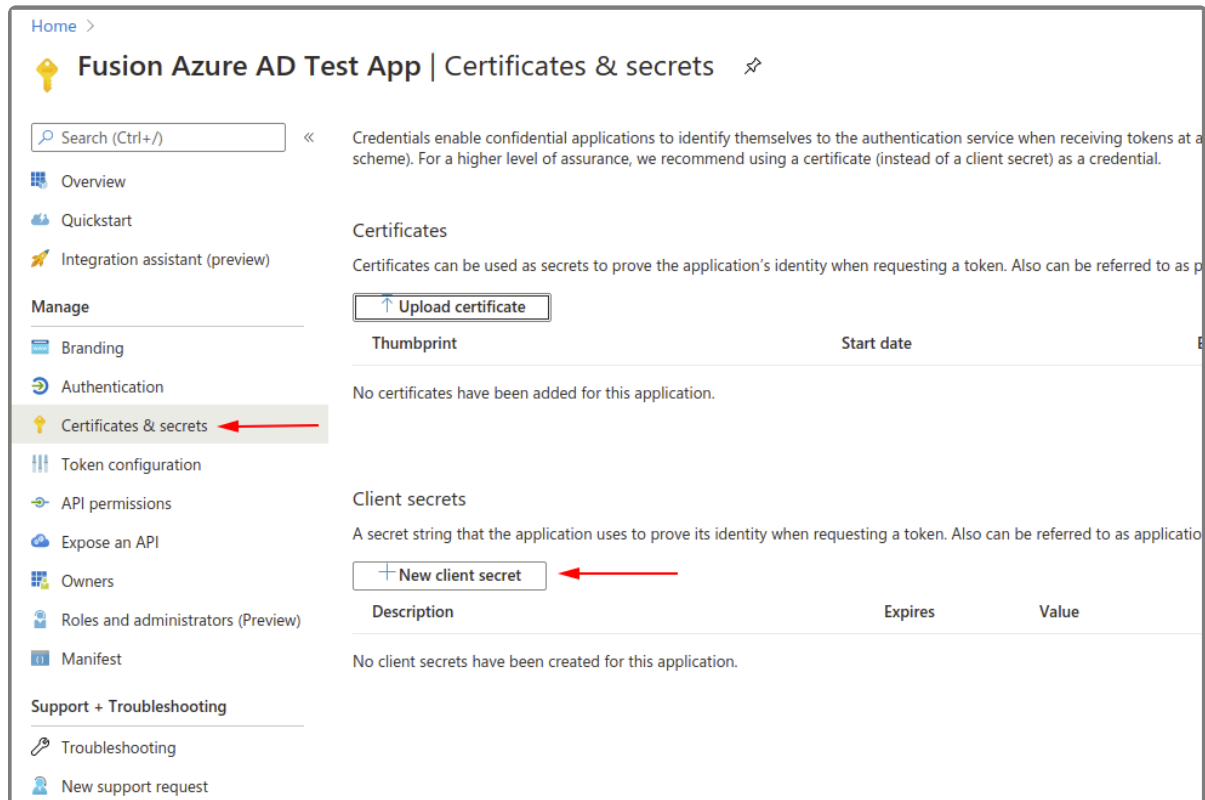
[+ Add a permission](#)
[Grant admin consent for IPConfigure Test Azure](#)

API / Permissions name	Type	Description
▼ Microsoft Graph (2)		
Directory.Read.All	Delegated	Read directory data
User.Read	Delegated	Sign in and read user profile

Azure AD App – Certificates & Secrets – Create a New Client Secret

1. Select *New client secret* to create a new secret value.
2. **Save** the secret value because it will not be available later. (Copy the secret value to a

secure location.)



Azure AD App – Save the Client ID and OAuth 2.0 Authorization Endpoint (v1)

1. Go to the *Overview*.
 - a. Make note of the *Azure Application (client) ID* value for later use.
2. Select *Endpoints*.
 - a. Make note of the *OAuth 2.0 authorization endpoint (v1)* value for later use.

Home > IPConfigure Test Azure | App registrations >

Fusion Azure AD Test App

Search (Ctrl+/) << Delete Endpoints

Overview Quickstart Integration assistant (preview)

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators (Preview)
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Display name : Fusion Azure AD Test App

Application (client) ID : 81efca5b-d0ac-426e-9b7f-f02fd862cfe0

Directory (tenant) ID : 5b7c499d-21e7-4004-987c-71131d12bd60

Object ID : fef86a6c-701e-44e4-8d97-03e70cb0e61e

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)?

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API permissions](#)

Endpoints

OAuth 2.0 authorization endpoint (v2)

<https://login.microsoftonline.com/5b7c499d-21e7-4004-987c-71131d12bd60/oauth2/v2.0/authorize>

OAuth 2.0 token endpoint (v2)

<https://login.microsoftonline.com/5b7c499d-21e7-4004-987c-71131d12bd60/oauth2/v2.0/token>

OAuth 2.0 authorization endpoint (v1)

<https://login.microsoftonline.com/5b7c499d-21e7-4004-987c-71131d12bd60/oauth2/authorize>

OAuth 2.0 token endpoint (v1)

<https://login.microsoftonline.com/5b7c499d-21e7-4004-987c-71131d12bd60/oauth2/token>

At this point, you should have all of the required values to enable Azure Active Directory-based authentication in Orchid Fusion VMS. Return to the previous section ([Enabling Azure Active Directory](#)) for instructions on modifying the Orchid Fusion VMS configuration file to enable Azure Active Directory authentication. Once enabled, you may add one or more Orchid Fusion VMS *Permission Groups* that pull users from your Azure Active Directory. (For details on adding *Permission Groups*, please refer to the *Add a Permission Group for Azure Active Directory* section in the [Orchid Fusion VMS Administrator Guide](#).)

Enabling FreeIPA Authentication

Orchid Fusion VMS allows FreeIPA authentication. By performing some configuration work on the front end, your Orchid Fusion VMS users will be able to sign in with their existing FreeIPA credentials.

* If you are using Orchid Hybrid VMS, remember that it is a managed system. IPConfigure Support staff will need to configure the system to use FreeIPA authentication.

Prerequisites

To configure Orchid Fusion VMS to work with FreeIPA, you will need to have an FreeIPA server that:

- Is reachable from your Orchid Fusion VMS server.
- Contains at least one FreeIPA user who is a member of at least one FreeIPA group.

Modifying the Configuration File

There are a couple of properties in the Orchid Fusion VMS configuration file that will need to be modified in order for FreeIPA authentication to work.

* For extra help with the steps below, please refer back to the *Installation* section that corresponds to the operating system in which you are working.

1. Set the following properties in the Orchid Fusion VMS configuration file:

- `authentication.freeipa.servers=`
`<domain1>|<domainServerAddress1>,<domain2>|<domainServerAddress2>`
 - Replace `<domain1>` with the domain on which your first FreeIPA server exists.
Replace `<domainServerAddress1>` with the address of your first FreeIPA server.
- `authentication.freeipa.domain.userdn=` `cn=<domain>-users,cn=<domain>-accounts`
 - Replace *domain* with one of the configured FreeIPA servers. Replace `<domain>` with the name of the alternate user container.

* `<domainServerAddress>` may be a DNS name or IP address and may be prefixed with either `ldap://` or `ldaps://` to specify the protocol.

2. After modifications to the configuration file are complete, restart the Orchid Fusion VMS service, then sign in to Orchid Fusion VMS.

Refer to the *Add a Permission Group for FreeIPA* section of the [Orchid Fusion VMS Administrator Guide](#) for instructions on setting *FreeIPA Permission Groups*.

Enabling Single Sign-On with SAML

Orchid Fusion VMS now supports Single Sign-On with SAML. SAML is an open standard that allows Orchid Fusion VMS customers to use a third-party identity provider (such as Ping, Auth0, Microsoft Entra ID, or Google Workspace) to manage the users and permissions for logging into Orchid Fusion VMS. By performing some configuration work on the front end, your Orchid Fusion VMS users will be able to sign in with their third-party credentials.

✿ If you are using Orchid Hybrid VMS, remember that it is a managed system. You will need to submit a ticket with IPConfigure Support for assistance in configuring SAML.

Configuration Overview

To configure Orchid Fusion VMS to work with SAML authentication, you will generally follow this sequence:

- Modify your Orchid Fusion VMS properties file to include the required SAML settings.
- Use your SAML Identity Provider's web interface to establish Orchid Fusion VMS as a web application.
- Restart the Orchid Fusion VMS service.
- Associate Fusion *Permission Groups* with the SAML groups that now have login access to Orchid Fusion VMS.

Please refer to the next several sections for expanded details on configuring the system for SAML.

Modify the Fusion Configuration File

There are several properties related to SAML authentication that will need to be added to the Orchid Fusion VMS configuration file. So as a first step, get the configuration file ready for these new settings. You won't be able to fully configure the last three properties until you have configured your Identity Provider (IdP) (which will be explained later).

✿ For extra help with the steps below, please refer back to the *Installation* section that corresponds to the operating system in which you are working.

1. Open the *fusion.properties* file.
2. Add the following properties to the Orchid Fusion VMS configuration file:
 - **fusion.public.url=https://your-url**
 - This is the public URL used to access your Orchid Fusion VMS.
 - **saml.common.setting.domain=yourdomain.com**
 - This is your domain name which will be used later to configure permissions.
 - **saml.provider.samlclient1.common.name=IdP Vendor**
 - This is the provider name that will be displayed on the Orchid Fusion login page (such as *Okta*, *Ping*, etc.).
 - **saml.provider.samlclient1.idp.metadata.filename=ap-idp-metadata.xml**
 - This is the name of the XML file you will download from your IdP. (We'll cover this in the next section.)
 - If you're working in Linux, this XML file must be placed in the following directory: `/etc/opt/fusion/`
 - If you're working in Windows, this XML file must be placed in the following directory: `C:\Program Files\IPConfigure\Fusion\conf`
 - **saml.provider.samlclient1.attr.key.name=name**
 - **saml.provider.samlclient1.attr.key.group=group**
 - These are the keys that the IdP uses to represent user names and user groups. (We'll cover this in the next section.)
3. Save changes to the properties file. (Don't restart the Fusion service yet. We need to fill in more information first.)

Here's what your Fusion configuration file might look like at this point:

```
Fusion VMS\\library
library.rclone.url=http://localhost:5572
maps.storage.dir=C:\\Program Files\\IPConfigure\\Orchid Fusion VMS
\\maps
library.rclone.token=QjY4SmVkdEpoOTVr2mJqdzBtdkY6b0lCOHBUQjk3TkVSR
lNoZWtXTlU=
properties.version=23.12.1
# URL used to access Orchid Fusion VMS
fusion.public.url=https://{your-url}

# Your domain name which will be used later to configure
permissions
saml.common.setting.domain=yourdomain.com

# Name displayed on the Orchid VMS login page (e.g., "Okta",
"Ping", etc.):
saml.provider.samlclient1.common.name=IdP Vendor

# Name of the XML file you downloaded from your Identity Provider
# (see next section). Make sure that this file is in the
directory
# /etc/opt/fusion/ for Linux, or C:\\Program Files\\IPConfigure
\\Fusion\\conf
# on Windows.
saml.provider.samlclient1.idp.metadata.filename=ap-idp-
metadata.xml

# The keys used by your Identity Provider to represent user names
# and user groups (see next section).
saml.provider.samlclient1.attr.key.name=name
saml.provider.samlclient1.attr.key.group=group
```

- ✿ Note that up to five separate SAML identity providers can be configured and used in Orchid Fusion VMS. Specify additional providers by copying the last four properties (those that include “samlclient1” in the name). You will need one complete set of four properties for each IdP you want to configure. Then for each additional set, replace “samlclient1” with the appropriate client name (“samlclient2”, “samlclient3”, “samlclient4”, or “samlclient5”).

Configuring an Identity Provider

SAML authentication may be used with a wide variety of Identity Providers. The steps required to configure each IdP will vary based on the IdP vendor's web interface. In this section, we will provide the basic steps that should work with any IdP, although the order of the steps may vary by vendor. After you read through these steps, you'll find more specific details in the topics that focus on these Identity Providers:

- [Google Workspace](#)
- [Microsoft Entra ID](#) (formerly Azure AD)
- [Auth0](#)
- [Ping](#)

If your vendor isn't listed, or you need additional assistance, please contact IPConfigure Technical Support.

Create a New Web Application Configuration

1. To configure your Identity Provider to support Orchid Fusion VMS, you will create a new web application configuration. For this, you will need to set the following properties: the *ACS URL*, the *Entity ID*, and the *Start URL*.
 - Set the *ACS (Assertion Consumer Service) URL*.
 - `https://your-url/service/sessions/login/samlCallback?client_name=samlclient1`
 - Set the *Entity ID*.
 - `https://your-url/service/sessions/login/samlCallback?client_name=samlclient1`
 - Set the *Start URL*. (This is the same as your Fusion public URL.)
 - `https://your-url`

✿ If you are configuring multiple identity providers, you will need to replace the value of "samlclient1" with the appropriate client name ("samlclient2", "samlclient3", and so on).

2. Within the IdP web interface, ensure that there are mappings from each user's IdP username (or email address) and group(s) to SAML attributes. The names of these mapped attributes are specified in the Orchid Fusion VMS properties file:

```
saml.provider.samlclient1.attr.key.name=name-mapping  
saml.provider.samlclient1.attr.key.group=group-mapping
```

3. Once you have the name and group mapping info, you will need to copy it into the

fusion.properties file (as covered in the previous topic).

Download an XML Metadata File

1. Next, download an XML metadata file from your IdP's web interface.
2. Copy this file into your Orchid Fusion VMS server's configuration directory.
 - a. In Linux: `/etc/opt/fusion/`
 - b. In Windows: `C:\Program Files\IPConfigure\Fusion\conf`
3. Now you need to copy the metadata filename into the *fusion.properties* file (as covered in the previous [topic](#)):

`saml.provider.samlclient1.idp.metadata.filename=file-name`

Additional Steps

1. Depending on your IdP vendor, you may also need to specify which users or groups are allowed to log in to Orchid Fusion VMS. (This will only affect users' ability to log in; it does not grant them access to any Orchid Recorders or cameras.)
2. Additionally, some IdPs may require that you explicitly enable the new web application from their web interface.
3. Once all other steps are complete, save the *fusion.properties* file and restart the Orchid Fusion VMS service.
4. Now, log into Orchid Fusion VMS as an Administrator and go to the *Permission Groups* screen. This is where you will add your new groups and assign permissions. (For more details, please refer to [Assigning Permissions to SAML Users](#).)

Identity Provider: Google Workspace

Orchid Fusion VMS now supports Single Sign-On with SAML. One of the Identity Providers (IdPs) supported by SAML is Google Workspace. By performing some configuration work on the front end, your Orchid Fusion VMS users will be able to sign in with their Google credentials.

Configuring a SAML App in Google Workspace

The steps below should help you create and configure an application in Google Workspace.

1. First, review the Google Workspace Admin Help article linked here: [Set up your own custom SAML app](#). This article includes detailed steps for creating and configuring your app.
2. As you configure your SAML app in Google Workspace, select *Option 1: Download IdP metadata*. Click the **Download Metadata** button.
3. Once downloaded, you will need to copy this file into the Orchid Fusion VMS configuration directory, and add the filename to the *fusion.properties* file (as detailed in [Modify the Fusion Config File](#)).
4. Now you need to configure the *Service Provider Details*.
 - a. The example pictured below shows which fields you need to complete.
 - b. For the *Name ID format*, use the drop-down list to select *EMAIL*.

Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. [Learn more](#)

ACS URL
https://{your-url}/service/sessions/login/samlCallback?client_name=samlclient1
Invalid format for ACS URL

Entity ID
https://{your-url}/service/sessions/login/samlCallback?client_name=samlclient1

Start URL (optional)
https://{your-url}

☐ Signed response

Name ID

Defines the naming format supported by the identity provider. [Learn more](#)

Name ID format
EMAIL

Name ID
Basic Information > Primary email

5. Now, go to *Attribute mapping* to configure the Google Workspace fields that Orchid Fusion

VMS will use to identify a user's username and permission group(s). This will also configure the Google Workspace groups that are allowed to sign into Orchid Fusion VMS.

- a. The example pictured below will help you complete the *Attributes* and *Group membership* sections.
- b. The Google groups that you specify here will also need to be assigned to Permission Groups in Orchid Fusion VMS. (More details on this in the last [SAML](#) section.)

The screenshot displays two configuration sections. The top section, titled 'Attributes', shows a mapping from 'Primary email' (under 'Google Directory attributes') to 'name' (under 'App attributes'). A red arrow points to 'Primary email' and another to 'name'. Below this is an 'ADD MAPPING' button. The bottom section, titled 'Group membership (optional)', shows 'orchid-hybrid-admins' and 'orchid-hybrid-viewers' (under 'Google groups') mapped to 'group' (under 'App attribute'). Red arrows point to 'orchid-hybrid-admins' and 'group'. At the bottom are 'BACK', 'CANCEL', and 'FINISH' buttons.

6. Based on the example above, the *attribute key name* and *attribute key group* properties would look like this when you add them to the *fusion.properties* file:

```
saml.provider.samlclient1.attr.key.name=name  
saml.provider.samlclient1.attr.key.group=group
```

Turning on the SAML Web App

By default, the SAML web app will be marked as *OFF for everyone* in the Google Admin Interface. Before you continue, make sure to enable the app for one or more organizational units.

Complete the Configuration

1. After all of the configuration steps have been completed, you'll need to do the following:
 - a. Restart the Orchid Fusion VMS service. For extra help, please refer back to the *How to Manage the Orchid Fusion VMS Services* section that corresponds to the operating system in which you are working.
 - b. Go to Fusion and associate your Permission Groups with your IdP (Google) groups. Please refer to the last [SAML](#) section for details.

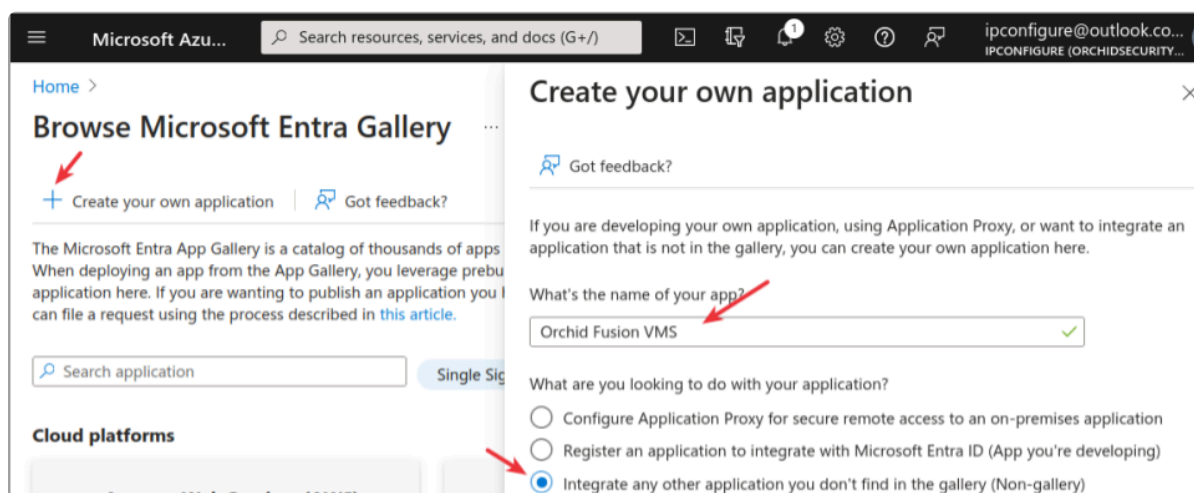
Identity Provider: Microsoft Entra ID (formerly Azure AD)

Orchid Fusion VMS now supports Single Sign-On with SAML. One of the Identity Providers (IdPs) supported by SAML is Microsoft Entra ID (formerly known as Azure AD). By performing some configuration work on the front end, your Orchid Fusion VMS users will be able to sign in with their Microsoft Entra credentials.

Configuring a SAML App in Microsoft Entra ID

The steps below should help you create and configure a SAML application in Microsoft Entra ID.

1. First, review the Microsoft article linked here: [Enable single sign-on for an enterprise application](#). This will provide you with the most detailed instructions to follow.
2. Since Orchid Fusion VMS is a “non-gallery” application, you will need to select *Create your own application* as shown below.



3. In the *SAML-based Sign-On/Basic SAML Configuration* section, you will need to set the following:
 - a. Identifier (Entity ID)
 - b. Reply URL (ACS URL)
 - c. Sign on URL (This is the Fusion public URL.)

We discussed these earlier in the [Configuring an Identity Provider](#) overview topic. These settings are pictured below.

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

✓ ☒ ⓘ

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

✓ ✓ ☒ ⓘ

[Add reply URL](#)

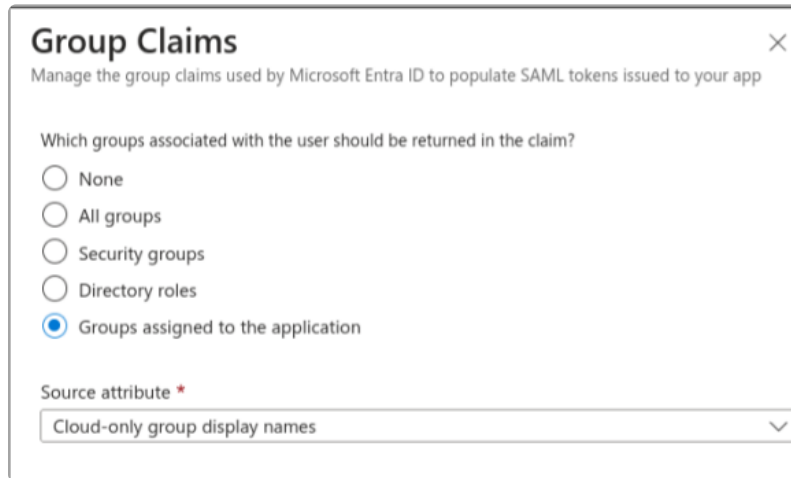
Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

✓

4. Next, you'll need to configure the *Attributes & Claims* section so that Microsoft Entra ID values correctly map to Orchid Fusion VMS users and groups.
 - a. First, map the Required "Name ID" claim to use `user.objectid` as its value.
 - b. Ensure there is a claim for the *value* `user.userprincipalname` with the *name* `name` (which may already exist).
 - c. Add a group claim for the *value* `user.groups[ApplicationGroup]` with the *name* `groups`. (This mapping will be created automatically when you create the *Group Claim*.)
 - i. Configure this *Group Claim* to work only with "Groups assigned to the application".
 - ii. As the *Source attribute*, select "Cloud-only group display names".

✿ In order to configure Microsoft Azure group names (and not raw GUID values) within Orchid Fusion VMS, you must have one of the following Azure product tiers: Azure Active Directory Premium P1 or Microsoft Entra ID P1.



5. Based on the settings described above, the *attribute key name* and *attribute key group* properties would look like this when you add them to the *fusion.properties* file:

saml.provider.samlclient1.attr.key.name=name

saml.provider.samlclient1.attr.key.group=groups

6. In the *SAML-based Sign-On/SAML Certificates* section, you will need to select *Federation Metadata XML → Download* to get the SAML configuration file needed by Orchid Fusion.
7. Once downloaded, you will need to copy this file into the Orchid Fusion VMS configuration directory, and add the filename to the *fusion.properties* file (as detailed in [Modify the Fusion Config File](#)).

Complete the Configuration

1. After all of the configuration steps have been completed, you'll need to do the following:
 - a. Restart the Orchid Fusion VMS service. For extra help, please refer back to the *How to Manage the Orchid Fusion VMS Services* section that corresponds to the operating system in which you are working.
 - b. Go to Fusion and associate your *Permission Groups* with your IdP (Microsoft Entra ID) groups. Please refer to the last [SAML](#) section for details.

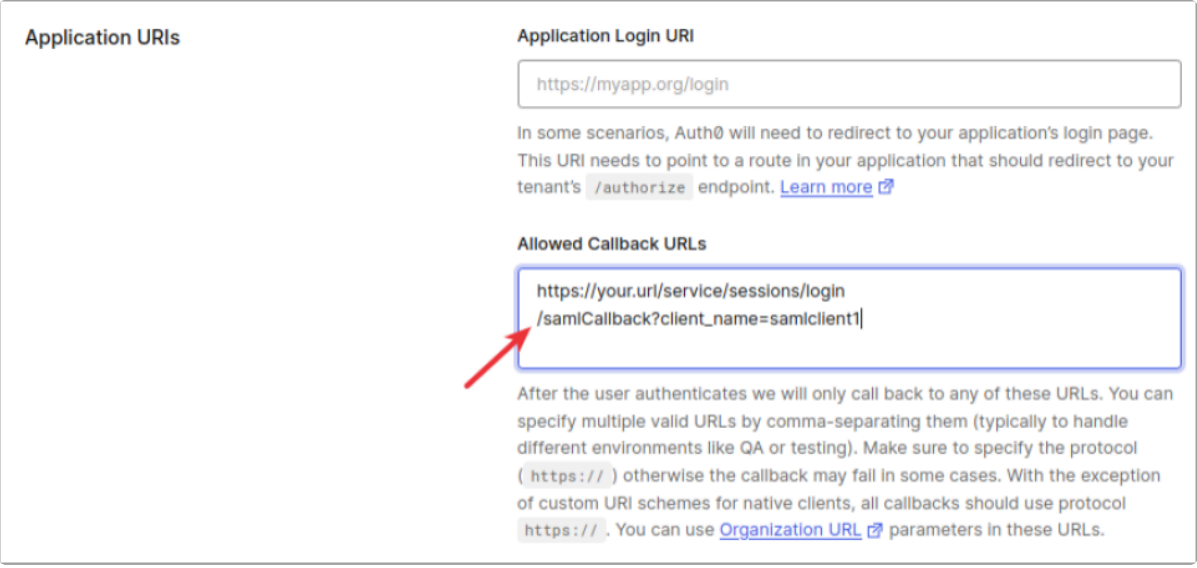
Identity Provider: Auth0

Orchid Fusion VMS now supports Single Sign-On with SAML. One of the Identity Providers (IdPs) supported by SAML is Auth0. By performing some configuration work on the front end, your Orchid Fusion VMS users will be able to sign in with their Auth0 credentials.

Configuring a SAML App in Auth0

The steps below should help you create and configure a SAML application in Auth0.

1. First, review the Auth0 article linked here: [Configure Auth0 as SAML Identity Provider](#). This will provide you with the most detailed instructions to follow.
2. After you create an Orchid Fusion VMS web application with type *Regular Web Application*, go to the *Settings* tab.
 - a. Under *Application URIs*, set the *Allowed Callback URLs* to the “ACS” value described earlier in the [Configuring an Identity Provider](#) overview section.



Application URIs

Application Login URI

https://myapp.org/login

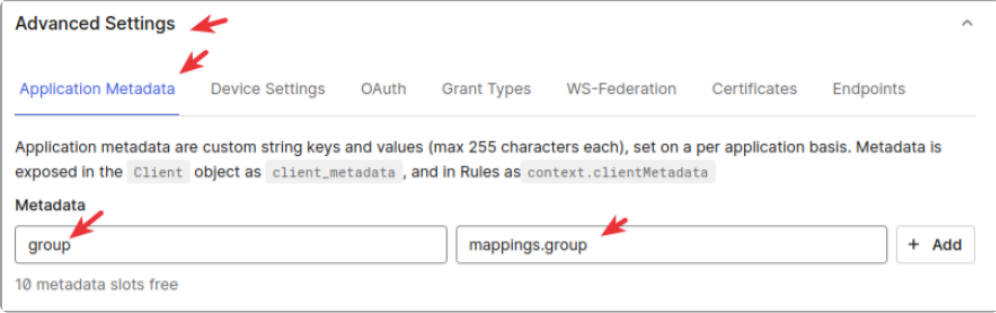
In some scenarios, Auth0 will need to redirect to your application's login page. This URI needs to point to a route in your application that should redirect to your tenant's `/authorize` endpoint. [Learn more](#)

Allowed Callback URLs

https://your.url/service/sessions/login/samlCallback?client_name=samlclient1

After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol (`https://`) otherwise the callback may fail in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol `https://`. You can use [Organization URL](#) parameters in these URLs.

3. Next, scroll down to *Advanced Settings* and create a Metadata mapping group called `mappings.group`.



Advanced Settings

Application Metadata | Device Settings | OAuth | Grant Types | WS-Federation | Certificates | Endpoints

Application metadata are custom string keys and values (max 255 characters each), set on a per application basis. Metadata is exposed in the `Client` object as `client_metadata`, and in Rules as `context.clientMetadata`

Metadata

group mappings.group + Add

10 metadata slots free

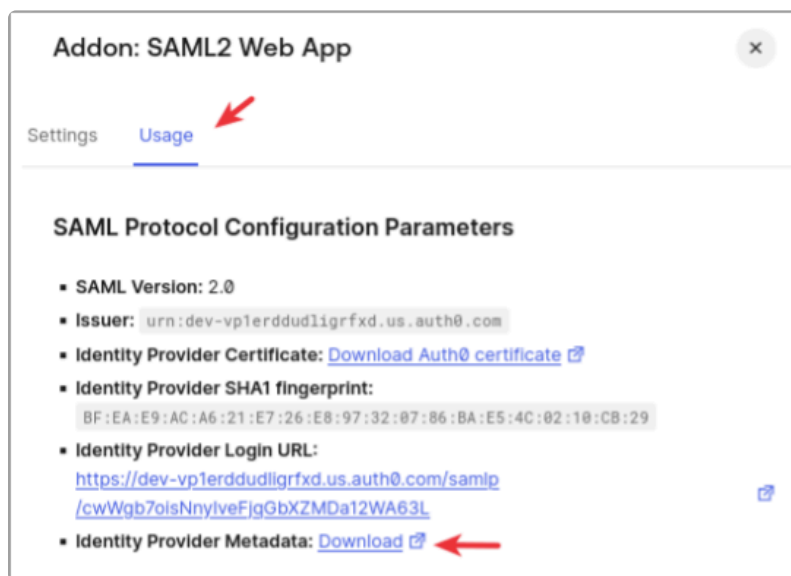
4. Save your changes.

5. Now, find the *Addons* tab and enable *SAML2W WEB APP*.
6. Under *Settings*, the *Application Callback URL* should be configured with the “ACS” value you set in step 2a.
7. Scroll down and click *Enable*, then click *Save*.

Based on the settings above, the *attribute key name* and *attribute key group* properties would look like this when you add them to the *fusion.properties* file:

```
saml.provider.samlclient1.attr.key.name=name  
saml.provider.samlclient1.attr.key.group=group
```

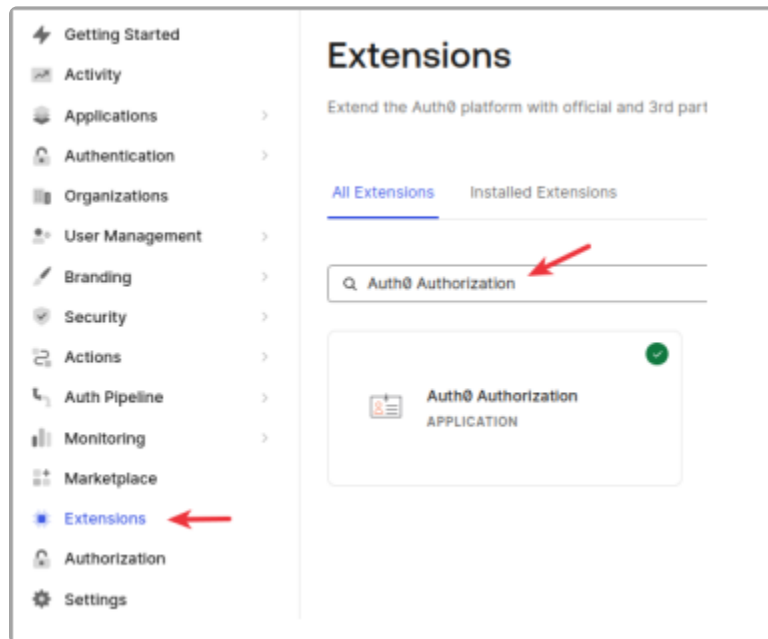
8. Next, in the *SAML2W WEB APP* section, go to the *Usage* tab.
9. Find *Identity Provider Metadata* and click *Download*.



10. Once downloaded, you will need to copy this file into the Orchid Fusion VMS configuration directory, and add the filename to the *fusion.properties* file (as detailed in [Modify the Fusion Config File](#)).

Now you need to associate Auth0 users with Groups whose permissions can be configured in Orchid Fusion VMS. To do this, you need to install the *Auth0 Authorization* extension.

11. In the Auth0 web interface, go to *Extensions*.
12. Click on the *All Extensions* tab.
13. Click *Auth0 Authorization* to create one or more Groups containing members who will be granted access to Orchid Fusion VMS.



Complete the Configuration

1. After all of the configuration steps have been completed, you'll need to do the following:
 - a. Restart the Orchid Fusion VMS service. For extra help, please refer back to the *How to Manage the Orchid Fusion VMS Services* section that corresponds to the operating system in which you are working.
 - b. Go to Fusion and associate your *Permission Groups* with the IdP (Auth0) groups. Please refer to the last [SAML](#) section for details.

Identity Provider: Ping

Orchid Fusion VMS now supports Single Sign-On with SAML. One of the Identity Providers (IdPs) supported by SAML is Ping. By performing some configuration work on the front end, your Orchid Fusion VMS users will be able to sign in with their Ping credentials.

Configuring a SAML App in Ping

The steps below should help you create and configure a SAML application in Ping.

1. First, review the Ping article linked here: [Add a SAML application](#). This will provide you with the most detailed instructions to follow.
2. Under SAML Configuration, select the *Manually Enter* radio button.
3. Now enter the ACS URL and the Entity ID in the fields provided. (These values are defined in the [Configuring an Identity Provider](#) overview section.)

Add Application

SAML Configuration

Provide Application Metadata

☐ Import Metadata ☐ Import From URL ☒ Manually Enter

ACS URLs *

+ Add

Entity ID *

4. Under *Attribute Mapping*, create two additional entries to map Ping identity values to Orchid Fusion VMS users and groups.

Attributes	PingOne Mappings	Required
saml_subject	User ID	<input checked="" type="checkbox"/>
group	Group Names	<input type="checkbox"/>
name	Username	<input type="checkbox"/>

Based on the settings above, the *attribute key name* and *attribute key group* properties would look like this when you add them to the *fusion.properties* file:

```
saml.provider.samlclient1.attr.key.name=name
```

```
saml.provider.samlclient1.attr.key.group=group
```

5. In the *Configuration* section, select *Download Metadata* to get the SAML configuration file needed by Orchid Fusion.
6. Once downloaded, you will need to copy this file into the Orchid Fusion VMS configuration directory, and add the filename to the *fusion.properties* file (as detailed in [Modify the Fusion Config File](#)).
7. Within the Ping web interface, in the *Applications* list, make sure that the Orchid Fusion application is *enabled*. (It may be disabled, by default.)

Complete the Configuration

1. After all of the configuration steps have been completed, you'll need to do the following:
 - a. Restart the Orchid Fusion VMS service. For extra help, please refer back to the *How to Manage the Orchid Fusion VMS Services* section that corresponds to the operating system in which you are working.
 - b. Go to Fusion and associate your *Permission Groups* with the IdP (Ping) groups. Please refer to the next [SAML](#) section for details.

Assigning Permissions to SAML Users

Once your Orchid Fusion VMS properties file and Identity Provider web interface have been configured, you need to assign Fusion permissions for each of the groups you created within the IdP.

1. With SAML fully configured, restart the Orchid Fusion VMS service.
2. Now you need to associate your Orchid Fusion VMS *Permissions Groups* with the Identity Provider's groups.
 - a. Log into Fusion as an Administrator.
 - b. Go to the *Permission Groups* screen.
 - c. For each of your IdP groups that need to log into Fusion, do the following:
 - i. Click the **Add Permission Group** button. (You may add these new groups to an existing *Permission Group* instead, if desired.)
 - ii. Enter a name and description for the new group.
 - iii. Go to the *External Group Mapping* section. (If this section does not appear, there must be a problem with the SAML configuration. The configuration may be incomplete or inaccurate, or you may have forgotten to restart the Fusion service.)
 - iv. Click in the *Domain* field and enter the name of the domain in which your target users exist. (This should match the value you configured as `saml.common.setting.domain` in the *fusion.properties* file.)
 - v. Click in the *Group* field and enter the name of a group in which your target SAML users exist. (This should match the name of a group from any one of your configured IdPs.)
 - vi. Click the **Add** icon to add this new external group.
 - vii. Grant and revoke abilities and access to cameras, as needed.
 - viii. Click the **Save** button to save the *Permission Group*.

In the following example, we have a *Permission Group* that provides Administrator access to users in the `orchid-hybrid-admins` SAML group. (In this case, that's the name of a Google Workspace group):

External Group Mappings ⓘ

Domain	Group
ipconfigure.com	orchid-hybrid-admins

Apps
All Apps

☒ Administrator Group ☐ Library Access ⓘ

CANCEL SAVE GROUP

For additional details on adding external *Permission Groups*, please refer to the [Orchid Fusion/Hybrid Administrator Guide](#).

Enabling External Cloud Storage

Beginning with version 21.3, Orchid Fusion VMS supports the exporting of *Library* files to an external cloud storage service. By performing some configuration work on the front end, your Orchid Fusion VMS will automatically send all *Library* files to the selected cloud service (instead of the local Orchid Fusion VMS server). You will be able to view and share exported video files using that cloud service.

The process is fairly straightforward. Orchid Fusion VMS utilizes an open-source library called *Rclone* to communicate with the external cloud storage service. Using *Rclone*, you may choose one of the many supported cloud storage options, such as Box.com, Dropbox, Google Drive, and Microsoft OneDrive. Once *Rclone* is set up, you'll configure Orchid Fusion VMS to use *Rclone* as the gateway to your external cloud storage.

* If you are using Orchid Hybrid VMS, IPConfigure Support staff will need to configure the system to work with an external cloud storage service.

Prerequisites

In order to work with an external cloud storage system:

- You must have installed a version of Orchid Fusion VMS that includes a bundled *Rclone* executable. (This includes versions 21.3.0 and higher.)
- You must use this bundled version of *Rclone* to configure your cloud storage account (remote).

Set Up Your Preferred Cloud Storage Service in Rclone

Follow the steps below to configure *Rclone* to use your preferred cloud storage solution and create the *remote*.


1. Go to the *Rclone* website at <https://rclone.org>.
 - a. Scroll down until you find the list of supported cloud storage providers.
 - b. Click the **Config** button next to your preferred provider for instructions on how to create an *Rclone remote*. (These instructions will vary based on the provider that you select.) Make note of the specific command required to configure *Rclone* for the selected cloud storage provider.
2. To begin configuration and create a *remote*, go to the command line on your Orchid Fusion VMS server. (In Windows, make sure you run the Command Prompt as an Administrator.) In this next step, we'll instruct the system to access the *Rclone* executable and *Rclone* configuration file that were bundled with Fusion, then we'll specify the *rclone* command we want to run.

- a. (In Linux) Type the following command: `sudo /opt/fusion/bin/rclone --config /etc/opt/fusion/rclone.conf (command)` (where the *command* is the one you noted in step 1b). Then press **Enter**.
- b. (For Windows) Type the following command: `C:\Program Files\IPConfigure\Orchid Fusion VMS\bin\rclone.exe --config "C:\Program Files\IPConfigure\Orchid Fusion VMS\conf\rclone.conf" (command)` (where the *command* is the one you noted in step 1b). Then press **Enter**.
3. Follow the on-screen prompts to finish creating the *remote*. (You may use the instructions provided on the rclone site as a guide.)

After you run the configuration and create the Rclone *remote*, you can then modify the Orchid Fusion VMS config file.

Modifying the Configuration File

In order for Orchid Fusion VMS to work with the external cloud storage service, you will need to modify the Fusion configuration file.

 For extra help with the steps below, please refer back to the *Installation* section that corresponds to the operating system in which you are working.

1. Set the following property in the Orchid Fusion VMS configuration file:
 - `library.rclone.remote = your-rclone-remote-name`
 - Replace *your-rclone-remote-name* with the name of your Rclone *remote*.
2. After modifications to the configuration file are complete, you'll need to restart the Orchid Fusion VMS service.

Orchid Fusion VMS APPs

Orchid Fusion VMS supports the Application Partner Platform (APP) feature. The *APPs* component allows third-party vendors to customize Orchid Fusion VMS by creating features that live within the Orchid Fusion VMS user interface.

✿ If you are using Orchid Hybrid VMS, IPConfigure Support staff will need to configure the system in order to use APPs.

To Activate the APPs Feature in Orchid Fusion VMS

Follow these steps to setup the *APPs* feature:

1. Obtain the custom application from your developer.
2. Install the application according to the developer's instructions.
3. Modify the Orchid Fusion VMS configuration file. This modification identifies the Orchid Fusion VMS server location at which your custom application is stored.
 - a. Open the Orchid Fusion VMS properties file. (If you need extra help, refer back to the *How to Edit a Configuration File* section that corresponds to the operating system you are using.)
 - b. Modify the `fusion.apps.path` setting to specify where on the server the custom application is being stored. For example: `fusion.apps.path=c:\\apps` (Don't forget to remove the `#` at the beginning of the line.)
 - c. Save your changes and close the configuration file.
4. Restart the Orchid Fusion VMS service. (If you need extra help, refer back to the *How to Manage the Orchid Fusion VMS Service* section that corresponds to the operating system you are using.)
5. Once Orchid Fusion VMS knows where to find the *APPs*, the program will respond by providing the *APPs* option on the *System Menu*.

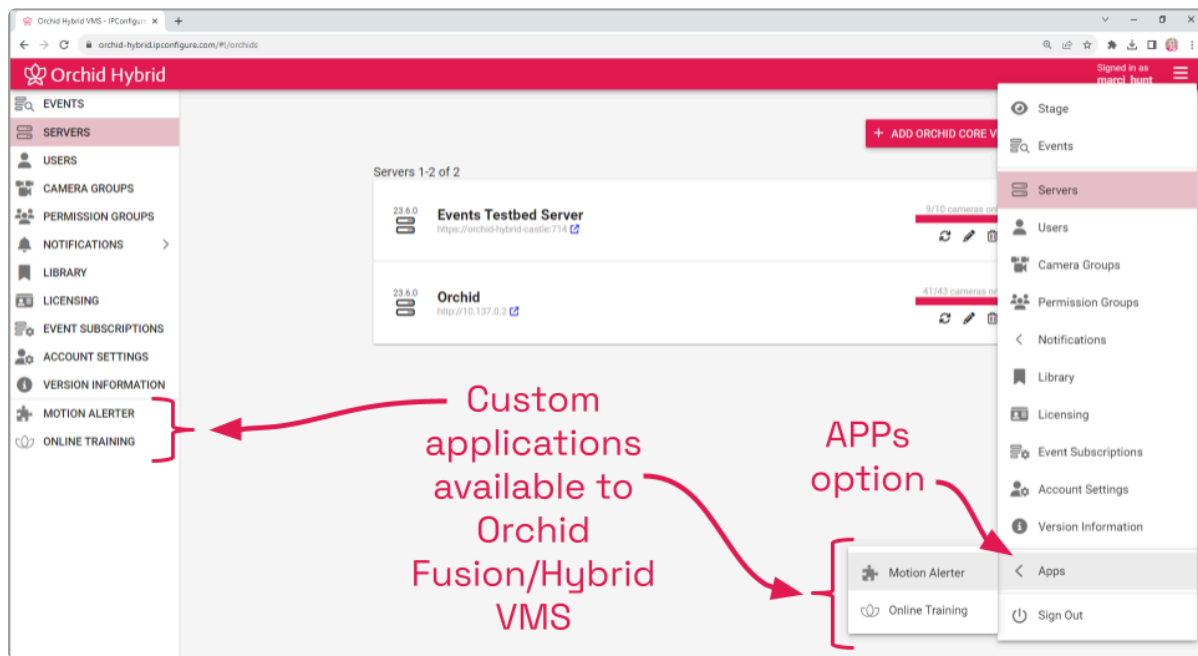
Access the Orchid Fusion VMS APPs Feature

Once the *APPs* feature is activated, you can access your custom applications within Orchid Fusion VMS.

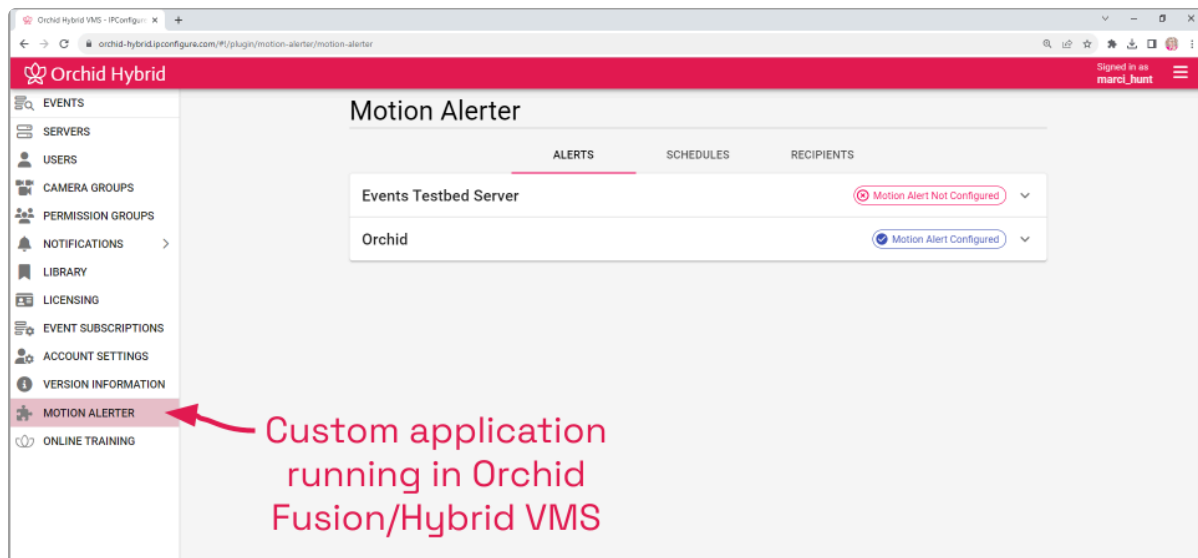
✿ To access the *APPs* feature, you must be a member of a *Permission Group* that has access (such as an *Administrator* group, the *All APPs* group, or an APP-specific group).

1. Open the *System Menu* in the top-right corner of the screen and select *APPs*.

- The *APPs* sub-menu will appear. This sub-menu will list all of the custom applications that Orchid Fusion VMS finds in the location noted in the Fusion properties file, and that you have access to. (Notice that all of your custom applications are now also listed on the *Configuration Menu*, when visible, on the left side of the screen.)



- Click on one of the custom applications to open it within Orchid Fusion VMS.



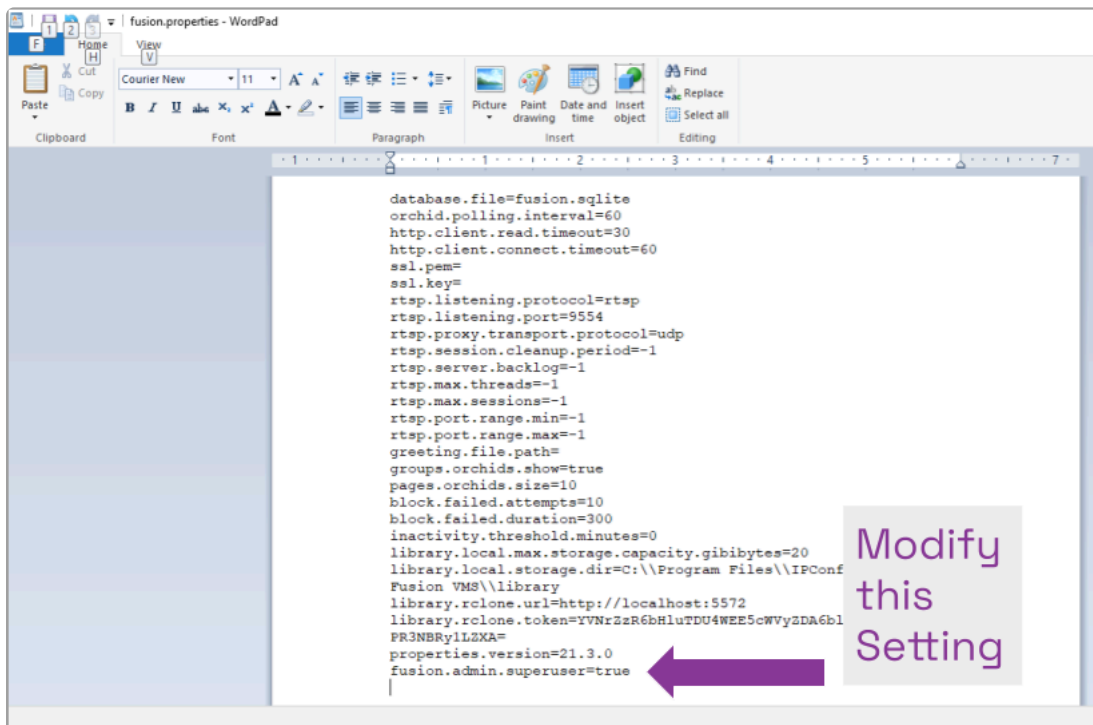
Creating a Superuser

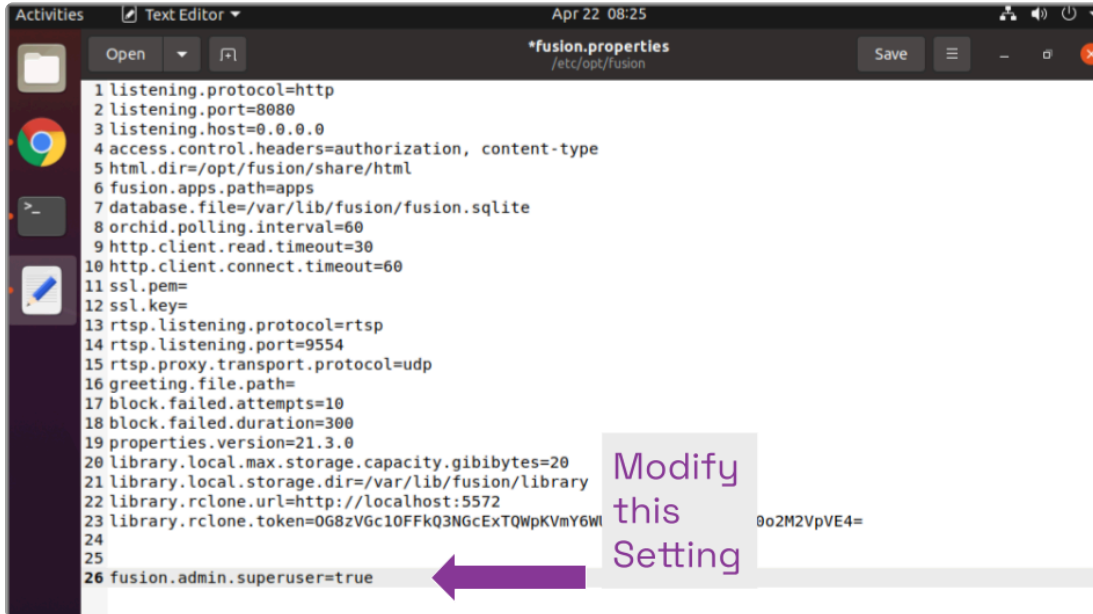
Orchid Fusion VMS allows you to create a *Superuser*. This special administrator account has all of the abilities and access of an administrator, and is protected from edits by any other user. You may create this account by modifying the Orchid Fusion VMS properties file.

✿ In order to perform this change, you must be signed in as an Administrator, and you must be using standard or Google authentication.

✿ If you are using Orchid Hybrid VMS, IPConfigure Support staff will need to configure the system to create a Superuser.

1. Open the Orchid Fusion VMS properties file. (If you need extra help, refer back to the *How to Edit a Configuration File* section that corresponds to the operating system you are using.)





```
1 listening.protocol=http
2 listening.port=8080
3 listening.host=0.0.0.0
4 access.control.headers=authorization, content-type
5 html.dir=/opt/fusion/share/html
6 fusion.apps.path=apps
7 database.file=/var/lib/fusion/fusion.sqlite
8 orchid.polling.interval=60
9 http.client.read.timeout=30
10 http.client.connect.timeout=60
11 ssl.pem=
12 ssl.key=
13 rtsp.listening.protocol=rtsp
14 rtsp.listening.port=9554
15 rtsp.proxy.transport.protocol=udp
16 greeting.file.path=
17 block.failed.attempts=10
18 block.failed.duration=300
19 properties.version=21.3.0
20 library.local.max.storage.capacity.gibibytes=20
21 library.local.storage.dir=/var/lib/fusion/library
22 library.rclone.url=http://localhost:5572
23 library.rclone.token=0G8zVGc10FFkQ3NGcExTQWpKVmY6Wl
24
25
26 fusion.admin.superuser=true
```

2. Modify the `fusion.(username).superuser` property to establish or revoke superuser status.
 - a. The username may be `admin` (for the default admin user) or any other Fusion username.
 - b. Set this property to `True` to elevate the user to superuser status.
 - c. Set this property to `False` to revoke the user's superuser status.
 - d. Don't forget to remove the `#` at the beginning of the line.
3. Save and close the configuration file.
4. After you update the Orchid Fusion VMS properties file, you must restart the Orchid Fusion VMS service. (If you need extra help, refer back to the *How to Manage the Orchid Fusion VMS Service* section that corresponds to the operating system you are using.)
5. Once the restart is complete, you can sign into Orchid Fusion VMS.

Linux Tips & Tricks

If you are using Orchid Fusion VMS with Linux, these tips will help you navigate the system so that you can perform tasks and find files faster.

Opening and Navigating a Terminal

Access a Linux command line terminal to perform system administration tasks by pressing **Ctrl-Alt-T**. Navigate the filesystem using a few simple commands:

```
pwd
```

Show the working (current) directory

```
ls
```

List the contents of the working directory

```
ls -lh --color
```

List detailed contents of the working directory

```
cd directory (where directory is the name of a directory)
```

Change to a new working directory

```
cd ..
```

Go up one directory

```
mv src dst (where src is the source and dst is the destination)
```

Move a file or directory

```
cp src dst (where src is the source and dst is the destination)
```

Copy a file

```
nano file (where file is the file you want to edit)
```

Edit a text file

```
sudo cmd (where cmd is the command you want to run)
```

Run any command (editing a file, for example) as the superuser (root/Administrator).

```
sudo gedit
```

Open a graphical text editor with superuser permission



Commands, files, and directories can be auto-completed by tapping the **Tab** key—use it liberally, it makes things much easier!

Important Directories and Files

Orchid Fusion VMS stores video, logs, configuration files, and a variety of other data in different directories. The default locations are as follows:

Directory/File	In Windows	In Linux
Installation directory	C:\Program Files\IPConfigure\Orchid Fusion VMS	/opt/fusion
Executable files	C:\Program Files\ IPConfigure\Orchid Fusion VMS	/opt/fusion/bin
Exported Library files	C:\Program Files\ IPConfigure\Orchid Fusion VMS\library	/var/lib/fusion/library
Library files	C:\Program Files\ IPConfigure\Orchid Fusion VMS\lib	/opt/fusion/lib
Log file	C:\Program Files\ IPConfigure\Orchid Fusion VMS\logs	/var/log/fusion
Database file	C:\Program Files\ IPConfigure\Orchid Fusion VMS\fusion.sqlite	/var/lib/fusion/fusion.sqlite
Configuration file	C:\Program Files\ IPConfigure\Orchid Fusion VMS\conf\ fusion.properties	/etc/opt/fusion/fusion.properties
Logback file	C:\Program Files\ IPConfigure\Orchid Fusion VMS\conf\logback.xml	/etc/opt/fusion/logback.xml
Uninstall file	C:\Program Files\ IPConfigure\Orchid Fusion VMS\uninstall.exe	N/A
Downloads (Exported video)	User's Downloads folder	~/Downloads

* If you are using Orchid Hybrid VMS, most of the files and data are stored in the Hybrid cloud. When you export video, the exported video files are saved in the *Downloads* folder on the client machine.

* For additional help with Orchid Fusion VMS, please visit our training site at training.ipconfigure.com.