Server Administration User Manual

Document Version 1.3

1. Table of Contents

2. Introduction and Preparation

2.1. Introduction

The FileFlex administration suite is comprised of two main components - server administration and user administration. This document describes the deployment and general operation of the server administration module.

By the end of this guide you will be able to start the user administration module which then allows you to configure companies, invite users, and perform daily administration tasks.

2.2. Preparation

The FileFlex server solution is packaged as a virtual machine image in the universal OVA format. Several virtualization systems are supported and one must be selected prior to deploying FileFlex within your infrastructure.

You will need to download the OVA file from the "Downloads" section of the FileFlex MSP portal Website at https://www.fileflex.com

Separate sections of this guide describe the details of deployment within those specific environments.

You will need to know whether you are planning a single-machine deployment, or a clustered deployment before going too far with these steps. This documentation is geared around a single-machine deployments at this time.

The following steps should be completed and understood prior to beginning the installation of FileFlex server.

1. Have a VirtualBox or VMWare hosting environment ready with at least 2 CPU cores and 2GB of RAM available.
2. Have a domain name with valid DNS entries ready to point to your virtual deployment.
3. Have your FileFlex Deployment ID and Deployment Key ready for entry.
4. Have a valid email delivery server or service with appropriate credentials ready.
5. Have a valid website SSL key and certificate ready.
6. (optionally) Have a customized splash screen ready for submission.

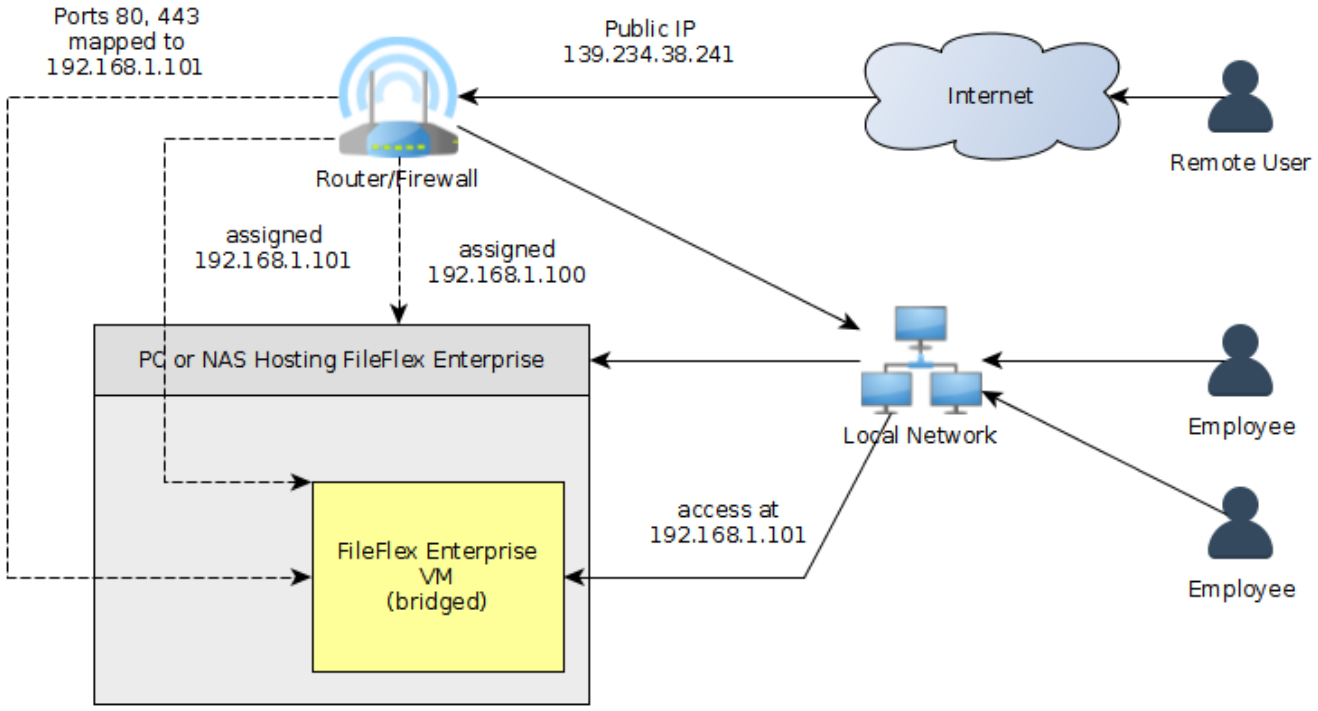
2.3. Considering External Access

This document is intended to aid the reader in configuring a working FileFlex Enterprise virtualized environment. That envrionment will be available within the local network in which it is deployed, but it's expected that external public access will also be desired. The method of external access should be understood in advance.

> ⚠ **External Access**
>
> Configuring external public access is very specific to the environment in which the deployment is being made, and is thus outside of the scope of this document. Presented here are two possible configurations to guide you. Please consult with your system administrator.

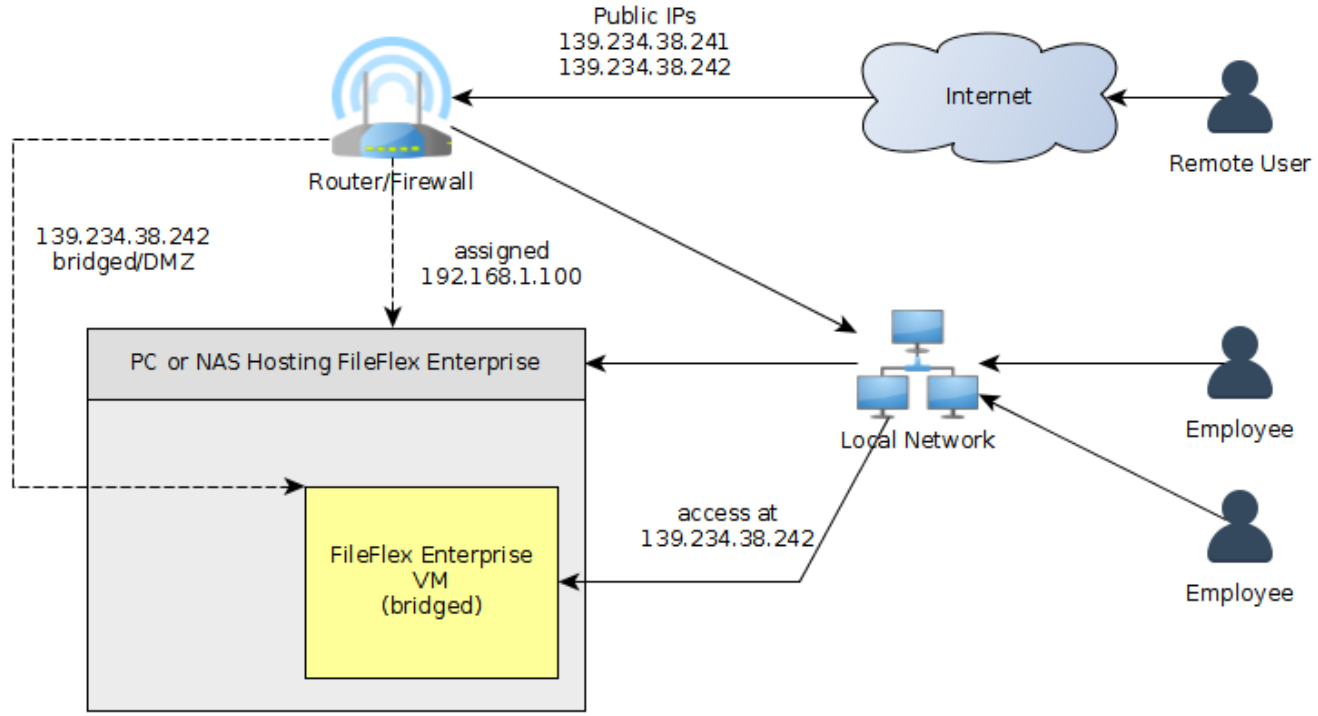
This documentation assumes that the VM will be given an IP using DHCP from the local network's router (or other DHCP server). This is made possible by using bridge mode networking at the VM level, and because of this, obtaining the privileged ports 80 and 443 should not be a problem. This means that users of the local network will be able to access the services without any trouble using the default ports.

2.3.1. Router Based Network Address Translation



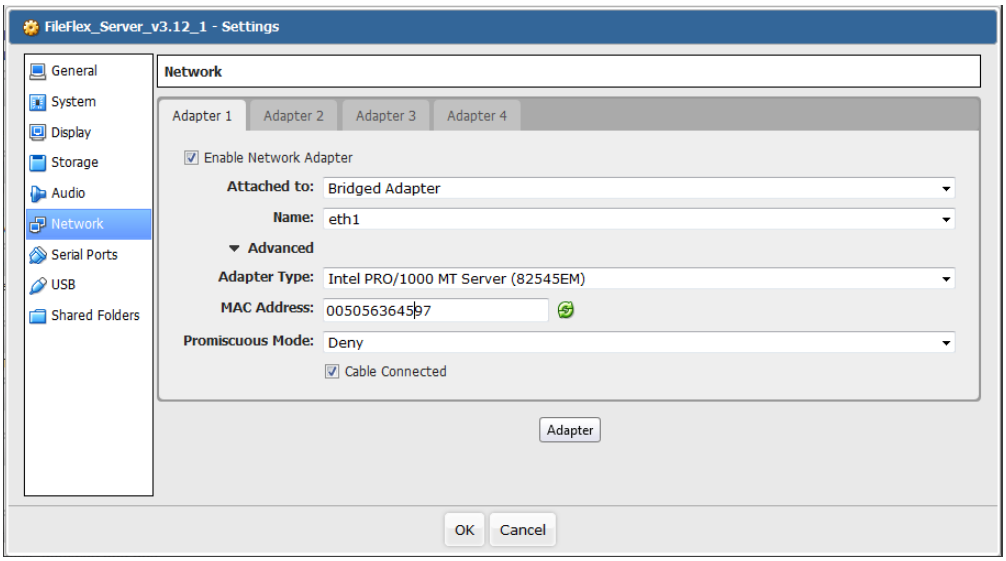
In this NAT scenario, local network users ("employees") are able to access the FileFlex Enterprise VM using the router-assigned local network IP on the default ports. Remote users going through the internet are able to access the FileFlex services by accessing the router's public IP address. The router uses NAT to forward the key ports (80, 443, 9443 4010, 4011) to the FileFlex VM.

2.3.2. Direct Public IP Assignment



In this direct public IP scenario, the VM is given a public IP address by bridging, DMZ, or some other mechanism. Local network users can use that public IP for access, as can remote users. This document assumes that it's possible to receive the public IP by DHCP. If not, some of the presented configuration steps will have to be tailored to provide a static IP.

It may also be necessary (depending on your specific ISP requirements) to use a specific MAC address in order to receive the appropriate public IP. If that is the case you must configure the VM to not re-initialize the virtual network adapter's MAC address and supply a specific one:



It's likely in this scenario that you will have to specific custom static IP, netmask, gateway and DNS information during the console-based installation steps.

3. Virtualization and Hardware

The FileFlex Enterprise system is a complex set of modules, and is therefore deployed as a virtual machine to greatly simplify deployment. Several different virtualization solutions are presently supported, including:

- VMware Workstation 11
- VMware Workstation 12
- VMware Workstation 12.5
- VMware ESXi 5.5 (vSphere)
- VMware ESXi 6.0 (vSphere)
- VMware ESXi 6.5 (vSphere)
- Oracle VirtualBox 5.1

Follow one of the provided guides to deploy the FileFlex Enterprise image using the virtualization technology of your choice.

> **Deploying on a NAS**
>
> When deployed on a NAS, a virtualization technology such as VirtualBox (or otherwise) will automatically be installed as a dependency of the solution.

3.1. Server Hardware Allocation Requirements

FileFlex Enterprise may be deployed on a variety of hardware configurations, with an underlying requirement of Intel x64 CPU architecture. When discussing deployment hardware, it is specifically with respect to the VM's allocation of hardware resources to the VM, rather than the total capacity of the underlying host machine.

This document is focused on single-machine/VM deployments rather than a clustered deployment.

3.1.1. Server Hardware Requirements

The following table describes typical deployment configurations and capacities. Server hardware refers to VM-assigned resources.

	Minimum	Mid-Range	High-End
CPU	itherIntel Core i3 2-Core @ 2ghz Supports VT-x and AES-NI	Intel Core i7 4-Core or 6-Core @ 3ghz Supports VT-x and AES-NI	Intel Xeon 8-Core or 10-Core @ 3ghz Supports VT-x and AES-NI
RAM (assigned to VM)	4gb	8gb	16gb
Network	Single 1GbE LAN Port	Dual 1GbE LAN Ports w /Aggregated Links	Dual 10GbE LAN Ports
OS	Linux based, with integrated virtualization support	Linux based, with integrated virtualization support	Linux based, with integrated virtualization support
Maximum Concurrent View-Only Conversions	1	3-4	6-8
Max Activations and/or Users	1000	2500	5000
Max Users in App (ram and cpu dependency)	150	500	1000
Max Typical Active Browsing Users	20	80	160
Max Typical Concurrent Transfers	10	30	60

3.1.2. Connector Agent Hardware Requirements

	Minimum	Mid-Range	High-End
CPU	ARM A8 Single Core @ 1ghz	ARM A9 Dual Core @ 1ghz	Intel Atom Quad Core @ 2ghz
RAM	256mb	512mb	512mb
Network	Single 1GbE LAN Port	Single 1GbE LAN Port	Dual 1GbE LAN Ports w /Aggregated Links
OS	Linux based	Linux based	Linux based
Storage	7200rpm SATA Drives, < 10ms seek	7200rpm SATA drive(s), <10ms seek	10000rpm SATA drive(s), <7ms seek and/or SSD caching
Max Activations and/or Users	100	250	500
Max Logged in Users (ram and cpu dependency)	30	125	350

Max Typical Active Browsing Users	10	35	100
Max Typical Concurrent Transfers	5	15	30 (may be IO limited)
Expected CPU% Use at Max Typical	50%	50%	50%

3.1.3. View-Only Conversions

The advanced panel of the server administration contains a configurable property "Maximum concurrent view-only conversions". This defines the maximum number of view-only conversions that may execute at the same time. When a user chooses to view an office document within the application, a conversion is necessary. The number of conversions that can happen at the same time is directly connected to the amount of CPU and RAM allocated to the server. Each "concurrent view-only conversion" requires 1 dedicated CPU core, and 1gb of RAM.

We recommend adding 1 CPU core and 1gb of RAM for each additional 1,000 users added to the system, depending on the frequency with which they are viewing documents within the application, and the size of the documents they are viewing.

3.1.4. Effect of RAM

The most important fundamental resource is RAM because several running processes are launched for data accumulation, proxying, data encryption, etc. A minimum of 4gb is required to run all needed services adequately. The maximum activations introduce a persistent RAM requirement, so a higher RAM total allows for more total activations /users. Simultaneous transfers also require more RAM. A larger cache allows for a larger number of "active users".

View-Only conversion is by far the largest consumer of RAM, and allocation must be made as indicated above.

3.1.5. Effect of Disk IO

The server is not critically bound to drive IO, so most typical well-functioning NAS drive deployments will be adequate. The connector however which is responsible for fetching files from the local device is tied to the IO performance of the device - especially the seek time. SSD caching schemes will greatly improve it's ability to deliver high numbers of files concurrently without overly slowing down the NAS's performance.

The exception is view-only conversions. If your use-cases involve a great deal of document viewing, then IO limitations may come into play and the deployment of an SSD-backed high performance data-storage solution is recommended.

3.1.6. Effect of CPU

The CPU is highly utilized for encoding/decoding of requests, so is directly related to the number of active users. It is also directly related to the number of high-speed transfers due to the active encryption. The CPU becomes especially important when dealing with 10GbE connections with clients located on the same high-performance network.

View-Only conversion is a large consumer of CPU, and allocation must be made as indicated above.

3.1.7. Effect of Network

The network is very important when dealing with a large number of concurrent transfers if one wants to maintain consistent local-network level performance. For the reasons described above, it's important to correlate the CPU with the network speed.

3.1.8. Clustering

When capacity becomes saturated, it is possible to deploy FileFlex in a clustered configuration. Supporting a clustered configuration requires dual networks, so it's important that such deployments have at least two network adapters. In a highly de-centralized deployment, the CPU and RAM become less important as the load is spread across several machines.

3.2. Deploying With Oracle VirtualBox

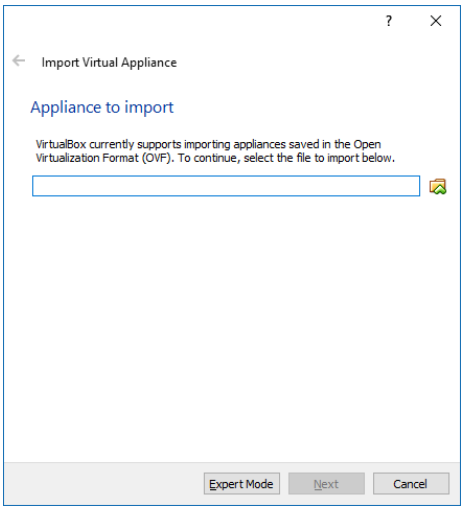
This section describes the process of installing FileFlex Enterprise on Oracle VirtualBox. The following versions of Oracle Virtualbox are supported:

- Oracle VirtualBox 5.x

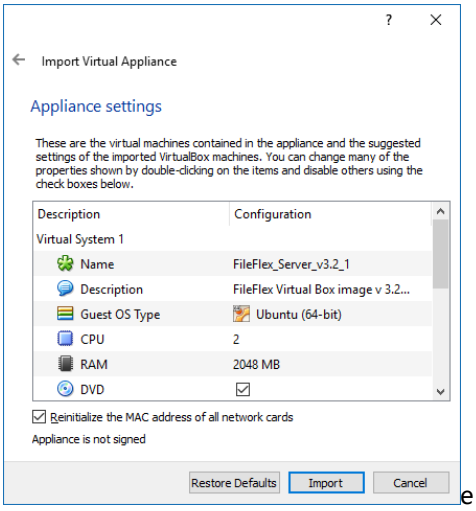
3.2.1. Deploying the Virtual Machine

Ensure that your VirtualBox version is at least 5.1. This quick start guide was generated using VirtualBox 5.1.10 under a Windows 10 host.

From VirtualBox's File menu, select Import Appliance. The following window will appear:

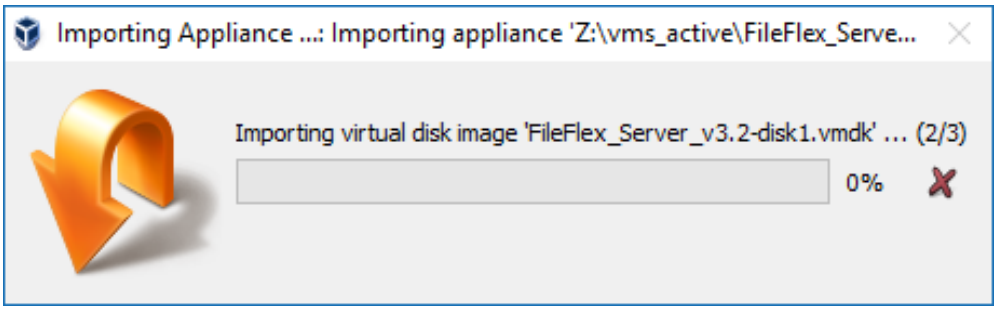


Select the OVA file you downloaded earlier and click the 'next' button. Check the "Reinitialize the MAC address of all network cards" box.

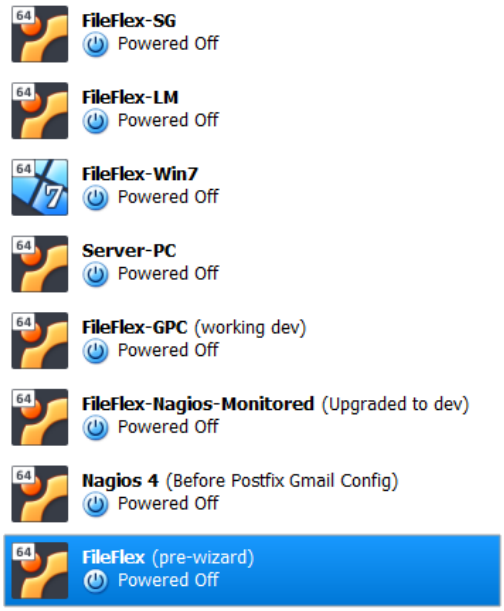


e

Click the "import" button and you will be presented with a slowly advancing progress dialog:



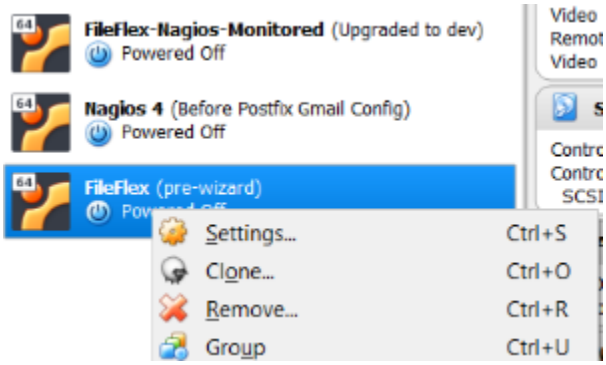
After a few moments you will see the virtual machine in your list of available VMs:



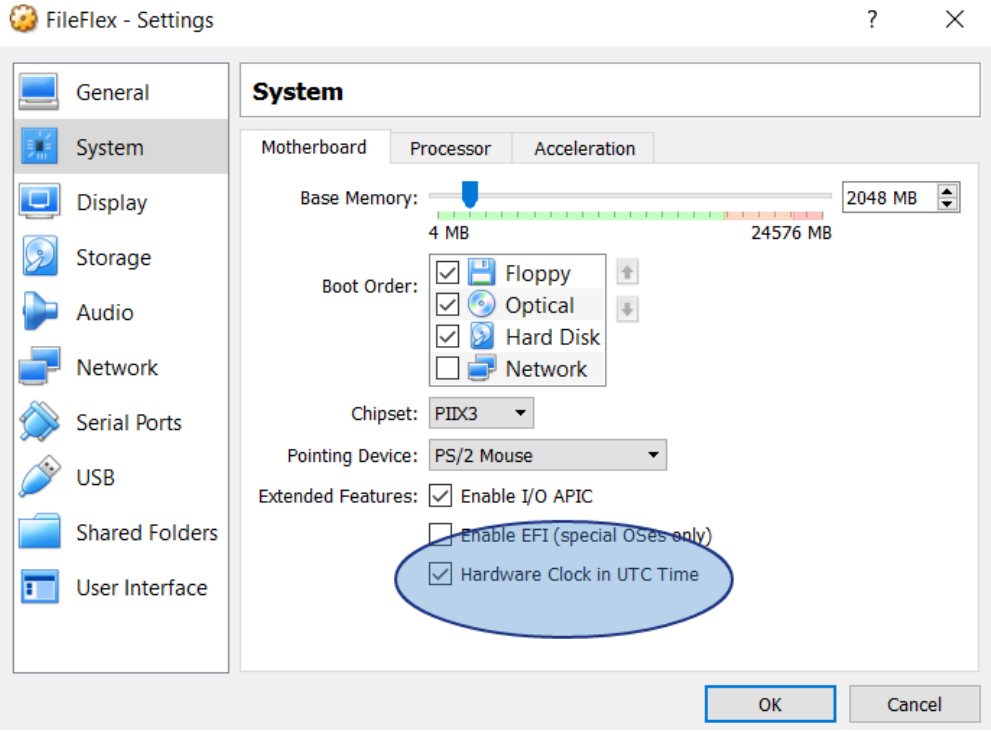
Right click on the new machine:

3.2.2. Adjusting the VirtualBox VM

The hardware clock in the VM must be adjusted in order for the backups to operate as expected. Select the machine from your list of VMs, and right click on it:



Click on "settings", then choose the "system" panel:



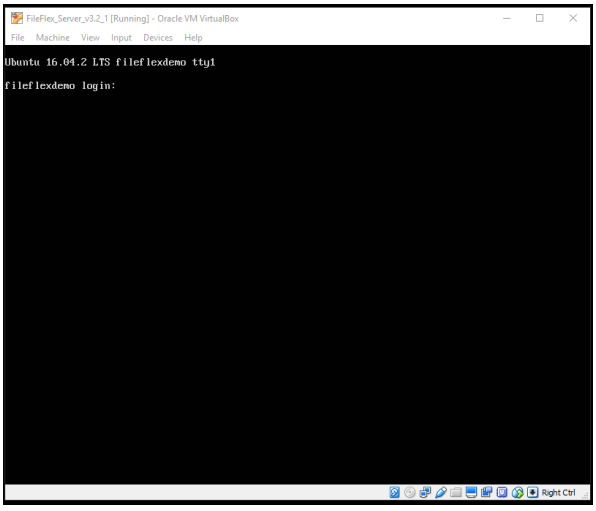
Ensure that the "Hardware Clock in UTC Time" checkbox is selected. Click OK.

3.2.3. Deploy the Virtual Appliance

Select the new virtual machine configuration from the left hand side of VirtualBox's main window:

Click the start button. You should not have to make any special customization to the virtual machine settings. The defaults should result in a bridged network configuration that will work as expected.

After a few moments you should be presented with a login prompt:



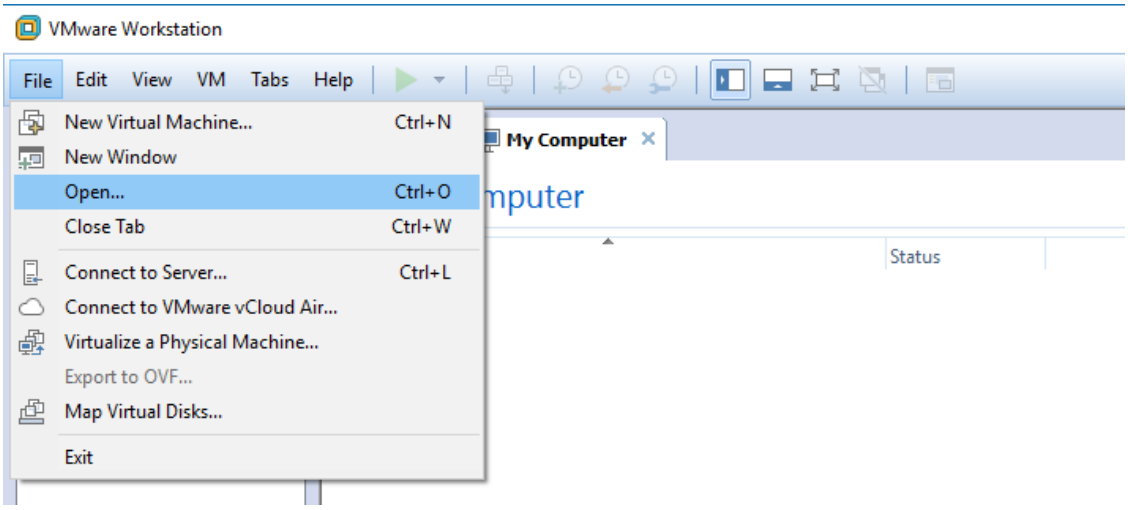
3.3. Deploying with VMware Workstation

This section describes the process of installing FileFlex Enterprise on VMware Workstation. The following versions of VMware Workstation are supported:

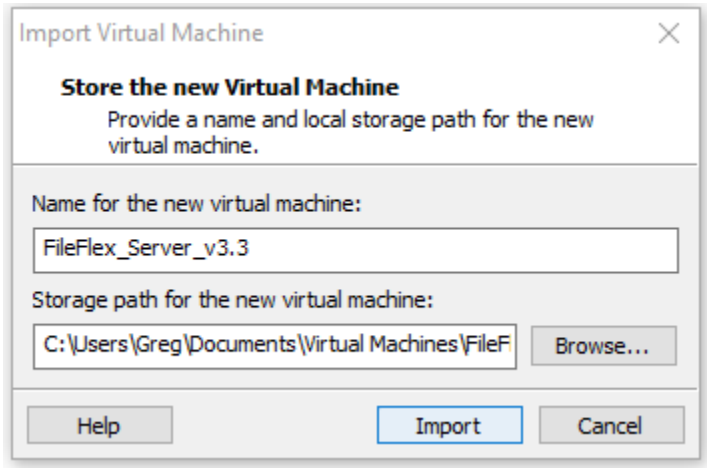
- VMware Workstation 11
- VMware Workstation 12
- VMware Workstation 12.5

3.4. Deploying the Virtual Machine

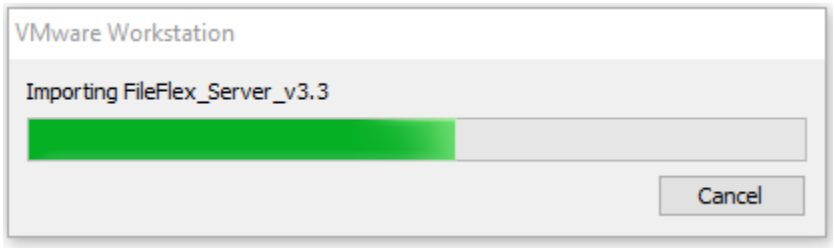
Open VMware Workstation, and select File/Open:



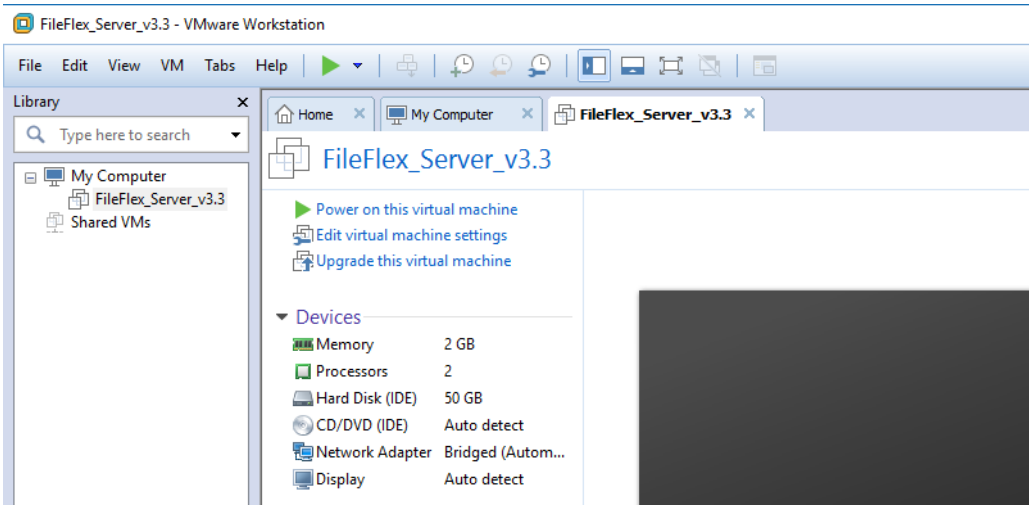
Navigate to your copy of the FileFlex_Server_v3_X.ova file, and select it.



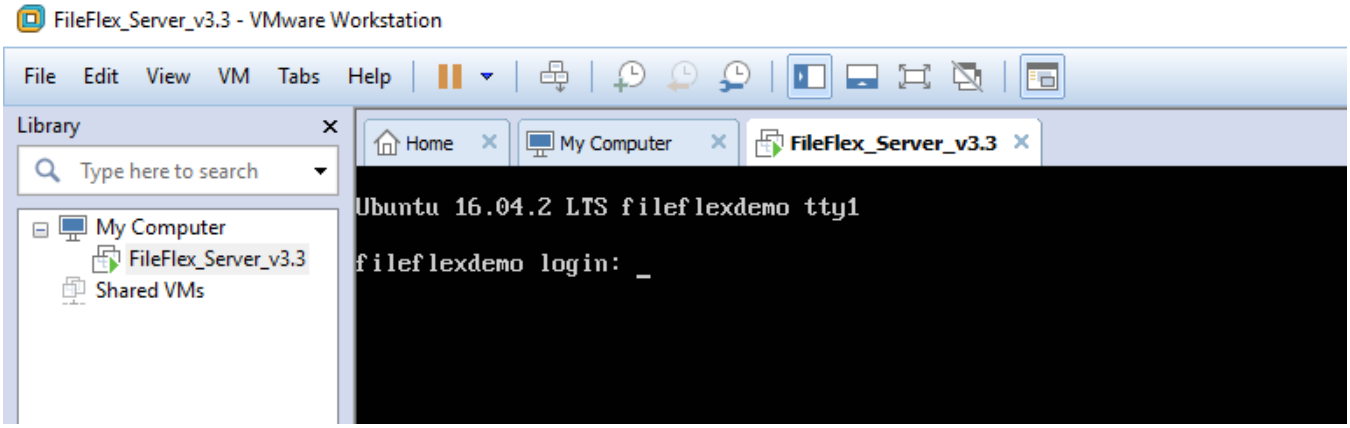
Choose to import the file, then wait a few minutes while it imports:



The network adapter will have automatically been set to bridged mode. You will now be able to start the virtual machine:



Choose to "power on" the virtual machine, and after few moments you will see the login prompt:



You can now proceed with the next section of the guide.

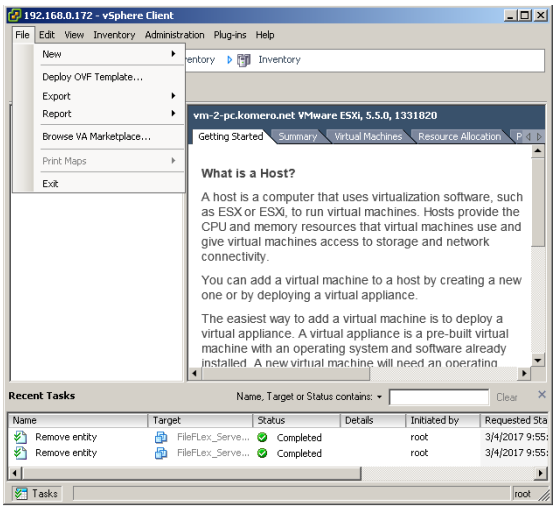
3.5. Deploying With VMware vSphere

This section describes the process of installing FileFlex Enterprise on VMware vSphere/ESXi using the vSphere client. The following versions of VMware Vsphere are supported:

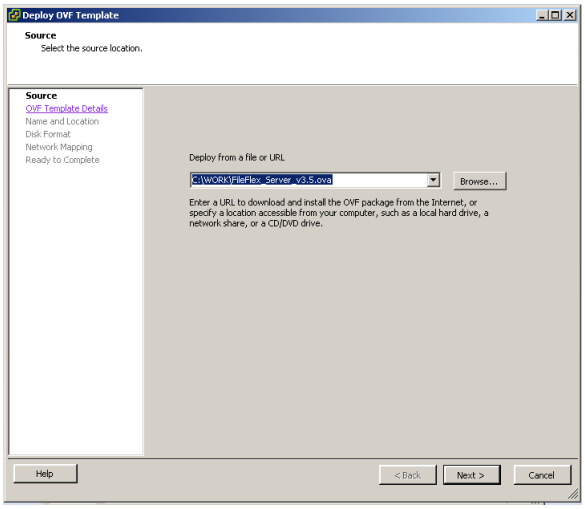
- VMware ESXi 5.5 (vSphere)
- VMware ESXi 6.0 (vSphere)
- VMware ESXi 6.5 (vSphere)

3.6. Deploying the Virtual Machine

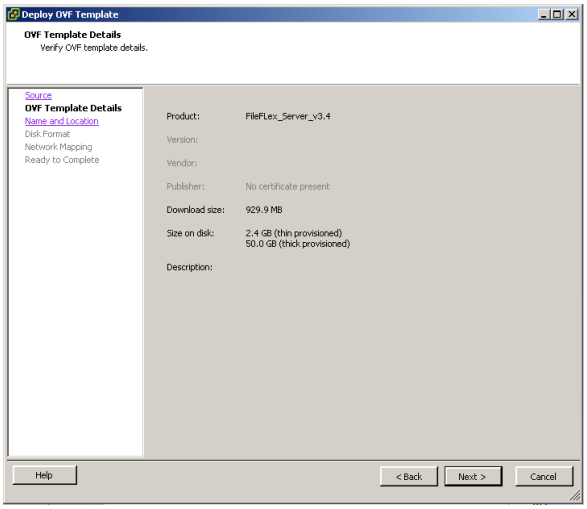
Open the vSphere client, and from the File menu select "Deploy OVF Template:



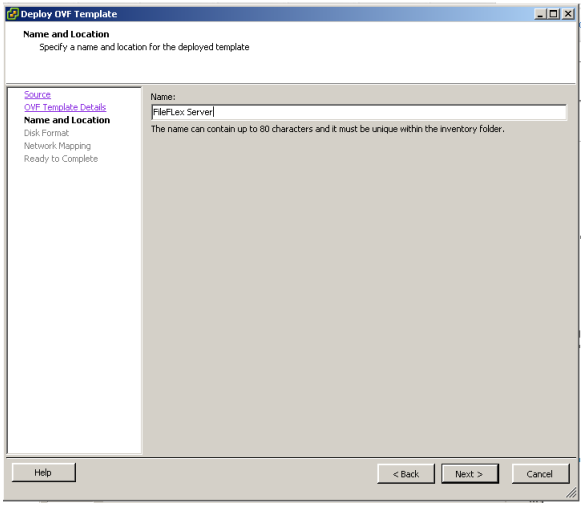
In the "Source" panel of VMware, click "browse" to locate your (previously downloaded) FileFlex_server OVA image:



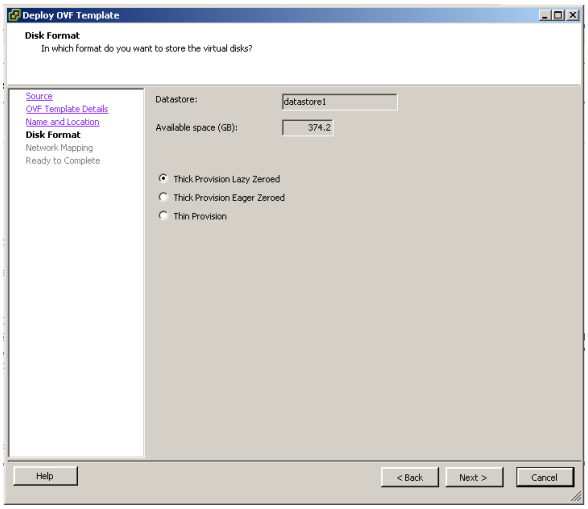
Click the "next" to enter the "OVF Template Details" panel which reveals information about the image:



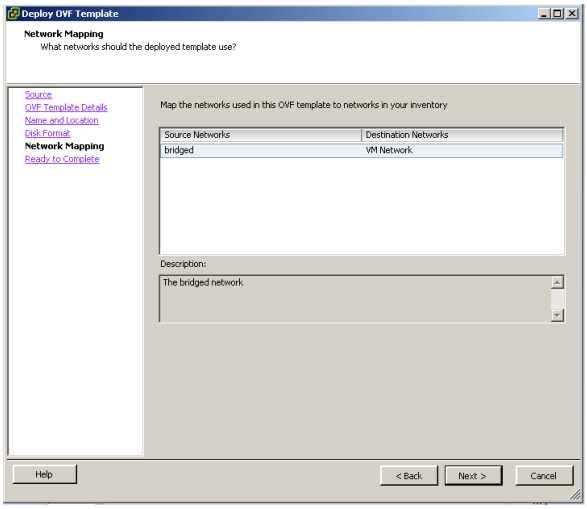
Click "next" to reveal the "Name and Location" panel. There you will be able to enter a new name (if you wish to override the default) for the deployed image:



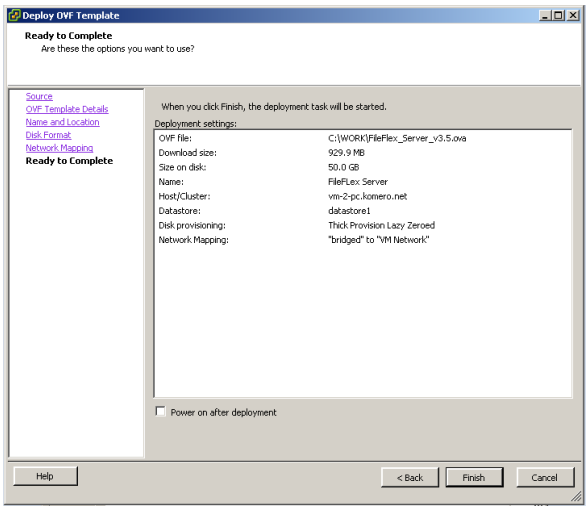
Click "next" to reveal the "Disk Format" panel:



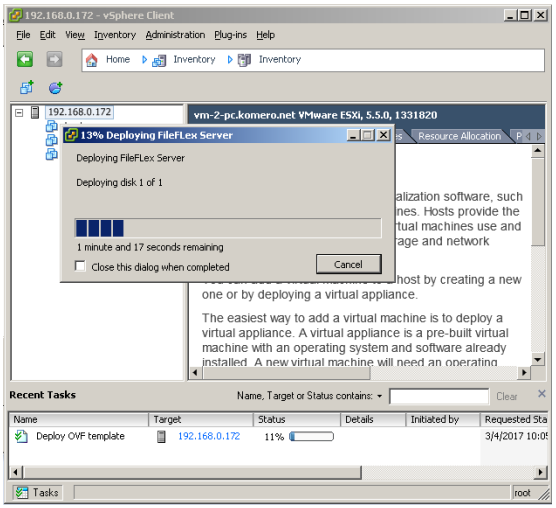
Select the "Thick Provision Lazy Zeroed" option, then click the "next" button to reveal the "Network Mapping" panel:



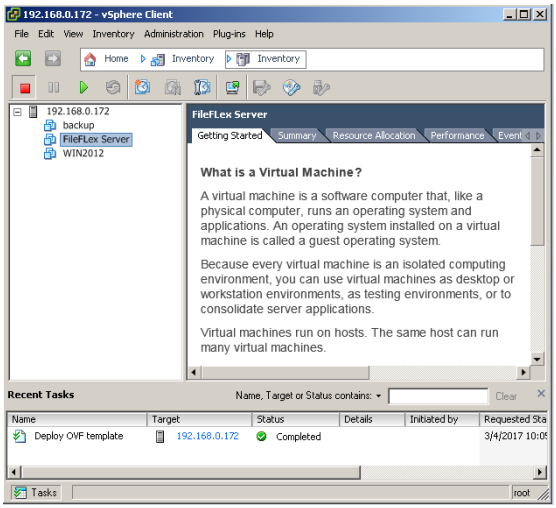
Select the bridged network entry for your VM network, then click the "next" button to reveal the confirmation panel:



Take a moment to verify the settings, and then click the Finish button to begin the deployment:



It will take a few minutes to complete. Once finished, you will see the new VM in your list of available VMs within vSphere Client:



Select the new virtual machine on the left, and click the "start/play" button to start the VM.

You can now proceed with the next section of the guide.

3.7. Deploying on Amazon EC2

This section describes the process of installing FileFlex Enterprise on Amazon EC2. Before proceeding, ensure that you have your Amazon EC2 login credentials available.

3.7.1. Deploying the Virtual Machine

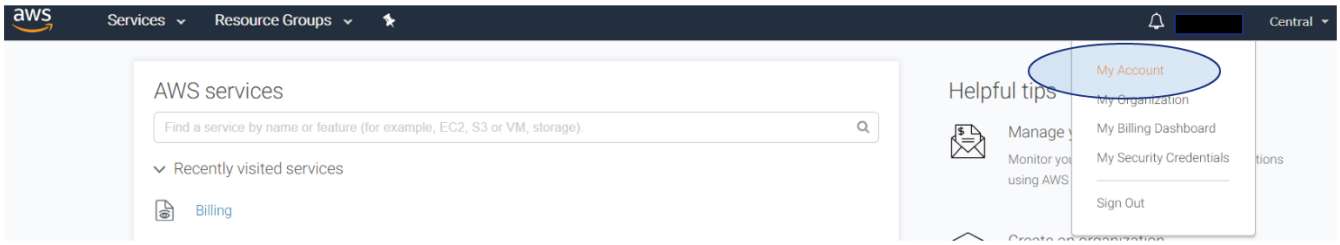
FileFlex provides an Amazon Machine Image (AMI), though it is not publicly available. In order to be able to use the image, you must provide our Enterprise Portal with your Amazon AWS Account ID.

3.7.1.1. Getting Your Amazon AWS Account ID

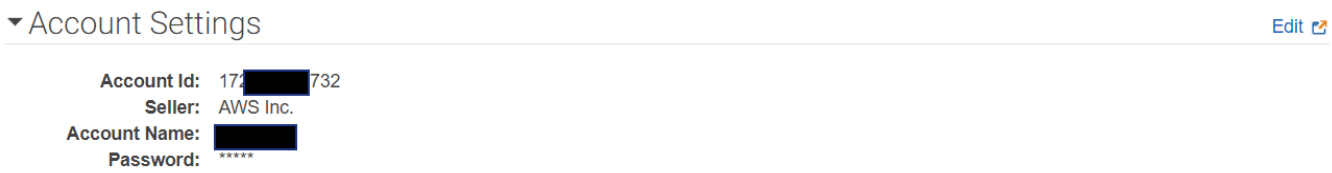
To obtain your Account ID, log in to your Amazon AWS console:

```
https://console.aws.amazon.com/console/home
```

Once logged in to the console, click on your account drop-down menu at the top right:



Click on the "My Account" menu item. You will see your account details:



Write down the account ID for later entry into the web portal.

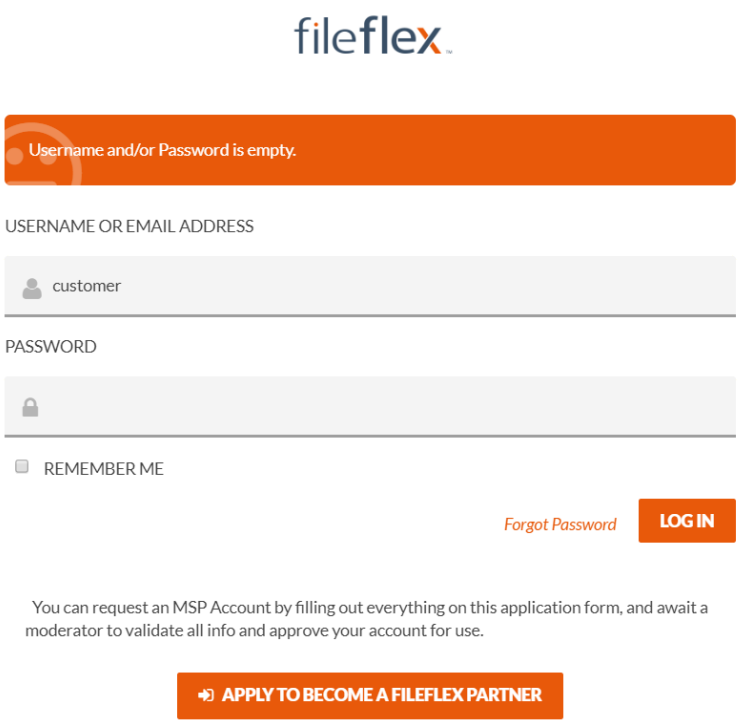
3.7.1.2. Linking Your Amazon AWS Account

The next step is to link your FileFlex Enterprise deployment with your AWS Account IT. This will enable you to use our provided Amazon Machine Image (AMI) for deployment into Amazon EC2.

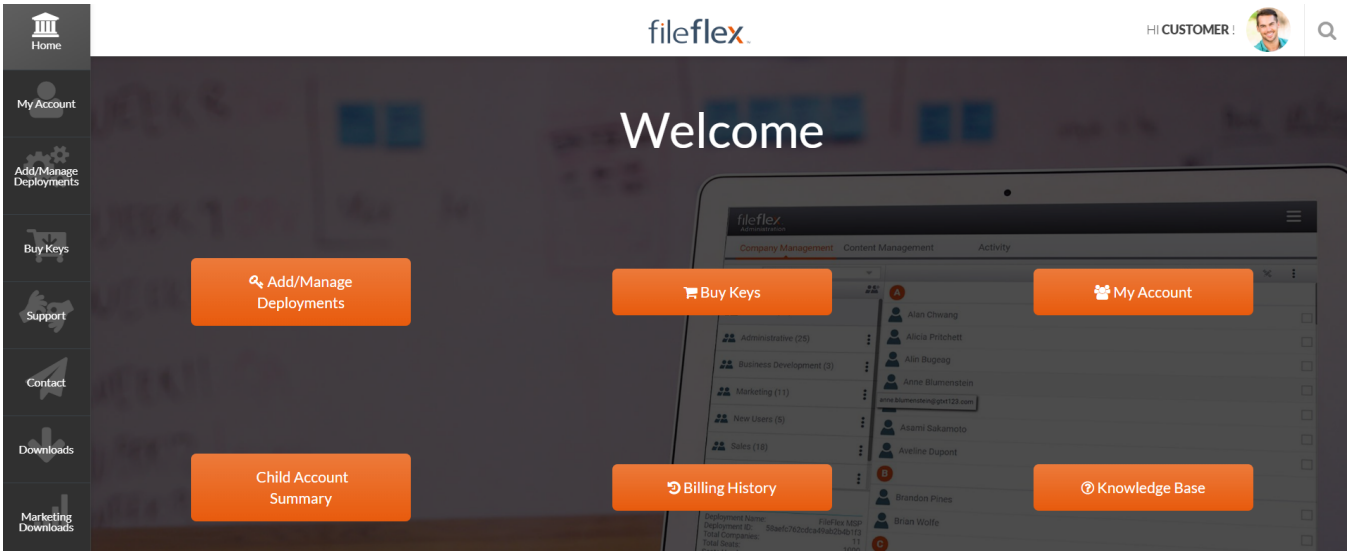
Navigate to the FileFlex Enterprise Portal:

```
https://enport.fileflex.com
```

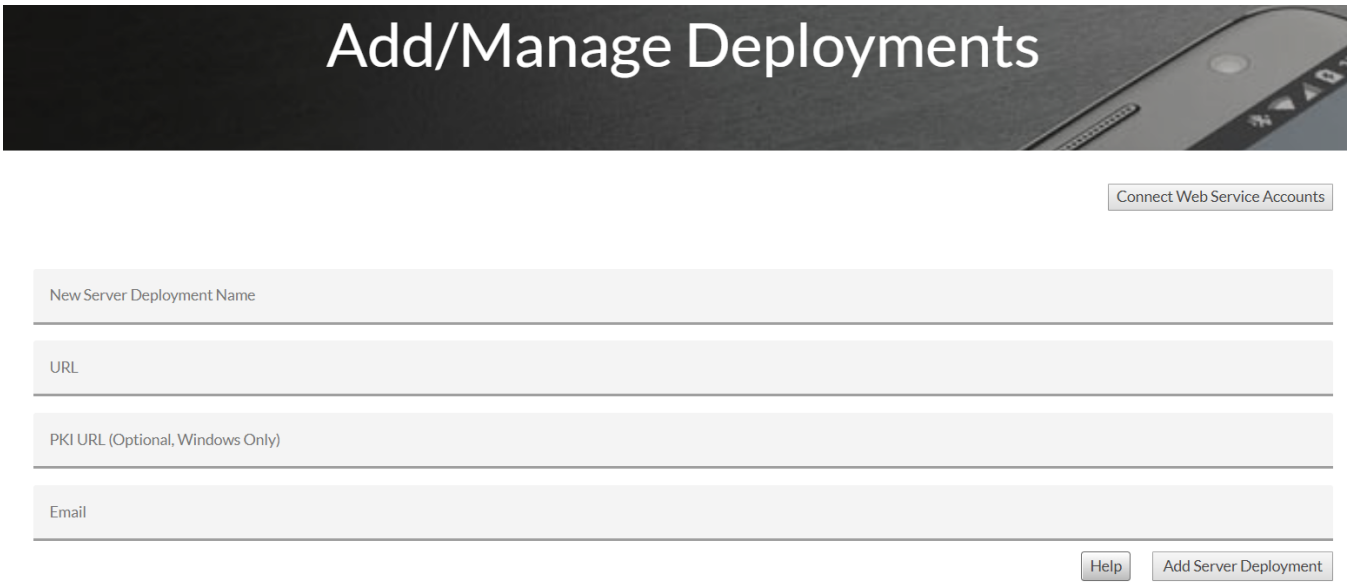
You will be presented with a login screen if you are not already logged in:



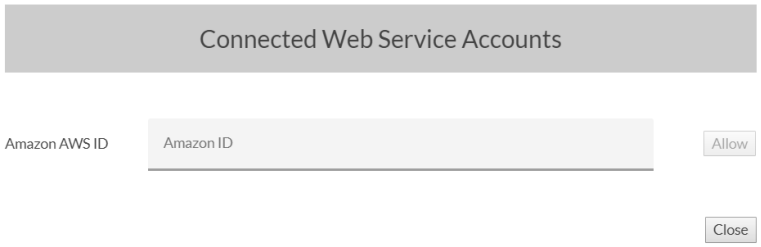
Enter your login credentials, followed by clicking on the "Log In" button. You will then be presented with the Enterprise Portal's control panel:



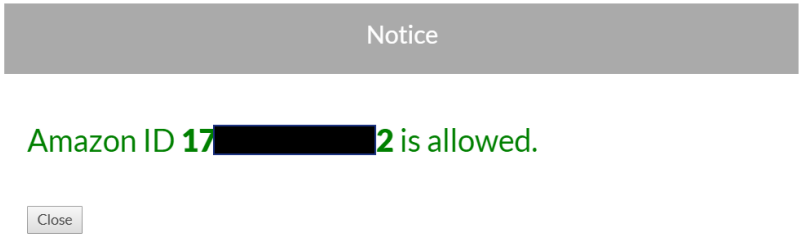
Click the "Add/Manage Deployments" button. You will see a screen similar to the following:



Click on the "Connect Web Service Accounts" button, and a new dialog will appear allowing you to enter your Amazon AWS Account ID:



Enter the Amazon ID you wrote down earlier, then click "Allow". You will receive a confirming when the accounts have been linked:

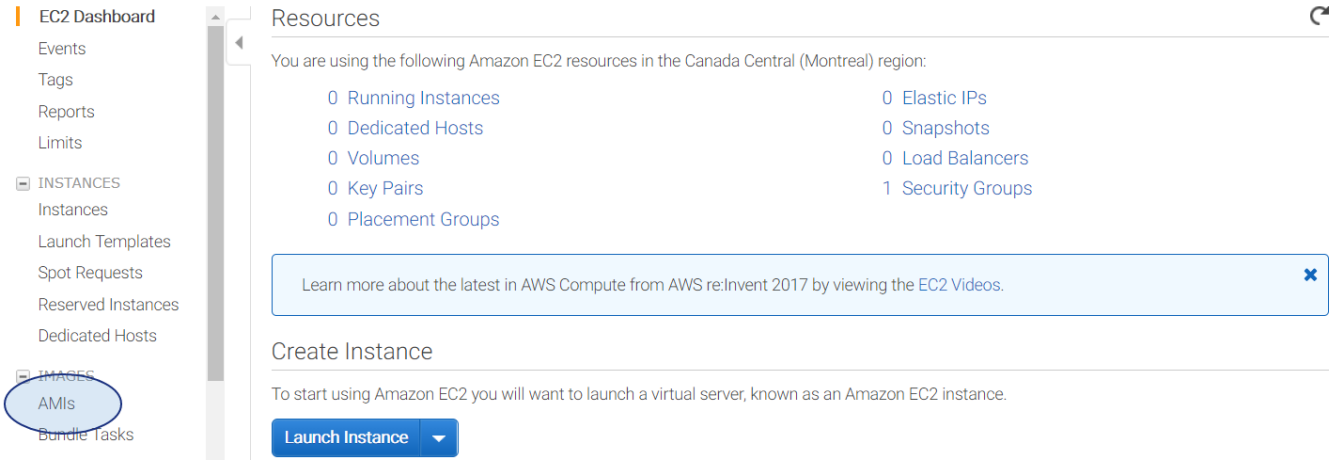


Click the "Close" button.

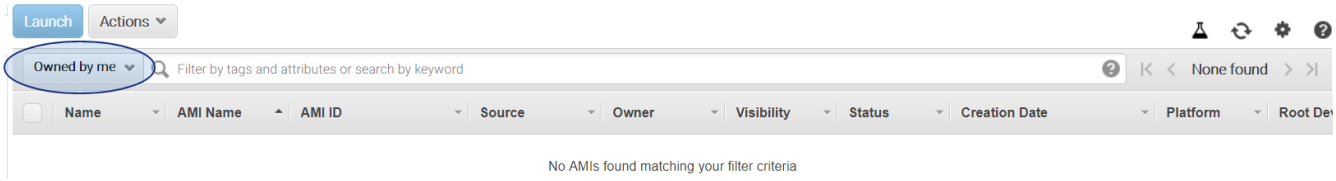
3.7.1.3. Deploying an EC2 Instance

Turning our attention to deploying an EC2 instance, the first step is to log in to your EC2 console. Once logged in, expand the "Services" menu from the top left of the screen:

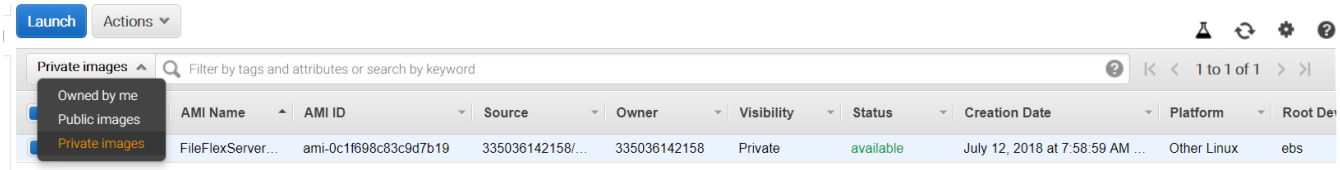
Click the EC2 menu item. You will see a screen similar to the following:



Click the "AMIs" link from the left hand side to access those options. This will provide a list of your AMI images, which may be empty:

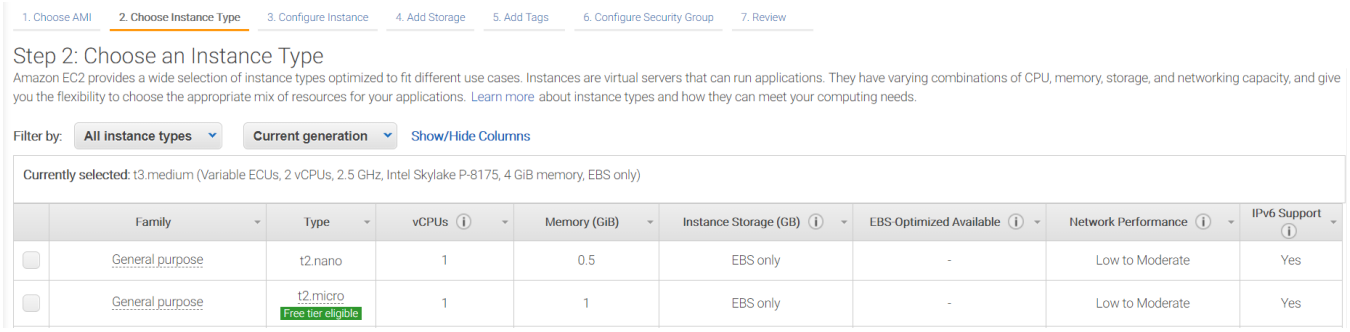


Click the AMI ownership drop down on the left of the search field:



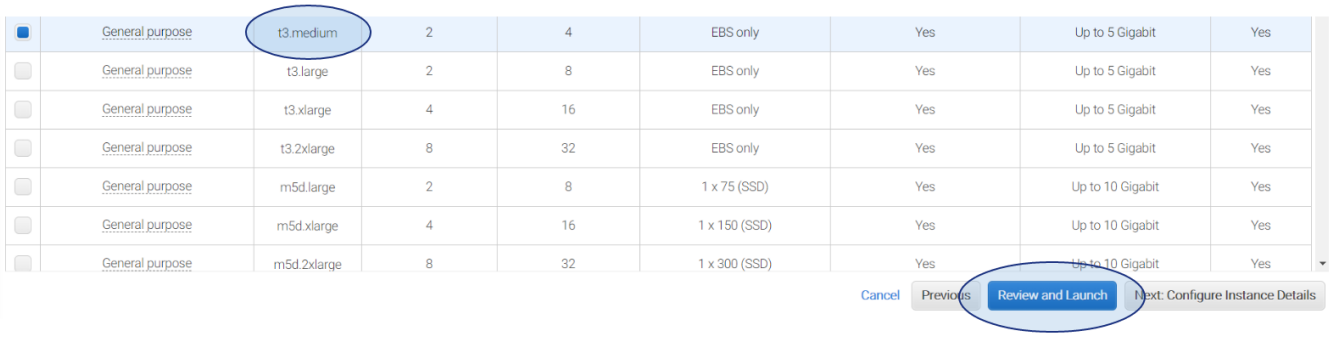
From the dropdown, select "Private images". Becase we linked the account, you wlll have gained access to the FileFlex AMI, and should see it in your list of available images.

Select the image from the list, and click the blue "Launch" button above the list. You will be presented with an instance type selection:

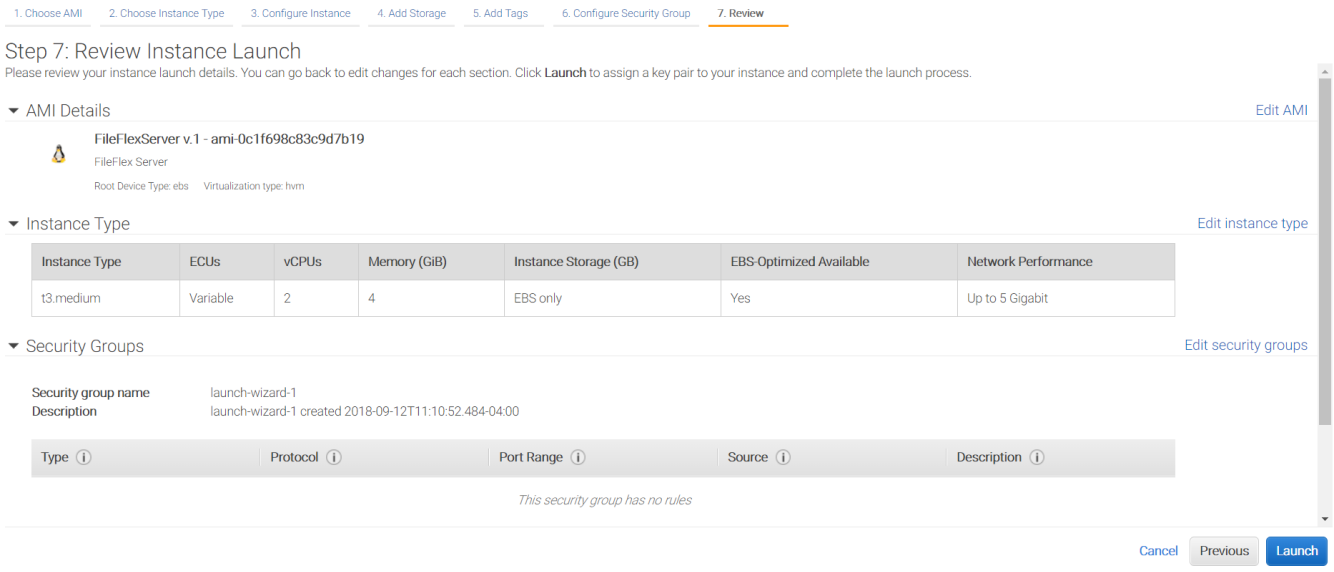


We recommend at least 2 CPU cores, and 4gb of RAM, with sufficient bandwidth for a large number of concurrent transfers. That that reason, that makes the "t3.medium" instance type a good starting point.

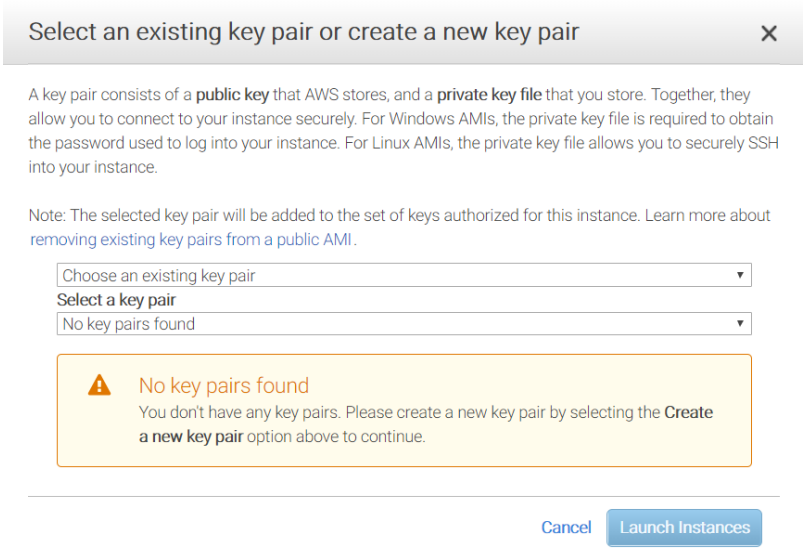
Select your desired instance type (as mentioned above, "t3.medium" is a good starting point).



Click "Review and Launch" to proceed with the review:



Verify that everything is as it should be, and click the blue "Launch" button at the bottom right. You will be presented with the key pair specification dialog:



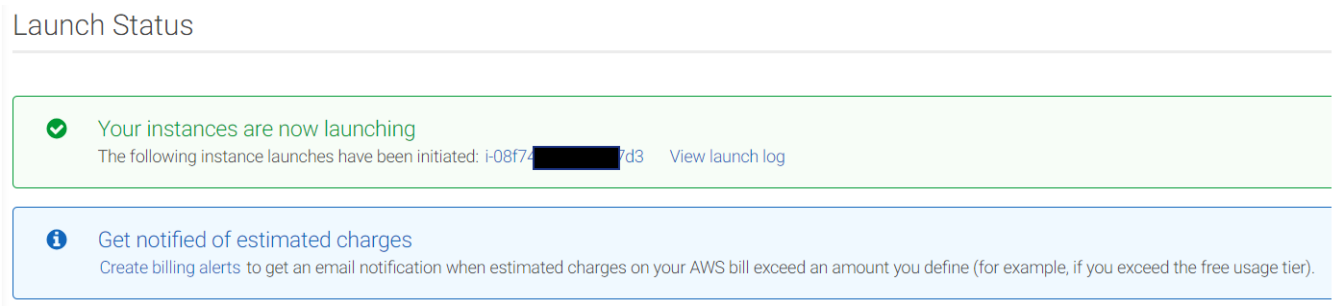
If you already have a key pair, you can select it from the list. If you do not, you will need to create one to be able to access your instance. Choose "Create a new key pair" from the first dropdown, and enter a name for the keypair. For example:

If creating a new key pair, click on "Download Key Pair". A PEM file will be downloaded.

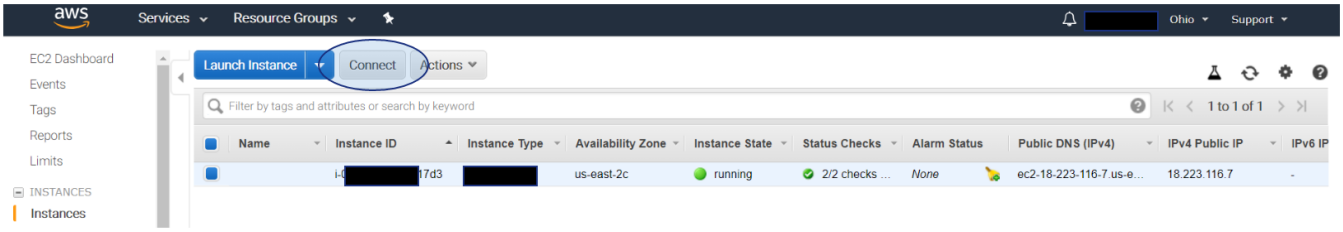
> It's important to keep your keys safely backed up as they will be required to access your FileFlex Enterprise images!

Click on the blue "Launch Instances" button at the bottom right of the dialog to proceed.

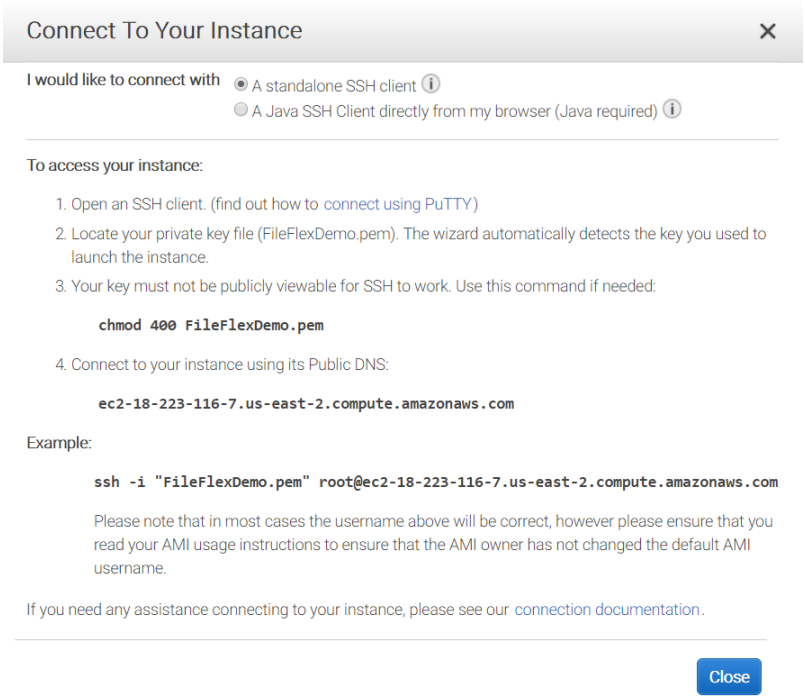
You will be presented with a launch status screen:



Click the blue "View Instances" button at the bottom right. You will see a list of your running instance, including the newly spooled up instance:



Click the connect button. You will be presented with information on establishing a connection to your virtual machine:



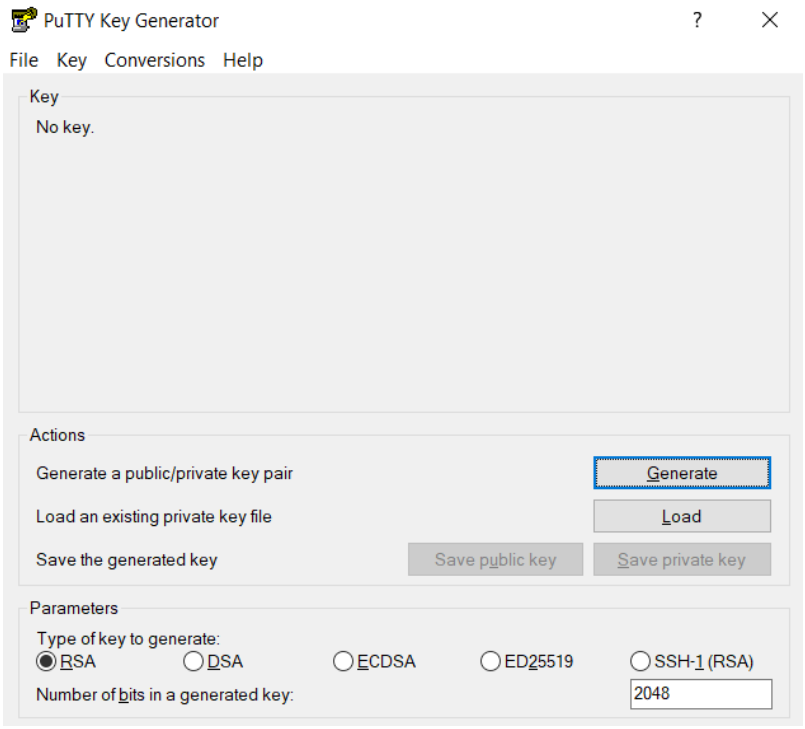
Select "A standalone SSH client" from the list of connection options (it should be the default). Follow the instructions provided for your SSH client of choice.

Write down the "Public DNS" URL provided by Amazon as in the screenshot above (ec2-18-223-116-7.us-east-2.compute.amazonaws.com in the example above).

3.7.1.4. Connecting to Your Virtual Machine

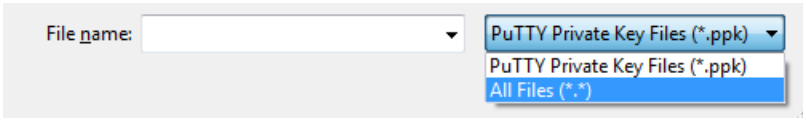
In this example, we will use Putty on Windows to connect to our virtual machine. We must now convert the key provided by Amazon into a format that's compatible with Putty.

From the start menu, load "PuTTYgen" which came with Putty when you installed it. You will be presented with an application looking like this:



Under "Type of key to generate" at the bottom of the application, select "RSA". If you're using an older version of PuTTYgen, choose SSH-2 RSA.

Choose "Load". By default, PuTTYgen displays only files with the extension `.ppk`. To locate your `.pem` file, select the option to display files of all types.



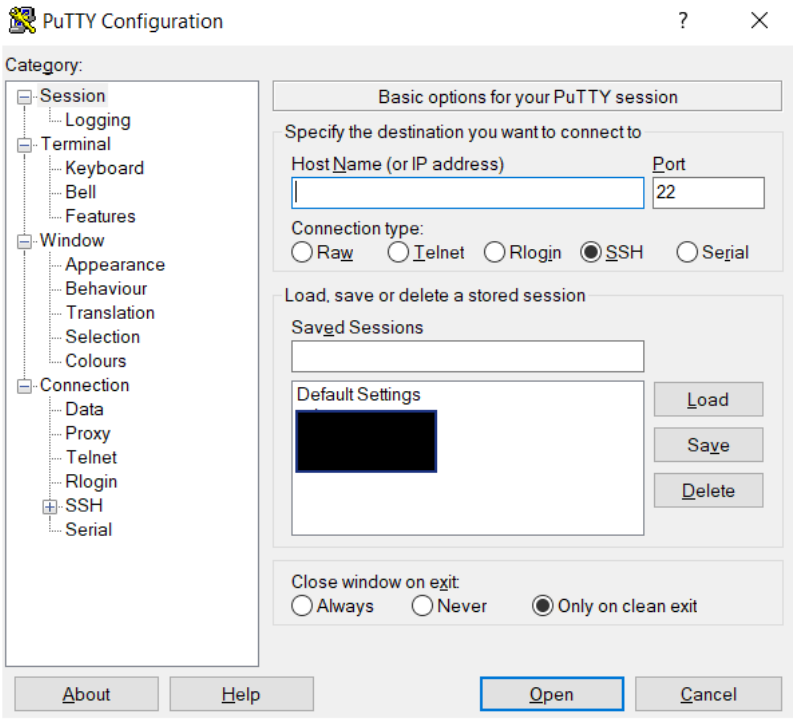
Select your `.pem` file for the key pair that you specified when you launched your instance, and then choose "Open". Choose "OK" to dismiss the confirmation dialog box.

Choose "Save private key" to save the key in the format that PuTTY can use. PuTTYgen displays a warning about saving the key without a passphrase. Choose "Yes".

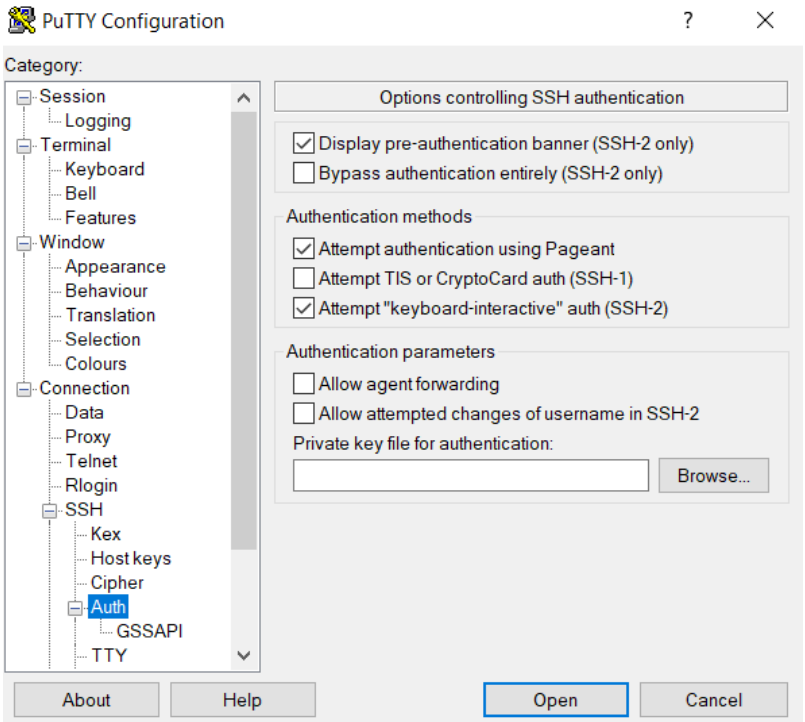
> ⚠ A passphrase on a private key is an extra layer of protection, so even if your private key is discovered, it can't be used without the passphrase. The downside to using a passphrase is that it makes automation harder because human intervention is needed to log on to an instance, or copy files to an instance.

Specify the same name for the key that you used for the key pair (for example, FileFlexDemo based on this tutorial's naming). PuTTY automatically adds the `.ppk` file extension. Your private key is now in the correct format for use with PuTTY. You can now connect to your instance using PuTTY's SSH client.

From the start menu, open the PuTTY client:

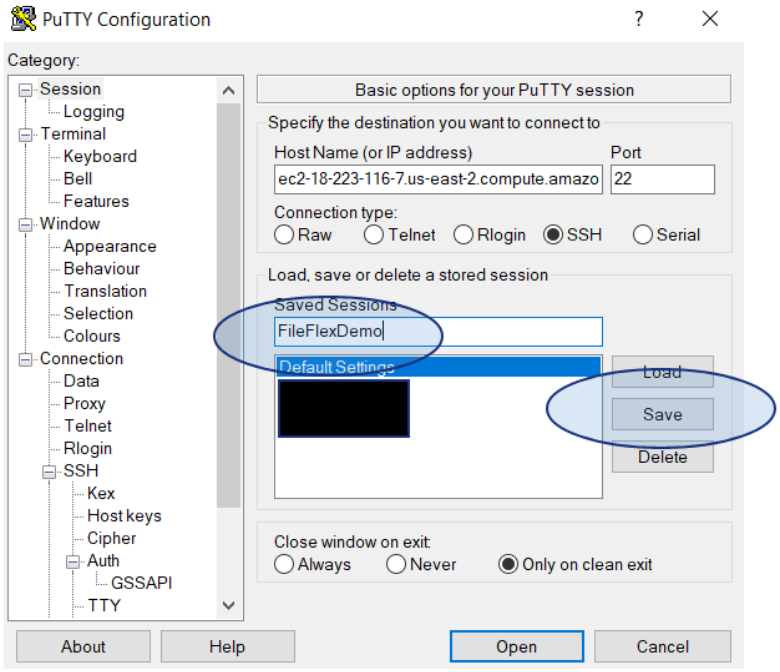


Enter the "Public DNS" URL you wrote down earlier in Putty's "Host Name" field. Next, we need to provide the private key to PuTTY. Do so by expanding the "Connection" node from the left panel, then the SSH node as well. You will then be able to select the "Auth" note:



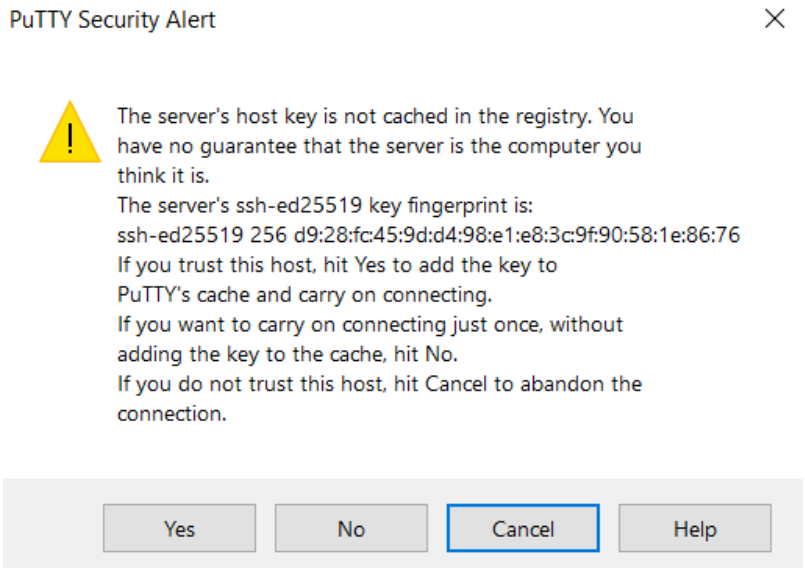
Click "Browse" and locate the key you recently generated with PuTTYgen.

Navigate back to the "Session" category from the left hand side to go back to the home screen. Under "Saved Sessions" enter a name for this connection. For example "FileFlexDemo" in in this case:

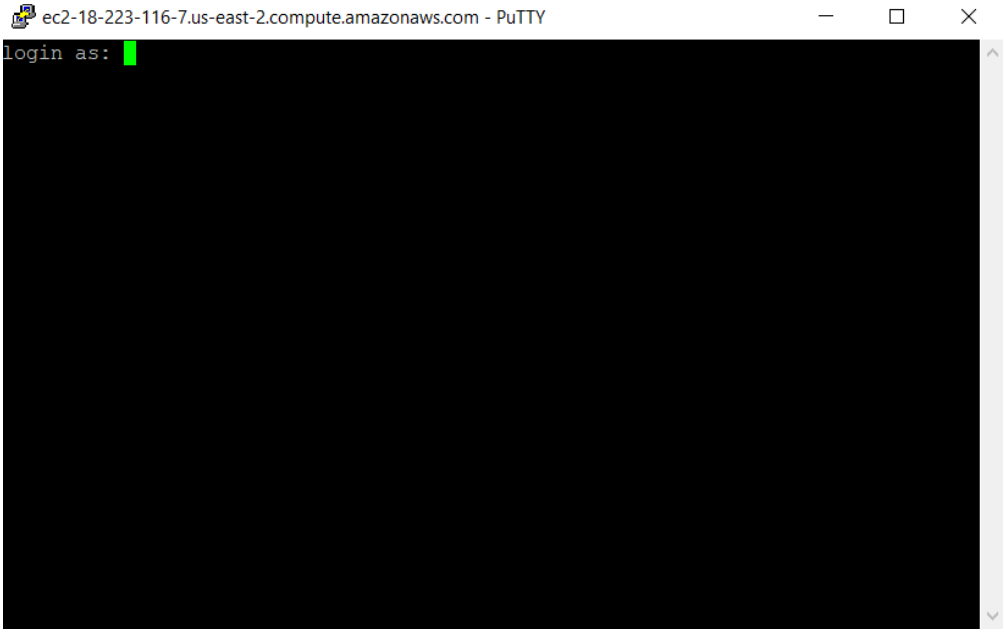


Click the "Save" button so you won't have to enter this information the next time you want to connect to this virtual machine.

Click the "Open" button at the bottom of the dialog to connect to the machine. You will be presented with a warning the first time you connect:



Accept the warning by clicking "Yes". You will then be able to access your virtual machine:

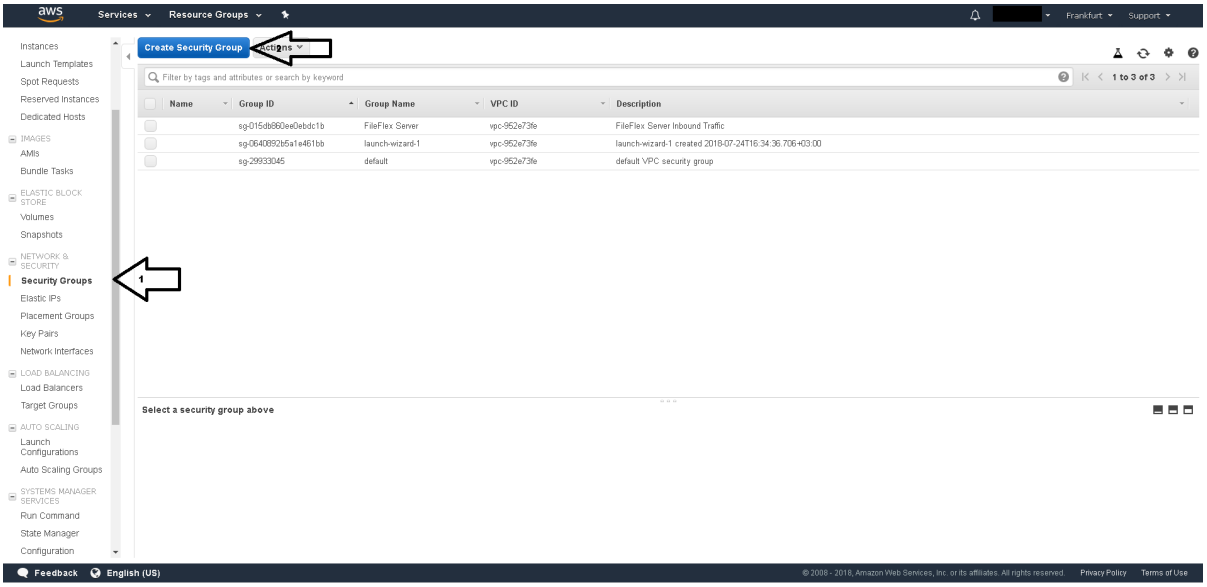


Your machine is now accessible by SSH!

3.7.1.5. Creating a Security Group

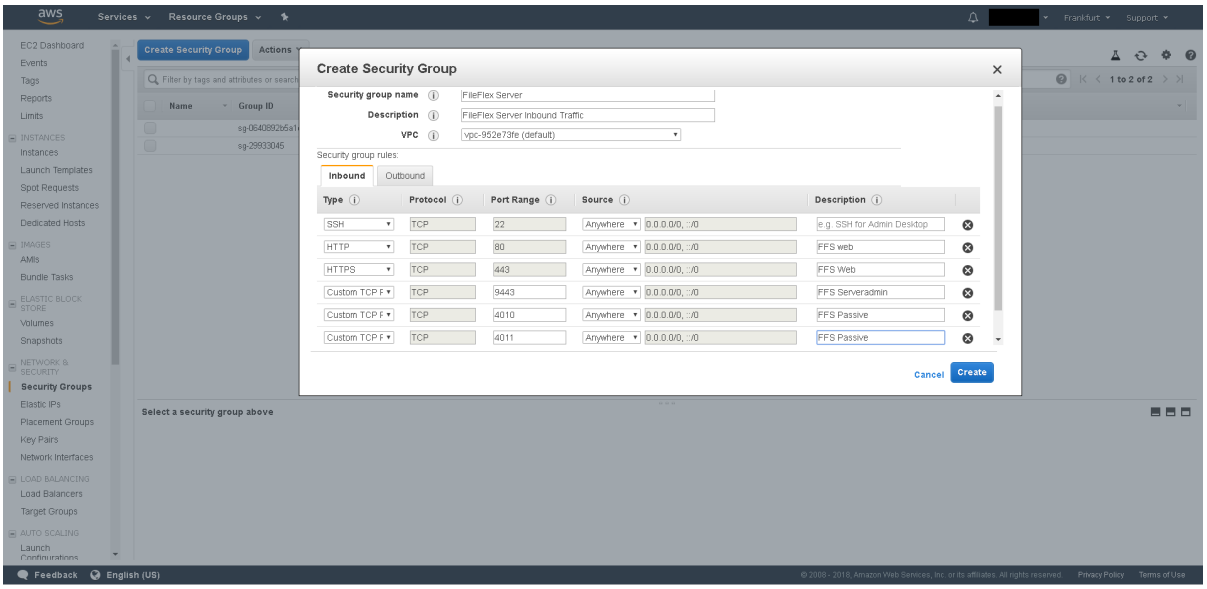
By default a new instance that's been created isn't allowed to receive any inbound external traffic other than on the SSH port 22. To resolve that we must create or modify an existing security group and apply it to our instance.

Navigate to security groups on the Amazon Dashboard:



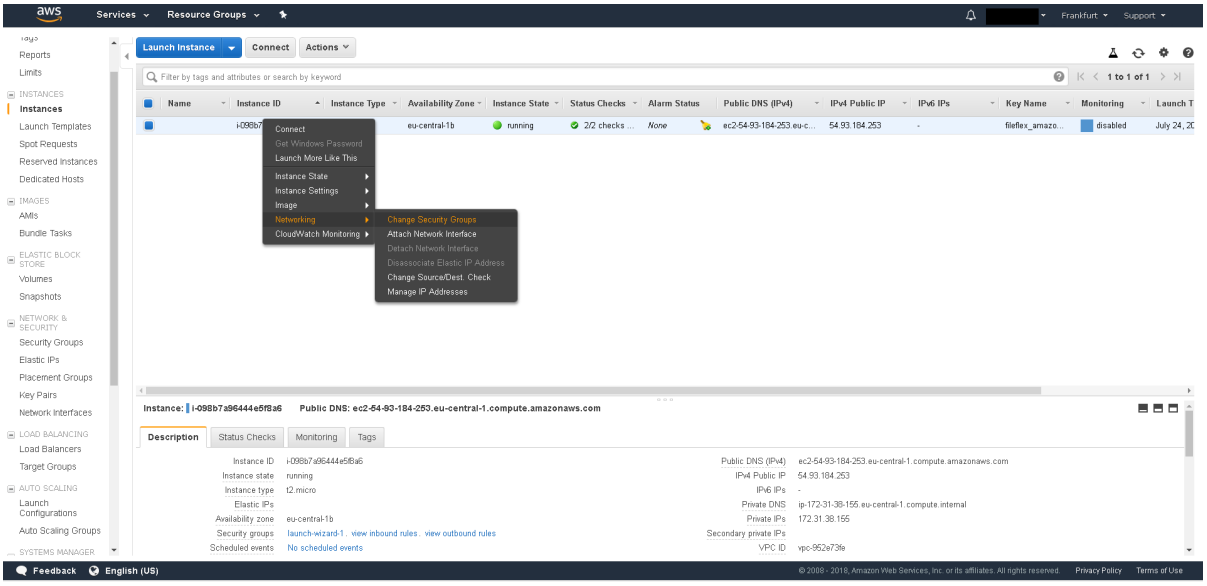
Create a security group. Name it "FileFlex", and ensure that the following TCP ports are allowed from "anywhere":

- 22 for SSH
- 80 for HTTP
- 443 for HTTPS
- 9443 for Server Admin
- 4010 for the FileFlex Connector
- 4011 also for the FileFlex Connector

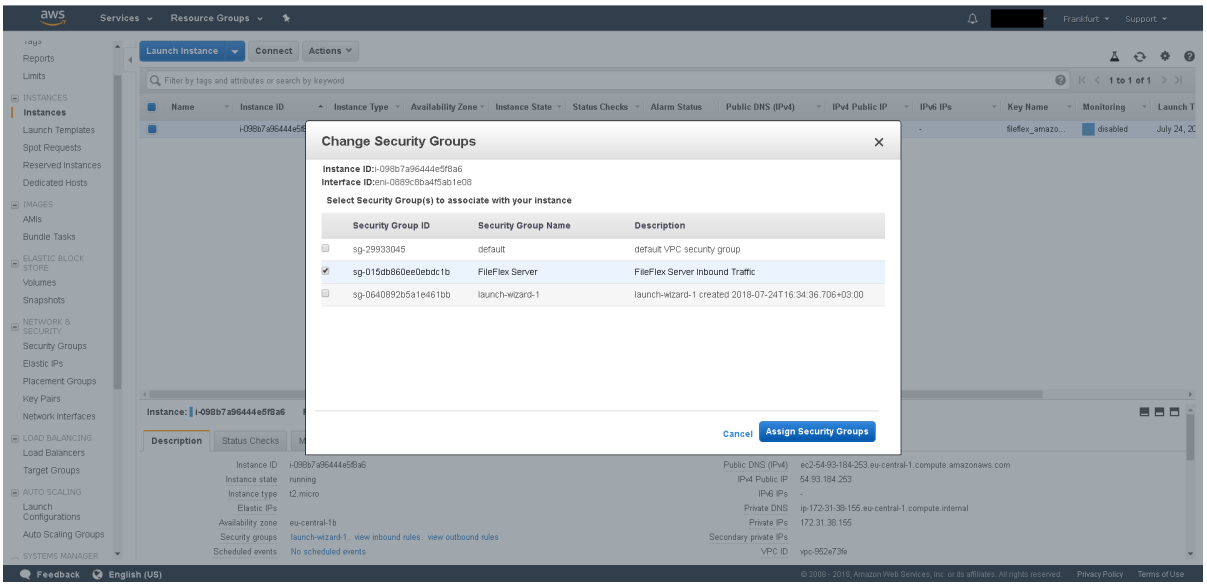


Click create to finish this and close the dialog.

Right click on the instance, and go to Networking, followed by "Change Security Groups":



Once selected, choose your security group from the list and click on "Assign Security Groups".



Congratulations - FileFlex Enterprise is now deployed under Amazon EC2!

4. Installing FileFlex Enterprise

This section of the documentation deals with installing the FileFlex Enterprise software in your newly deployed virtual machine.

> **Internet Connectivity**
>
> To successfully complete this section of the guide, you must have external internet access available on this virtual machine's (bridged) network!

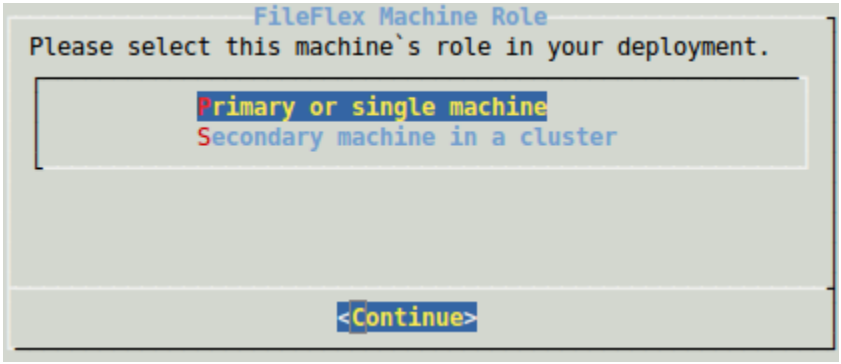
After starting the virtual machine, you will be presented with a console login prompt:

```
Ubuntu 16.04.2 LTS fileflexdemo.com tty1

fileflexdemo login: sadmin
Password:
```

Login using the default credentials:

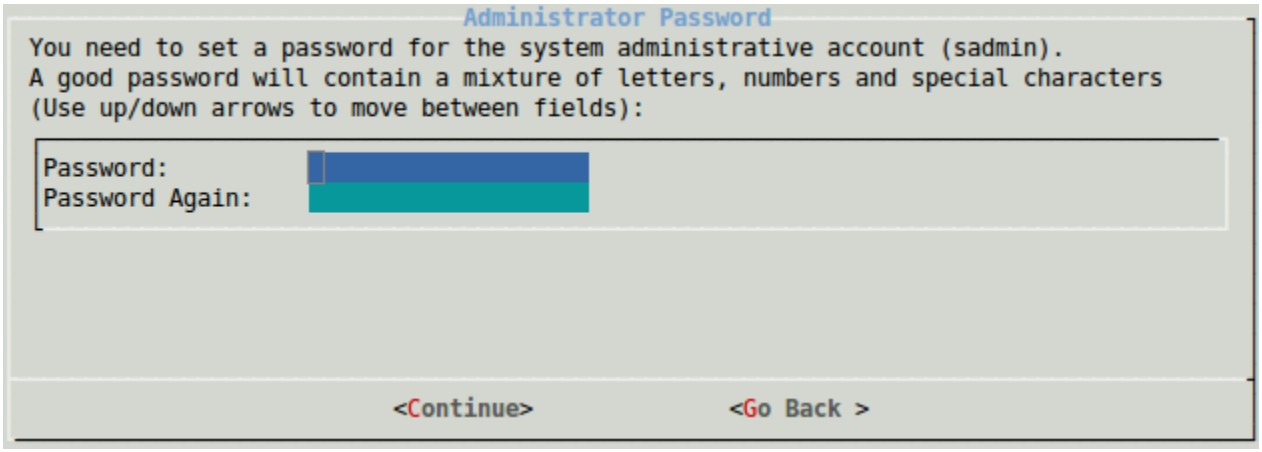
> Default FileFlex Enterprise OS credentials:
>
> | | |
> |---|---|
> | **Username** | sadmin |
> | **Password** | Q!w2e3r4 |

After logging in, the text-mode configuration application will be launched. You will be presented with a mode selection dialog.



This guide assumes that you're deploying a single-machine VM, and the instructions contained on this page reflect that assumption.

Select "Primary or single machine" followed by OK or enter at which point you will be asked to enter a password twice for the OS user for logging in to the VM.



You must now enter a password for the "sadmin" user which you'll use for logging in to the VM and to the server administration application.

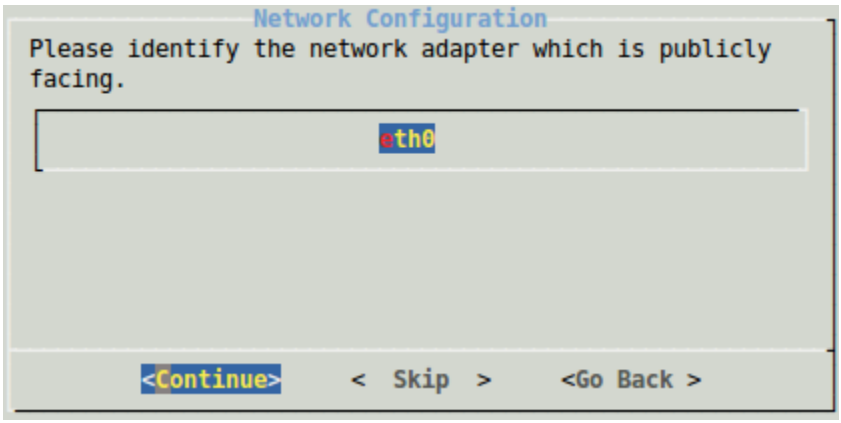
Server administration passwords must contain:

- At least 8 characters
- Upper and lowercase letters
- Numbers, and/or special symbols such as punctuation

You will need to enter the password a second time. Use the arrow keys to move down into the "Password Again" field, and enter the password a second time. When you're done, hit enter to continue.

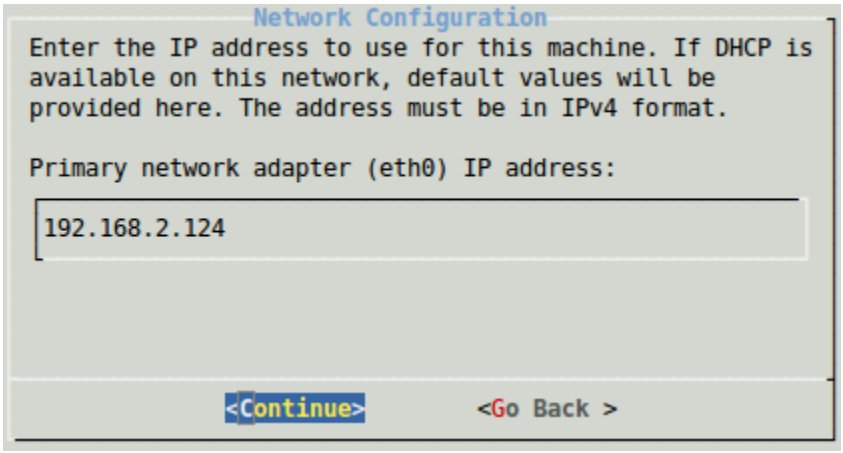
You must use the arrow keys to navigate between the password fields!

You will then be prompted to select the publicly facing network adapter.



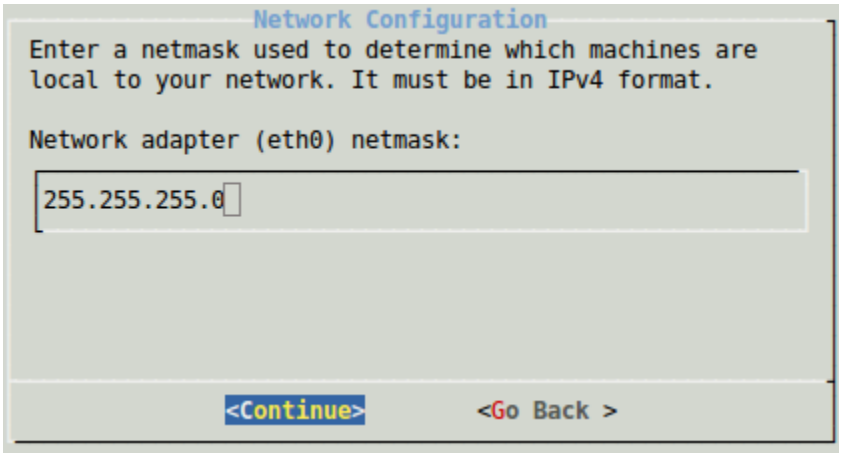
In this case (a single machine deployment) there should be only one, so hit enter to continue.

You will then be prompted to enter an IP address for your primary (externally facing) network adapter:



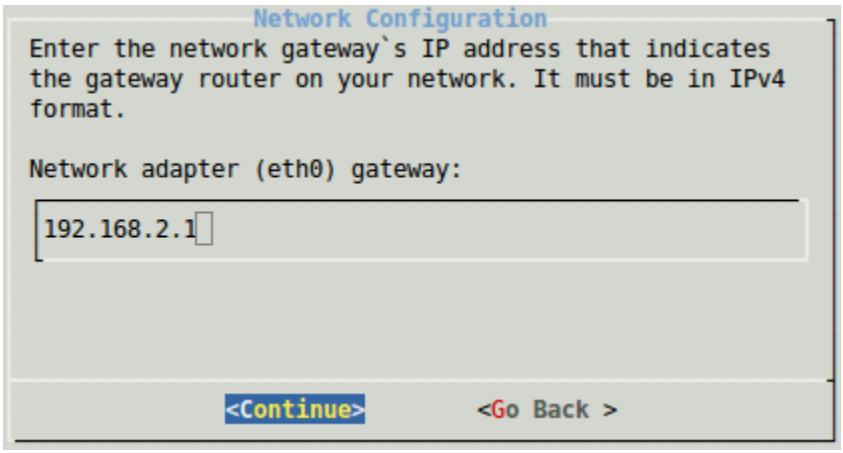
The default values will have been provided by DHCP assuming DHCP services are available on your network. If not, you must enter a valid IP address for the VM on your network. After entering it (if the default is not what you want), hit enter or click OK.

You will then be prompted to enter an IP mask (netmask):



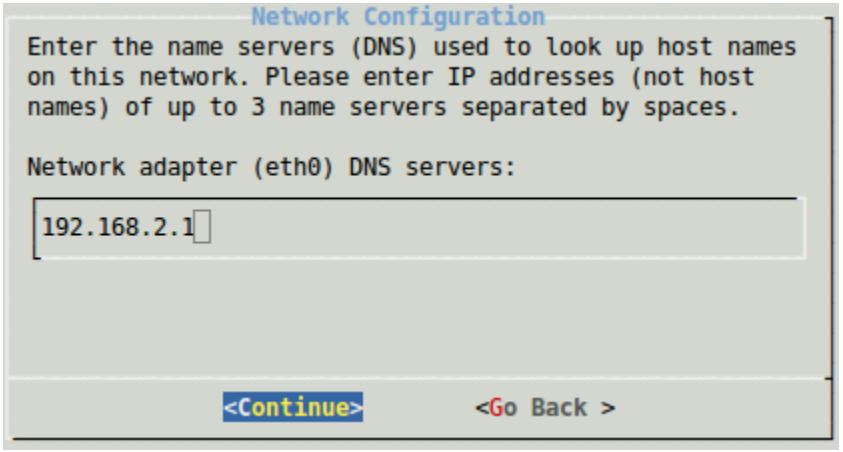
As before, the default value will be provided by DHCP if available on your network. If not, please enter a valid value for your network. Once complete, hit enter or click OK.

You will then be prompted to enter the gateway address:



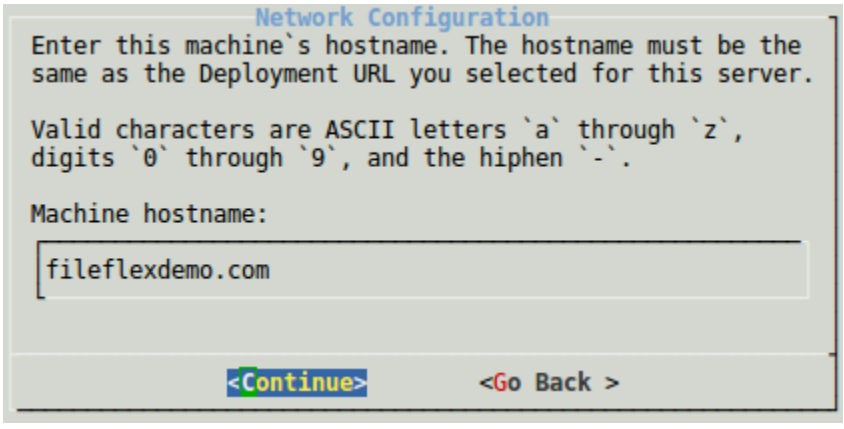
The default value is once again provided by DHCP if available. If not, please enter a valid value for your network. Once complete, hit enter or click OK.

You will then be prompted to enter DNS server addresses:



As before, the default values are provided by DHCP if available. If not, please enter values for your network. You may enter multiple servers (if available) separated by spaces. Once complete, hit enter or click OK.

A new screen will be shown requesting your host name:

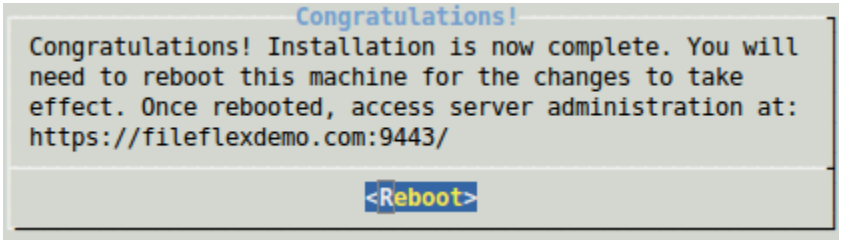


Enter a valid host name for this virtual machine. A value such as "fileflexdemo.com" is appropriate here. Enter the value which you expect will be used by your end-users in a web browser to reach your FileFlex services. Ensure this is in your hosts file or DNS server for proper operation. Select OK and hit enter.

> **Hostname and Deployment URL**
>
> When deploying a single-machine VM, it is important that the Deployment URL entered in the FileFlex Enterprise Portal matches the hostname entered here!

The installer will then connect to the internet to download specific FileFlex packages from the FileFlex repository. Ensure that internet access is available:

Once completed, you will see a "success" dialog:



Hit enter to proceed. Your virtual machine will then restart to finalize configuration.

> If you wish to configure the VM at the command prompt later, ensure that you use the updated password you entered previously. To run this installation again (for example to reconfigure your network settings), issue the following command:
>
> ```
> sudo /opt/ffs/setup.sh
> ```

Your installation is now complete, and you may proceed with the next section of the documentation.

5. Initial Configuration Wizard

Once the FileFlex console installer has completed its work you should be able to open the FileFlex Server Administration tool. This section of the guide presents the steps needed to successfully open the tool, and to provide its initial configuration.

5.1. Local Network Access

The tool operates on port 9443 rather than the standard 443 allowing you to configure your network firewalls to block external access to this tool, which is the recommended configuration.

> ⚠ The FileFlex Server Administration tool is intended to be configured from local network addresses only. Block port 9443 from being access externally.

The locally deployed firewalls (iptables via Ubuntu's ufw) already disable remote access to the tool, but it's a good idea to enforce this higher up the networking chain as well.

5.2. Logging in to FileFlex Server Administration

To access the running server administration tool, you must open a browser of your choice to the hostname you configured earlier using port 9443.

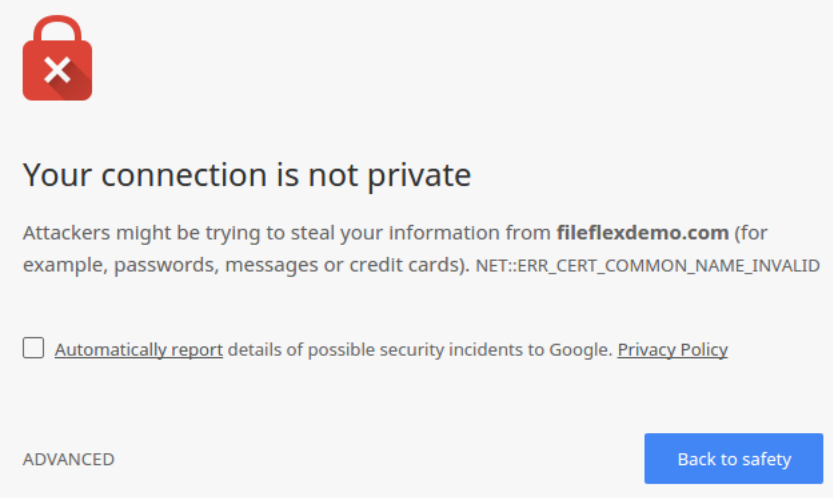
> ⚠ Ensure that virtual machine you recently configured is available on your local network using port 9443 and a fully qualified domain name.

Your DNS servers (or hosts files) must be correctly configured to point the configured host names to the IP given to the VM, and your fire walls must not block port 9443 for local network access to that VM.

For example, open the following url assuming your DNS is fully configured (substitute your configured host name):

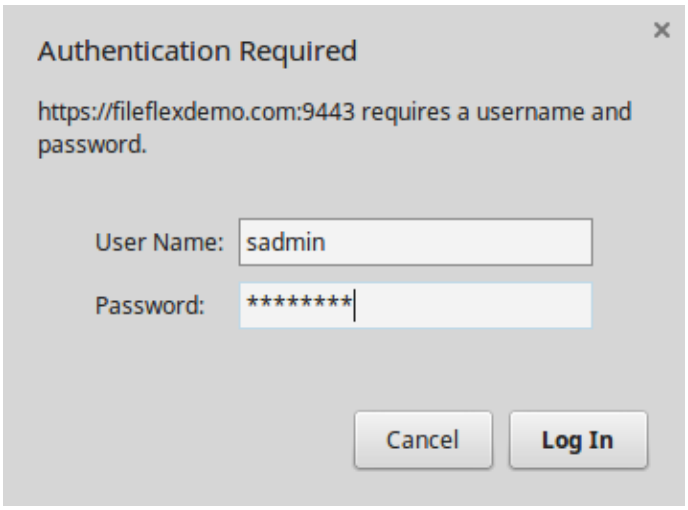
Example Server Administration URL
`https://fileflexdemo.com:9443`

Since we have not yet configured an SSL certificate, you may receive a warning from your browser, which is normal at this point. For example on Chrome you might see:



Take the necessary steps with your chosen browser to open the web page regardless of the warnings. In this case of Chrome, open the "advanced" section and click on the "proceed" link.

You will then be presented with an authentication challenge dialog:



Here you must enter the 'sadmin' credentials you configured previously in the console installer. Once complete, click "log in" (as appropriate with your browser of choice) to enter the Server Administration tool.

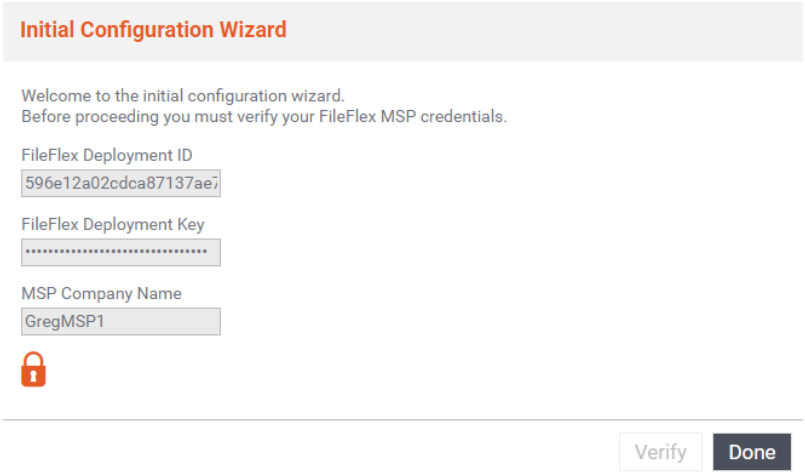
You will be presented with the initial configuration wizard, the first screen of which has three fields which must be entered. These are the fields which bind your MSP server deployment to a FileFlex billing account.

> ⚠ You must have already configured an account at the FileFlex partner portal, at which point the necessary Deployment ID and Deployment Key will have been provided to you.

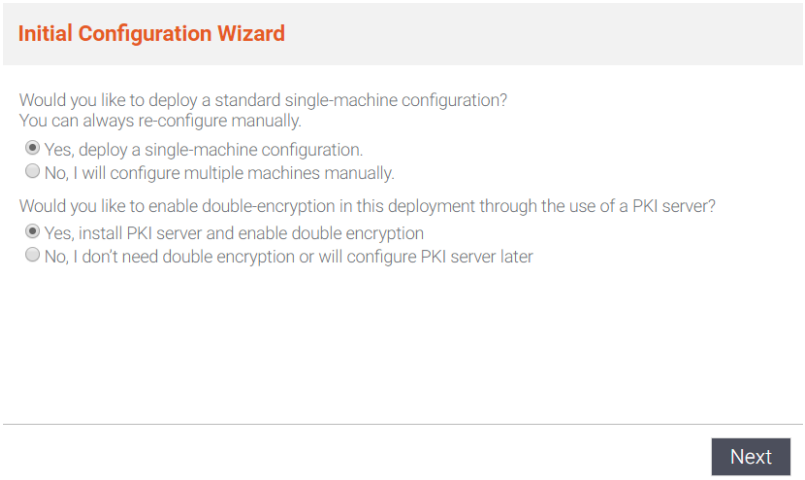
The fields in the wizard are described below. Enter the values given to you by the FileFlex team (and/or from the partner portal):

1. The FileFlex Deployment ID which identifies this deployment of one or more servers.
2. The FileFlex Deployment Key which acts as a password for this deployment.
3. The MSP Company Name which will be fetched automatically based on the ID and Key provided earlier.

Once you've located and entered the Deployment ID and Deployment Key, click the "verify" button to complete the validation sequence. Once validated, the lock symbol should then be closed, and the "Done" button will become enabled.



Click the "Done" button. You will then be presented with a screen in which you must select the type of deployment you're looking for.



This page of the initial configuration wizard requires you to select if you want a single machine deployment, or a more complicated setup involving multiple machines.

> This guide assumes a single-machine deployment except where otherwise explicitly stated.

The first option is a single machine deployment which this guide assumes. If you were configuring a single node within a cluster, then the second option would be chosen.

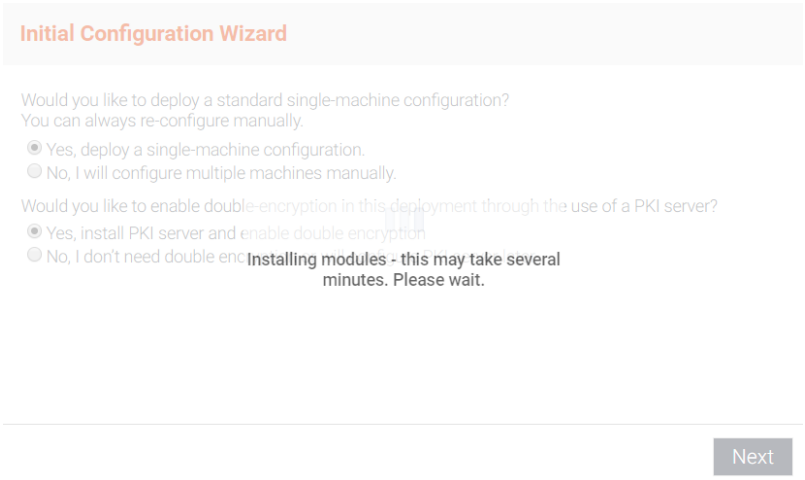
Select "Yes, deploy a single-machine configuration" from the radio button group (it should already be selected as the default).

You will also be asked if you want to enable double-encryption.

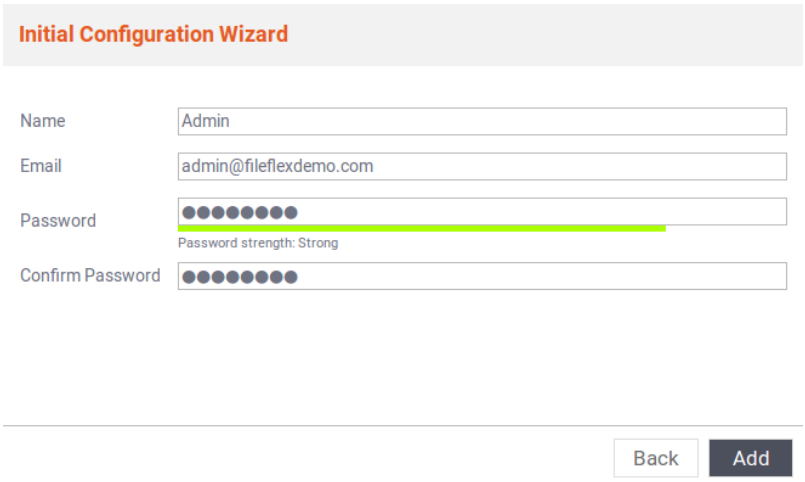
> Double encryption is a feature which allows end-to-end encryption from content source all the way to the client, and provides very strong security. When selected, content owners will be able to select whether or not they want to enable double encryption on a per-content-source basis. A side effect of such a configuration (when enabled by the content owner) is that the content cannot be consumed from a web browser. Users will still be able to use traditional encryption, which allows for browser-based consumption.

This guide assumes that double encryption will be enabled, so selected "Yes, install PKI server and enable double encryption", then click "next" to proceed to module installation.

The modules will then be installed. You will need to wait a few minutes for this step to complete:



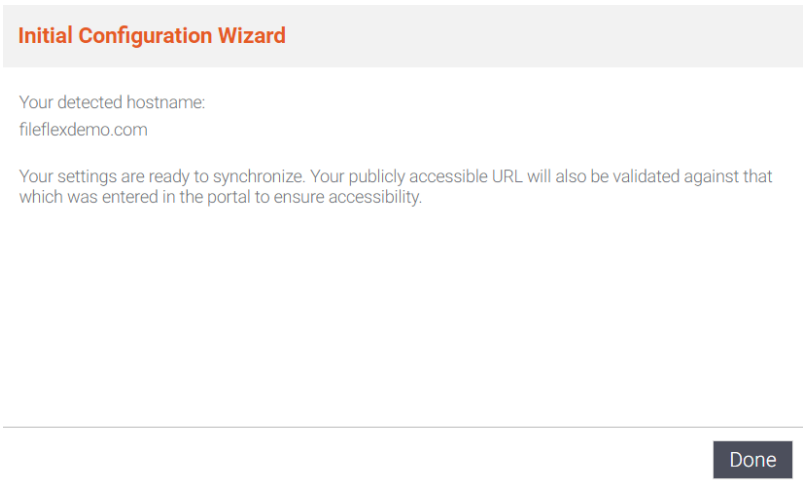
After a few minutes you will be presented with a screen with which you will create the user administration account:



Enter a name, email and password for the user which will be used (later) to access User Administration.

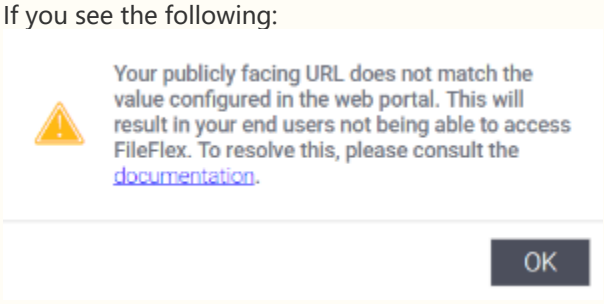
> ⚠ Be sure to keep the user administration credentials safe - you will need them later

Click "next" to proceed to the final wizard screen:



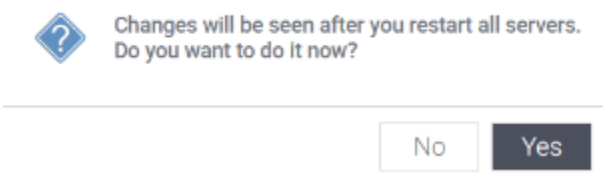
Here your host name is confirmed, and you must complete the installation by clicking "done". Do so now.

If you see the following:



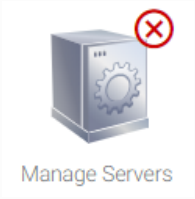
... it means that the hostname entered during this setup phase does not match the one you registered with in the FileFlex Enterprise Portal. You should re-configure this virtual machine to use an alternative hostname. The hostname is not editable in the Enterprise Portal, because changing it would cause connectivity problems for existing users.

You will then be asked to restart your servers:



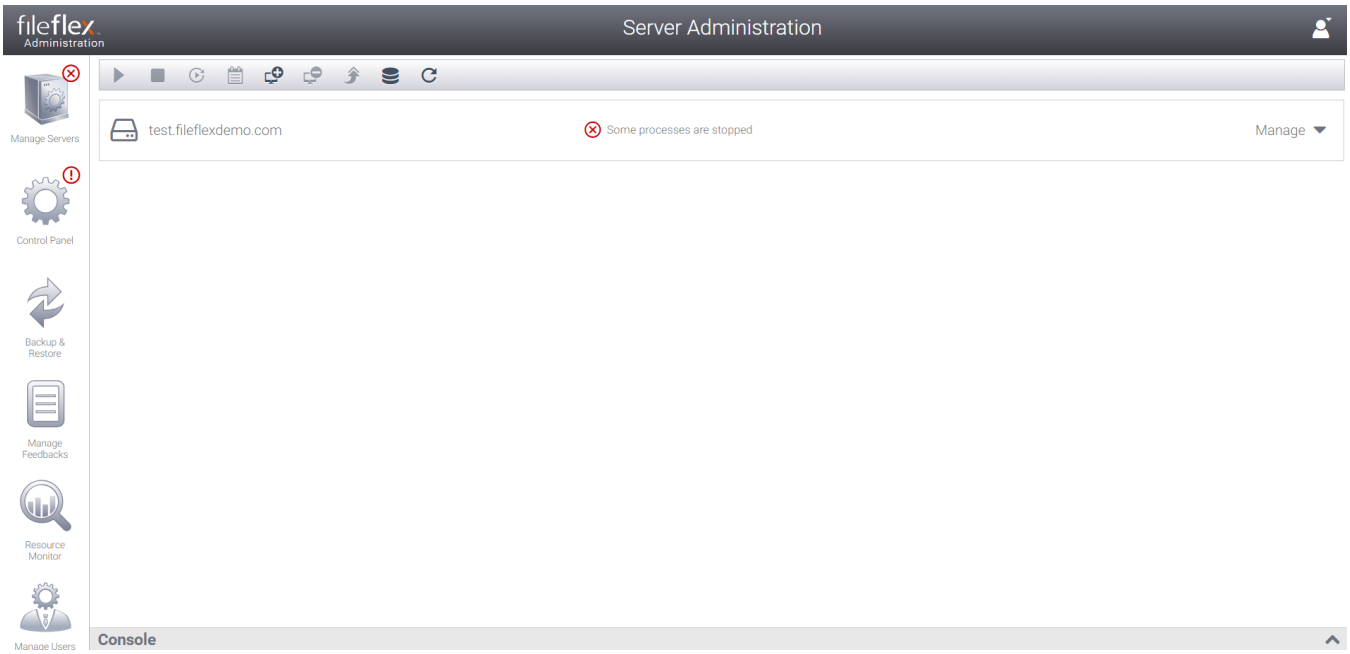
Click "yes" to proceed. Wait about 30 seconds and you will be presented with the Server Administration web application.

The warning icons are expected until some mandatory configuration steps are completed in the forthcoming steps!



More specifically, a certificate must be installed, and email delivery must be configured prior to having a working deployment.

You will see a screen similar to the following:



You're now ready to perform the configuration steps required to customize the deployment to your specific requirements.

6. User Interface Overview

The Server Administration module is divided into several distinct categories (represented by tabs) to separate functionality based on the intended management operation.

6.1. Functionality by Section

Icon	Name	Description
	Manage Servers	The "manage servers" tab opens the server manager in which you can start or stop servers, or processes within those servers. The total number of machines contained with a cluster is called a "deployment".

	Control Panel	The "control panel" tab opens the control panel which is an area to perform the detailed configuration necessary to having a fully operational FileFlex deployment.
	Backup and Restore	The "backup and restore" tab allows you to define back sets, schedule backups, define offsite backup locations, and to directly execute backup and restoration actions.
	Manage Feedbacks	The feedback tab allows you to collect user feedback reports for support purposes, and to submit them to the FileFlex team for further analysis if so desired.
	Resource Monitor	The "resource monitor" tab allows you to view and monitor the CPU utilization, memory use, and network throughput of the machines within the deployment cluster.
	Manage Users	The "manage users" action launches the user administration application in a new browser tab. This tool will allow you to define companies, departments, and their associated roles and privileges. You can also add or import users into your defined companies and define content sources made available to your users.
	Help	The "help" action launches the FileFlex help into a new browser tab. From there you can locate information to help you navigate the FileFlex systems.

6.2. Global Notifications

Global notifications indicate a configuration or running state concern within one of the application sections. You will see an icon overlayed on top of the sectional icons described above indicating that your attention is required. The following breaks down the various possible states:

Icon	Name	Description
	Manage Servers Attention Required	Indicates that your attention is required in the "manage servers" section. Typically indicates that updates are available.
	Manage Servers Execution Failure	Indicates that one more more server processes did not start as expected.
	Control Panel Urgent Notification	Indicates that a mandatory section of the control panel has not yet been configured, and is required for proper operation of the system.

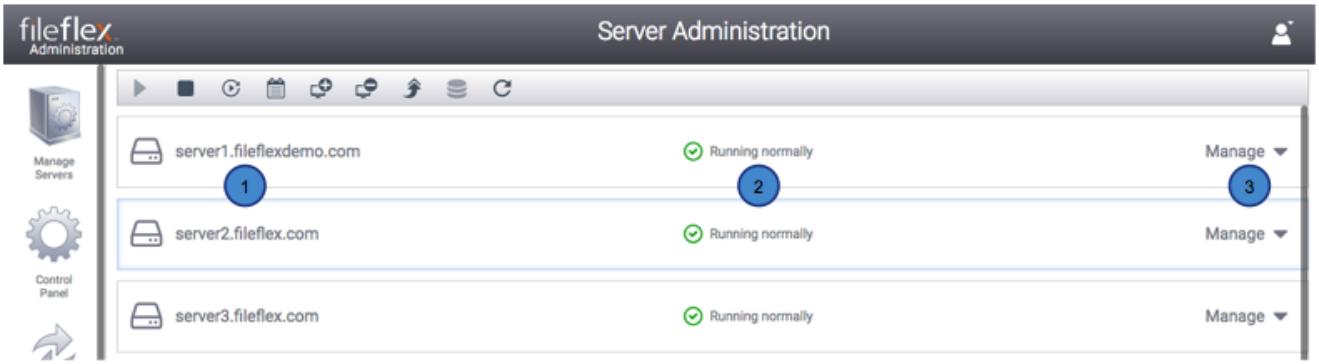
	Backup & Restore Urgent Notification	Indicates that a backup failure occured.

7. Managing Servers

This section describes the server management functionality available in the Server Administration module.

7.1. The Server List

The primary area available within the server management tab is the server list. It shows you a list of one or more servers available within your deployment. For example:



1. The name of the server in the deployment cluster.
2. The status of the server. It could be running normally, be stopped, or require updates.
3. The manage tool allows you to expand a single server to show more options available.

Here we see a list of one or more servers. In this example we have three servers within a deployment, with the middle server (server2.fileflex.com) being actively selected (shown by a thin blue border around it). We can see that all three servers are "running normally". We can also see that each server has an option to "manage" it further which will be explained shortly.

> It's important to keep an eye on the status information (e.g. running normally). This will quickly help you see if a server is not running, or if updates are required

7.2. Server Action Toolbar

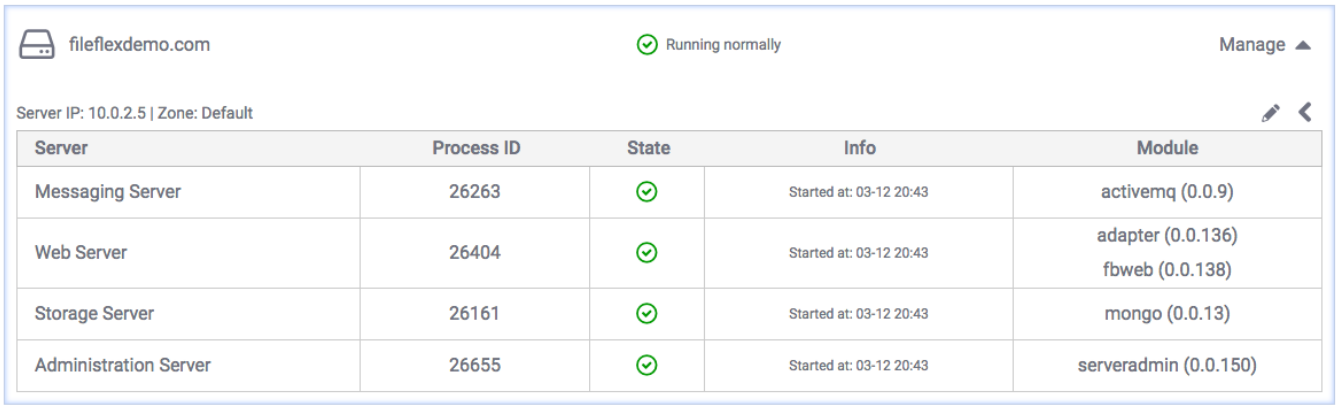
At the top of the server list we see a toolbar containing some server actions:

1. Start the currently selected server processes (does not start the operating system).
2. Stop the currently selected server processes (does not stop the operating system).
3. Restart the currently selected server processes (does not restart the operating system).
4. Download a zip file containing the server logs. Useful for debugging issues with the FileFlex team.

5. Add a machine to the cluster (cluster specific action).
6. Remove a machine from the cluster (cluster specific action).
7. Upgrade the machine's FileFlex software packages.
8. Storage replica-set initialization (used for clusters having a replicated data store - cluster specific action).
9. Refresh the visualized server list.

7.3. Managing a Machine's Processes

One machine will likely contain more than one server process within it and this is true in the typical case of a single machine deployment. Clicking the "manage" action on the right of a server will expand it's area to show you it's available processes. For example:

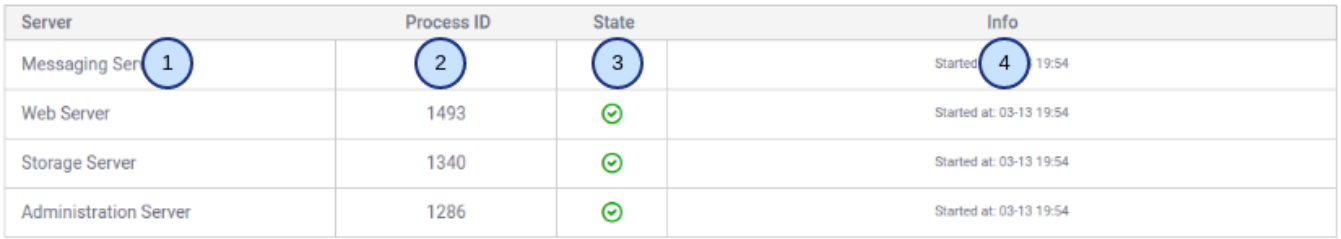


Server	Process ID	State	Info	Module
Messaging Server	26263		Started at: 03-12 20:43	activemq (0.0.9)
Web Server	26404		Started at: 03-12 20:43	adapter (0.0.136) fbweb (0.0.138)
Storage Server	26161		Started at: 03-12 20:43	mongo (0.0.13)
Administration Server	26655		Started at: 03-12 20:43	serveradmin (0.0.150)

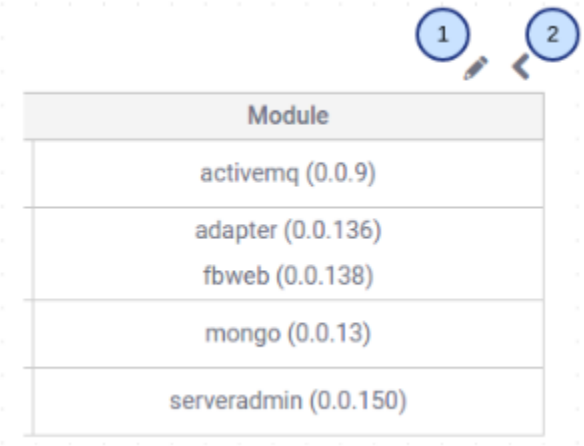
From this panel you are able to select discrete server processes available on the virtual machine, and perform toolbar actions over them. For instance you can select the web server, and stop it, and then start it using the server action toolbar described earlier.

> Single machine deployments contain an 'Administration Server' process, which is the tool you are presently using to manage the deployment. Because of it's presence the stop machine feature is disabled since it would render your current session inoperable. Stopping other processes is still permitted however.

The columns within server process expansion are as follows:



1. A server process running on the virtual machine (for example a messaging server, a storage server, etc)
2. The process ID associated with the running server process. This will likely not be needed except for debugging purposes.
3. The present state of the process running within the machine. For example is it running, stopped, or does it require an upgrade?
4. Additional information about the server process - specifically when it was last started



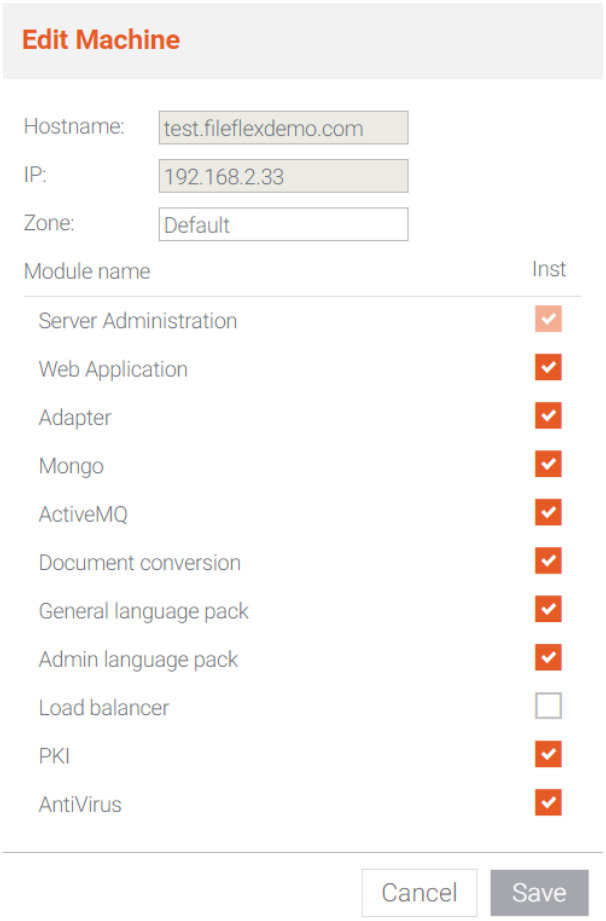
1. Clicking the pencil icon will allow you to edit the processes installed on a virtual machine.
2. Clicking the expander arrow will reveal additional information about the processes running on the virtual machine. Specifically it will reveal a list of the modules deployed within that server process.

In the example above, after clicking on the expander arrow we see that two modules were deployed in the web server process: The "adapter" and the "fbweb" modules, along with their specific versions. This information is primarily used when deploying clustered solutions to separate the web and adapter portions for the purposes of isolation and scalability. It can safely be ignored in the case of single machine deployments except when communicating with FileFlex support.

7.4. Adding and Editing Machine Server Processes

Selecting the "add machine" icon from the top toolbar, or the "edit machine" icon from the right will reveal a dialog box allowing you to edit which processes are installed on a given virtual machine instance.

⚠ There is typically no need to edit the processes running in a single machine deployment.



Field	Explanation
Hostname	The hostname identifies the name of your virtual machine and is used when communicating between virtual machines.
IP	The IP address of the virtual machine.
Zone	A geographic zone used when deploying multiple geographically separate clusters. Typically set to "Default" (or any consistent value across all nodes in the single cluster)
Modules	A list of processes and/or modules deployed within a virtual machine

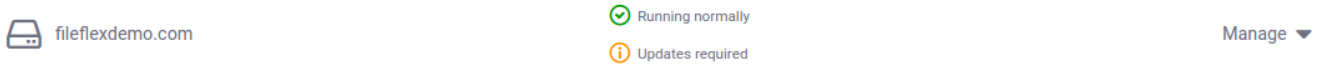
7.4.1. Deployable Modules

Module	Module Purpose
Server Administration	A process and module allowing the administrator to configure the deployment.
Web Application	The primary client facing application used by user administration and end users.
Adapter	The content adapter module that lives within the web server process and connects to external data sources.
Mongo	The database server (possibly deployed three times in a replica set).
ActiveMQ	The messaging server used for communication between the nodes of a cluster.

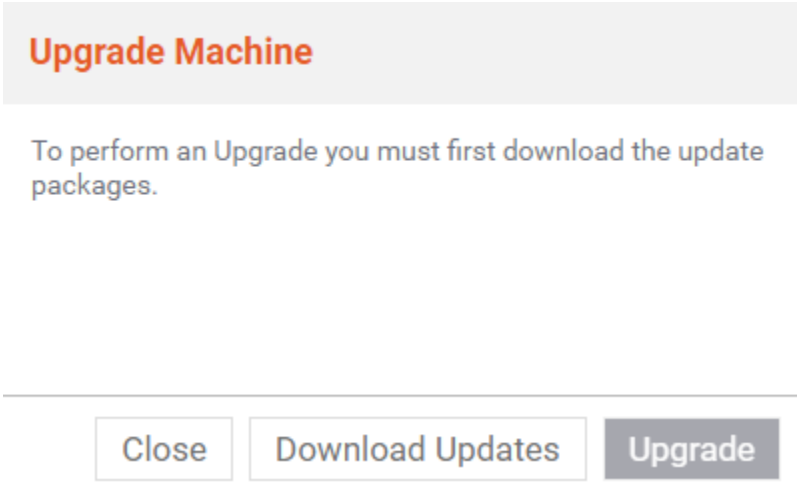
Document Conversion	Document visualization package.
General language pack	The primary application's internationalization files.
Admin language pack	The server administration internationalization files.
Load balancer	A load balancer used when deploying cluster configurations.
PKI	Public key infrastructure server used to enable double encryption support.
AntiVirus	An antivirus scanning module used when uploading to third party services.

7.5. Upgrading a Virtual Machine

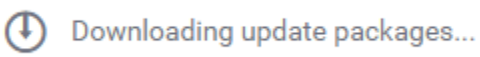
The FileFlex team will deploy security updates and bug fixes from time to time. When your machines are out of date, you'll see a notification as follows:



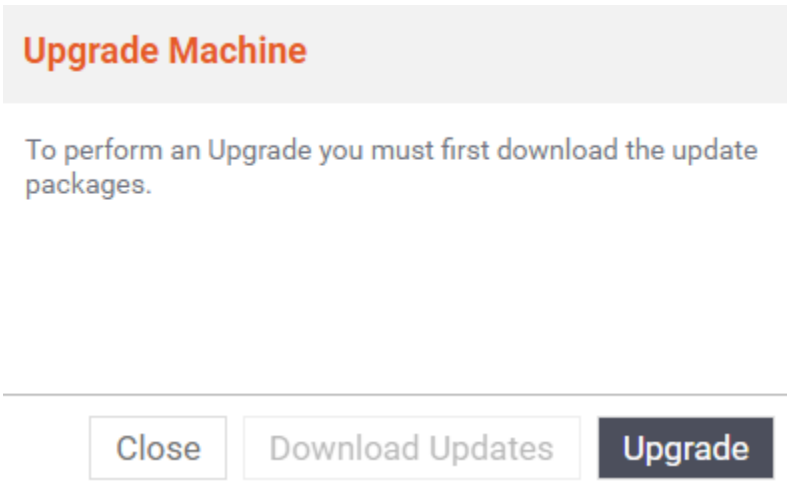
To upgrade the machine, click it's row in the listing (there may only be a single machine if it's a single-machine deployment), then select the upgrade icon  from the server action toolbar. You will then be prompted to download the update packages:



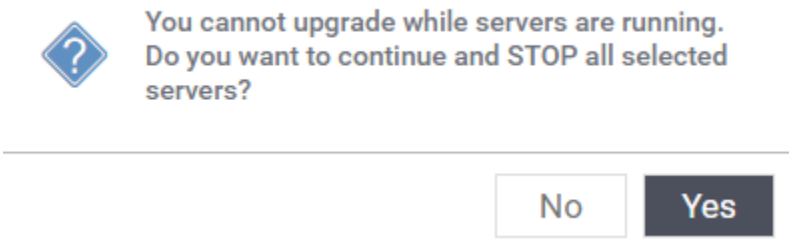
Click "download updates" to continue. You will then see a downloading message:



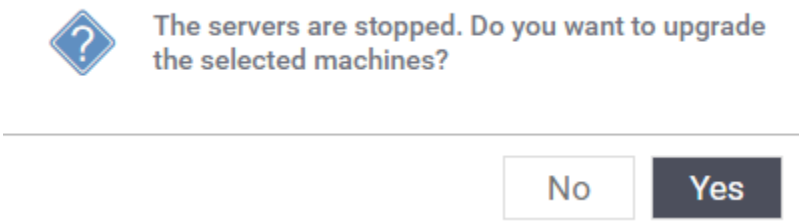
After a few minutes the download will complete and the upgrade button will become enabled:



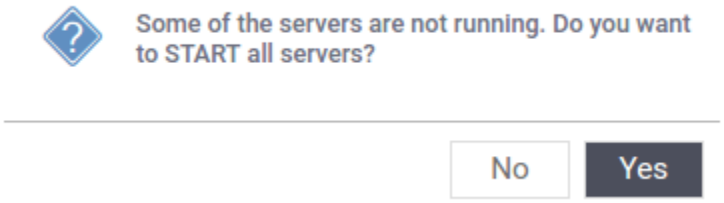
Click on the upgrade button. If your servers were previously running you will be presented with the following dialog:



Click Yes to stop the servers. Once the servers have stopped you will receive a confirmation:



Click yes to upgrade. After a few minutes the upgrade will have completed and you'll be asked if you want to start the servers back up:



Click yes to continue. After a few moments you'll see confirmation that your servers are running normally, and no longer require upgrades:

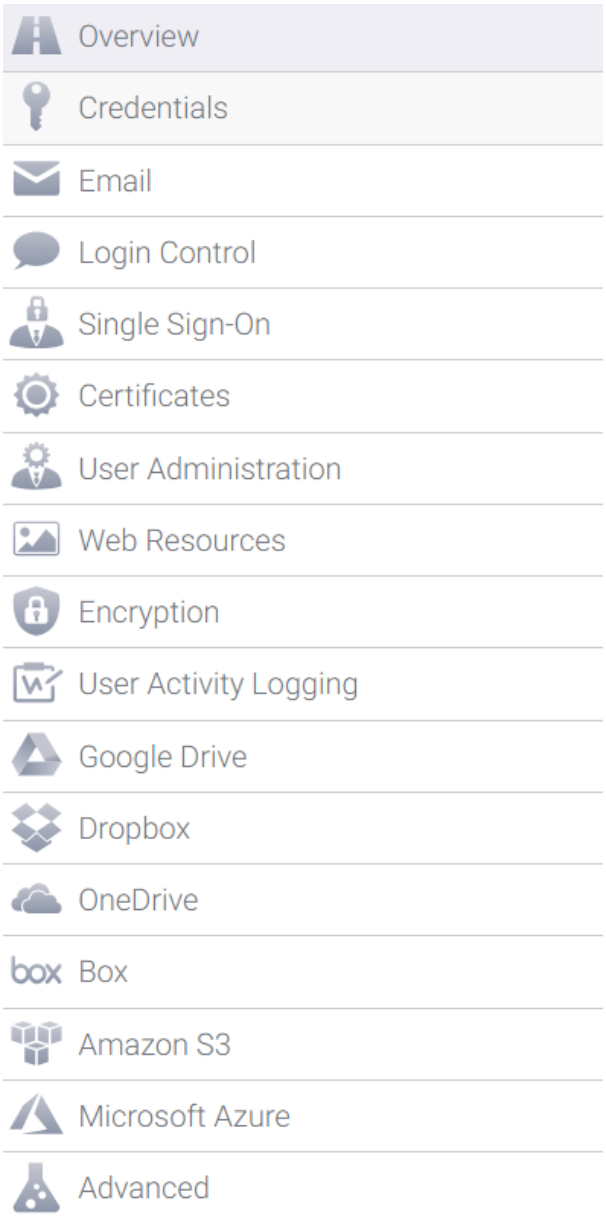
8. Control Panel and Configuration

The control panel is where all FileFlex Enterprise configuration is performed and is divided into 7 panels in order to group related functionality. It will be necessary to configure settings across several categories before having a fully configured FileFlex Enterprise deployment.

> If you requested a single-machine deployment, you can log in to the user administration module immediately without having to configure everything in the control panel. Open a browser to your selected host name using HTTPS. For example, navigate to https://www.fileflexdemo.com. You will receive a certificate warning until you've configured one in the control panel.

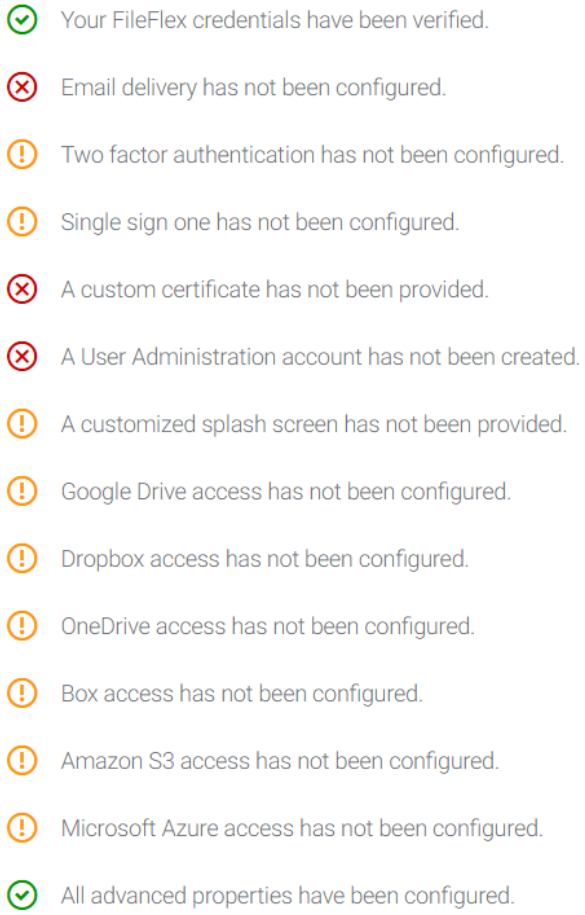
8.1. Configuration Overview

The first and default section of the control panel is the overview, and it helps you see at a glance which sections have been configured, and which are still outstanding. To access it select "overview" from the control panel menu:



The overview section is intended to help you understand which aspects of FileFlex Enterprise still need configuration. Once all the yellow or red information symbols have been replaced by green check boxes, you'll have completed configuring FileFlex Enterprise.

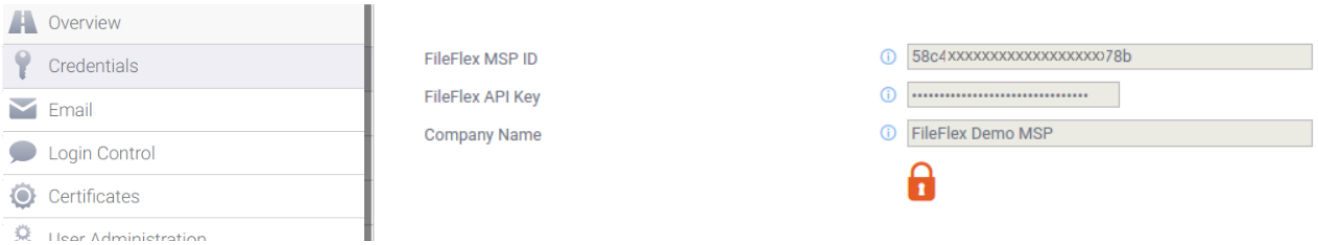
For example you should initially see a screen similar to the following:



Your FileFlex configuration is not complete until all information symbols (either yellow or red) are replaced by green check boxes.

8.2. Your FileFlex Enterprise Credentials

Clicking on the "credentials" menu item from the left will reveal the credentials configuration page:



The credentials screen allows you to select new FileFlex credentials to associate with your deployment. This will not be something that you typically have to do, but it is a convenient place to get them for referential purposes.

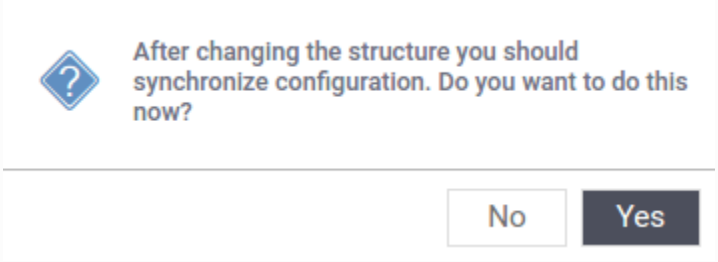
If you do need to associate the current deployment with a different FileFlex Enterprise billing account, click the lock symbol and enter a new ID and key. The company name will be fetched automatically based on those credentials.

Applying Configuration Changes

At the bottom of most configuration panels are the following buttons:

1. The "synchronize" button is used to force synchronization between machines in a cluster, and is not needed for single machine deployments.
2. The "reset" button will undo all changes temporarily made in the control panel and restore the previously saved values.
3. The "apply" button will save all locally made changes and synchronize them across the cluster (or single machine deployment).

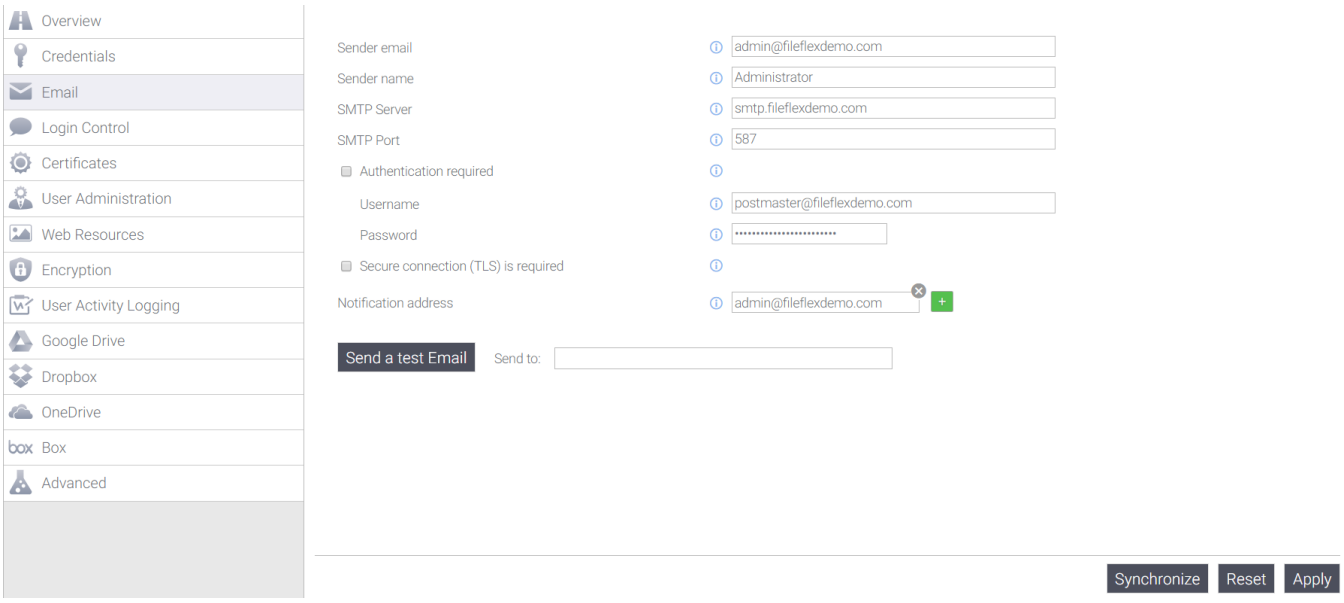
Once you've made changes, you will be prompted to synchronize the changes across the cluster which is a necessary step.



Select "yes" to ensure your changes are applied as expected.

8.3. Configuring Email Delivery

Selecting "email" from the left hand control panel menu will show the email configuration page:



Email delivery is a crucial aspect of FileFlex enterprise configuration. It is used for share notifications, password reset functionality, account password delivery and more.

The default sender email email is similar to noreply@{web.hostname.public}. This is using a macro, and would resolve to noreply@fileflexdemo.com in our case. This may or may not be the value you want as your "sent from" address.

8.3.1. Email Configuration Parameters

Configure your email delivery fields using the following table as a guide:

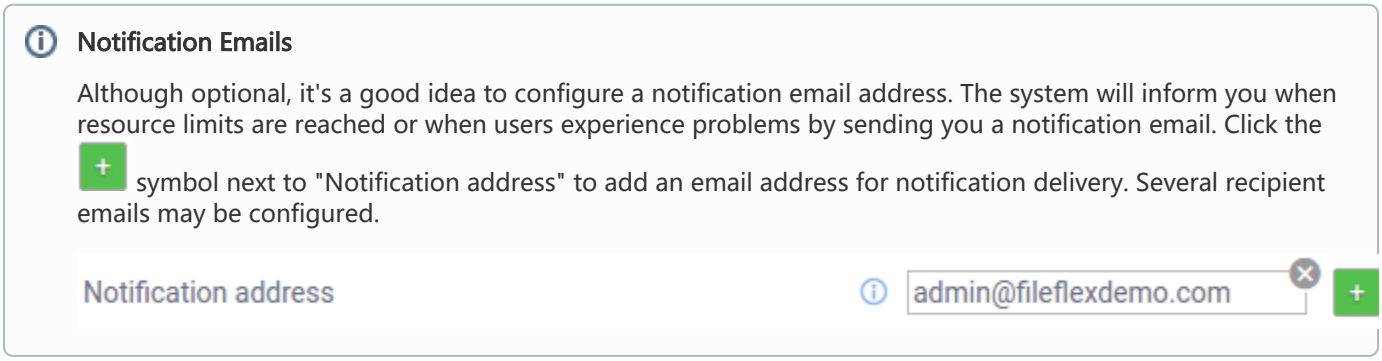
Sender Email	The email address that appears as "sent from" in all emails delivered. Example: johnsmith@place.com.
Sender Name	The name that appears as "sent from" in all emails delivered. Example: John Smith
SMTP Server	The SMTP server hostname used for email delivery. Example: smtp.mycompany.com
SMTP Port	The SMTP port number used. This is typically 25, or 587 for secured connections. Example: 587
Authentication Required	Does your email server require authentication to delivery emails? Typically true. Example: True (check box).
Authentication Username	The SMTP username if authentication is required. Typically required. Example: johnsmith@place.com
Authentication Password	The SMTP password if authentication is required. Typically required.
Secure Connection Required	Does your email server required a secured (encrypted with TLS) connection? Typically true. Example: True (check box)
Notification address	One or more email address that will receive notifications from the system. Examples include CPU and memory utilisation warnings and user feedback submissions.

8.3.2. Example Email Configuration

As an example, to configure for MailGun transactional email delivery, we can use values similar to the following (substitute your own credentials from Mailgun):

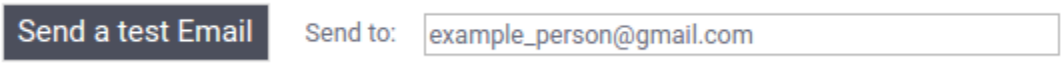
Sender Email	admin@fileflexdemo.com
Sender Name	FileFlex Demo
SMTP Server	smtp.mailgun.org
SMTP Port	587
Authentication Required	True
Authentication Username	postmaster@fileflexdemo.com

Authentication Password	xxxxxxxxxx (use the password provided by Mailgun)
Secure Connection Required	True



8.3.3. Testing Email Delivery

The final step is to confirm that email delivery works as expected. For example:

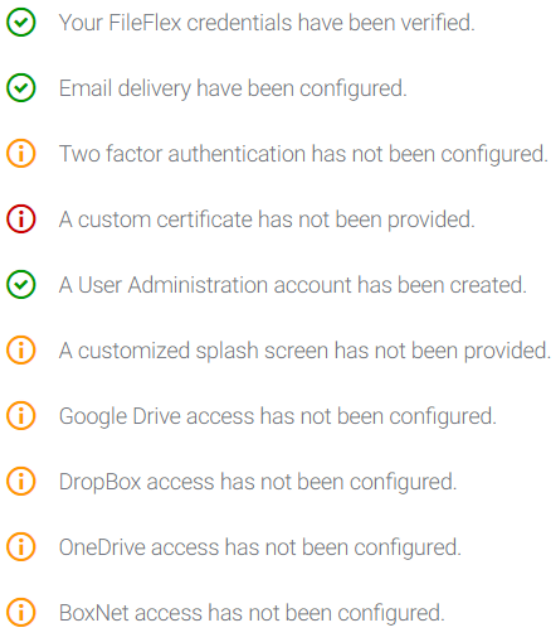


Enter a personal email to which you want a test email delivered using your email delivery configuration, then click the button to send a test email. Wait a few moments for the settings to be synchronized and the test email delivered.

You will receive an email similar to the following (in this case, in the gmail web client):

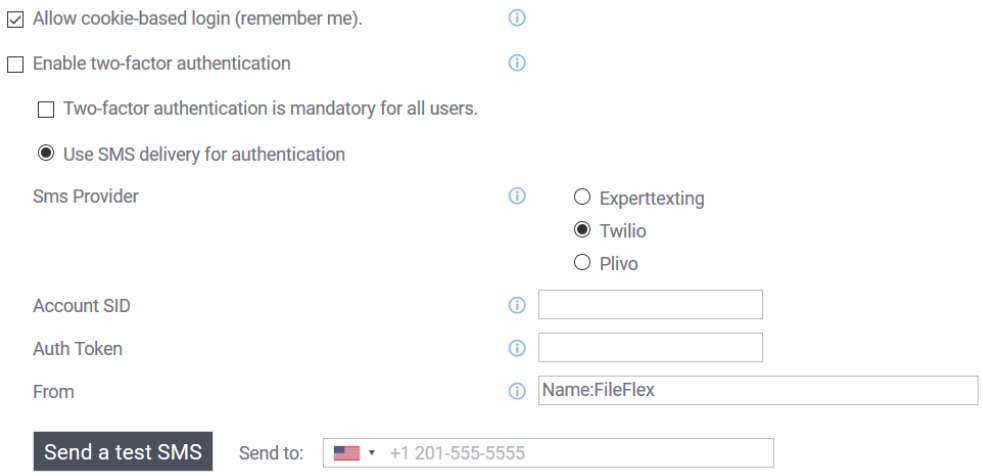
If you've received that email, then email delivery is working as expected!

Once you're satisfied with the configuration click the "Apply" button at he bottom. Clicking back to the overview you should now see a green checkmark indicating that email delivery has been configured and is ready to use:



8.4. Setting up Login Control

Selecting "Login Control" from the control panel menu will reveal login control options including TFA (two factor authentication) and cookie login options.



TFA is also known as multi factor authentication, and is used as an extra layer of security that requires not only a password and username to login, but also something only the user physically has on them. The FileFlex implementation requires the user to have an SMS-reachable phone as the TFA delivery target.

8.4.1. General TFA Settings

Setting	Meaning	Possible Values

Allow cookie-based login	Enabled the "remember me" option so users can be automatically logged in from devices storing the cookie for a limited amount of time.	True, False
Enable two-factor authentication	Two factor authentication will be enabled for this deployment if enabled.	True, False
Two-factor authentication is mandatory for all users	Determines whether users choose to enable TFA for themselves, or whether it is mandatory for all users of this deployment.	True, False
Use SMS delivery for authentication	Deliver TFA codes using SMS.	True, False
Use email delivery for authentication	Deliver TFA codes using email.	True, False
SMS Provider	Which SMS provider will be used for delivery of the TFA codes. Only available when SMS delivery has been selected.	Twilio, Expertexting, Plivo
From	The is the phone number configured in your SMS provider's portal as the delivery number for your TFA codes.	

When TFA is enabled and mandatory, all users will need to supply an SMS-delivered code along with their password when they login.

Using email for TFA code delivery is not a secure form of TFA unless email delivery is encrypted at all stages, and the user's device used for FileFlex access is incapable of receiving that email. Email delivery is typically best-used as a means of testing only.

8.4.2. SMS Provider Credentials

Each SMS provider has a different set of credentials which must be entered in order for FileFlex to make use of their services. You will have to sign up for an account with a provider of your choice. Your selection of an SMS provider may be guided by an existing account with them, the cost of delivery in your target market, or other factors.

There is a fee associated with SMS delivery depending on the provider and region. Delivery of an SMS message typically costs between 1 and 10 US cents.

8.4.2.1. SMS via Twilio

URL	https://www.twilio.com/
Account SID	This is Twilio's account ID used for accessing their services. Only available when Twilio delivery has been selected.
Auth Token	This is Twilio's account token used for accessing their services. Only available when Twilio delivery has been selected.

8.4.2.2. SMS via Plivo

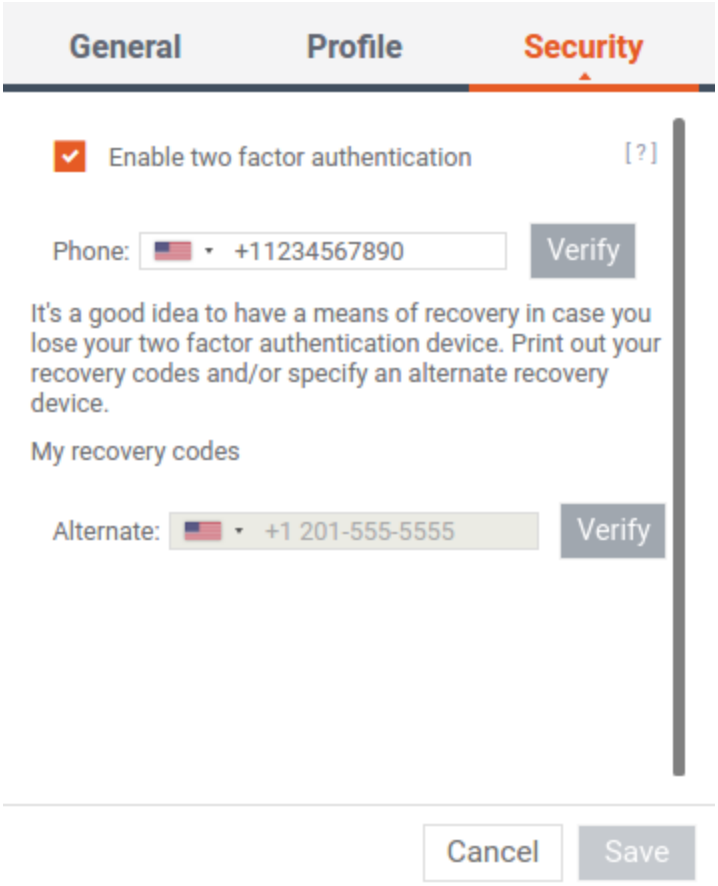
URL	https://www.plivo.com/
Auth ID	This is Plivo's authorization ID used for accessing their services. Only available when Plivo delivery has been selected.
API Auth Token	This is Plivo's API token used for accessing their services. Only available when Plivo delivery has been selected.

8.4.2.3. SMS via ExpertTexting

URL	http://www.experttexting.com/
Username	This is ExpertTexting's account username used for accessing their services. Only available when ExperTexting delivery has been selected.
Password	This is ExpertTexting's account password used for accessing their services. Only available when ExperTexting delivery has been selected.
API Key	This is ExpertTexting's API key used for accessing their services. Only available when ExperTexting delivery has been selected.

8.4.3. TFA for the End User

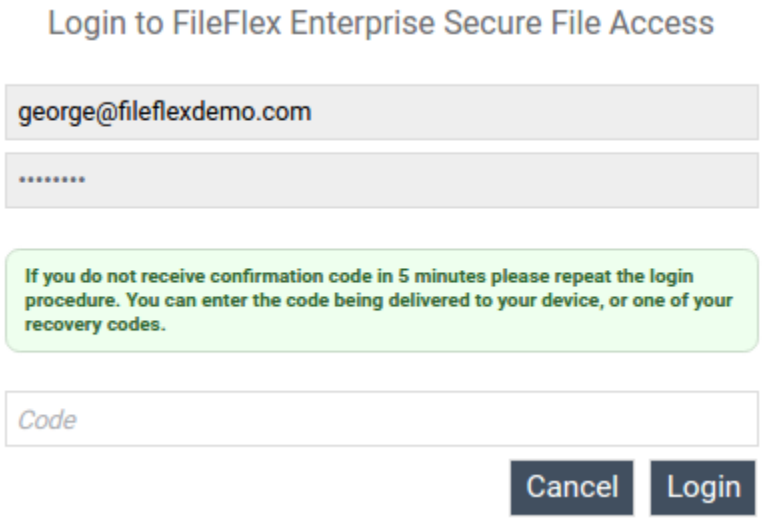
If TFA is enabled in server administration (without it being mandatory), the user will have the option of enabling it for himself after logging in as follows:



If TFA is enabled with the additional mandatory setting, all users must configure TFA prior to logging in.

Mandatory TFA is a deployment-wide setting. You cannot make it mandatory for one company, while keeping it optional for another

Once configured, when logging in TFA code will be generated by the system and immediately delivered to the user's mobile device. The user must then enter that numeric code into the field provided at login time as follows:

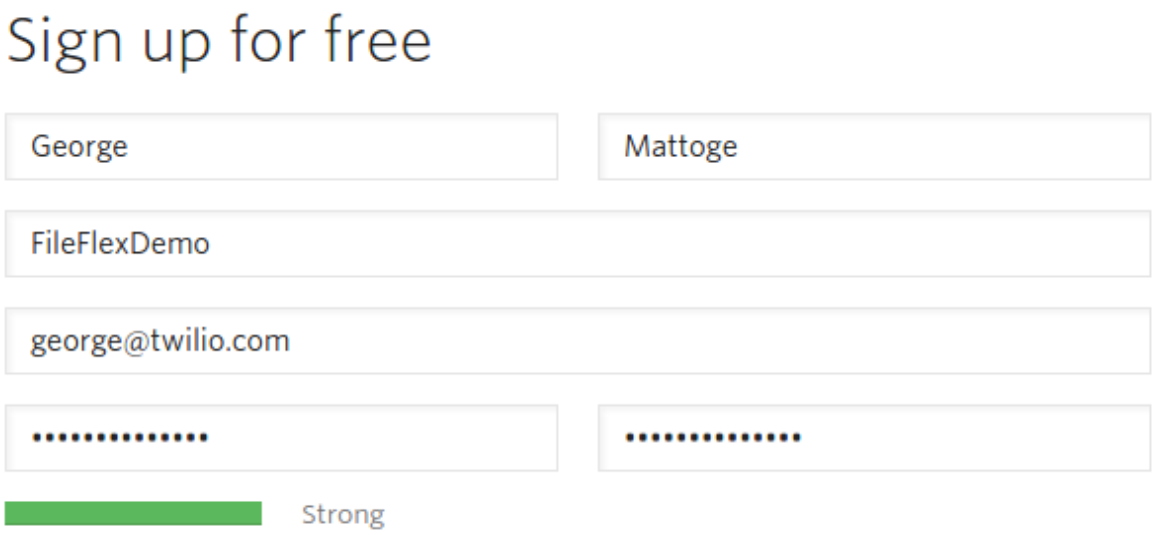


8.4.4. Example Twilio TFA Configuration

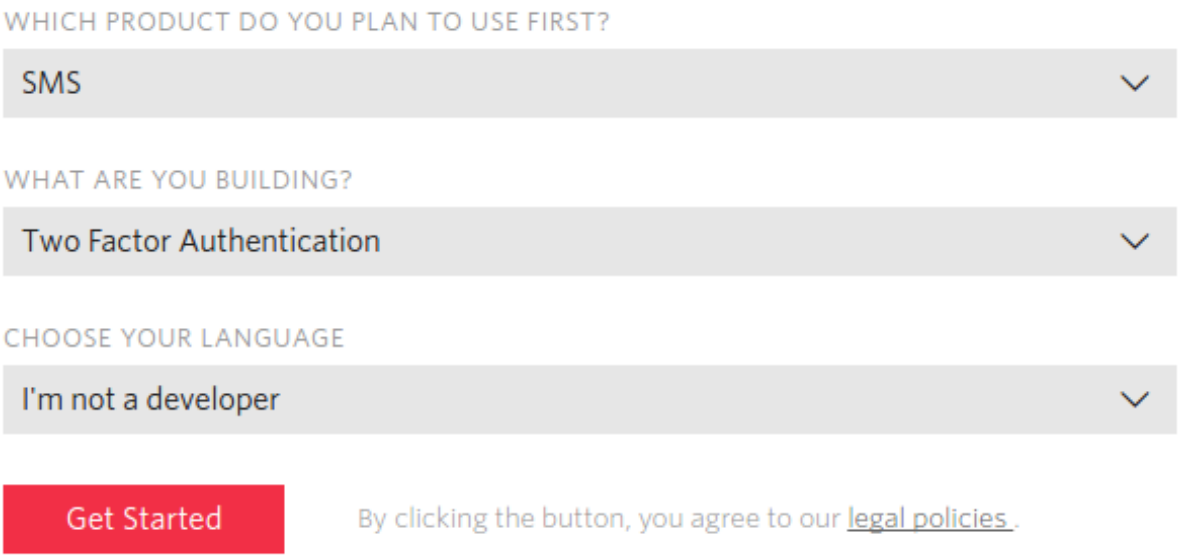
This section describes how to configure TFA step-by-step using Twilio.

8.4.4.1. Create a Twilio Account

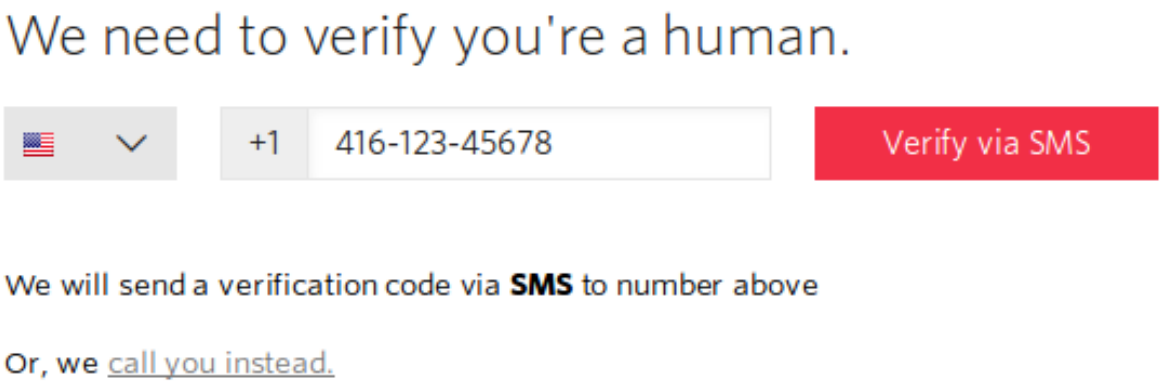
The first step is to create a twilio account. Open a new tab or browser and navigate to https://www.twilio.com/try-twilio and enter your credentials as requested by Twilio.



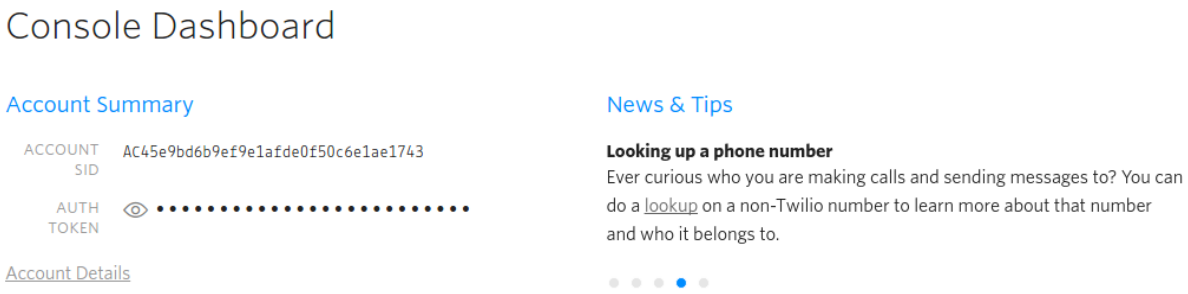
Select "SMS" are the product, "TFA" as what you're building, and indicate that you're not a developer:



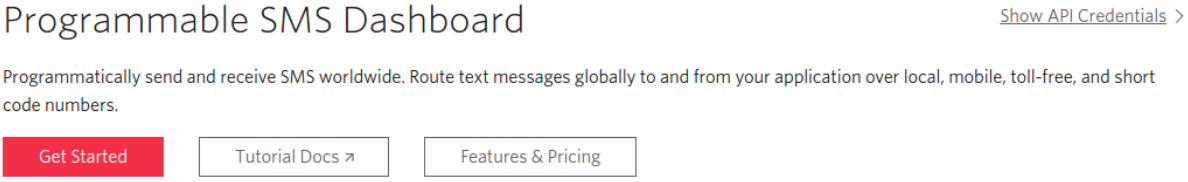
They will ask you to verify that you're human, and issue you an SMS to a mobile device of your choice.



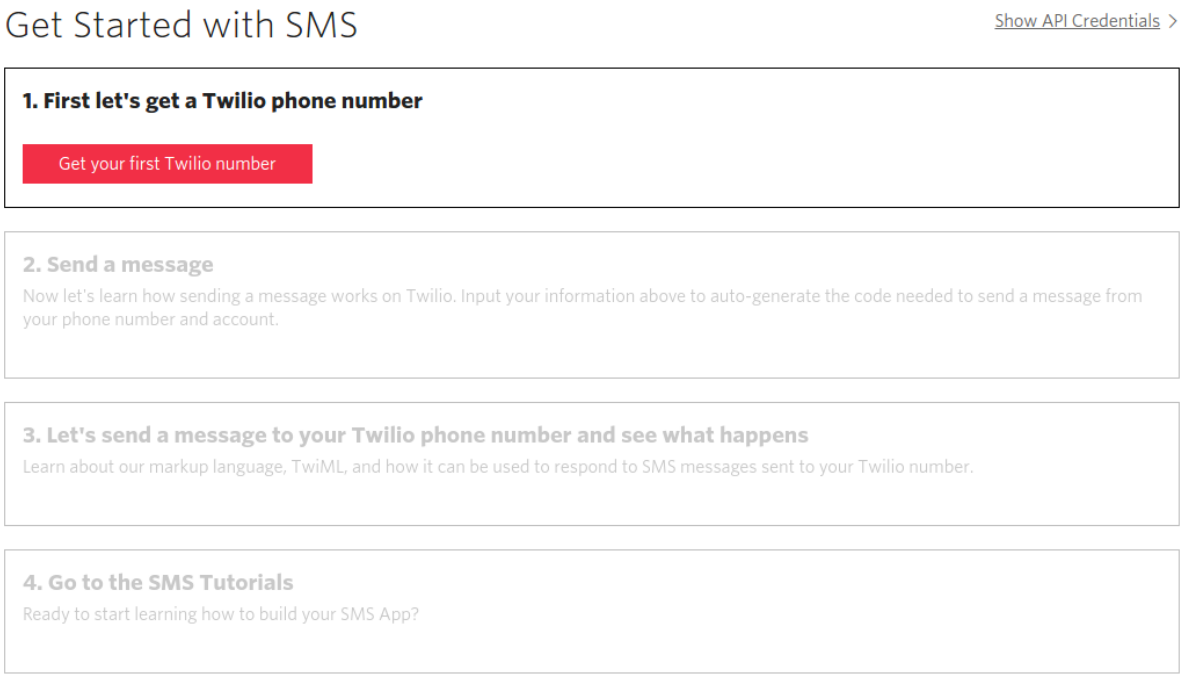
You will then be logged in and may need to dismiss some popups. Once dismissed, you will be placed in the Twilio console:



Click on the "Programmable SMS" icon on the right hand side to reveal the "Programmable SMS Dashboard":

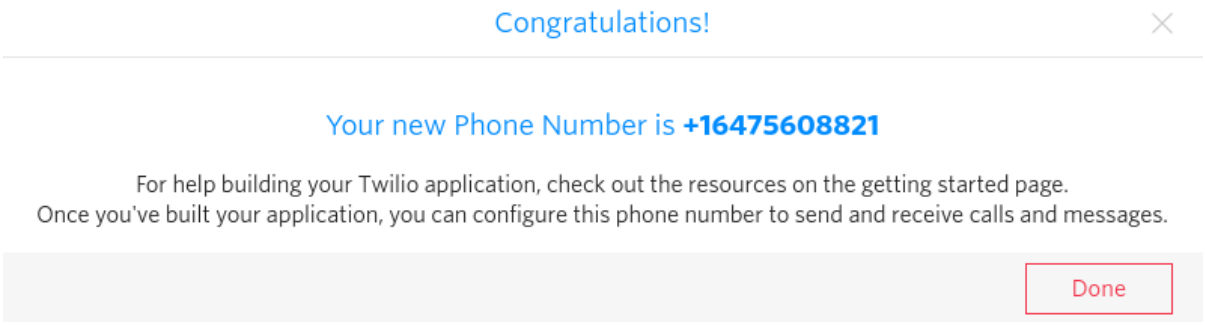


Click on "Get Started" and you will be presented with their getting started wizard:



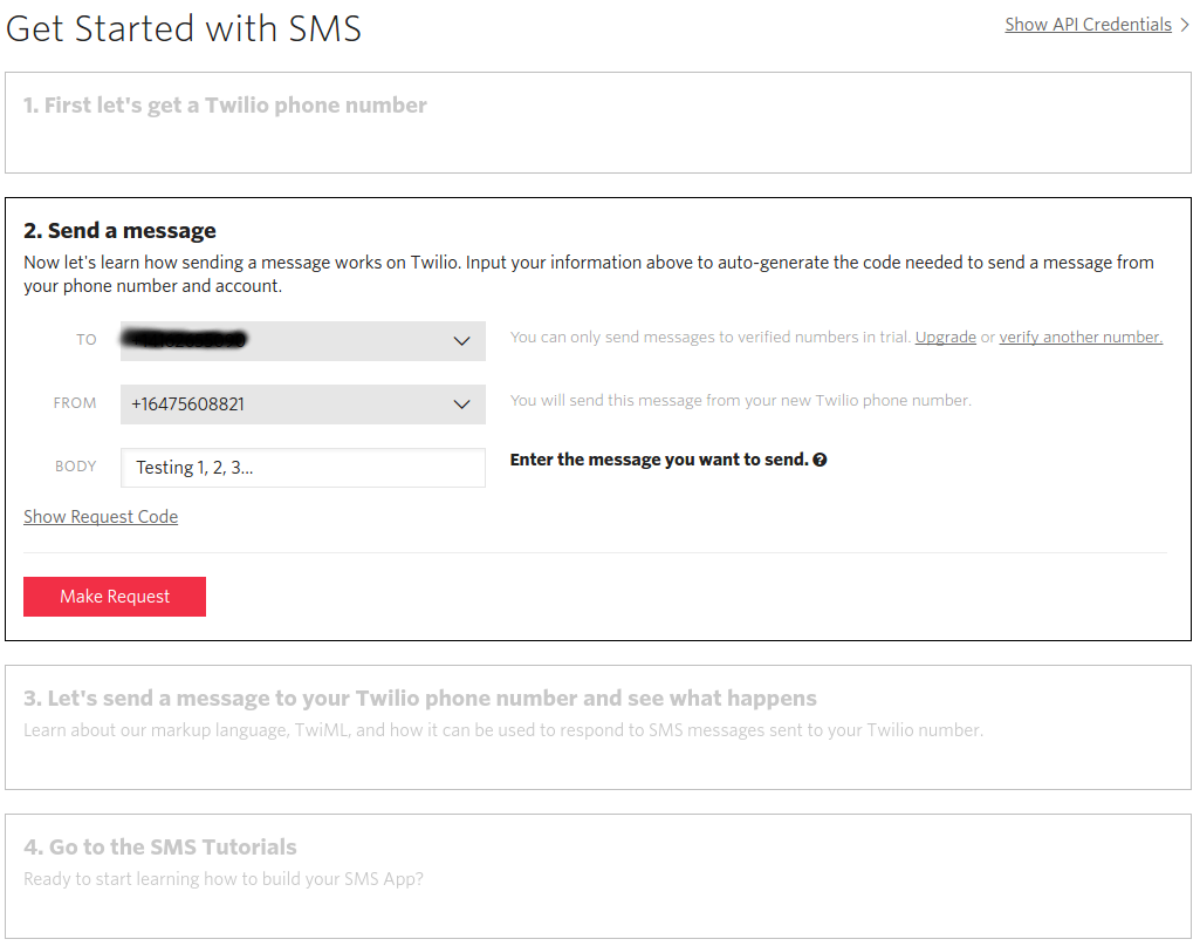
Click on "Get your first Twilio number" to have a phone number generated for you:

Ensure your number has SMS capability. If it does not, select another number from the link presented above. Once you are happy with your number click "Choose this Number". Your number will then be confirmed:

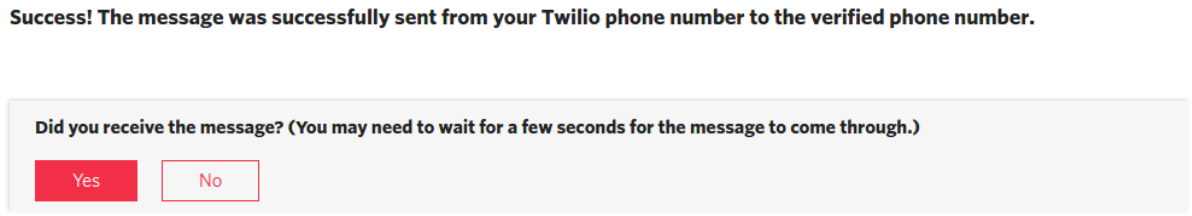


Write down your Twilio phone number for later entry into the Server Administration.

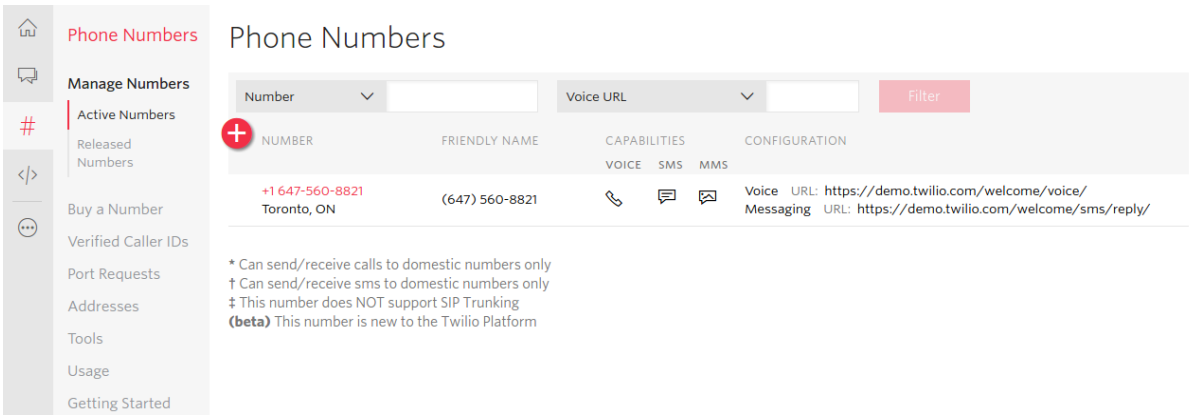
Click "Done" to continue the wizard where the delivery testing will begin:



Enter a message to deliver to your verified phone number as a test, followed by clicking "Make Request". You will then see a confirmation request:



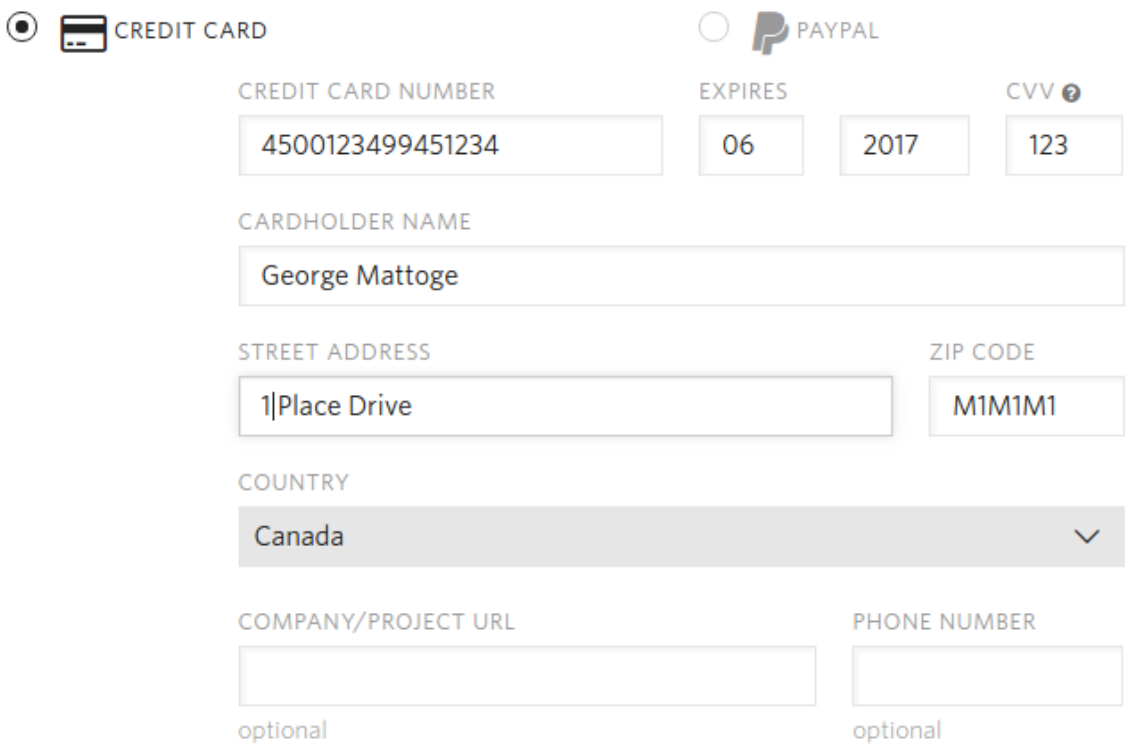
Assuming that you receive the message, click yes. The following steps of the wizard are not needed to continue (e.g. steps 3 and 4). Click on "Phone Numbers" from the left hand menu to ensure your number is configured. You should see something similar to the following:



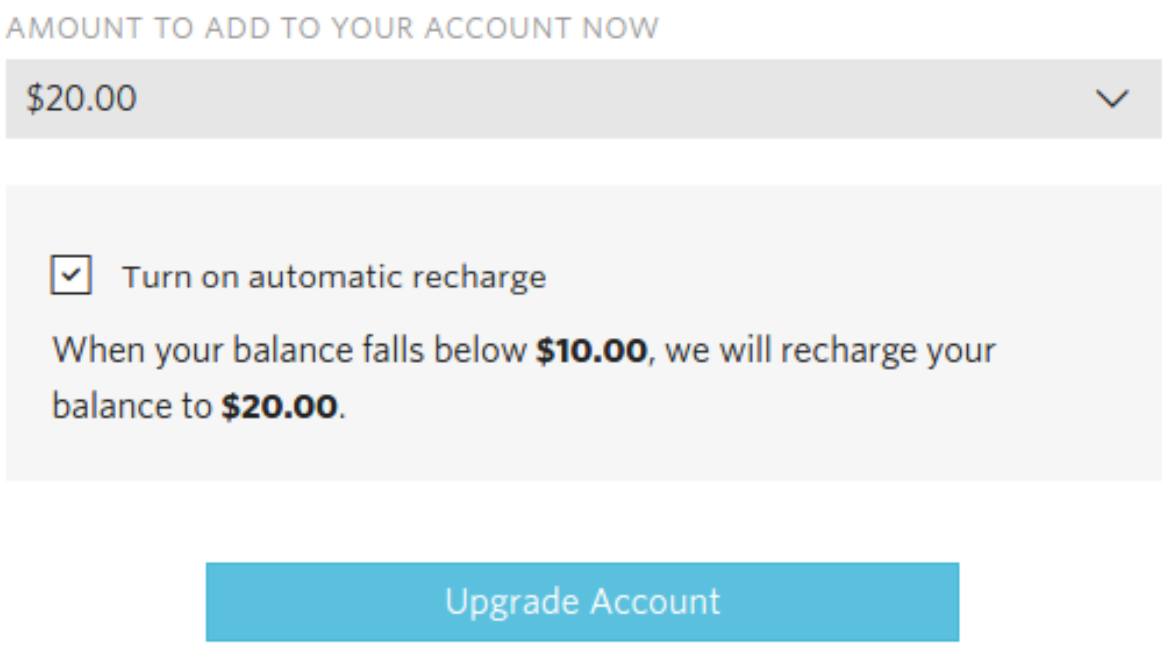
8.4.4.2. Configuring Twilio Payment Details

You will be able to enter the Twilio API credentials now, but you won't be able to deliver messages to outside numbers until you submit payment details. Click on the upgrade button at the top of the twilio screen:

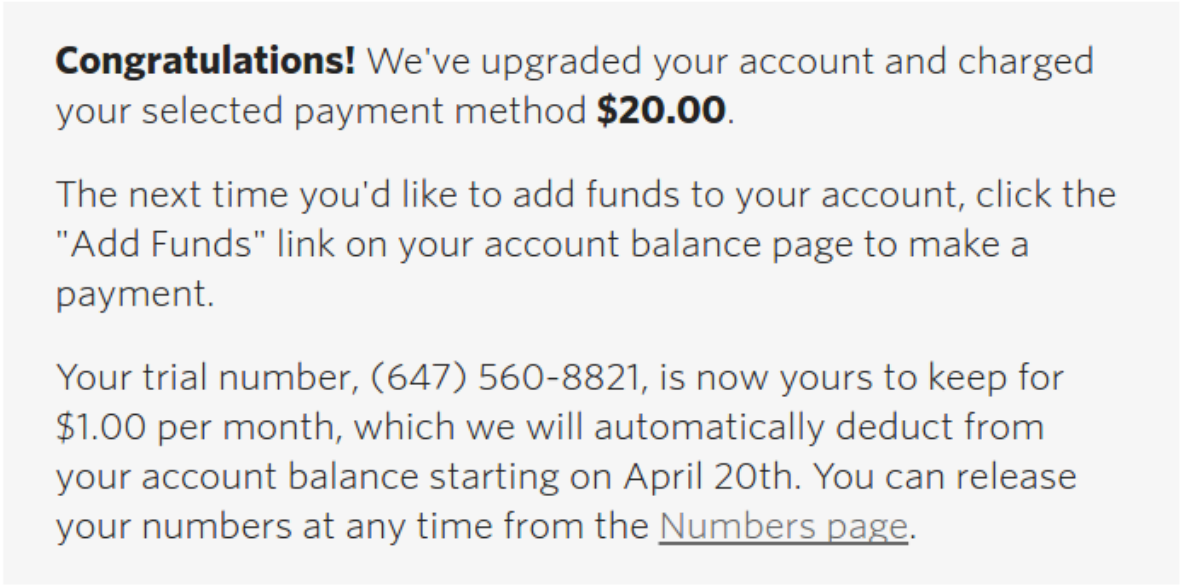
You will then be presented with a 3 step account upgrade process. Enter your credit card or paypal details in step 2 similar to the following:



Payment is made in monetary steps. For example, in steps of $20 as shown below. Depending on your expected volume you may want to enter something larger. Ensure automatic recharging is enabled:

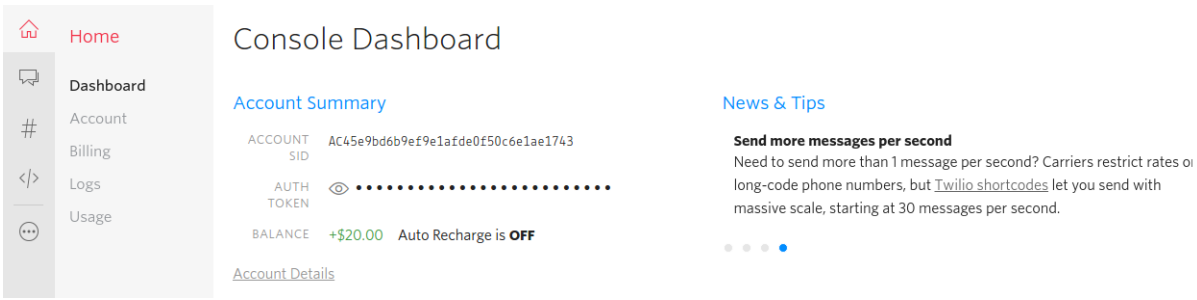


Click on "Upgrade Account" and after a few moments you should be presented with a confirmation screen:

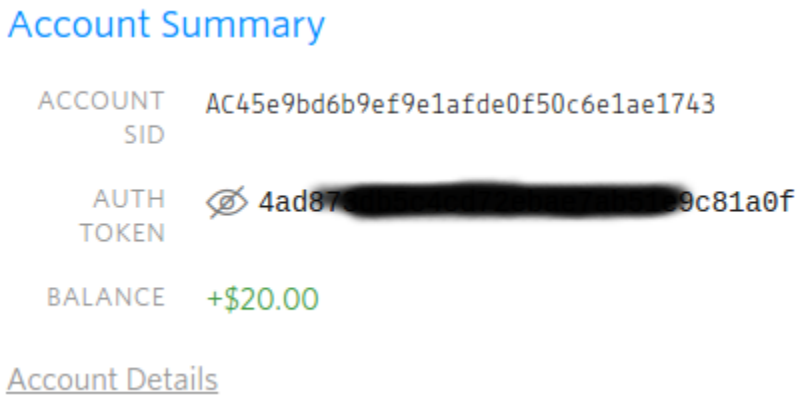


Now it's time to get your account SID and Auth Token for entry into the Server Administration panel.

Click on the "Dashboard" link under the home panel at the top left:



Click on the eye symbol to reveal your "Auth Token". You should then see a screen similar to the following:



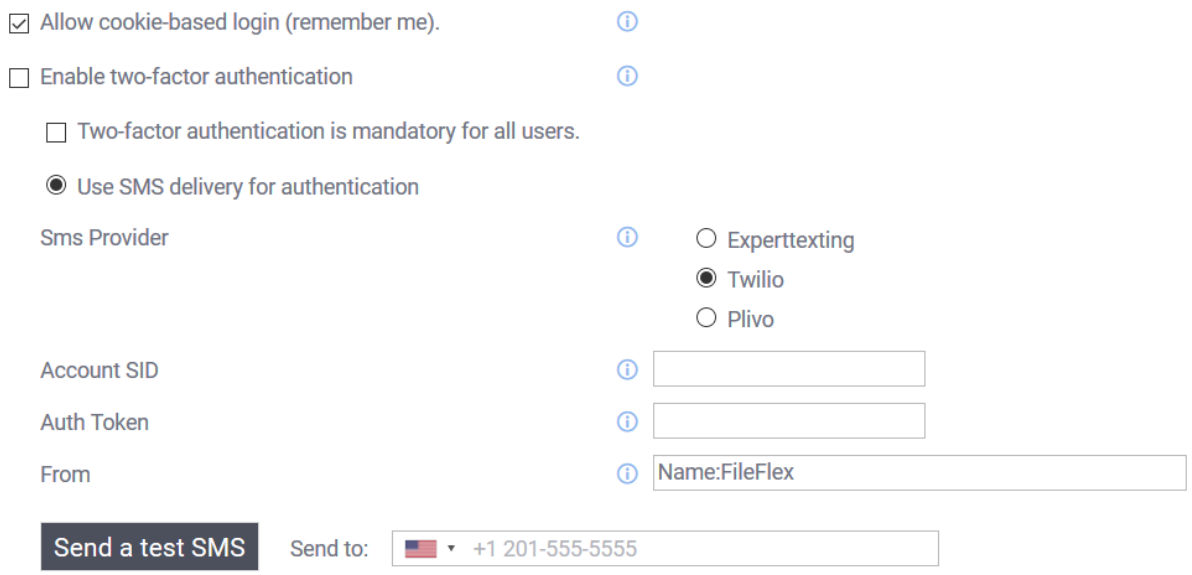
Take note of your Account SID and Auth Token.

8.4.4.3. Entering Your Twilio Credentials

Now it's time to enter your Twilio credentials into the FileFlex Server Administrator.

Navigate to your FileFlex Enterprirse Server Administration application (or switch to another tab). In this case, we navigate to https://www.fileflexdemo.com:9443.

Select "Control Panel" tab from the left, and then "Login Control" from the menu:



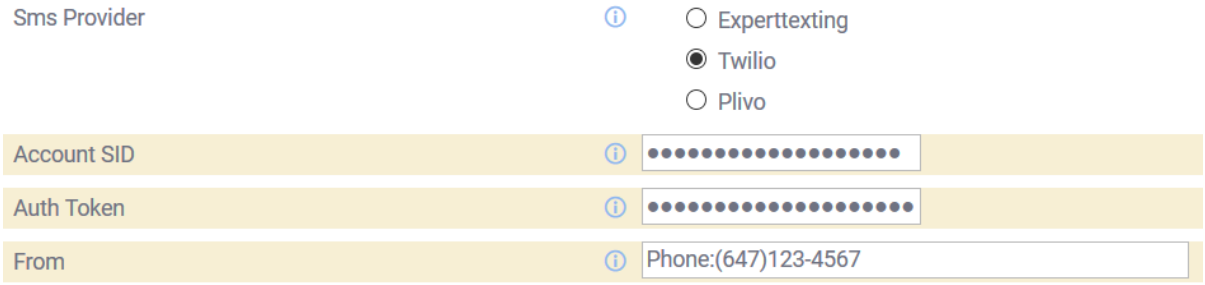
In this case, we will configure optional TFA using Twilio.

Select "Enable two-factor authentication".

Do not select "Two-factor authentication is mandatory for all users".

Select "Use SMS delivery for authentication".

It's now time to enter the Twilio credentials you saved earlier:



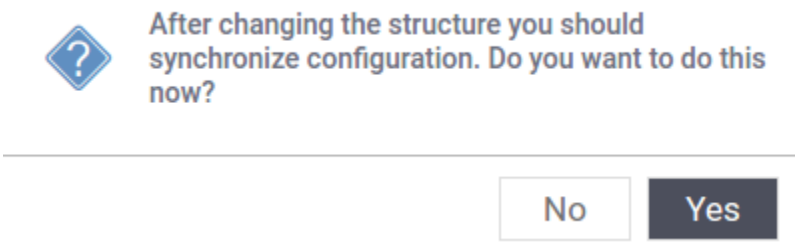
You will have to enter the Account SID and Auth Tokens which you recorded earlier. Also, enter the Twilio phone number in the "From" field as per the screenshot above substituting your own number in place of this sample.

> ⚠ You must enter the prefix "Phone:" in front of the phone number provided by Twilio.

Click the "Apply" button to save your changes.

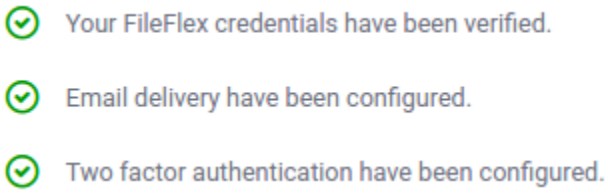
The final step is to test your SMS configuration. Enter a number attached to a device you have access to in the "Send to" field. You should see a confirmation flag indicating the appropriate country:

Click "Send a test SMS" to finalize the test. You will be asked to synchronize your configuration prior to the test:



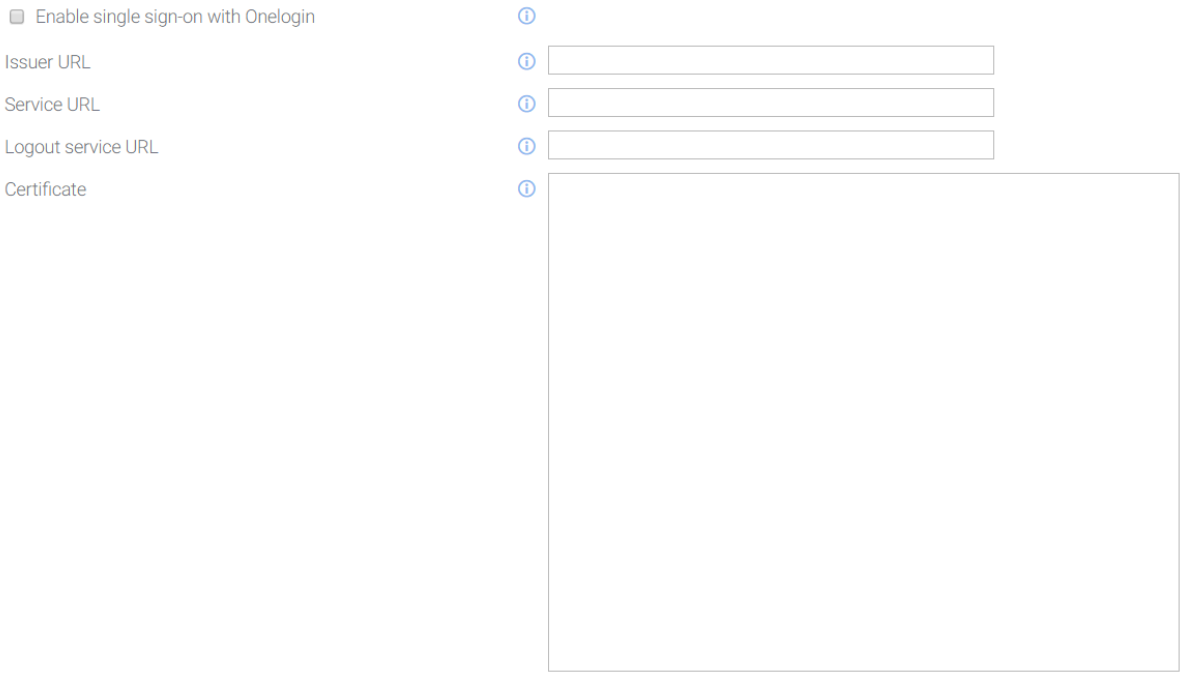
Click "Yes" to proceed and wait a few moments. You should then receive an SMS!

Congratulations, your SMS is now configured! When you visit the 'overview' panel of the control panel you should now see a green check mark next to the certificates listing:



8.5. Configuring Single Sign-On

Clicking on the "Single Sign-On" tab of the control panel will present you with a screen similar to the following:



8.5.1.

FileFlex supports multiple Identity providers for single-sign on. Please refer below for configuration details of each of the providers.

8.5.2. Single Sign-On with OneLogin

This documentation provides a tutorial on how to configure a OneLogin "app" such that users can be directed to your particular FileFlex deployment.

> When connected to OneLogin, user accounts which exist both in FileFlex, and in the OneLogin directory will be able to login using their OneLogin credentials only.

> Each FileFlex deployment having it's own URL will require a separately created OneLogin application in order to support single sign-on!

8.5.2.1. Creating a OneLogin Application

The first step is to create a developer account. Such accounts are restricted to 3 applications and 25 users.

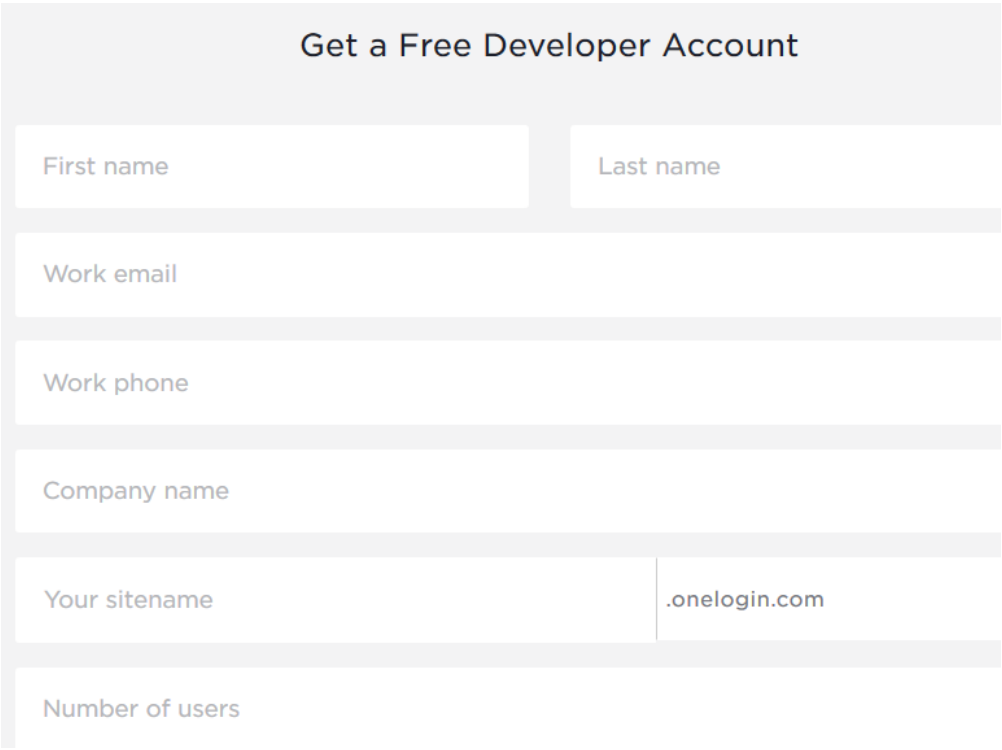
> If you have a paid account with OneLogin, there will be no restrictions on the quantity of apps that you can define, and a 'developer' account will not be needed. Use that instead and skip ahead to the next section.

8.5.2.1.1. Creating a OneLogin Account

We will create a free "developer account" at OneLogin. As of the time of writing, that allows 3 applications with 25 users. Proceed by navigating to onelogin.com and select the developers tab:

From there, select the "get a developer account" button:

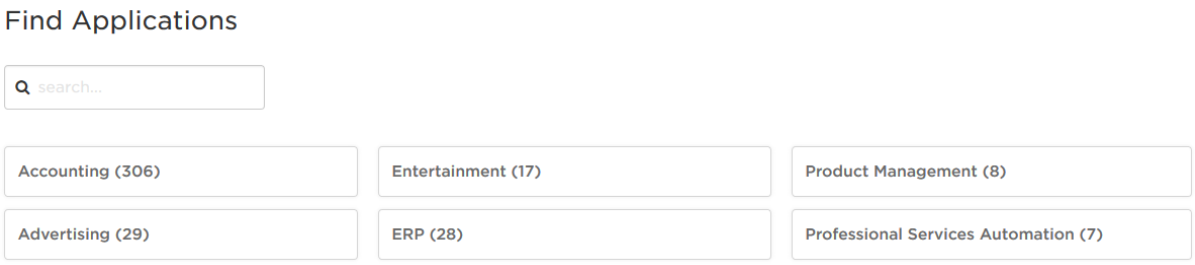
You will be presented with a form in which you must provide your contact details:



Fill out out the details, clicking the "get started" button at the bottom to proceed to the next step. You will need to complete any email-based account validation steps that are presented to you. This guide assumes that you have successfully logged in to your newly created account.

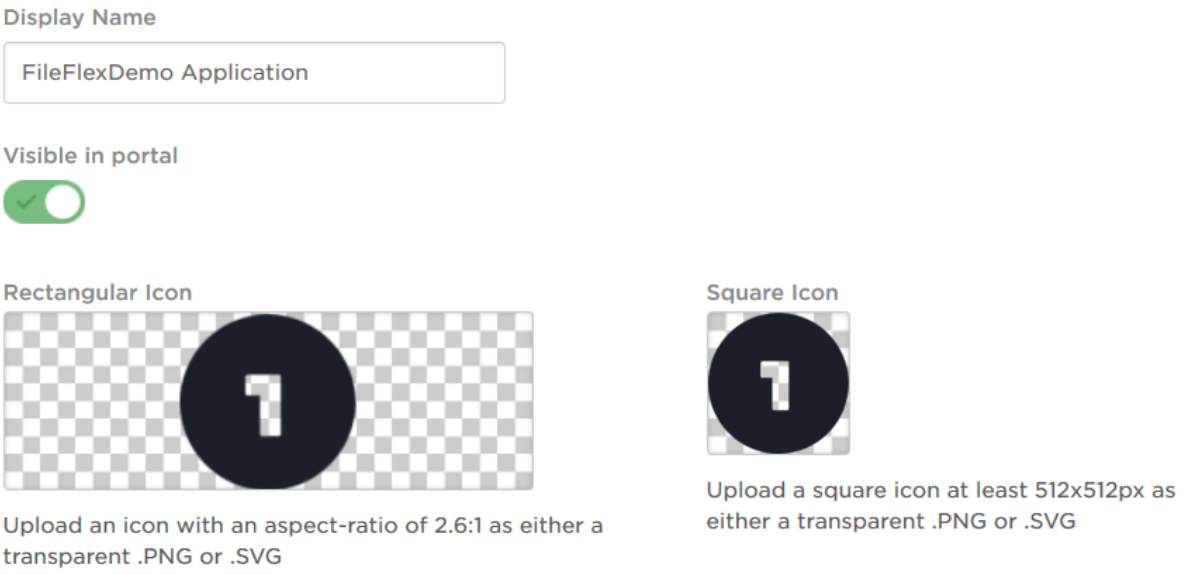
8.5.2.1.2. Adding a SAML Application

The next step is to define a SAML-based OneLogin application that will map to your server deployment. Navigate to the app browser located at https://qnext-dev.onelogin.com/apps/find and you should see a list of categories similar to:

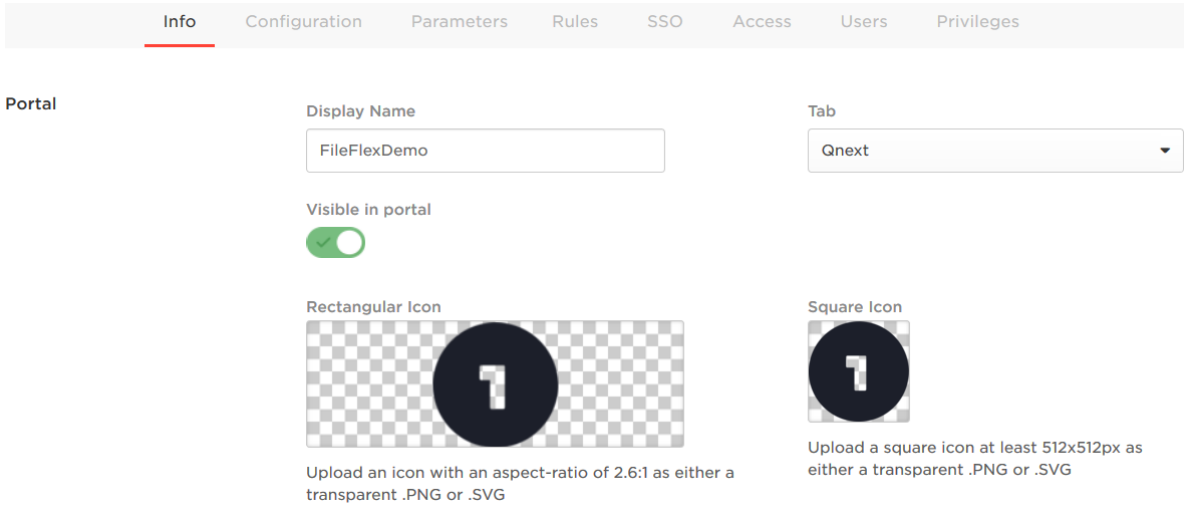


Enter "SAML" in the search filter, and you will be presented with a matching set of "applications". Since we are defining an application location, select the "SAML Test Connector (IdP w/attr)" option:

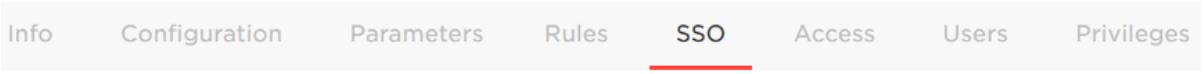
You will then be presented with a screen in which you can define your application's name and icons:



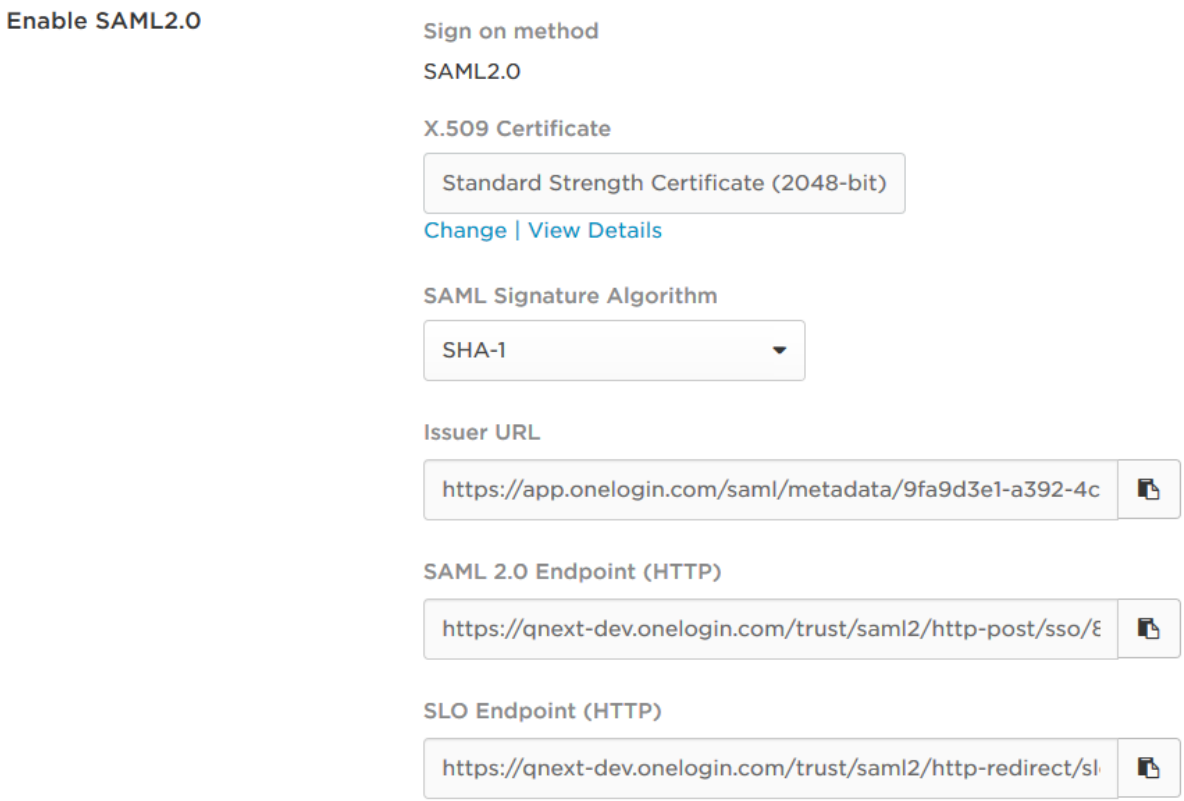
Rename the application's display name to something more appropriate (FileFlexDemo in this example). You may also supply icons if desired. Click save to proceed, and new tabs will be presented to you:



Select the SSO tab to extract values required by FileFlex:



There you'll find the values we need to transcribe for later entry into FileFlex:

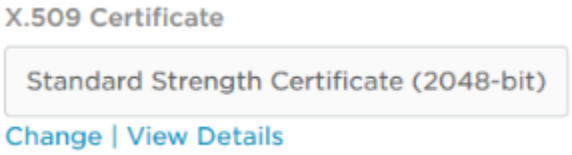


It's recommended that you copy these values into an empty text document for safe-keeping and easier entry into FileFlex at a later time. For example, open Notepad, and paste the values there, because later you will be asked to enter them into FileFlex.

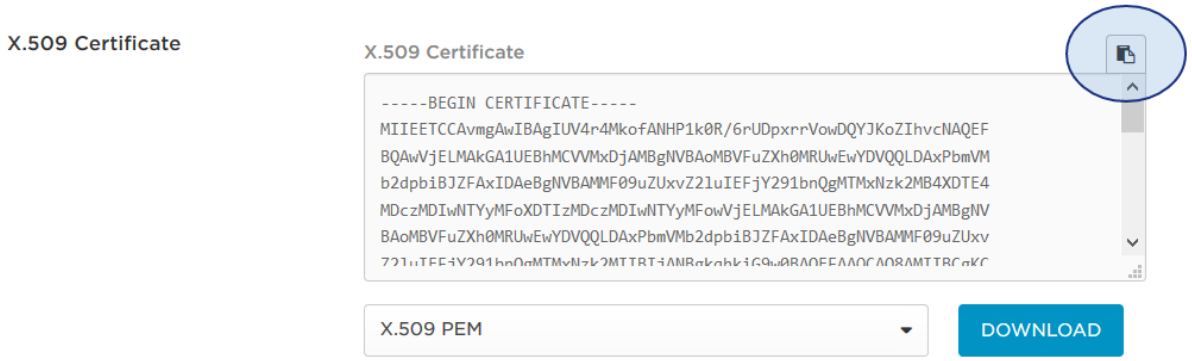
Capture the following values:

- Issuer URL
- SAML 2.0 Endpoint (HTTP)
- SLO Endpoint (HTTP)

Click "View Details" on the X.509 certificate field:

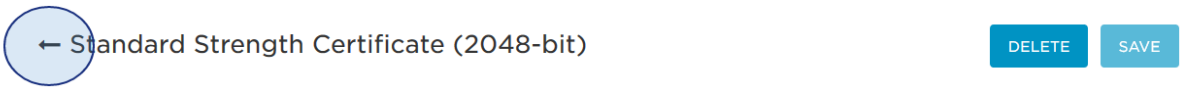


Doing so will reveal additional fields. Click on the "copy" icon to copy the X.509 certificate to your clipboard:

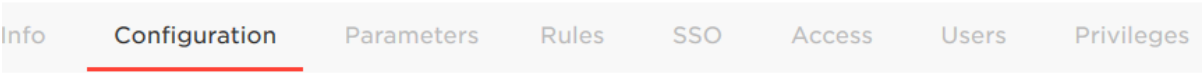


- Paste the X.509 Certificate into your document along with the other values

Go back to the prior screen by clicking on the back arrow:



Now, we must tell OneLogin where to find our deployment. Select the "Configuration" tab:



The next several steps require you to know your public hostname. For example, given the following URL:

```
https://test.fileflexdemo.com/fbweb/something/or/other
```

... the "public hostname" would be "test.fileflexdemo.com". The next steps will specify URLs with {{PUBLIC_HOST}} - replace that value with your public hostname. If we assume in this example that our public hostname is defined as above, then the following:

```
https://{{PUBLIC_HOST}}/fbweb/app/public/view/metadata_partner_saml
```

would be entered by you as the following:

```
https://test.fileflexdemo.com/fbweb/app/public/view/metadata_partner_saml
```

Locate the "Audience" field and enter the following URL (substituting your public host name as mentioned above):

Audience
`https://{{PUBLIC_HOST}}/fbweb/app/public/view/metadata_partner_saml`

Locate the "Recipient" field and enter the following:

Recipient
`https://{{PUBLIC_HOST}}/fbweb/app/public/view/login_partner_saml`

Locate the "ACS (Consumer) URL" field and enter the following (it's the same as for the Recipient field):

ACS (Consumer) URL
`https://{{PUBLIC_HOST}}/fbweb/app/public/view/login_partner_saml`

Locate the "Single Logout URL" field and enter the following:

Single Logout URL
`https://{{PUBLIC_HOST}}/fbweb/app/protected/view/logout_partner_saml`

Locate the "ACS (Consumer) URL Validator" and enter the following:

ACS (Consumer) URL Validator
`^https:\/\/{{PUBLIC_HOST}}\/fbweb\/app\/public\/view\/login_partner_saml$`

However, you must then go and add a backslash in front of any "dots" in your public host name. For example, using the sample public host name provided above, we would have had:

```
^https:\/\/test.fileflexdemo.com\/fbweb\/app\/public\/view\/login_partner_saml$
```

... however as you can see every slash "/" has a proceeding back-slash "\". We must do the same for the dots that we injected into it. It will become:

```
^https:\/\/test\.fileflexdemo\.com\/fbweb\/app\/public\/view\/login_partner_saml$
```

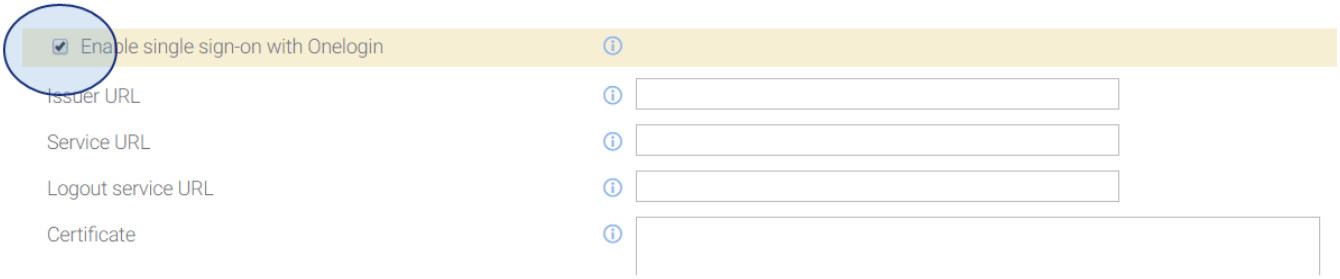
Regular Expressions

The validator URL uses regular expressions to ensure that calling websites (e.g. in this case FileFlex) don't request redirection to rogue locations. We must "escape" the dots that we inject into the regular expression. This is a very important step from a security perspective, so please ensure the back slashes are added as instructed!

For more information on regular expressions, see https://en.wikipedia.org/wiki/Regular_expression

You can now click save since the application has been configured from OneLogin's perspective.

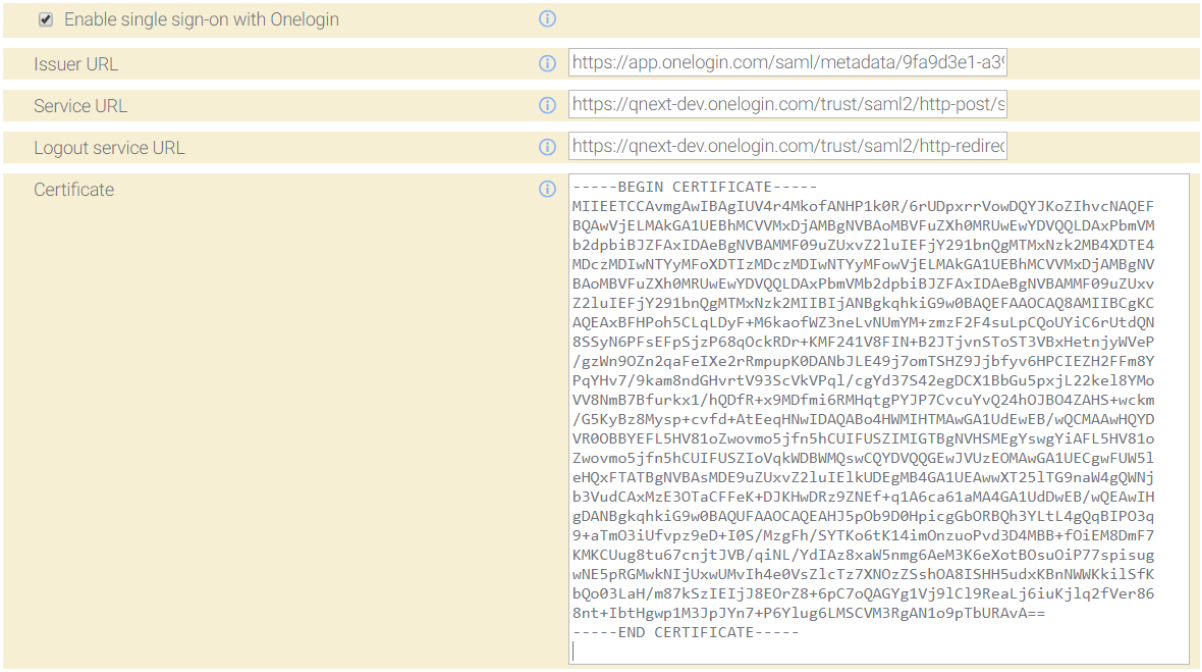
Now you must enter the data you captured earlier into the FileFlex Server Administration application. Navigate to the "Single Sign-On" panel of the control panel tab in server administration, and enable the single-sign on checkbox:



Refer back to your notes where you captured values from OneLogin, and prepare to enter them as follows:

- Copy the "Issuer URL" into the Server Administration field bearing the same name.
- Copy the "SAML 2.0 Endpoint (HTTP)" field into the Server Administration "Service URL" field.
- Copy the "SLO Endpoint (HTTP)" field into the Server Administration "Logout service URL" field.
- Copy the "X.509 Certificate" field into the Server Administration "Certificate" field.

When you're done, it should look something like the following:

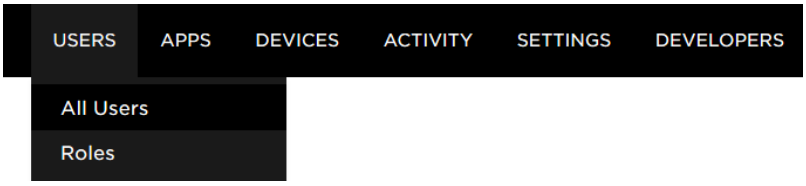


Click "Apply" to save your changes. Restart the server when prompted.

8.5.2.2. Testing Single Sign-On

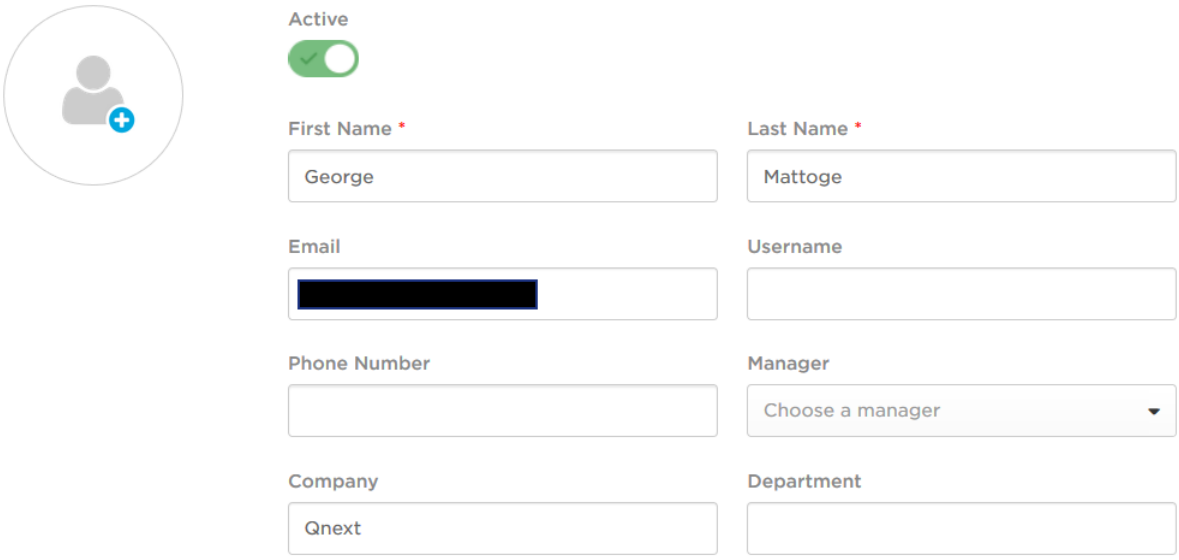
In a typical deployment users will already exist within the "OneLogin" ecosystem such as those brought in by LDAP or ActiveDirectory directories. In this example however, we don't have any users, so we need to add one prior to being able to test the integration.

Start by going to users/all users in the menu:

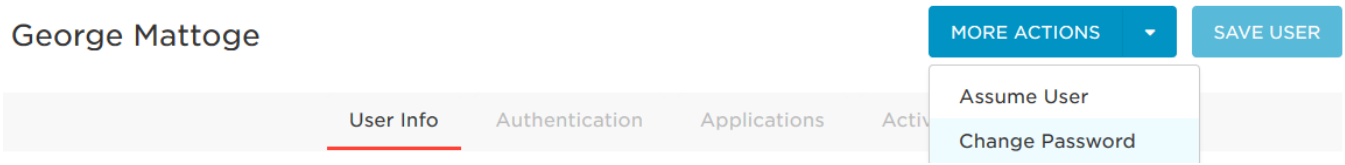


From there, actuate the "new user" button:

You should see a screen allowing you to enter user details. Do so now, ensuring that the email is a known valid email address. Only the first name, last name, and email are necessary.

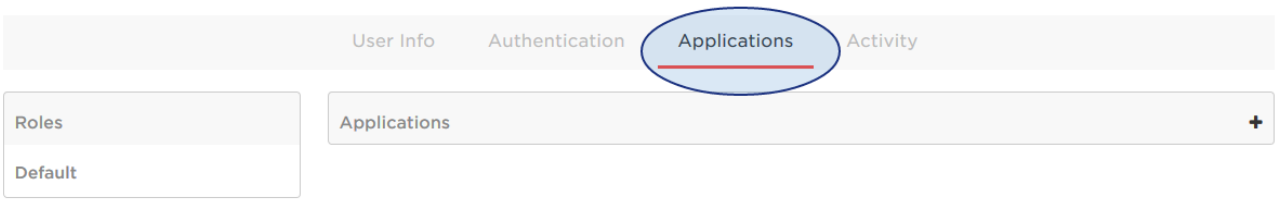


Click the "save user" button when completed. Click on "more actions" then "change password" to set a password for this user:

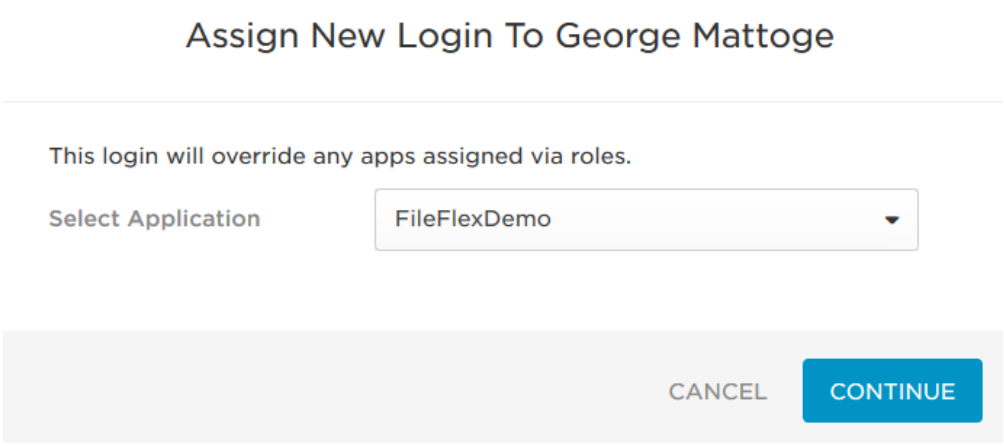


Set the password, then click "update". There is no need to force the user to update his password in this example.

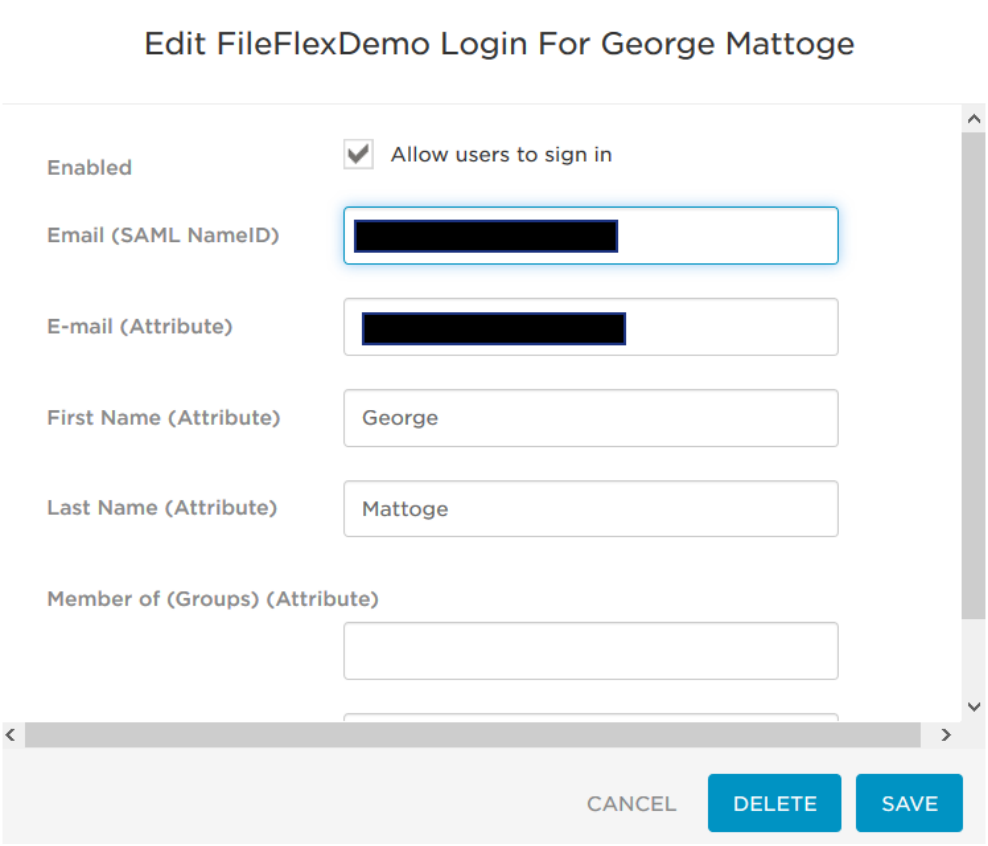
Select the applications tab for the user:



Click the "+" symbol add assign the user to our newly created "app". A dialog will be shown:



Select the app from the dropdown, then click continue. A new dialog will be shown:

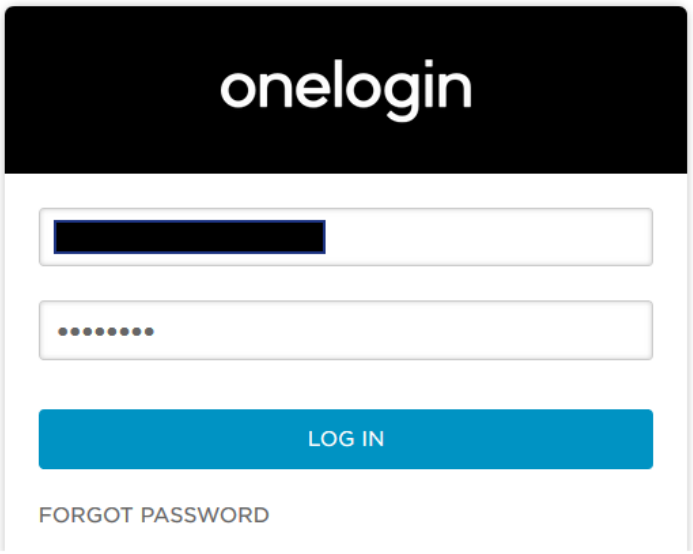


The email you entered should be shown twice in the dialog. Click the "save" button to finish this process.

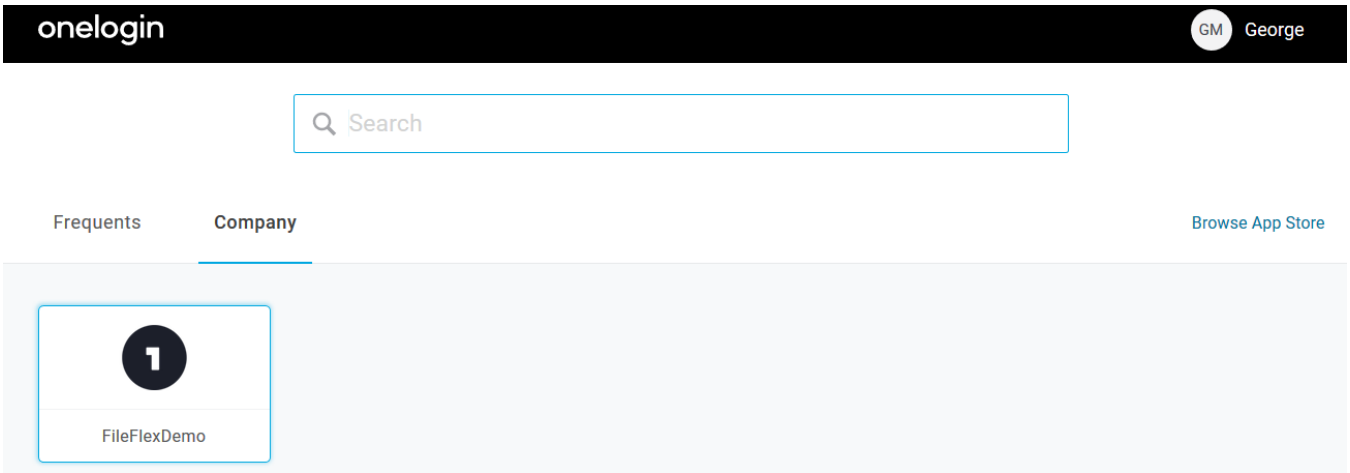
We must now ensure that the app appears to the user when logging in to the OneLogin portal. Navigate to the OneLogin portal. In this example case, it is at:

```
https://qnext-dev.onelogin.com
```

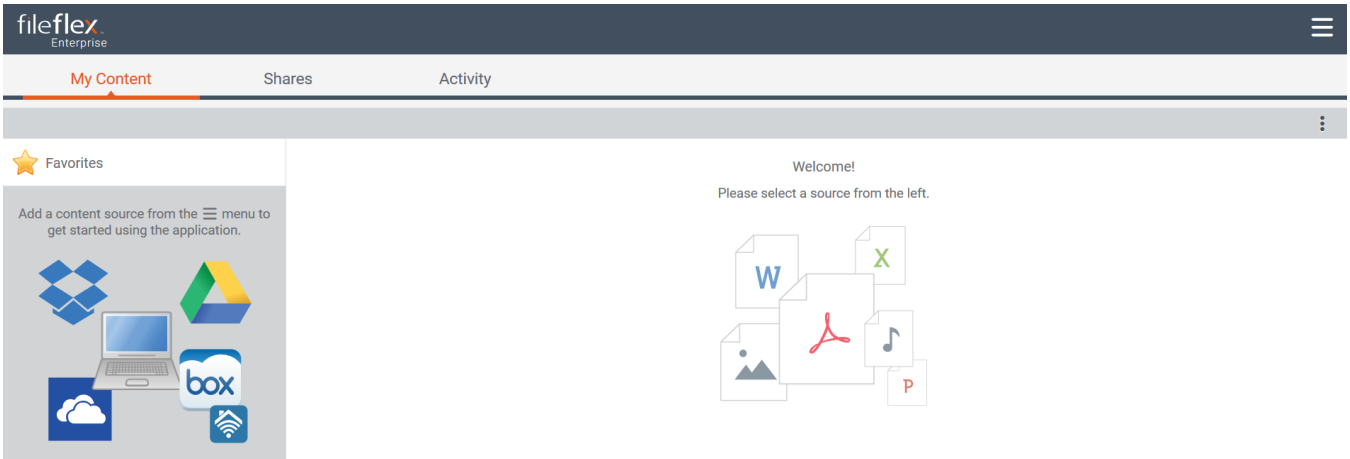
Enter the email and password for the user we just created:



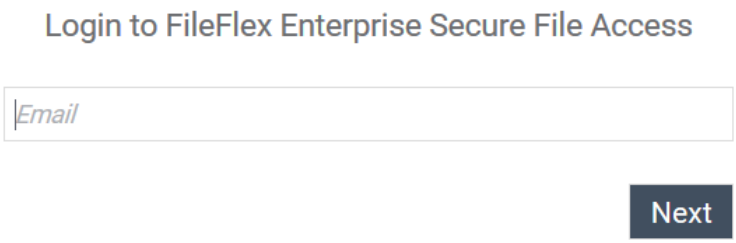
Click login, and you should be presented with the app within OneLogin:



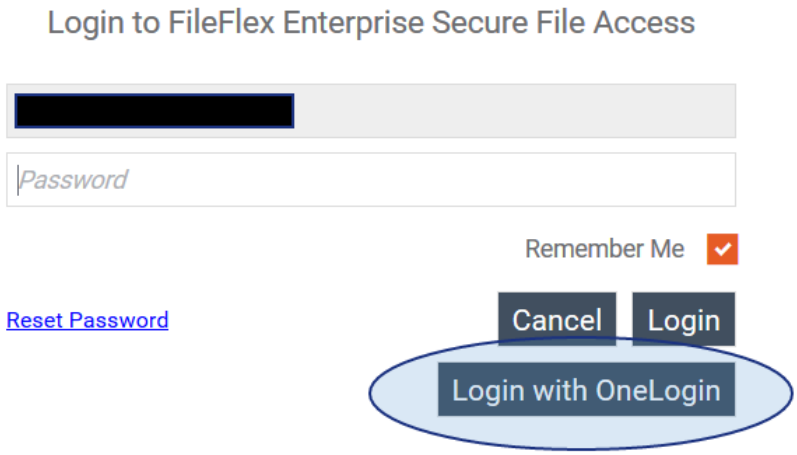
Clicking the FileFlexDemo app will bring up the FileFlex login screen, and the user should be logged in automatically:



Alternately, you can log in by starting from the FileFlex page. Log the user out, resulting in the following login screen:



Enter the user's email address, then click next:



Instead of entering the password, select Login with OneLogin" and the user will be logged in automatically without entering a password.

8.5.3. Single Sign-On with HelloID

This documentation provides a tutorial on how to create a Hello ID "app" and configure FileFlex Server such that users can be directed to your particular FileFlex deployment.

> Once HelloID is integrated with FileFlex Server deployment, users can use their HelloID credentials to log in to the FileFlex. FileFlex admin while adding users needs to ensure the user email-id matches with email id registered in the Identity Provider.

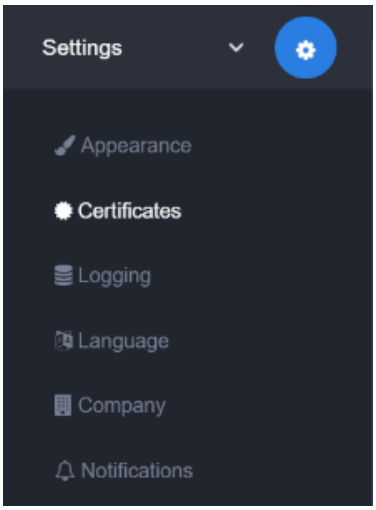
8.5.3.1. Creating a self-signed Certificate

Log in to the Admin Dashboard of HelloID.

> This documentation assumes that you already have the admin credentials for your HelloID account. If you are doing a test setup, please contact HelloID to get a Test account for your setup.

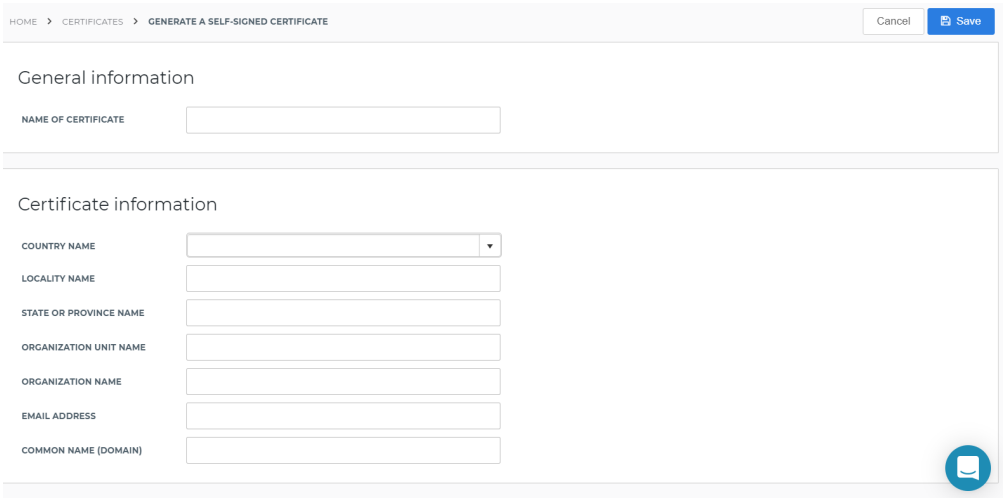
You first need to create a self-signed certificate which will be later used to sign the application in the next step. If you already have a certificate skip this section and move to the next section "Create a SAML based Application"

Expand the Settings drop-down and then click on Certificates.



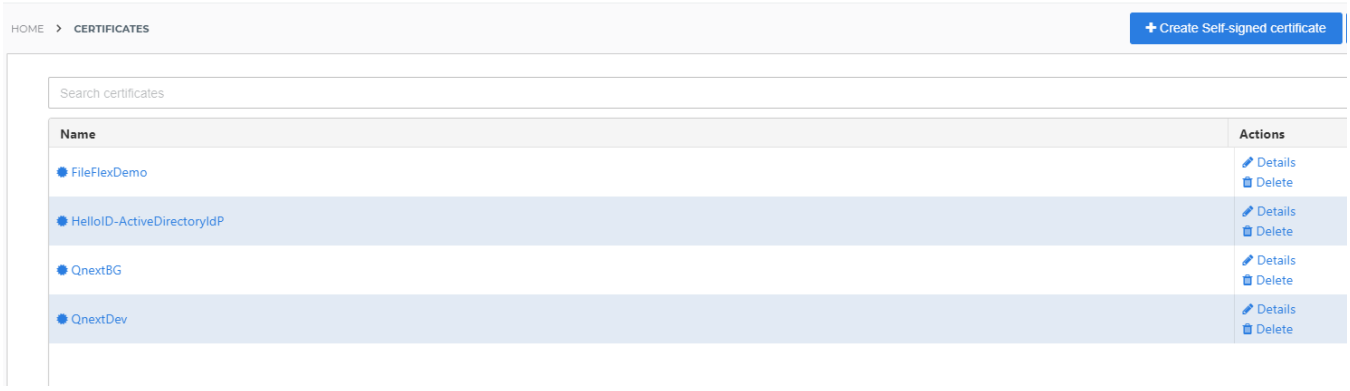
Click on "Create Self Signed Certificate" button and you are shown a form to provide your details.

Complete the form with the required information and click on Save to generate your self-signed certificate.

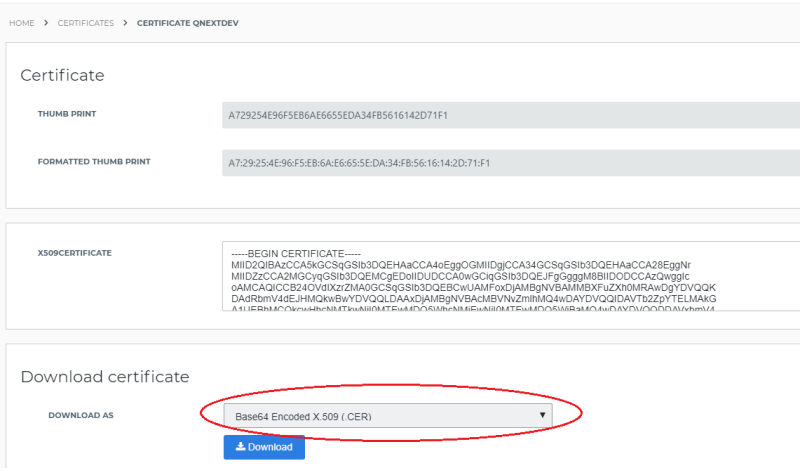


You will need the certificate later when you need to provide application details to FileFlex. It should be saved to local storage for future use.

Click on the Settings→ Certificate again and it would list all the certificates.



Click on the certificate created in the previous step and it will be displayed like as below.



Ensure to change the download type to "Base64 encoded format" as shown above.

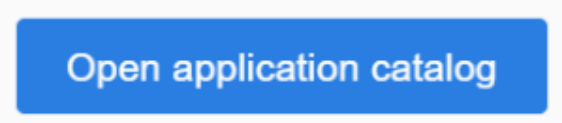
Click download and save this on local storge.

8.5.3.2. Creating a SAML based Application

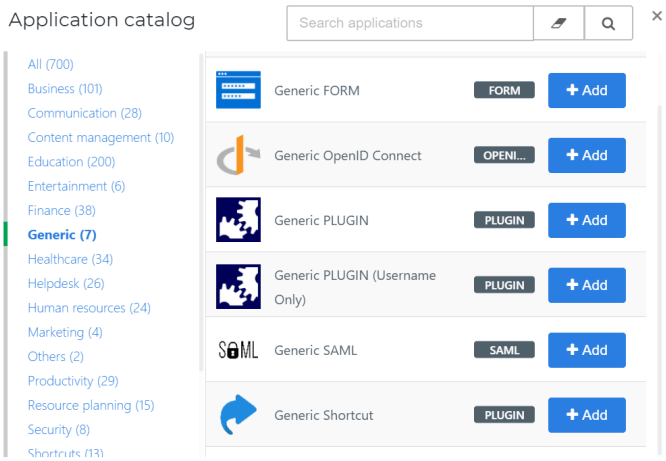
The next step is to create a SAML based application in HelloID that will map to your server deployment.

Navigate to your Admin Dashboard and click on the Applications tab. This provides a list of exiting applications created by your account.

Click on "Open Application catalog" at the top right.



This opens up the complete application catalog. Click on the "Generic" tab and look for "Generic SAML".



Click the "Add" button next to "Generic SAML".

The next step requires you to know your public hostname. For example, given the following URL:

```
https://test.fileflexdemo.com/fbweb/something/or/other
```

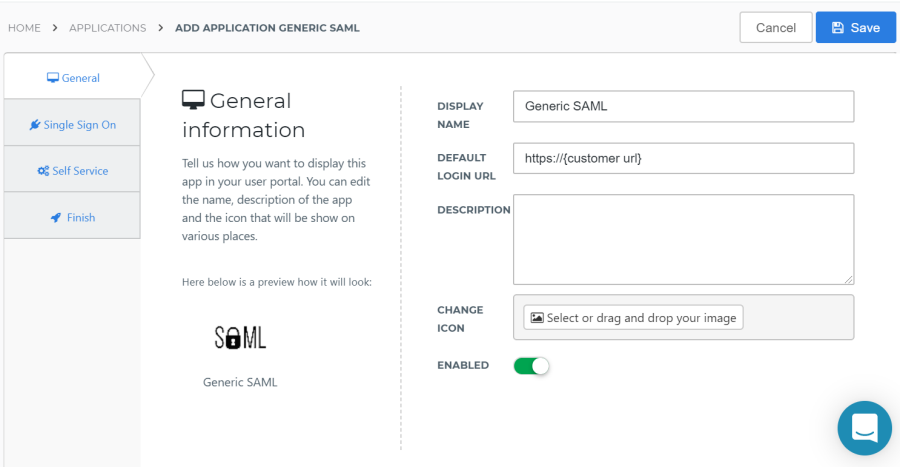
... the "public hostname" would be "test.fileflexdemo.com". The next steps will specify URLs with {{PUBLIC_HOST}} - replace that value with your public hostname. If we assume in this example that our public hostname is defined as above, then the following:

```
https://{{PUBLIC_HOST}}/fbweb/app/public/view/login_partner_saml
```

would be entered by you as the following:

```
https://test.fileflexdemo.com/fbweb/app/public/view/login_partner_saml
```

You will now be asked to provide the details to the newly added application. Below is how by default it will look like.



Locate Display name and provide the name you want for the application

Display Name

```
e.g.  FileFlex
```

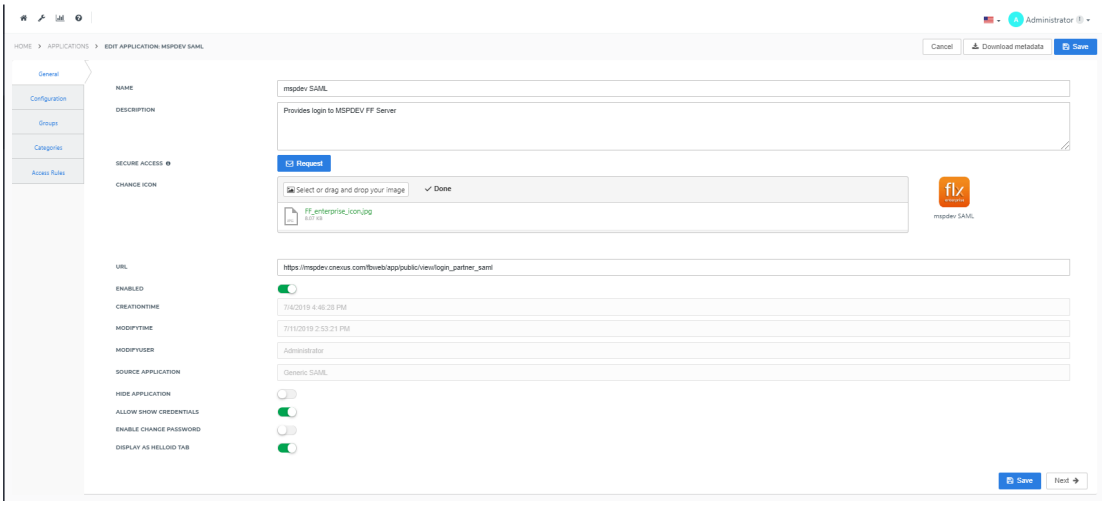
Locate the Default Login URL and enter your domain URL in below format.

Default Login URL

```
https://{{PUBLIC_HOST}}/fbweb/app/public/view/login_partner_saml
```

Keep other parameters as default or change as per your requirement.

An example of a sample application is shown below for reference.



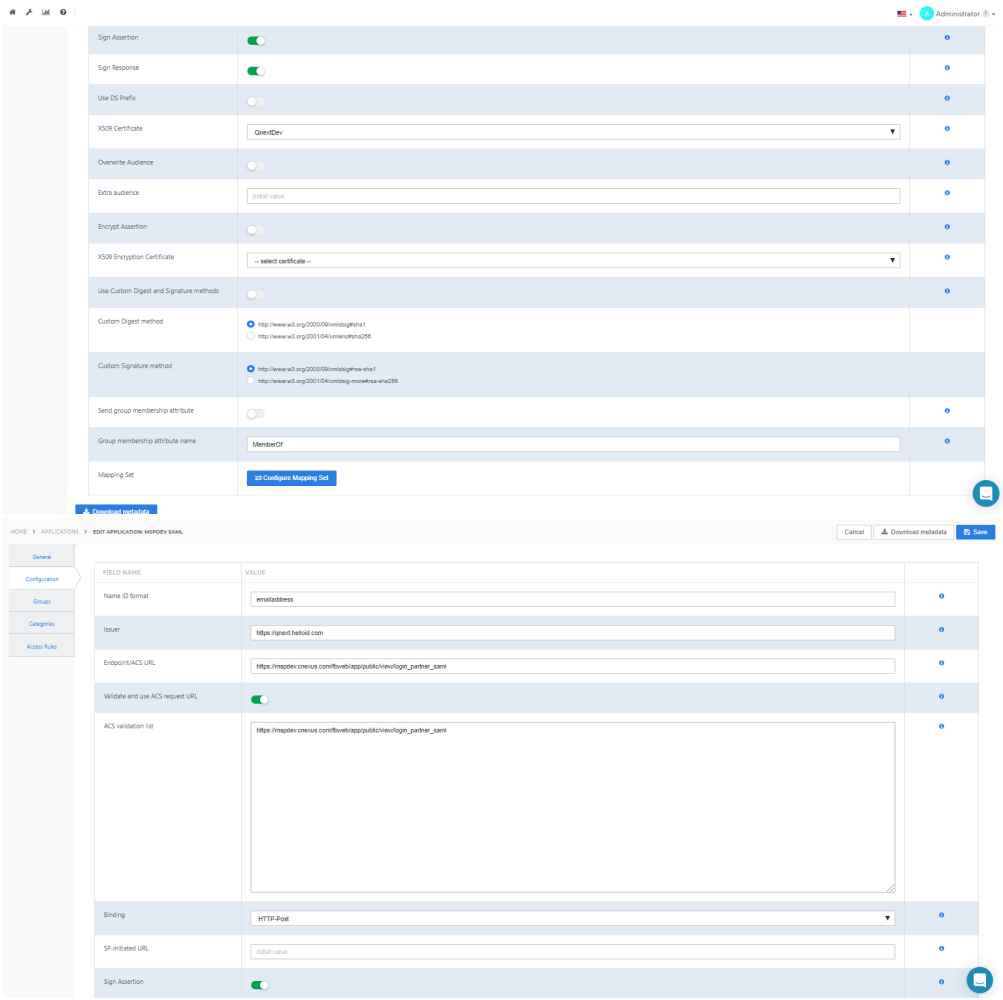
Once the above form is completed with all the required information, click Next. This takes you to the Single Sign-on section of the application.

This section has several fields and not all require changes. Unless mentioned in below table or required for other reasons, please keep the default values unchanged.

Fields requiring a change	Description
Issuer	Provide the path of your HelloId domain. For e.g. https://qnext.helloid.com
End Point/ACS URL	This should be same as Default LoginURL specified in the previous Step.
ACS/Validation List	This should be same as Default LoginURL specified in the previous Step.
x509 Certificate	Select the self-signed certificate created earlier in the setup process from the drop-down.
Sign Assertion	Enabled
Sign Response	Enabled

All other fields are optional and can be configured as per requirements.

An example of a sample application is shown below for reference.



The next tabs "Group", "Categories" and "Access Rules" are optional and can be configured as per requirement or kept as default.

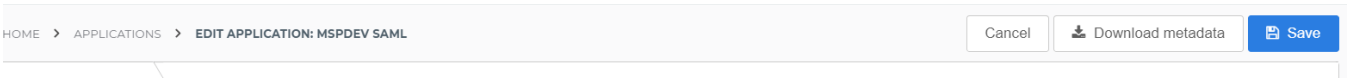
Complete the above-mentioned fields and click on SAVE. Your application is now created.

8.5.3.3. Downloading Application Metadata

We need to download the details from HelloID application and provide to FileFlex server to enable the linking. HelloID provides all the details in one file which can be downloaded as per below steps.

Click on Dashboard and then click Applications.

You should see the newly created application in the table. Click the application name and open it.



You should see the option "Download Metadata" on the top right corner of the screen.

Click it and save the XML file to your system.

This will be used in the next section where you need to provide values from it to link to your FileFlex deployment.

8.5.3.4. Linking FileFlex Server and HelloID Application

We will use a sample metadata XML file and explain what values need to be copied from it. Open the XML file in any XML editor. In case you don't have an editor you can even use browser to view and copy attribute values.

```
<?xml version="1.0" encoding="utf-8"?>
<md:EntityDescriptor entityID="https://qnext.helloid.com/" ID="_8F1C6575SDFG4563F23041EF3D485B
382"
                     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
    <md:IDPSSODescriptor ID="_D0B89DDFBED1AF7C7723F0B487E2D18D"
                         protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
                         WantAuthnRequestsSigned="false">
        <md:KeyDescriptor use="signing">
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>
                    <X509Certificate>
                        MIIDNDCCAhygAwIBAgIIHbg5V0hfOtkwDQYJxxxxxxxx=
                    </X509Certificate>
                </X509Data>
            </KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:
NameIDFormat>
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                                Location="https://qnext.helloid.com/relayservice/redirect
/f382bd6g-xxxxx"/>
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
                                Location="https://qnext.helloid.com/relayservice/redirect
/f382bd6g-xxxxx"/>
    </md:IDPSSODescriptor>
    <md:ContactPerson contactType="technical">
        <md:SurName>Support</md:SurName>
        <md:EmailAddress>isupport@tools4ever.com</md:EmailAddress>
    </md:ContactPerson>
</md:EntityDescriptor>
```

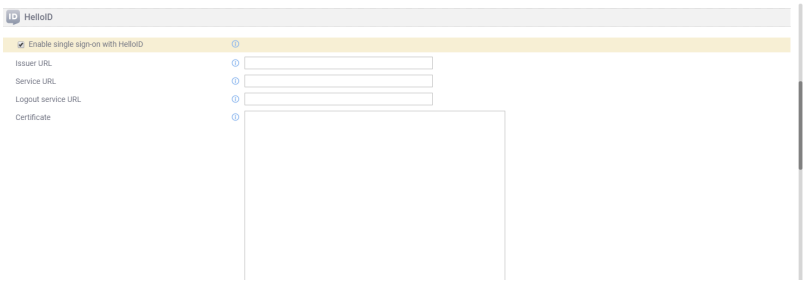
You need to search for two values from this metadata.

1. entityID : This is usually present right at the start of file, and in the above example is "https://qnext.helloid.com"
2. SingleSignOnService URL for HTTP-POST: In this above example is the URL "https://qnext.helloid.com/relayservice/redirect/f382bd6g-xxxx"

Save all the values in a text file and launch FileFlex Server Admin Page.

Click Control Panel from the Admin Panel and search for Single Sign-on.

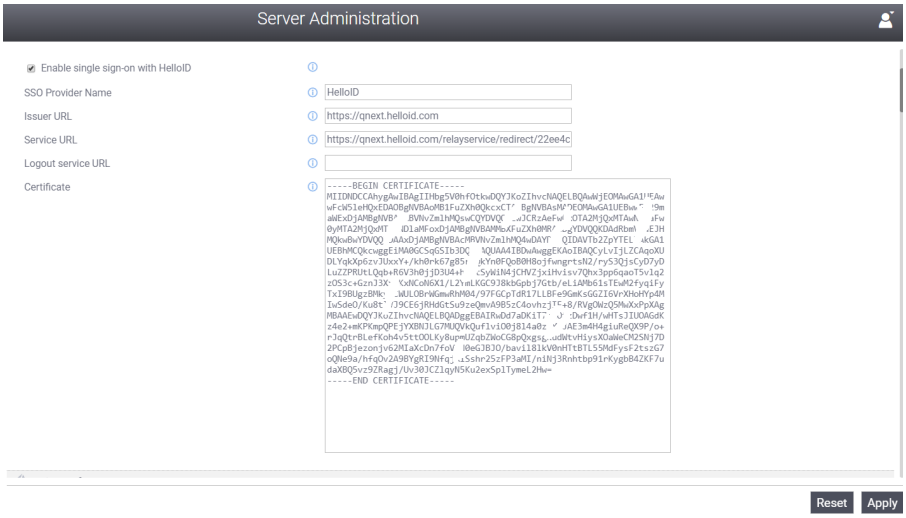
Scroll the page and go to the section for HelloID configuration as shown below.



Use the values stored from metadata download (in the previous step) to complete HelloID configuration.

1. Issuer URL: Use entity ID
2. Service URL: Use SingleSignOnService URL for HTTP-POST
3. Logout service URL: Keep it blank and don't enter anything in it.
4. Certificate: Open the self-signed Base 64 encoded certificate which was saved in the first step of the instructions. Open the certificate in any editor (e.g. Notepad) and copy-paste the entire content in this field.

An example of a completed sample application is shown below for reference.



Click Apply and you have now completed the HelloID configuration !!

8.5.3.5. Testing Single Sign-On

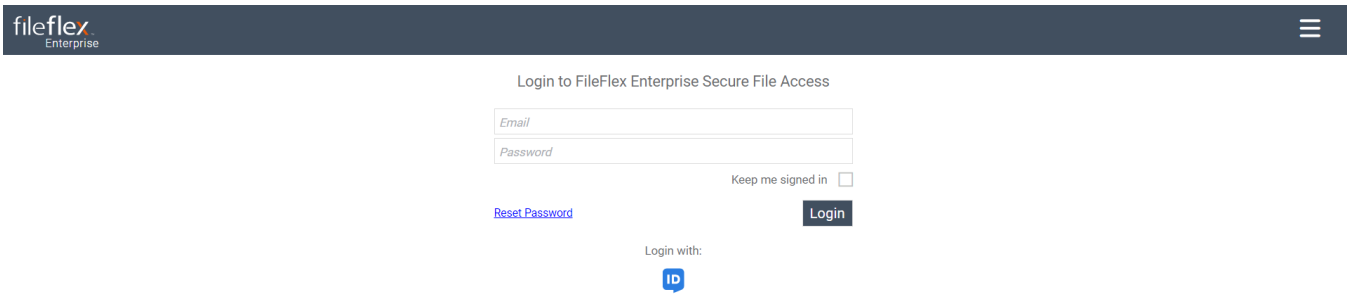
By default, all users created in HelloID have access to all applications, so there is no assignment of users to the application required within HelloID.

You can use Admin Dashboard (Directory - > Users) to view and add more users in the system.

For Testing the integration, please create a user in Fileflex instance using the standard admin console to create new users. (You can also refer to Add user section in the help guide to see more details on this topic).

Ensure that same user has also been created on HelloID Directory as well.

Launch the FileFlex app (or webapp) and connect to your FileFlex server instance.



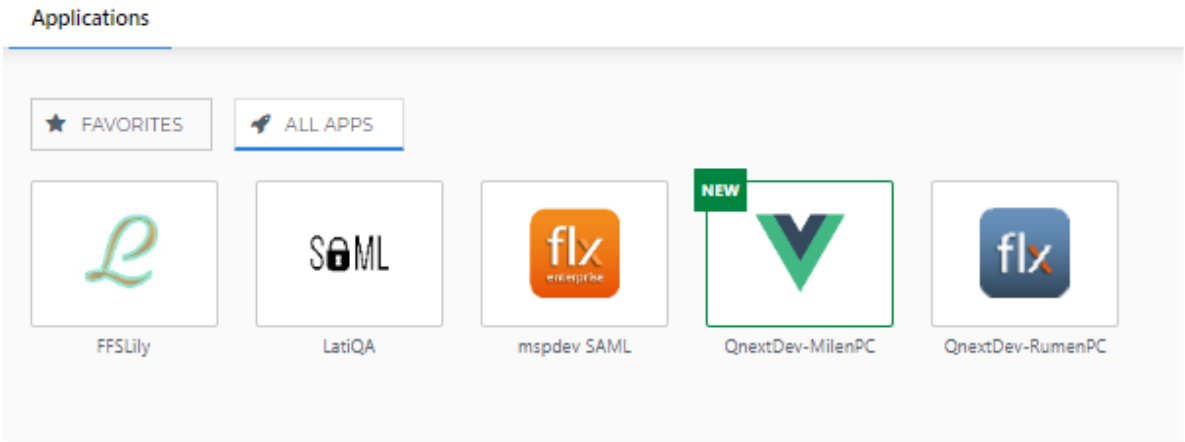
Click on "Login with Hello ID" and provide hello credentials in the pop-up. (In case you are testing in a browser where HelloID credentials are already provided to some other application then below pop will be skipped and the user will be taken directly to FileFlex app without asking for any further credentials).

Once credentials are provided, the user is taken directly to FileFlex app and this completes our verification of HelloID Setup.

You can also verify launching the application from HelloID portal.

Goto the HelloID Application Dashboard and click on the application name that was created in earlier steps.

(e.g. we created an application named mspdev SAML with the Fileflex icon for easier identification). Clicking on the icon should launch FileFlex with the same user credentials used in HelloID portal.



8.5.4. Single Sign-On with SmartLogin

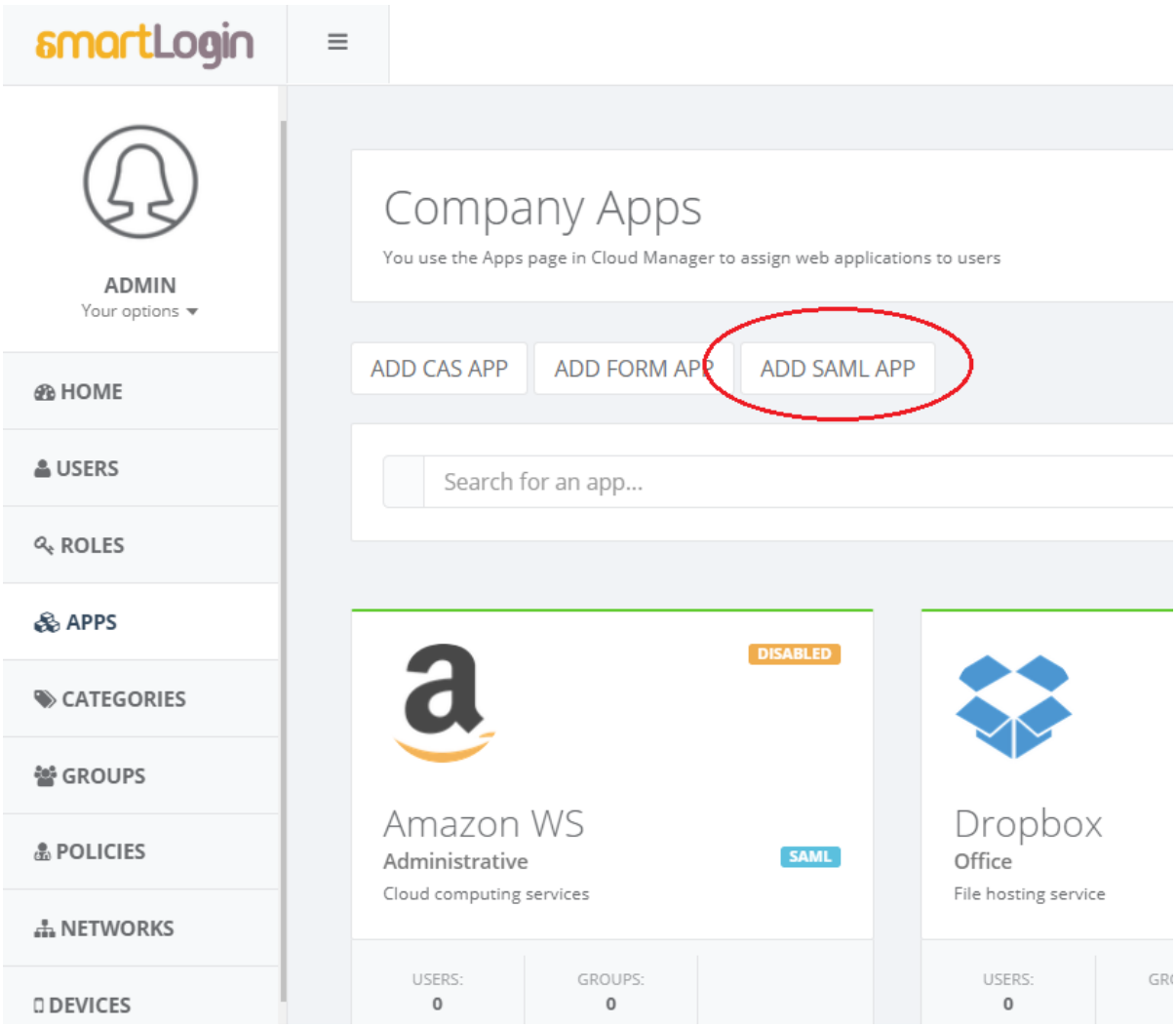
This documentation provides a tutorial on how to configure the Smarlogin app such that users can be directed to your particular FileFlex deployment.

> When connected to OneLogin, user accounts that exist both in FileFlex, and in the OneLogin directory will be able to login using their OneLogin credentials only.

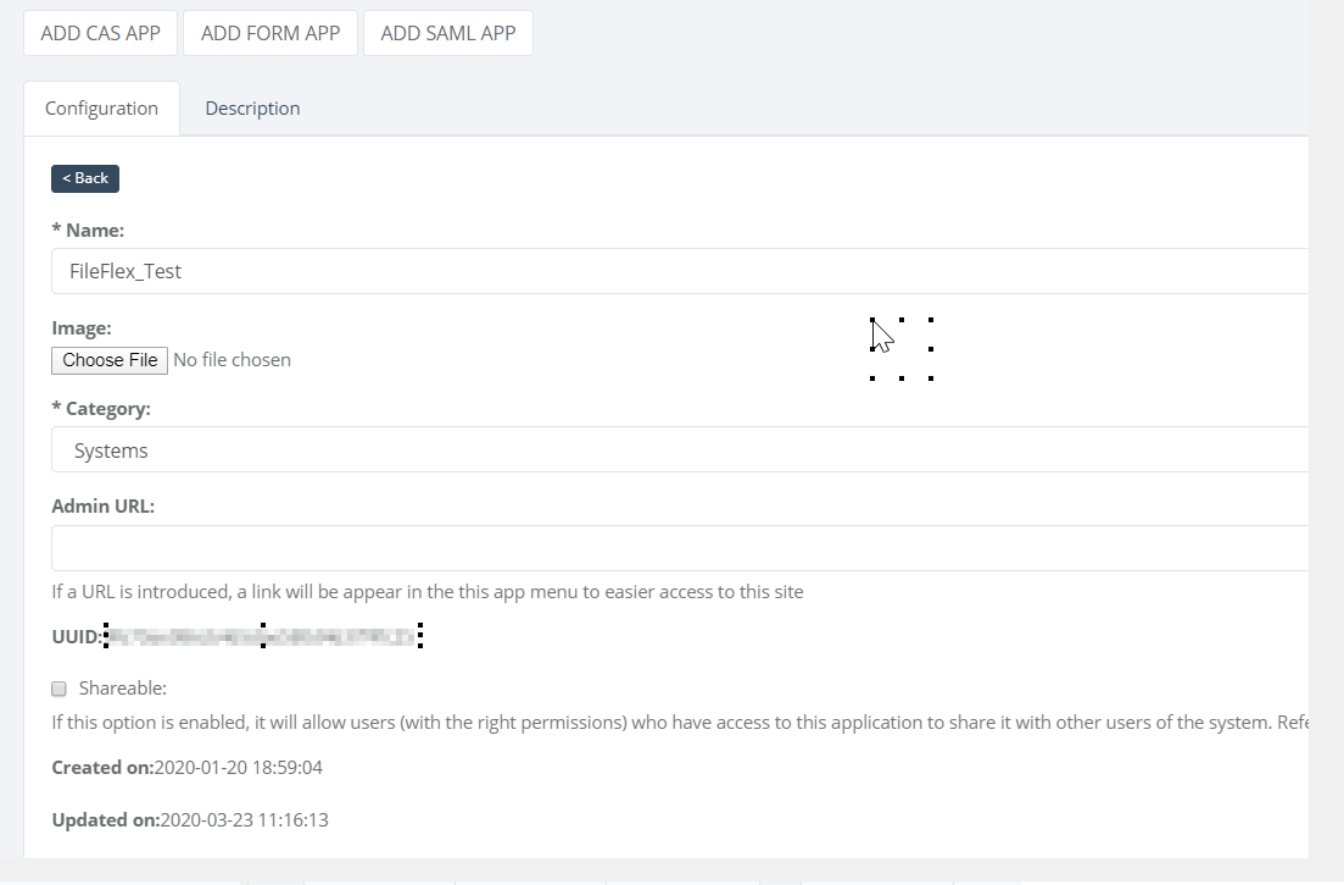
8.5.4.1. Creating a SAML App

Login to Smartlogin Server as an admin and click Admin Dashboard.

Click APPS and then click "ADD SAML APP".



Provide the basic details (name, icon) as per need. The name will be shown to users if they are launching FileFlex from Smartlogin Dashboard.



Complete the remaining details as shown below and in the example shown below:

Entity ID: <FileFlex Server domain>/fbweb/app/public/view/metadata_partner_saml?AuthService=SamlSmartLogin

Sign Assertion: Checked

Name ID format: EMAILADDRESS

Name ID : EMAIL as NAME ID

Consumer service redirect : <FileFlex Server domain>/fbweb/app/public/view/login_partner_saml

Consumer service post: <FileFlex Server domain>/fbweb/app/public/view/login_partner_saml

Discover Attributes : Select (first_name, last_name, email)

* Entity ID:

https://mspdev.cnexus.com/fbweb/app/public/view/metadata_partner_saml?AuthService=SamlSmartLogin

*** Entity ID:**

https://mspdev.cnexus.com/fbweb/app/public/view/metadata_partner_saml?AuthService=SamlSmartLogin

☑ Sign_assertion:

Specifies if the IdP should sign the assertion in an authentication response or no

☐ Sign_response:

Specifies if the IdP should sign the authentication response or no

☐ Encrypt assertion:

☐ Request signed?:

*** Name ID format:**

EMAILADDRESS

User mapping:

◉ **Use system user id**

○ **Everybody shares a single user name**

NameID:

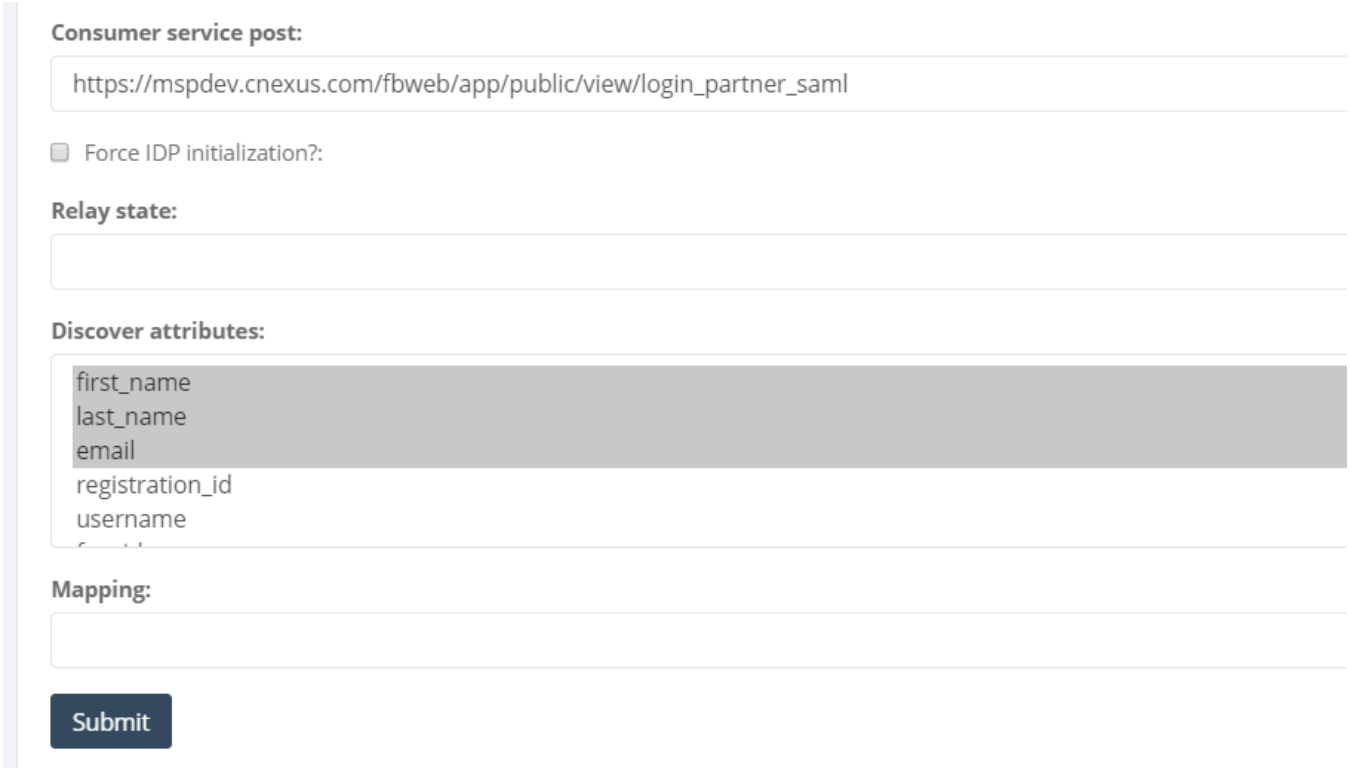
EMAIL AS NAME ID

Login URL:

Consumer service redirect:

https://mspdev.cnexus.com/fbweb/app/public/view/login_partner_saml

Consumer service post:

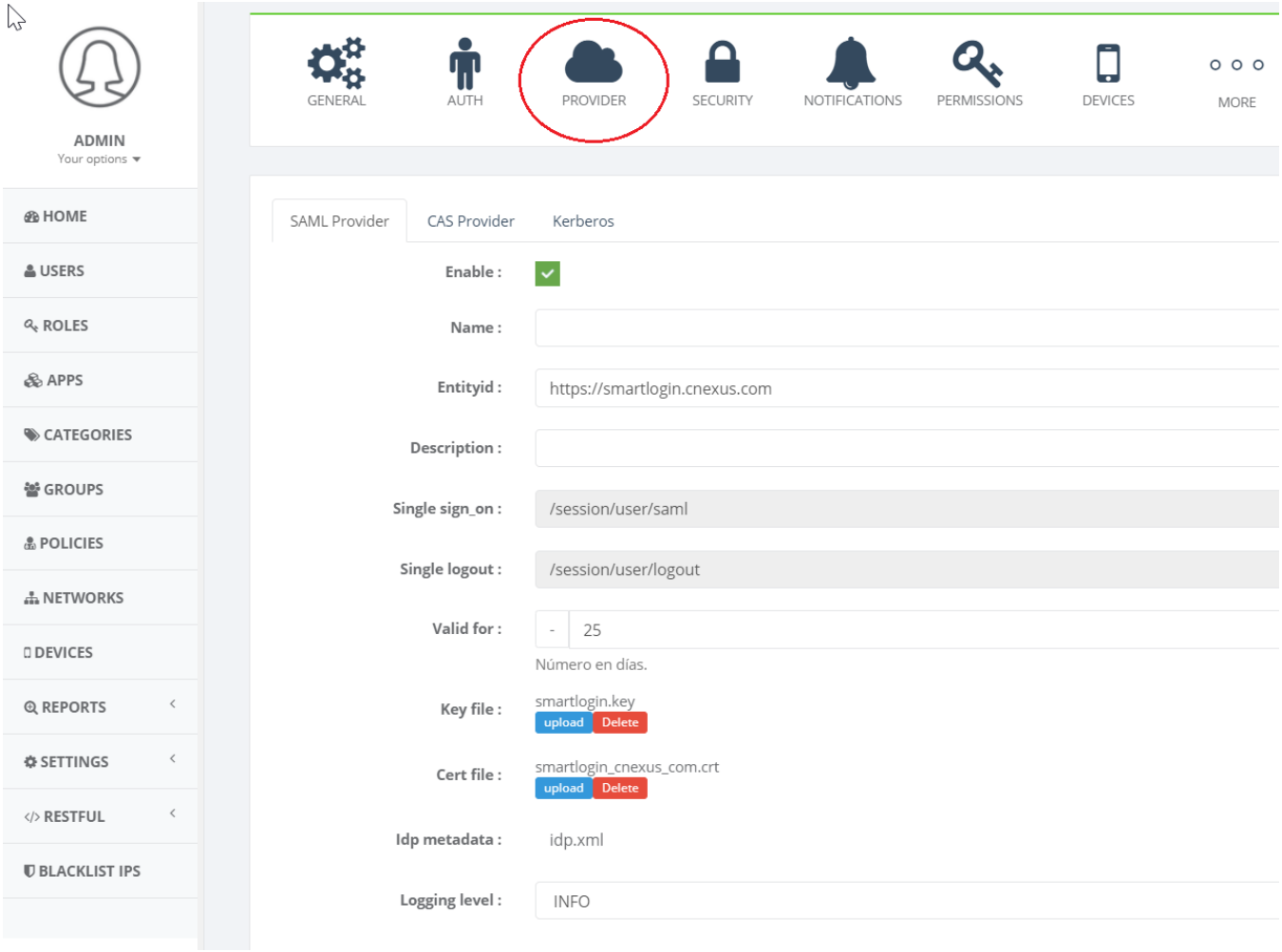


Click Submit

This completes the application creation task. Now you can download the metadata which will be required when you configure FileFlex to connect to Smartlogin.

8.5.4.2. Downloading Application MetaData

On the Sidebar of Admin dashboard, click Settings → System → Provider



Provide the Entity id, this should be the domain where Smartlogin is configured.

Note down below values as they will be required in later steps

- Cert FIle : Download and save to a text file.
- Single Sign_on URL : Copy the string and save it to a text file.
- Single logout: Copy the string and save it to a text file.

Click SUBMIT and this completed the task. You can now proceed to next step to FileFlex server Admin

8.5.4.3. Linking FileFlex and SmartLogin Server Application

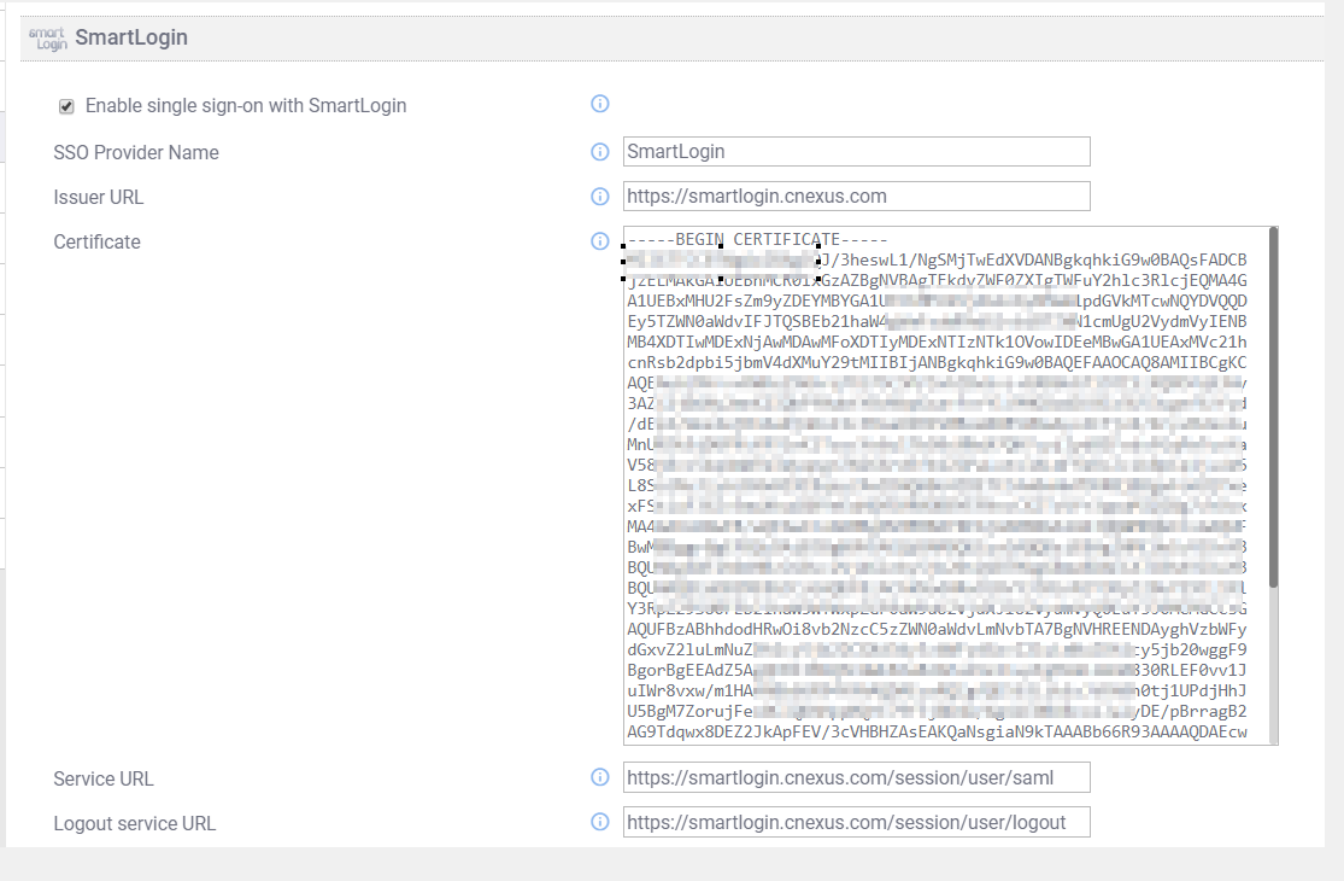
Login to FileFLEx Server Admin console.

Click Control Panel → Single Sign-on

Locate the Smartlogin Section and complete the section as shown below.

1. Check the box "Enable singl sign-on with SmartLogin.
2. SSO Provider Name: End user facing name. Default value : SmartLogin
3. Issuer URL: Domain of the server where SmartLogin is configured.
4. Certificate: Provide the same file which was copied in the previous section.
5. Service URL: Provide the URL Single Sign_on copied in the previous section.
6. Logout Service URL: Provide the URL Single Logout copied in the previous section.

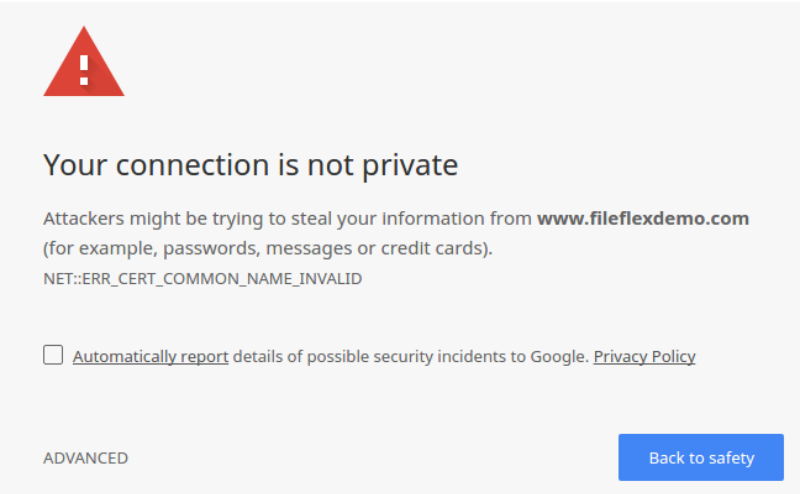
A sample filled section is shown below :



Click "Apply" to save your changes. Restart the server when prompted.

8.6. Supplying an SSL Certificate

In order for FileFlex to function correctly and to display the "green lock symbol" on browsers it's important to deploy a valid SSL certificate for your domain. Without it, users will be concerned about the security of your deployment since they will see warnings similar to the following (depending on the browser):



Before proceeding, ensure that you have a valid certificate for your deployment's domain, and that it's encoded in the standard PEM format.

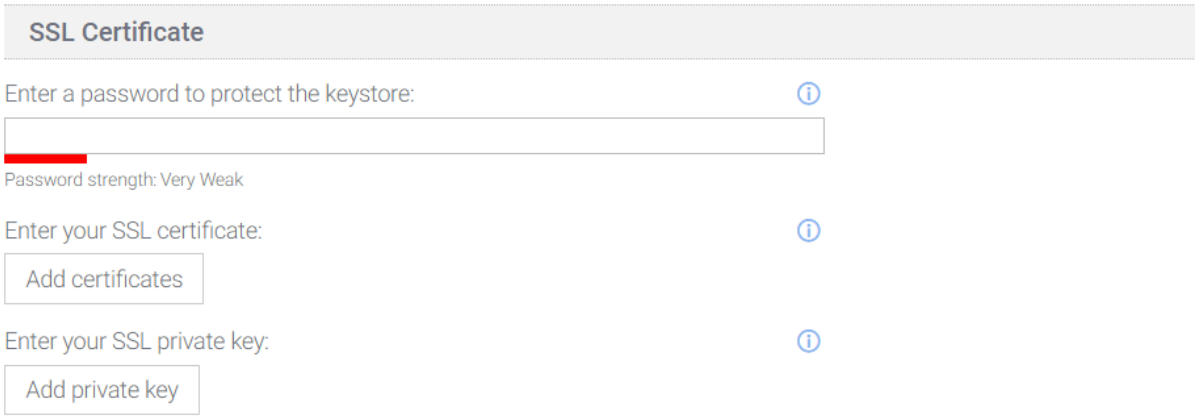
Need help obtaining a certificate?

If you need help obtaining a certificate, please refer to the appendix of this document

Certificate Passwords

FileFlex does not presently support the use of passwords-protected certificates. A password will be added to the keystore to ensure it remains protected, but the base certificate must be clear.

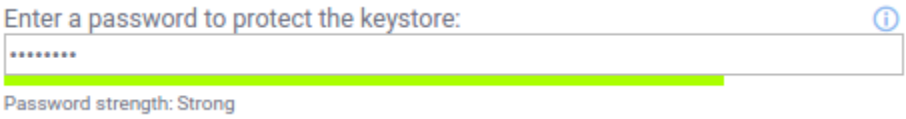
Navigate to the server administration's Control Panel tab, and then into the "Certificates" panel:



The certificates panel is divided into 3 seconds:

1. A mandatory keystore password which protects your SSL keys once entered. You will not have to enter this password on each server restart.
2. An SSL certificate uploading button.
3. An SSL private key uploading button.

Start by entering a password for your certificate. It is acceptable to use the same password as for your sadmin user. You should then see a green bar under the password entry indicating that the password is of sufficient strength:



8.6.1. Certificate Format

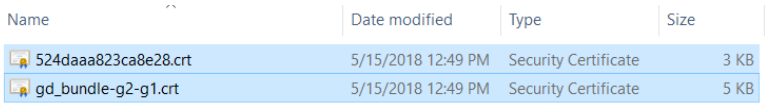
It's expected that your certificate has been provided to you by your certificate issuer in PEM format. You should have received the following files (or have generated them):

1. A certificate file in PEM format.
2. One or more intermediate certificate files in PEM format.
3. A private key file in PEM format.

8.6.2. Uploading your Certificates and Key

Begin by clicking the upload certificates button:

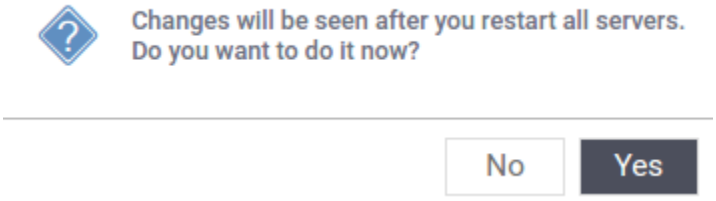
You will need to select your own domain's certificates, as well as any intermediate certificates. They must be in the same folder, and selected together using multi-selection (holding down the shift or control keys):



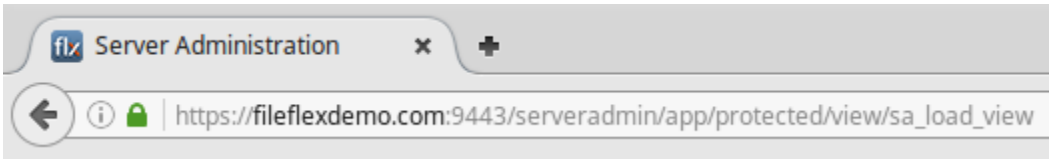
You will then see the certificate files listed in the control panel:

Click the "Add private key" button to submit that file. Once complete, you should see it listed in the control panel as well:

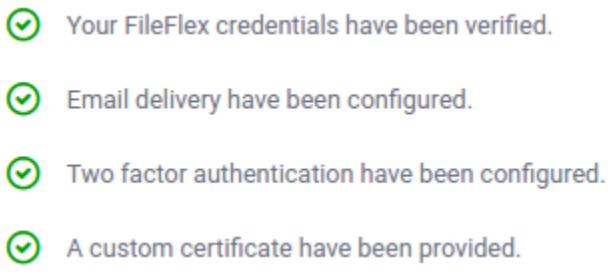
When you've finished entering your certificate and key, click Apply and wait a few moments. You will then be prompted to restart your servers:



Click yes to continue. After a few minutes, the servers will be restarted and you should see a green lock symbol in your browser for Server Administration:

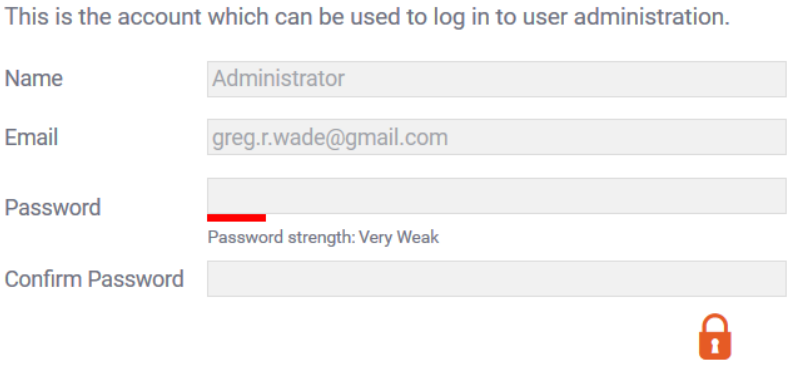


Congratulations - you've completed this step! Back on the overview panel, you will have confirmation that you've completed that stage of the configuration:

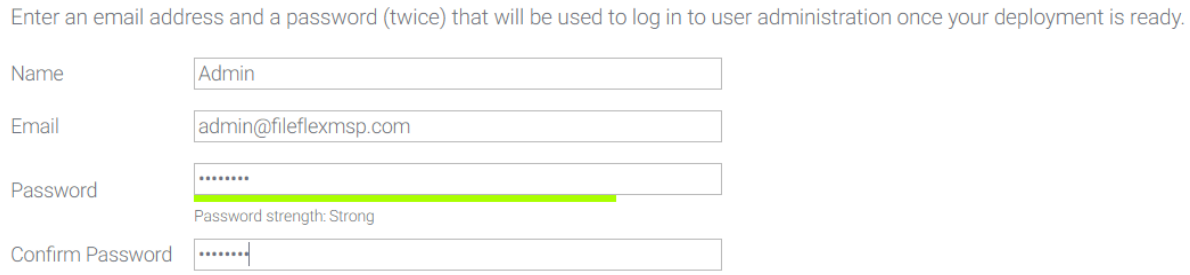


8.7. User Administration Credentials

The control panel entry labeled as "User Administration" reveals the user admin credentials which were created during the initial wizard configuration phase:



This account will have been created for you during the initial configuration steps performed earlier. If you need to change the user administration user and/or password, click the lock symbol to edit the values:



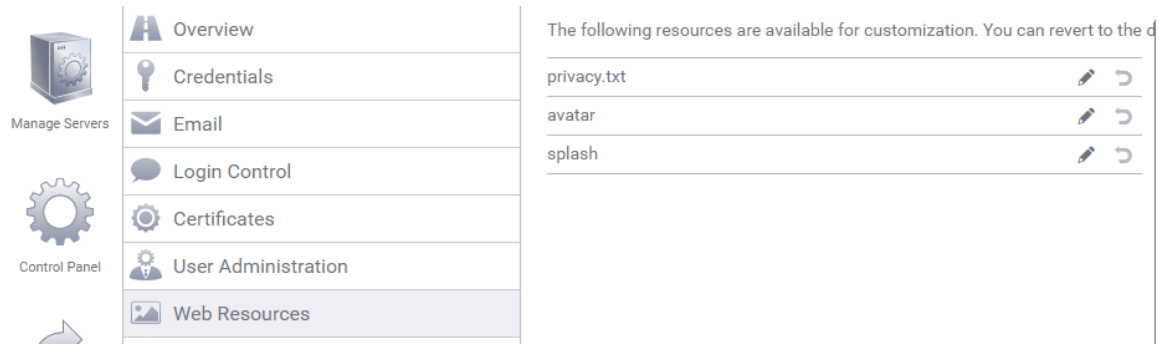
Click Apply when you're satisfied.

8.8. Updating Web Resources

8.8.1. Customizing the Splash Screen

Although not mandatory, it's nice to have a customized application splash screen. Ensure that you have a PNG or JPG file of appropriate size ready for submission.

Start by navigating to the "Web Resources" panel of the Control Panel tab:

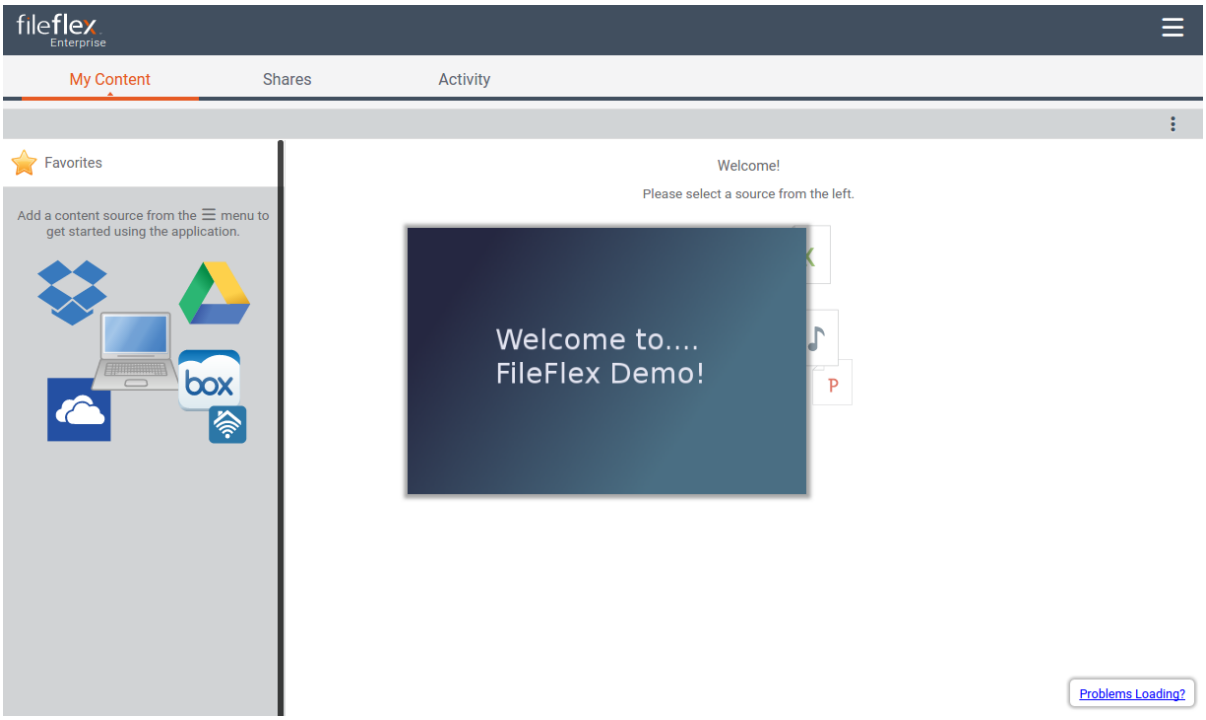


Once there, click the pencil icon next to the "splash" row and you will be prompted to upload a file.

Select your chosen file for upload.

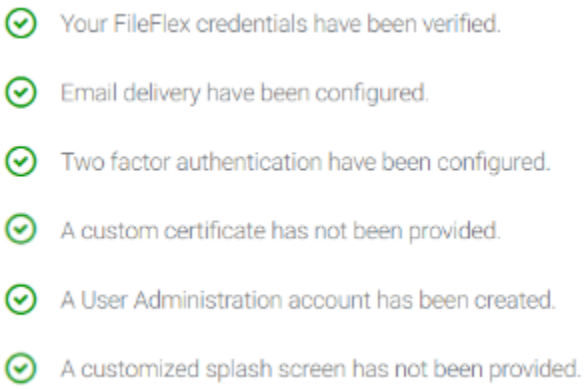
Although any image may be used, the recommended image size is 450x300 pixels in PNG format.

When a user logs in to the application they will be presented with a screen similar to the following including your customized splash screen:



Congratulations - you've configured your splash screen!

Back in the overview panel of the control panel you will now see that each configuration step has been completed:



8.8.2. Customizing the Privacy Policy

When configure a cloud provider such as Google Drive, it may be necessary to provide a privacy policy that originates from the same domain as the one handling the FileFlex Enterprise Solution. This section describes where you can get a template for a privacy policy, how to modify it, and how to upload it to the virtual machine.

8.8.3. Generating a Privacy Policy

We have provided you with a sample privacy policy template. You can use it as the basis of your own privacy policy.

> It is imperative that you update the privacy policy to reflect the manner in which your deployment will use customer data. The same provided speaks for the information collected by our solution only, and cannot accurately express how that data will be used by you the deploying corporation.
>
> ***The privacy policy being supplied here is a general template only! Please ensure it's updated for accuracy.***

8.8.3.1. Downloading the Privacy Policy Template

- The privacy file is accessible from your domain at the following URL:

```
https://[yourdomain]/fbweb/static/docs/privacy.txt
(for example)
https://fileflexdemo.com/fbweb/static/docs/privacy.txt
```

> The default privacy policy file is the template variant. Once you've replaced it, the original template will be gone. Ensure you make a backup copy of that file for future use if needed.

8.8.3.2. Customizing the Privacy Policy Template

- Replace all instances of [COMPANY] in the document with your company name. For example, replace [COMPANY] with ACME Tools Inc
- Replace all instances of [APP_DOMAIN] with the domain used to configure FileFlex Enterprise. For example, replace [APP_DOMAIN] with www.acmetoolsinc.com
- Replace all instances of [SUPPORT_EMAIL] with an email used for support requests relating to FileFlex Enterprise. For example, replace [SUPPORT_EMAIL] with support@acmetoolsinc.com

8.8.4. Uploading a Privacy Policy

Once you've finished editing the privacy policy template, click the pencil icon next to the "privacy.txt" row and you will be prompted to upload a file.

Select your chosen file for upload. Once the file is uploaded, you will see a confirmation message:

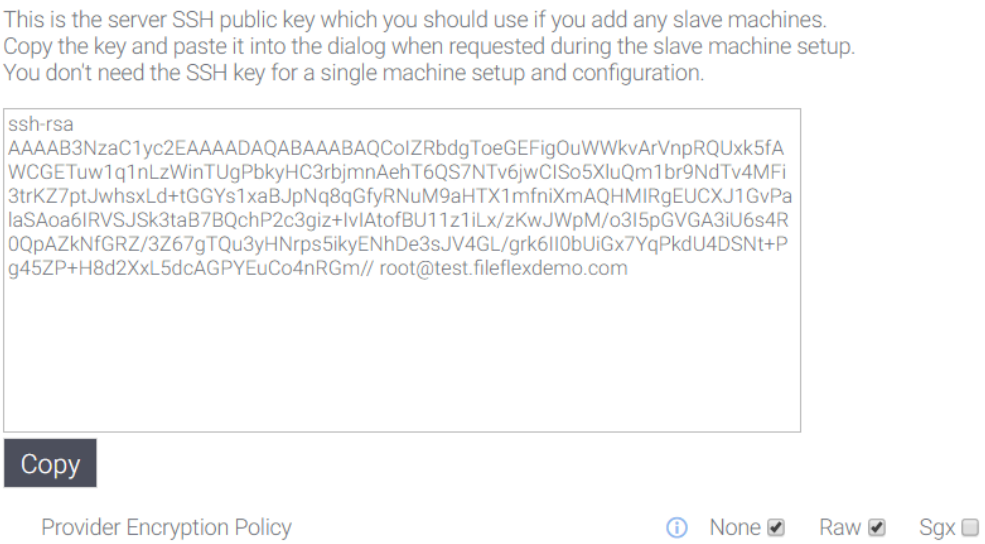
To verify that the new version of the privacy policy has been uploaded successfully, you can open a browser at the specified URL to view the content:

```
https://fileflexdemo.com/fbweb/static/docs/privacy.txt
```

8.9. Encryption Settings

The encryption panel of the control panel tab exposes two encryption related settings:

1. Exposing your deployment's public SSH key for cluster configuration.
2. Setting the preferred Provider Encryption Policy



8.9.1. SSH Key Handling

Click the "copy" button to have the key copied into your system's clipboard. You will then be able to paste it into the terminal of your cluster node virtual machines for easier configuration.

> ⚠ Your SSH public key is only needed when deploying a cluster node. If your deployment is a single-machine configuration, you can safely ignore this panel.

8.9.2. Provider Encryption Policy

The provider encryption policy allows you to determine if any additional encryption will take place over transferred data for supported data sources.

> ⚠ Before proceeding with the configuration of your encryption settings, you must first ensure that an SSL certificate has been installed in your deployment. Refer to the related section of the documentation.

> ⚠ Data is ***always encrypted*** during transfers with FileFlex! The feature described here represents ***additional, secondary*** encryption which can optionally be placed on top of the regular SSL encyrption, allowing for true point-to-point encryption of data. The consequence if mandating secondary encryption is that web browsers will not be able to consume the data.

The encryption policies are those which will be made available to content sources supporting the additional level of encyrption (PC, server, NAS, etc). The content source owner has the ability to determine which subset of these will be used for a given content source, within the limits established here.

The following table breaks down the options:

Encryption Policy Option	Data is SSL Encrypted	Browser Support	Double Encryption (End-to-End)	Description
None	Yes (always)	Yes	No	This option allows transfers to use only the basic single-level encryption. Content sharing with browsers is supported.

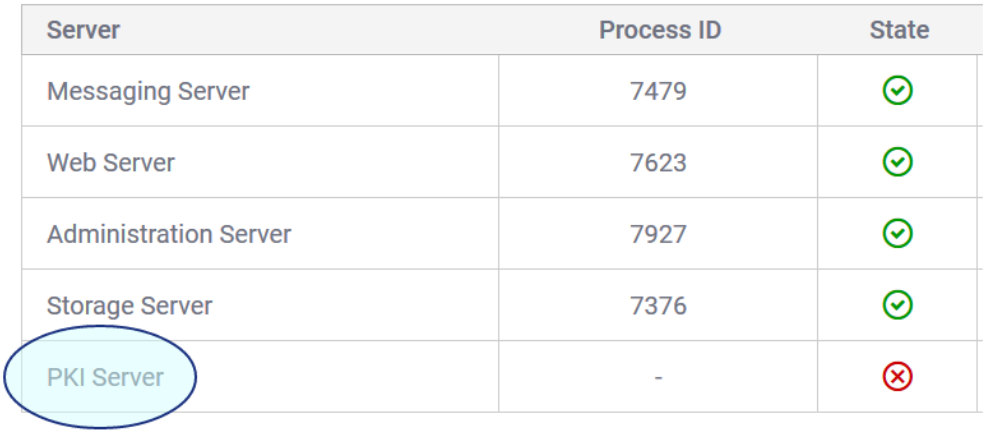
Raw	Yes (always)	No	Yes	This option allows end-to-end encryption. Supported clients are required for data consumption.
SGX	Yes (always)	No	Yes	This option allow end-to-end encryption with additional Intel Dataguard protection. Supported clients are required for data consumption, while running on an Intel Dataguard supported system.

If you want your users to be able to share content with other people using web browsers, you must ensure that "None" is selected. On the other hand, if you want to ensure that end-to-end encryption is always enforced, do not select "None", and ensure all users have a supported client.

8.9.3. Enabling Double Encryption

In order to enable double encryption (without SGX support), you must select "Raw" encrytion from the provider encryption policy checkboxes:

Note that an SSL certificate must have been installed before this functionality can be used. Once you have verified than an SSL certificate has been deployed, confirm that the PKI server is running (this is assuming a single-machine deployment). Switch to the "manage servers" tab:



If the PKI server is stopped (indicated by a red cross warning icon), select the "PKI Server" row, and click the triangle "start" button to start the process. You should see something similar to:

Your deployment is now capable of double encryption (without SGX).

8.9.4. Enabling SGX Capability

In order to enable SGX double-encryption capabilities in your FileFlex deployment you must have PKI server deployed on an SGX-enabled Microsoft Windows machine. These machines are typically labelled as "vPro" compliant.

Important Before Proceeding!

Before proceeding with this section, please ensure:

1. That your target system is vPro compliant.
2. That the target system is externally accessible for PKI operations on port 4007.
3. You have a valid certificate for the domain used to access your PKI server in PEM format.
4. You have any required intermediate certificates required by your domain certificate, and issued to you by your certificate signing authority, in PEM format.
5. You have the private key associated with your domain certificace in PEM format.

For more information on Intel vPro, follow the link:

https://www.intel.ca/content/www/ca/en/architecture-and-technology/vpro/vpro-platform-general.html

The first step is to download the Windows version of the FileFlex PKI server. Use the link provided from within the FileFlex Enterprise Portal to download the PKI server.

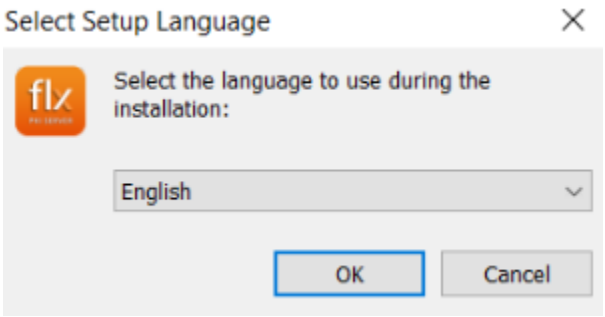
PKI Server Download

If you are having trouble locating the PKI download URL from the FileFlex Enterprise portal, you can obtain it from this link:

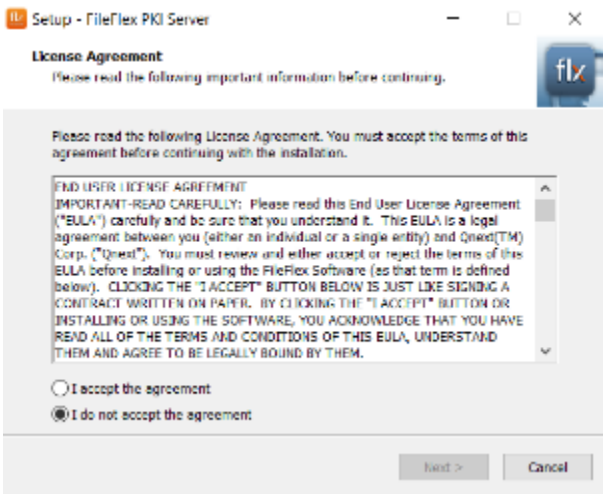
https://res.fileflex.com/packages/installers/pki/PKIServerInstaller_Latest.exe

8.9.4.1. Installing the PKI Server

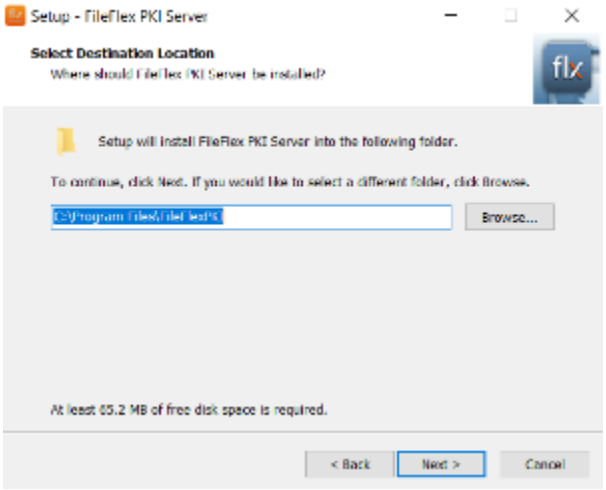
Once you've downloaded the PKI server, and have it available on a compliant machine, it's time to run the installer. Doing so will open the installation, and request your language of choice:



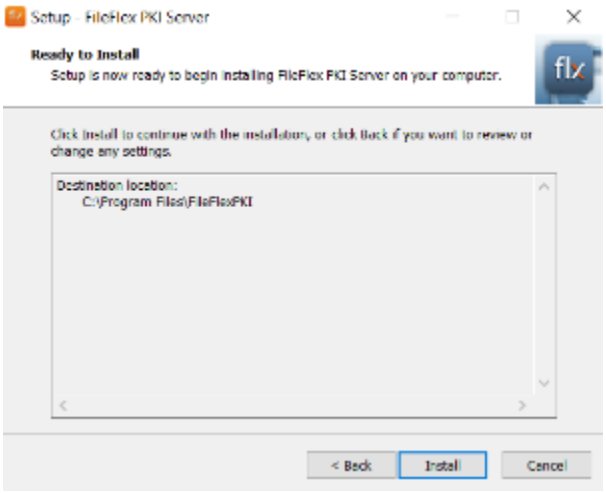
Select the language you prefer, then click OK. You will then be presented with the licensing agreement:



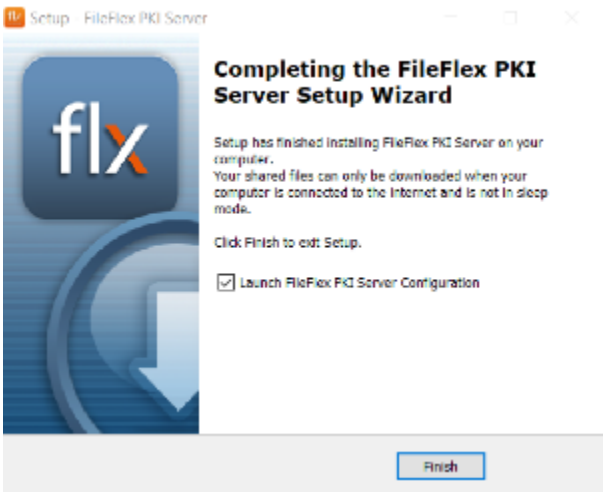
If you accept the terms, click "I accept the agreement" and click "next". The next screen will ask you where you want to install the application.



Choose the path of your choice. Here we assume the default location. Click Next. You will then be asked to confirm the installation.



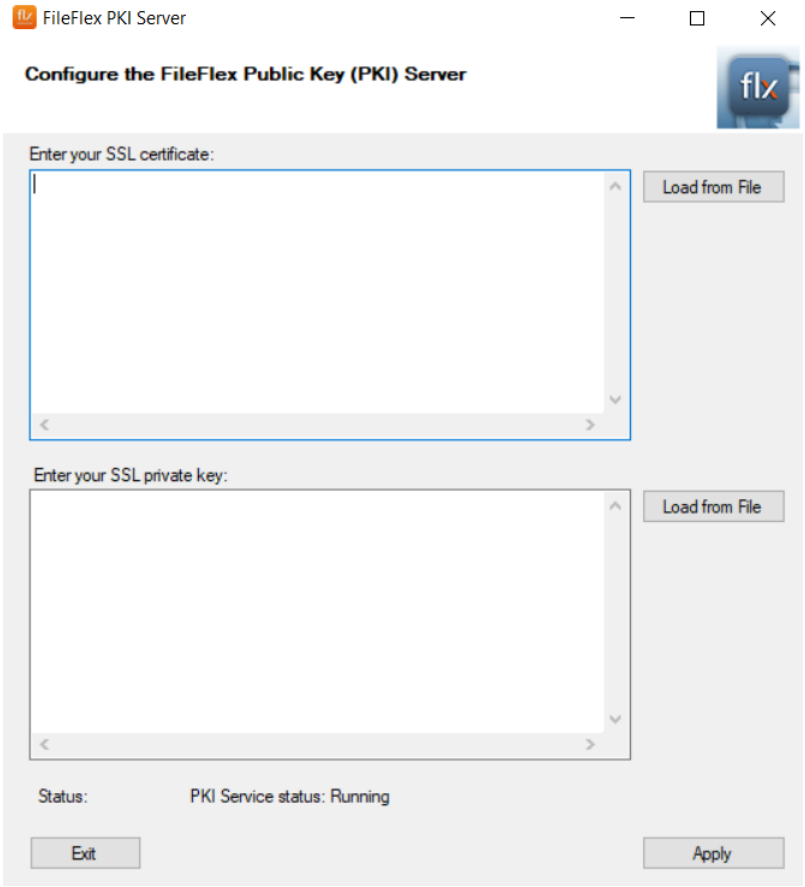
If you're satisifed with your choices, click "Install" to proceed. The files will then be installed, as will Intel's DataGuard runtime which may take some time. When the process completes you will receive a confirmation:



Click "Finish" to complete the process.

8.9.4.2. Configuring the PKI Server Certificate

Upon running the FileFlex PKI server you will see a screen similar to:



The next step is to enter your SSL certificate. You may use a wildcard certificate, or a regular one.

It's important to understand that most certificates provided today consist of multiple parts. You must concatenate these into a single file prior to pasting into the PEM-encoded data into the certificate field. You can do this in a text editor, or using the command line. When doing so in a text editor ensure no empty rows between the certificate files. The certificate for your domain should be listed first in the file, followed by the chain of CA certificates.

It's important that the certificate entered include all components of the chain as provided by your SSL certificate issuer. Additionally, ensure that the files are concatenated together starting with domain certificate, followed by the chain of CA certificates.

A Linux command-line example of concatenating your certificate files follows:

Concatenate Certificate and Bundle

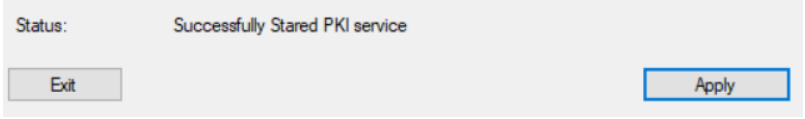
```
cat *yourdomainname*.crt *yourdomainname*.ca-bundle >> cert_chain.crt
```

Direct Certificate Entry

It is possible to enter the certifficate directly (and sequentially) into the text box in your browser rather than running a concatenation command as exemplified above, but this is more prone to typographical errors since the view-able area is small.

Enter your combined certificate into the certificate field. Do the same for your private key:

Click the Apply button. After a few moments, you should see a confirmation message that the PKI server was restarted:

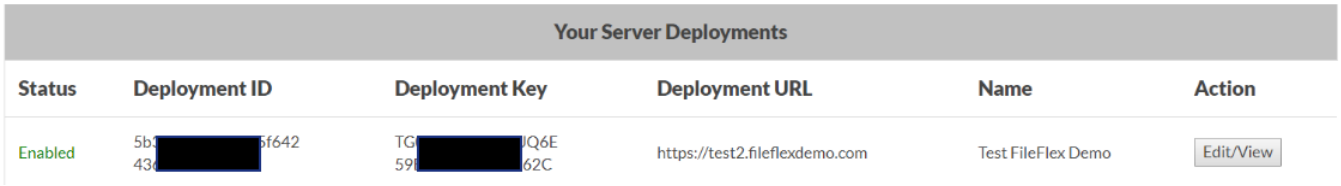


8.9.4.3. Registering your PKI Server

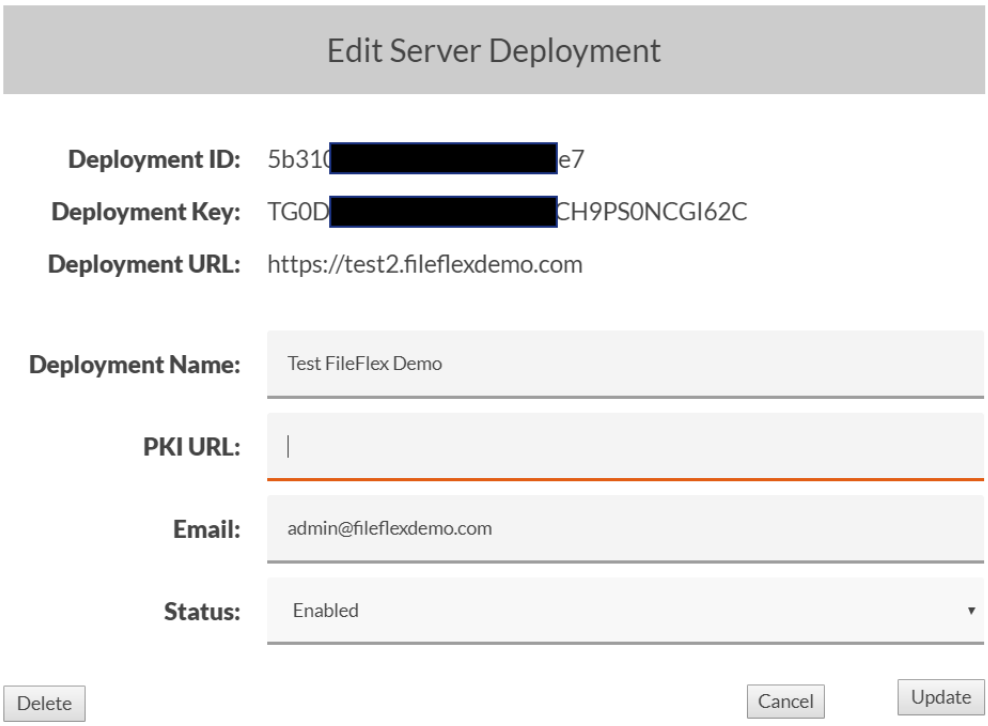
Now you must inform FileFlex that you have a PKI server deployed. Do so by navigating to the enterprise portal's control panel using the following URL in your browser of choice:

Enterprise Portal Control Panel
`https://enport.fileflex.com/msp-control-panel/`

Once there, find your server deployment. For example:

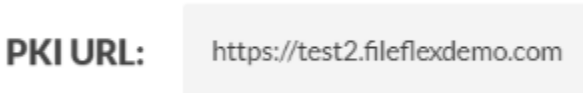


Click on the "edit" button to bring up the editing screen:



Enter the URL to your PKI server.

> ⚠ It's important that the domain entered here match the domain who's certificate you deployed in the PKI server earlier.



Click "update" to save your changes. Confirm your choice if prompted.

Congratulations - your PKI server is now ready to be used for double-encryption!

⚠ When deployed without SGX support (typically, in single-machine deployments), a Linux-based PKI server will be installed. In this scenario, there is no need to inform the FileFlex Enterprise Portal about your PKI server since the default handling will work appropriately.

8.10. User Activity Logging

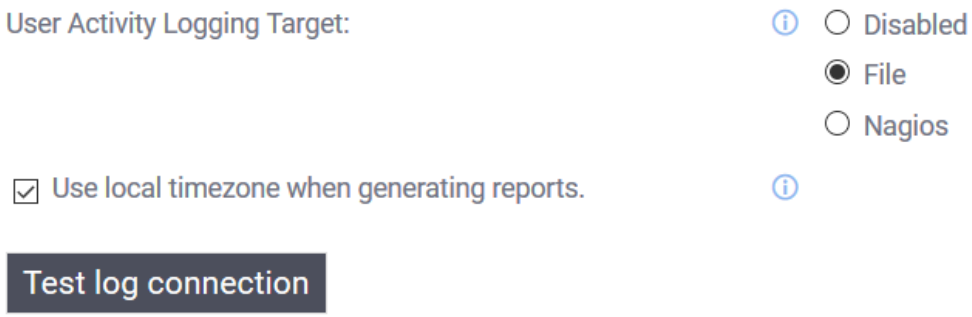
User activity logging allows you to export user activity of the FileFlex system to external sources such as a file or a Nagios Enterprise log server.

⚠ User activity represents a set of discrete user activities, and tracks everything that users do with the system. User activity is the same content as that contained within the activity' tab of the application, but exported to a content source of your choosing.

You will find entries similar to the following:

```
11/12/17 15:12:01       ProviderCreate [prcr]   User A (userA@gmail.com) added content source (google).
12/12/17 12:54:09       SessionCreate [secr]    User B (userB@gmail.com) was logged in.
```

To configure user activity logging, navigate to the 'User Activity Logging' panel of the Control Panel:



There are three logging targets that determine where activity logs are stored. The available options are:

Target	Description
Disabled	Activity logging will not be exported to any location. Activity logging is still tracked, and may be access from the application's 'Activity' tab.
File	Activity is logged to a file in FileFlex Enterprise's logging folder, and can later be downloaded for storage.
Nagios	Activity is communicated in real-time to an externally configured Nagios Enterprise Log Server. Using that application, it's possible to configure email notifications based on matching keywords, and other automated responses to user activity.

8.10.1. Local Timezone Reporting

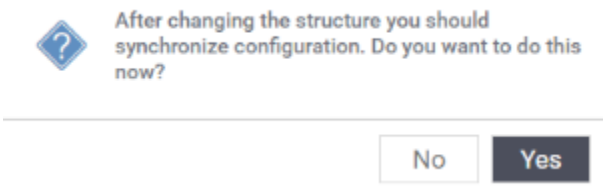
When generating a user activity report from within the user administration module, changing this option will caused the times to be stored with local time, rather than the default UTC+0 timezone. If unsure, leave this unchecked.

8.10.2. Logging Activity to a File

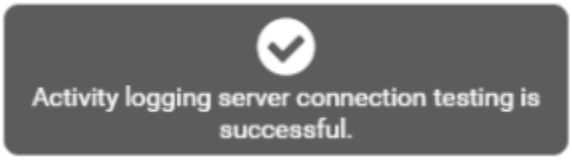
To enable logging user activity to a file, click on the target dropdown and select the "File" option.

To confirm that everything is working as expected, click the "Test log connection" button that appears after selecting the File option.

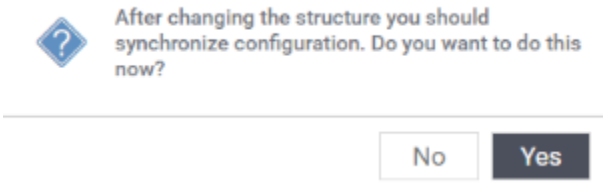
If you previously had a different value set, you may be promoted to synchronized the changes:



Click "Yes" to proceed with the synchronization, and after a moment you should see the following confirmation message:



Click the Apply button at the bottom to save your changes, and you will be presented with a confirmation dialog:



Click "Yes" to proceed with the synchronization, and your change will be made immediately.

8.10.3. Downloading the Activity Log File

The activity log file is located in the FileFlex Enterprise deployment virtual machine instance. Log in to the terminal as the "sadmin" user of the FileFlex Enterprise instance:

```
login as: sadmin
sadmin@fileflexdemo.com's password:
sadmin@fileflexdemo:~$
```

Once you've logged in to the server instance, navigate to the Jetty Logs folder:

```
sadmin@fileflexdemo:~$ cd /opt/ffs/jetty/logs/
sadmin@fileflexdemo:/opt/ffs/jetty/logs$
```

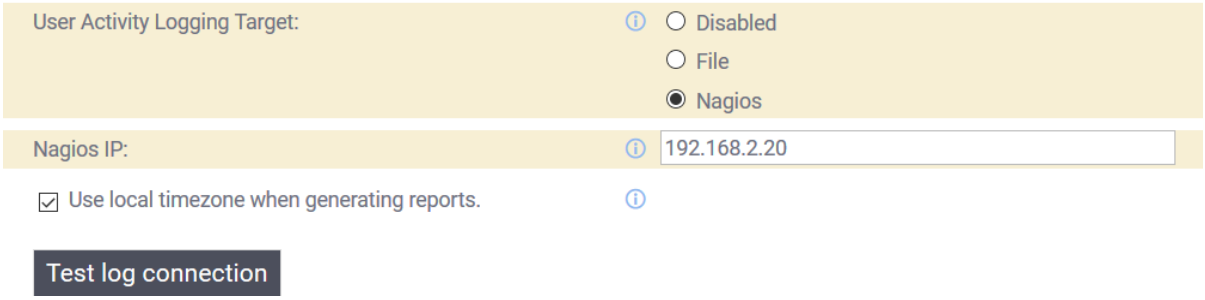
From there you can transfer the log file to a remote server to which you already have access using SCP or SFTP:

```
sadmin@fileflexdemo:/opt/ffs/jetty/logs$ scp activity.log remote_user@192.168.2.60:~/temp/
The authenticity of host '192.168.2.60 (192.168.2.60)' can't be established.
ECDSA key fingerprint is SHA256:nnRgNKfQxxxxxxxyz2X5O3Yw9MISNtnoIM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.60' (ECDSA) to the list of known hosts.
remote_user@192.168.2.60's password:
activity.log                                  100%   85     0.1KB/s   00:00
```

8.10.4. Logging Activity to Nagios Enterprise Log Server

It is assumed that prior to configuring this, Nagios Enterprise Log server. Alternately, the open source tool stack of ElasticSearch, Logstash and Kibana may be deployed since they are the foundations of Nagios Enterprise Log Server.

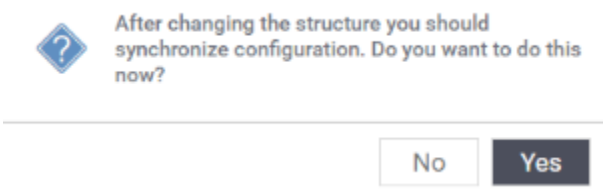
Start by select "Nagios" from the list:



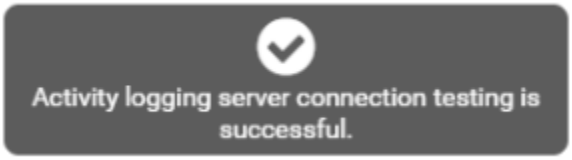
Enter the IP address of a running Nagios server in the "Nagios IP" field.

To confirm that everything is working as expected, click the "Test log connection" button that appears after selecting the File option.

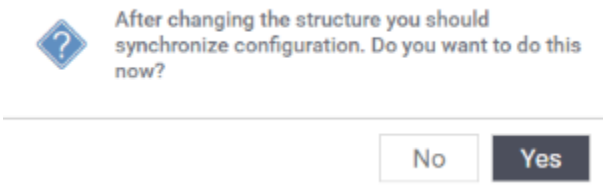
If you previously had a different value set, you may be promoted to synchronized the changes:



Click "Yes" to proceed with the synchronization, and after a moment you should see the following confirmation message:



Click the Apply button at the bottom to save your changes, and you will be presented with a confirmation dialog:



Click "Yes" to proceed with the synchronization, and your change will be made immediately.

> This guide does not discuss how to configure Nagios Log Server itself. Please refer to the Nagios Log Server documentation:
>
> https://library.nagios.com/library/products/nagios-log-server/documentation/
>
> FileFlex Enterprise communicates with Nagios Log Server via the 'syslog' format.

Open Nagios Log Server's log viewer:

Though not discussed here it is possible to configure NLS to notify you based on the presence of certain keyword matches. Each of our activities is logged with with a code in square brackets. For example:

In this example, the "prvr" code indicates that a provider (content source) was verified. These codes are useful for configuring NLS to notify you of important activities within your system.

8.11. Configure Google Drive Access

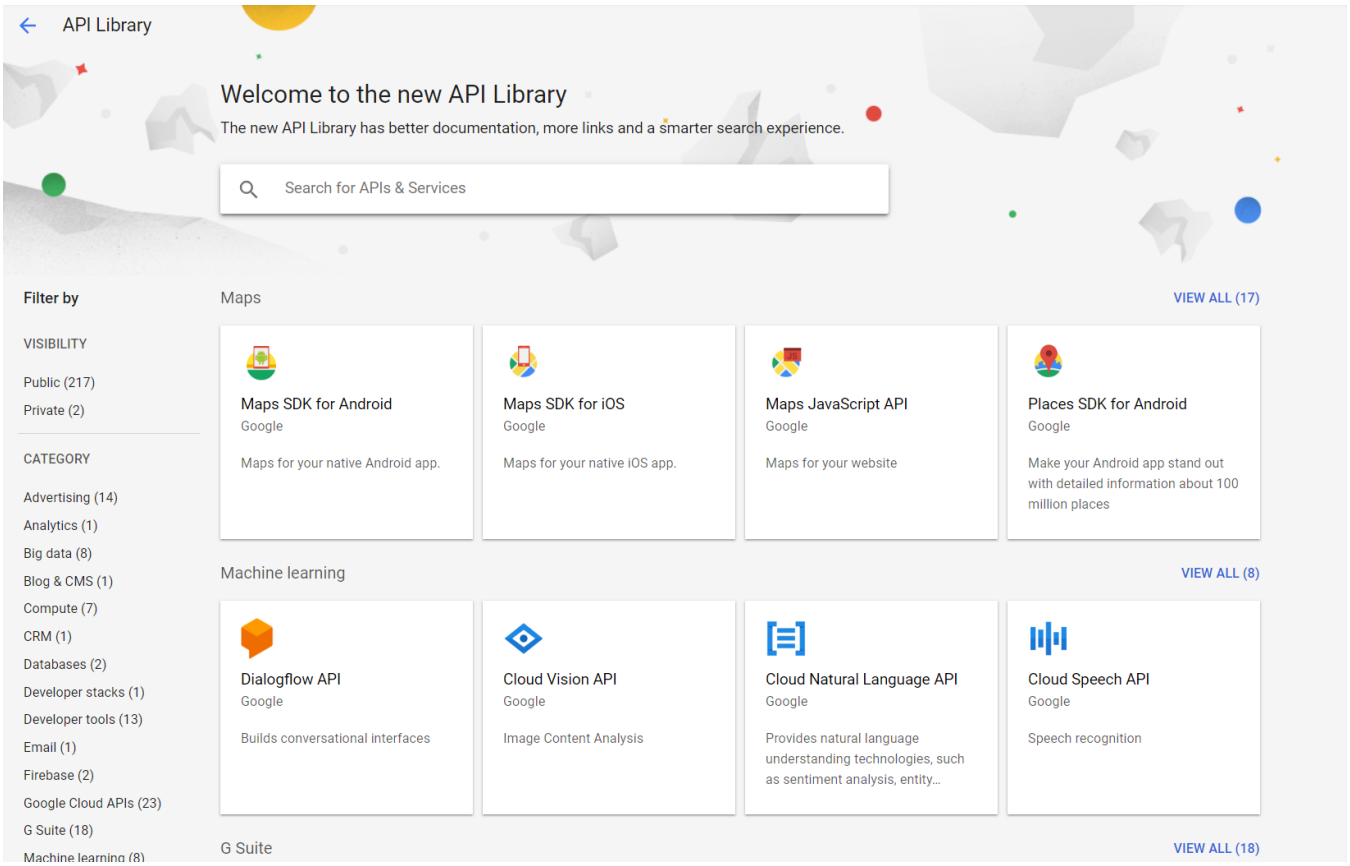
8.11.1. Registering for Google Drive API Credentials

> It's important to complete the "Supplying an SSL Certificate" steps prior to configuring Google Drive Access.

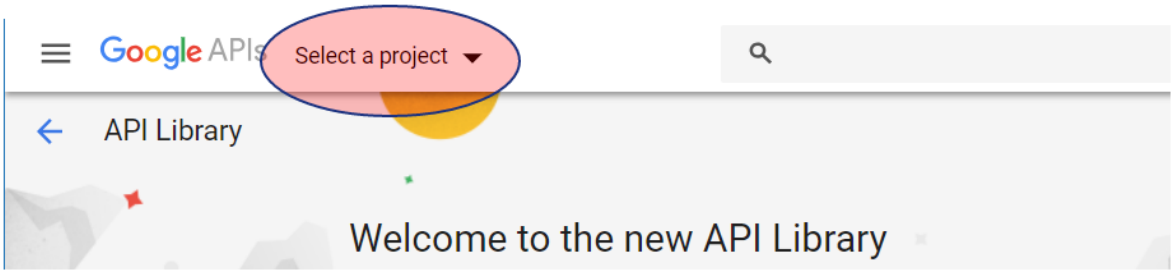
In order to configure Google Drive access from within FileFlex Enterprise, you must obtain a Google API Key and Secret from Google. Sign in to your Google account, and navigate to the following Google URL which is used to configure their APIs:

```
https://console.developers.google.com/apis/library
```

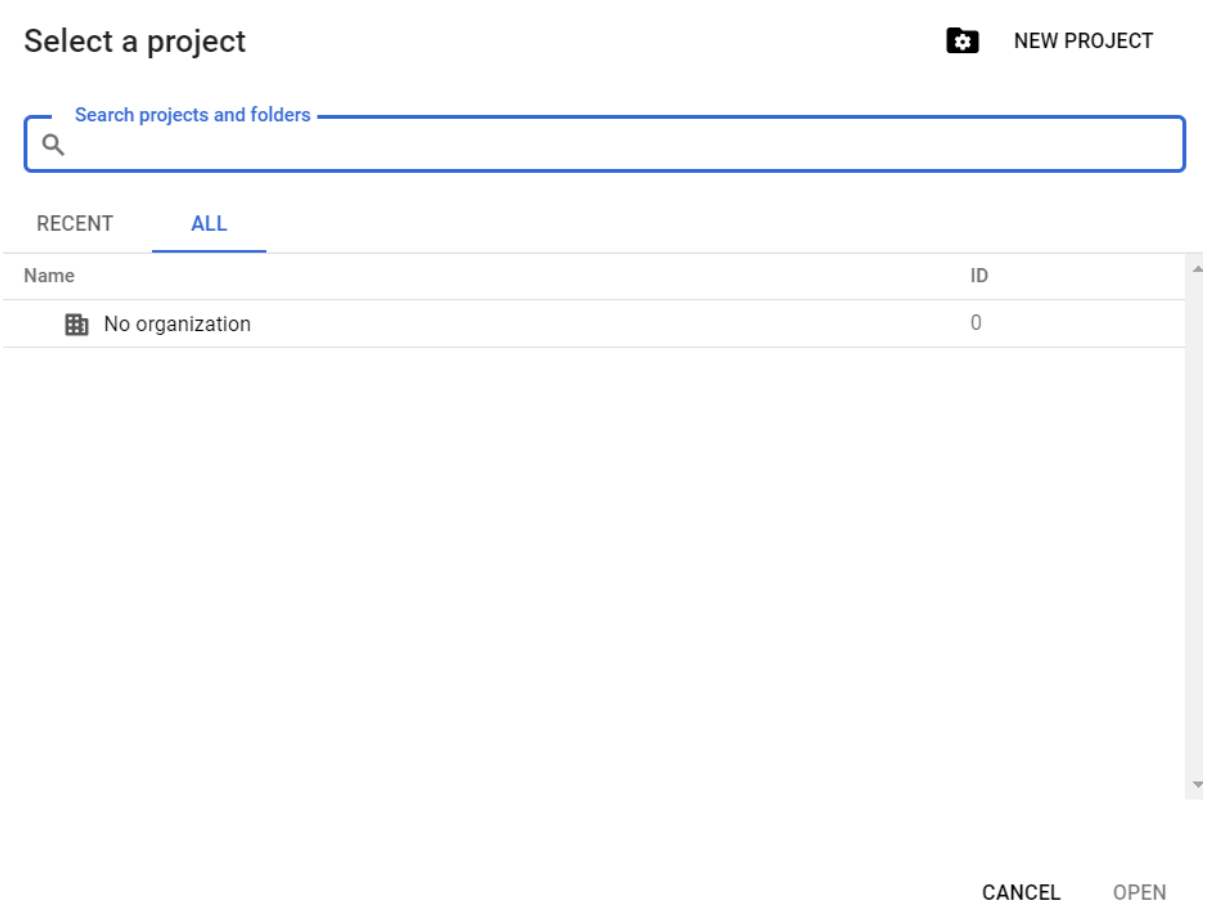
You will be presented with a screen similar to the following:



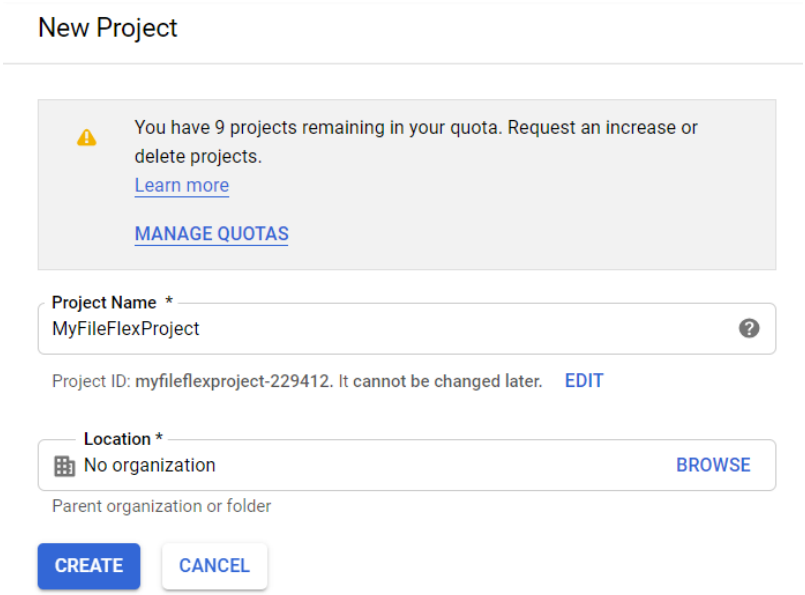
First you must create a project by clicking on the down arrow to open the project list:



That will reveal a dialog as follows:

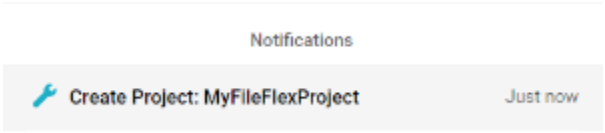


Click on the "new project" button to create a new project:

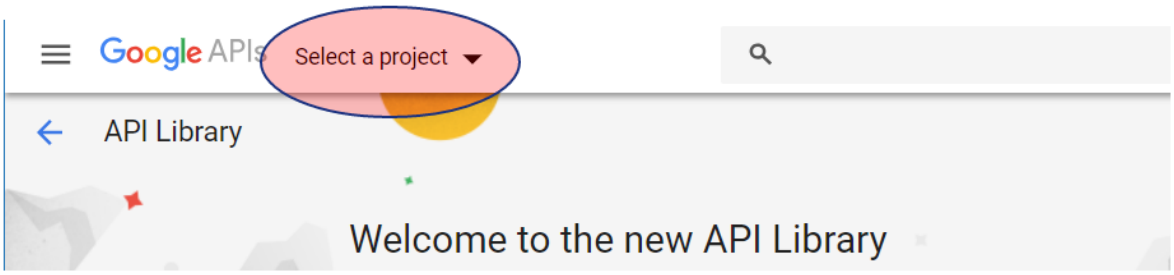


Enter a project name, and click on 'create'. You will then be returned to the API Library.

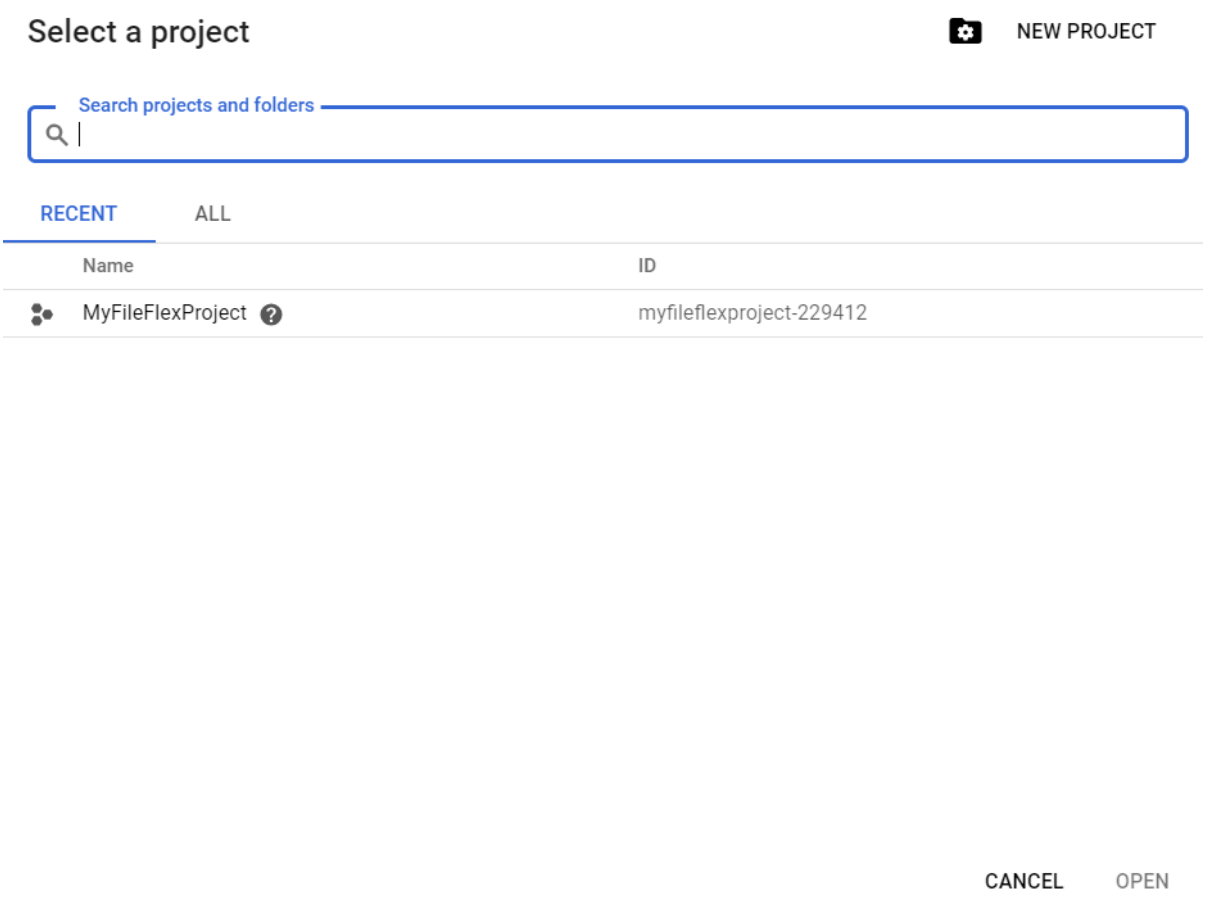
You will see a notification when the project is ready:



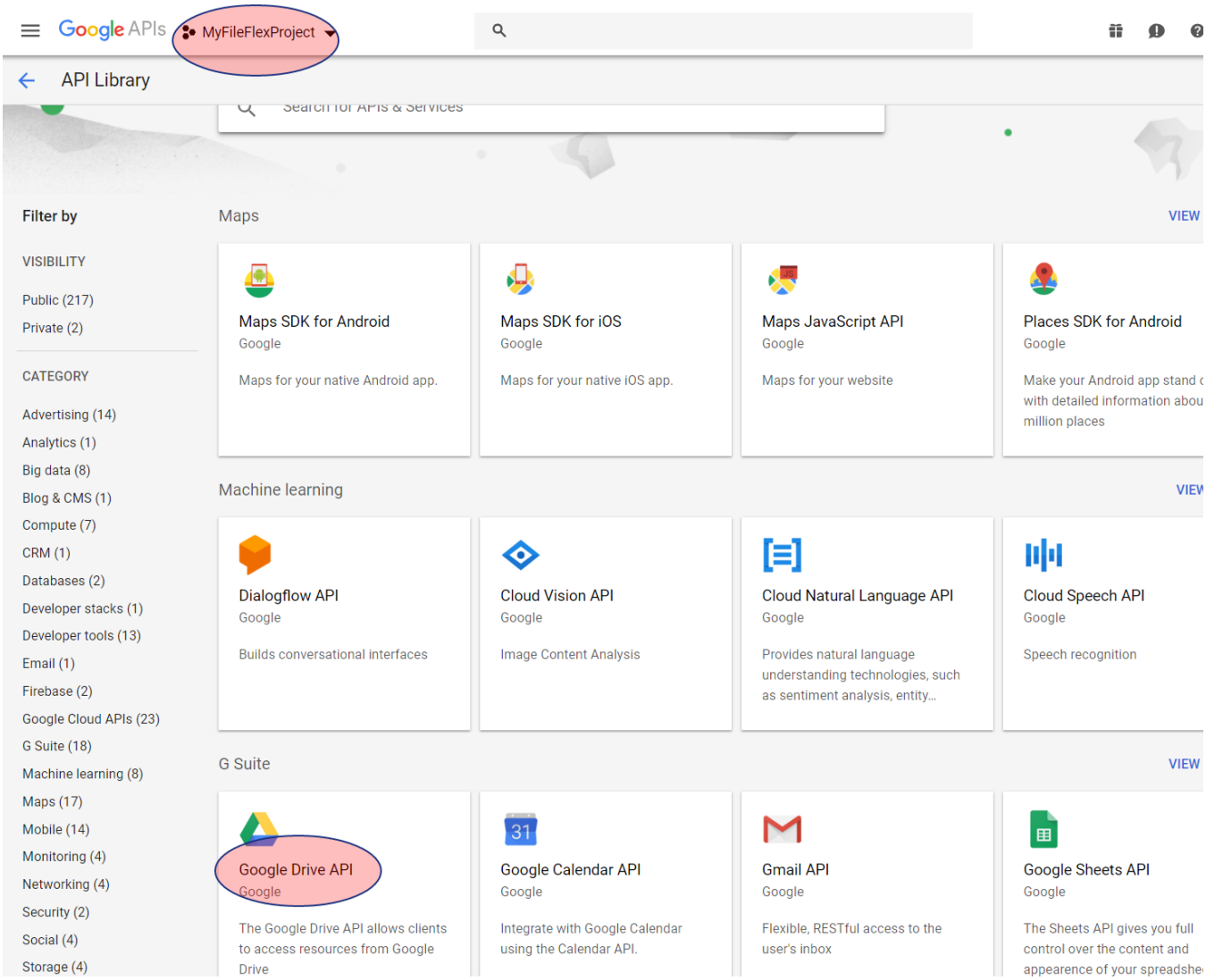
Ensure that the new project is selected by clicking on the dropdown:



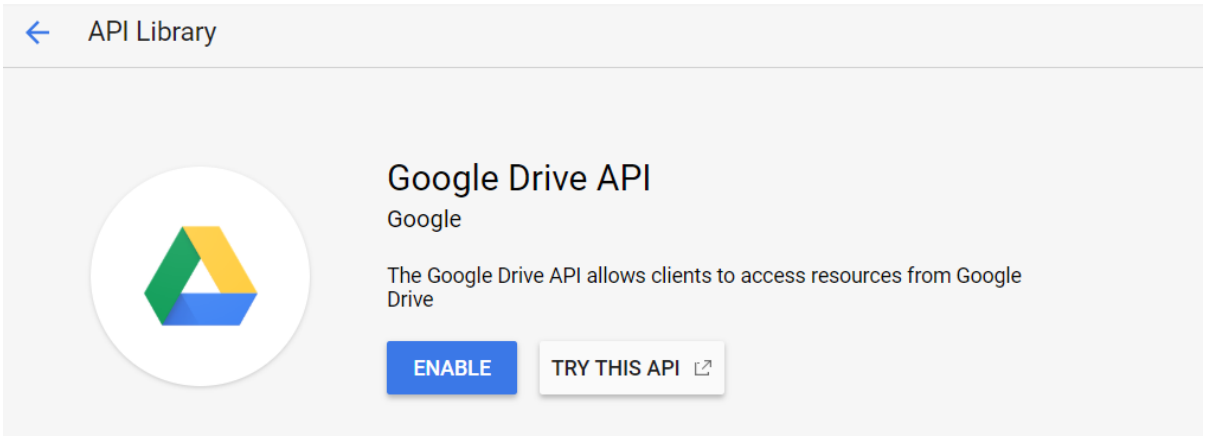
Select your project from the list:



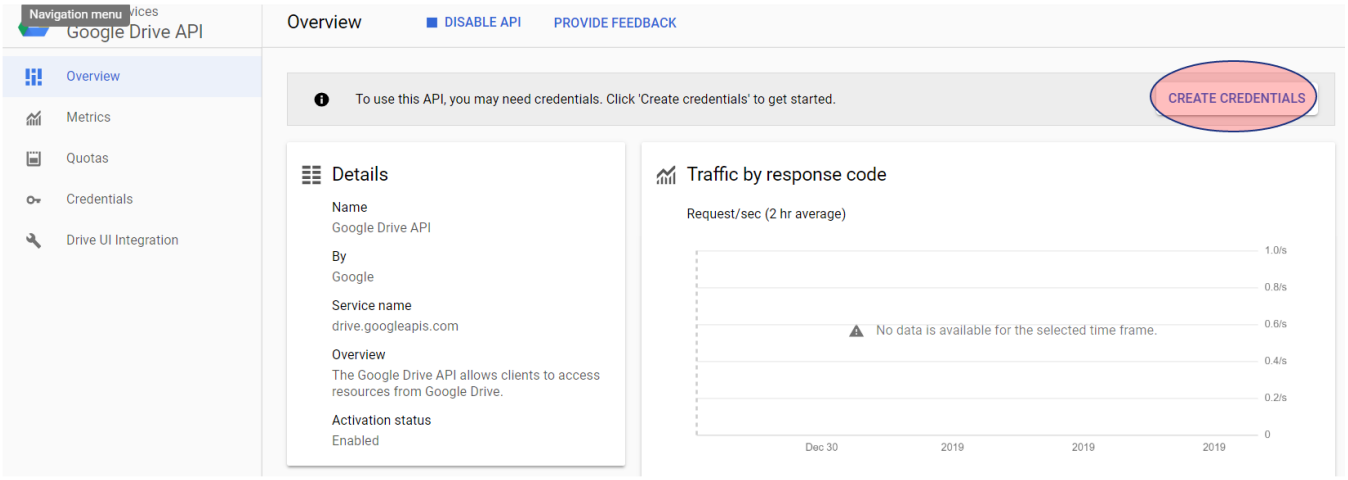
You will be returned to the API Library (with your project visible in the dropdown):



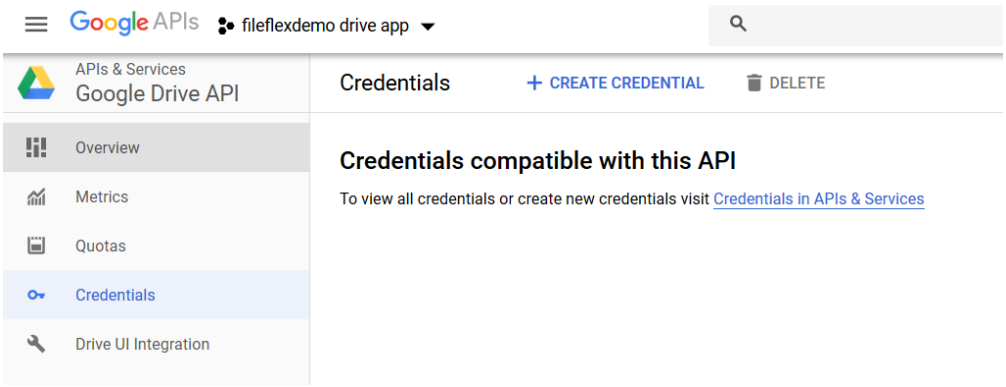
Click on "Google Drive API" and you will be presented with a screen similar to the following:



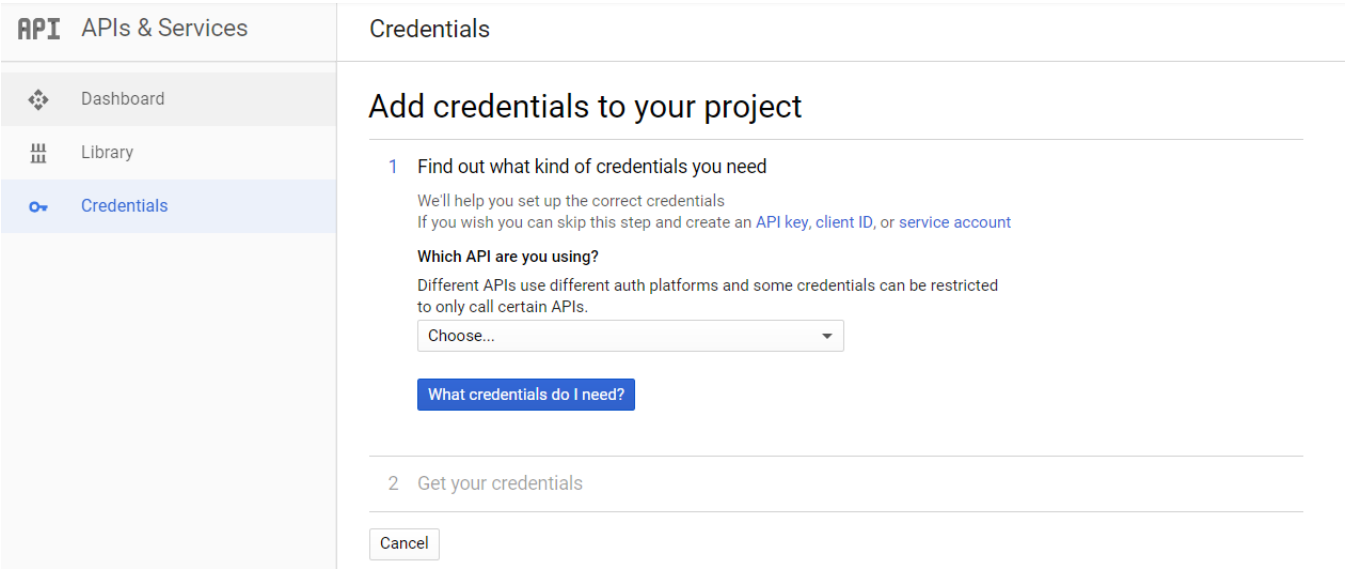
Click on 'enable' to enable the Google Drive API. You will see the following:



Click on credentials from the left hand side, and you will see a screen similar to:

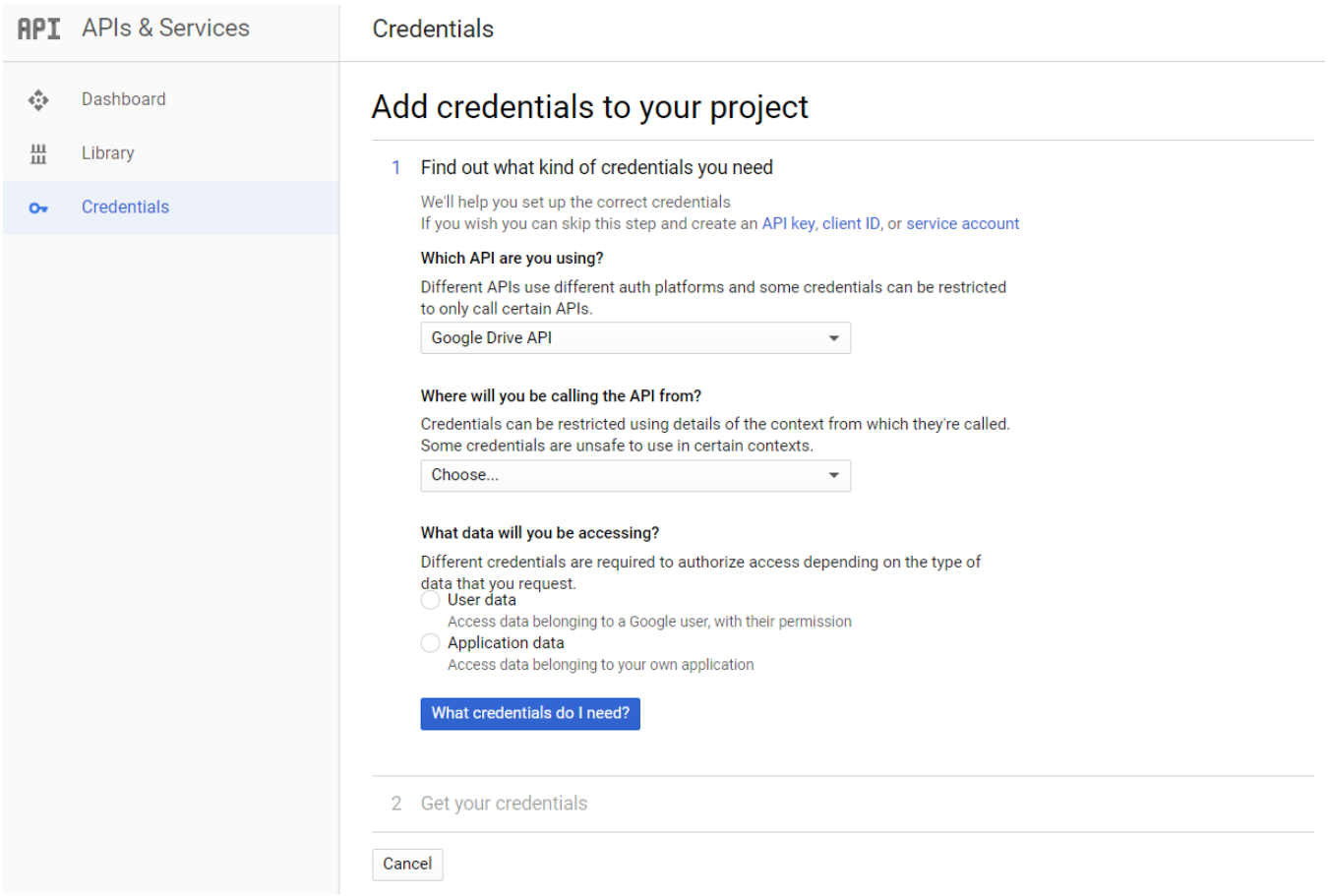


Click on "create credential" from the top to reveal the following:



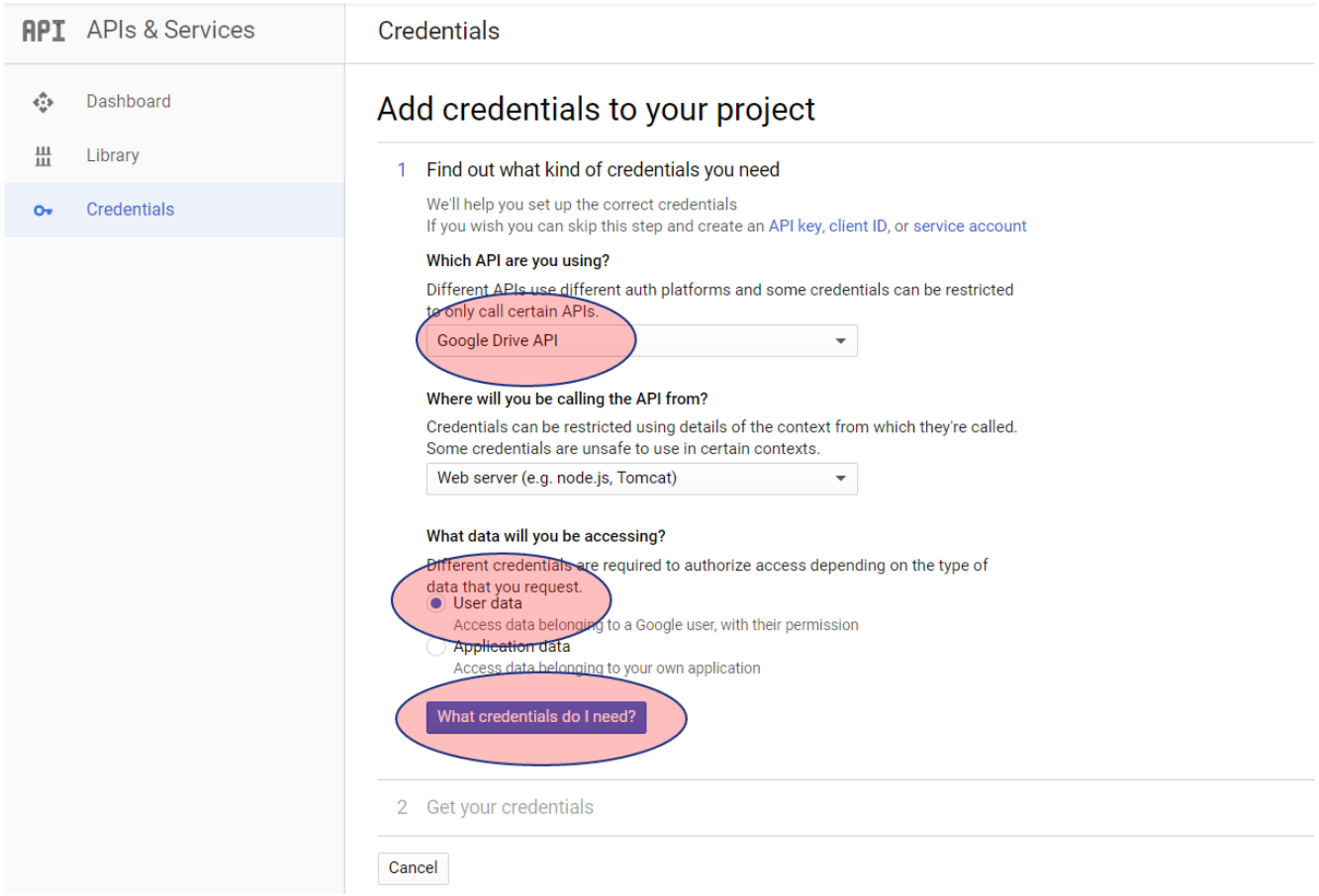
From the "Which API are you using?" dropdown, select "Google Drive API".

The dialog box will then change to the following:

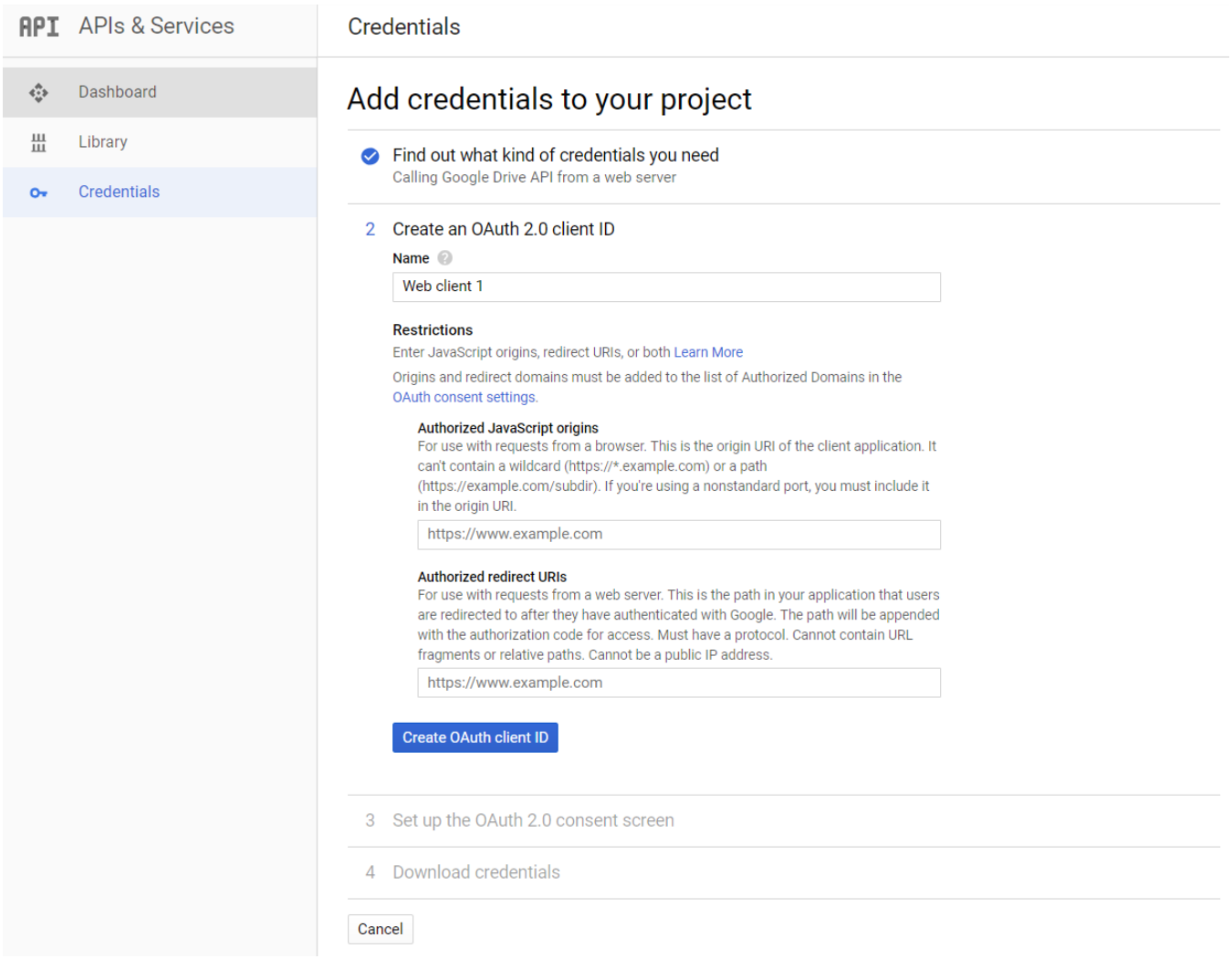


From the "Where will you be calling the API from?" dropdown, select the "Web Server" option.

From the "What data will you be accessing?" panel, select "User data". Your dialog show now look like the following:



Click on "What credentials do I need?" and the dialog will change into the following:



Enter a name for your client ID. This is not the name shown to users. In this example we are entering "MyFileFlexClientID".

Under the "Authorized JavaScript origins", you can leave the field empty.

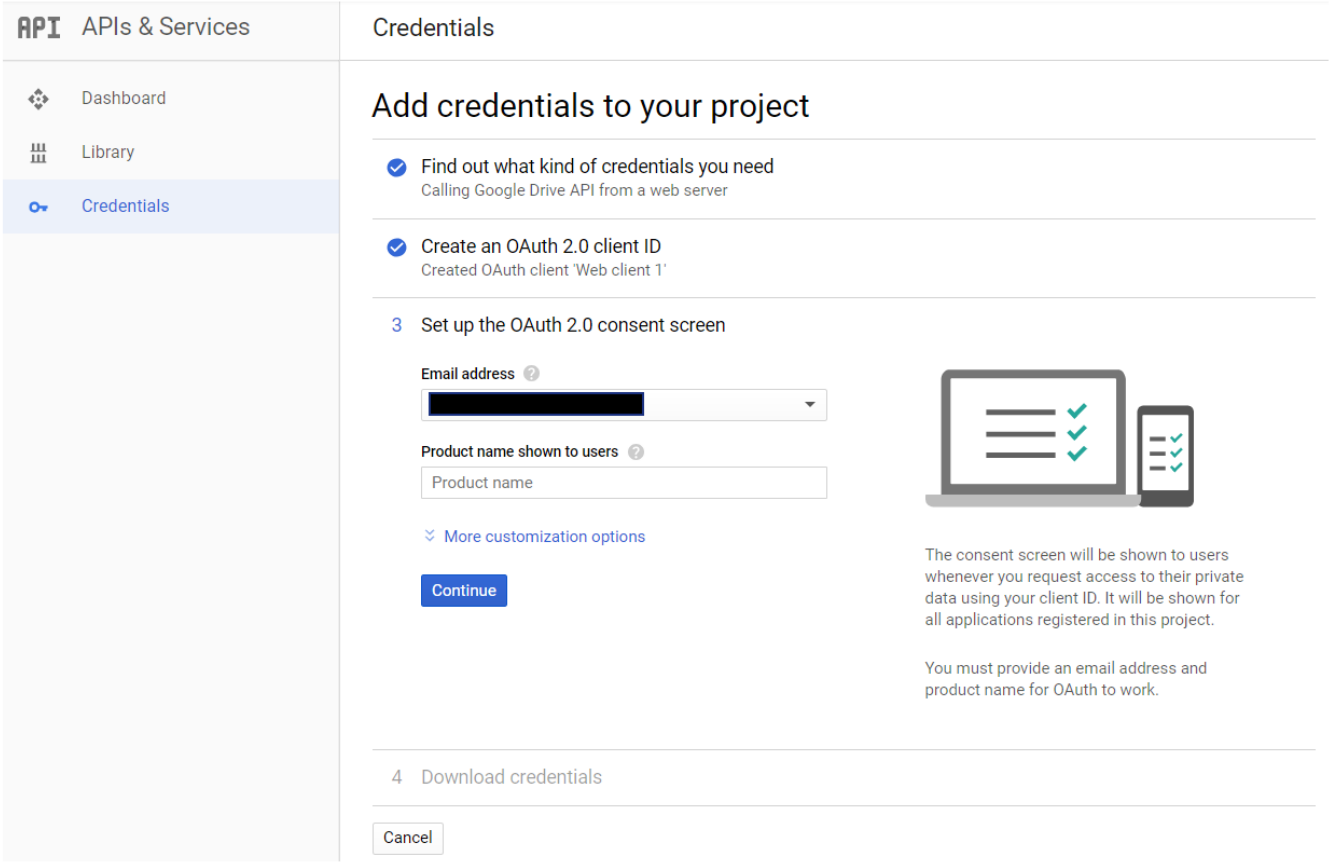
You must now enter an authorized redirect URI. That is the URI on which Google will redirect you to for authorization.

The formatting of the redirection URL is very important. Use the following format, substituting 'www.fileflexdemo.com' for your domain name:

```
https://www.fileflexdemo.com/fbweb/app/public/view/authorize_partner/google
```

Hit enter to confirm the URL entry.

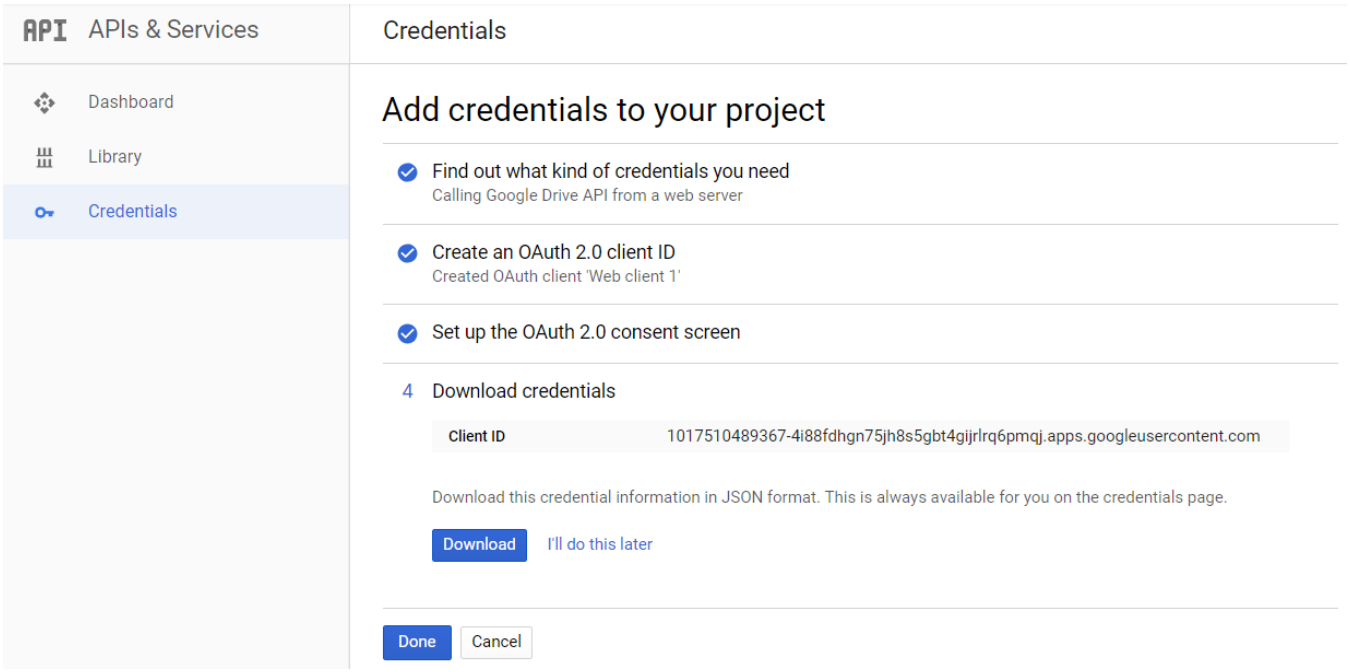
Click on "Create OAuth client ID" to proceed to the next step. The screen will change to the following:



Verify the email address associated with this project. It can be changed to the email of the signed-in user or the email of a Google Group managed by the signed-in user. Doing so is not discussed here and it's assumed that that email address used in this Google account is acceptable in this situation.

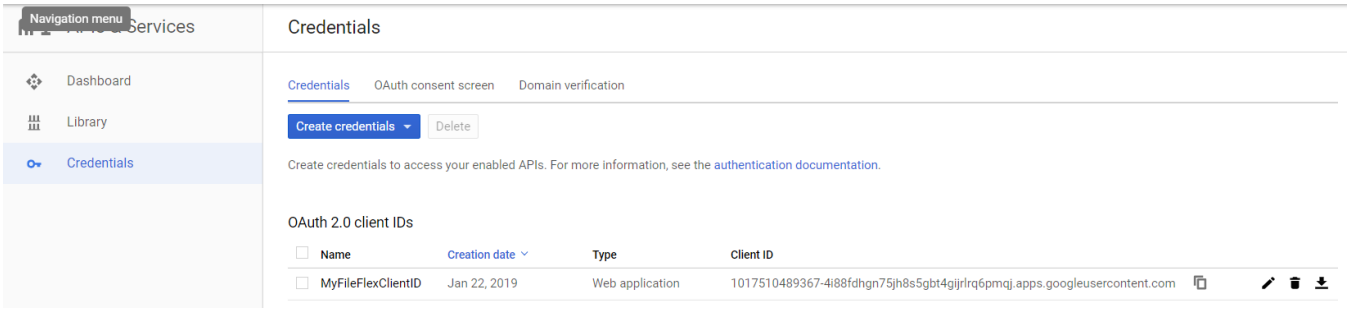
Enter a product name. Here we will enter "FileFlex Demo" in our example.

Click continue to proceed. You will be presented with the following screen:

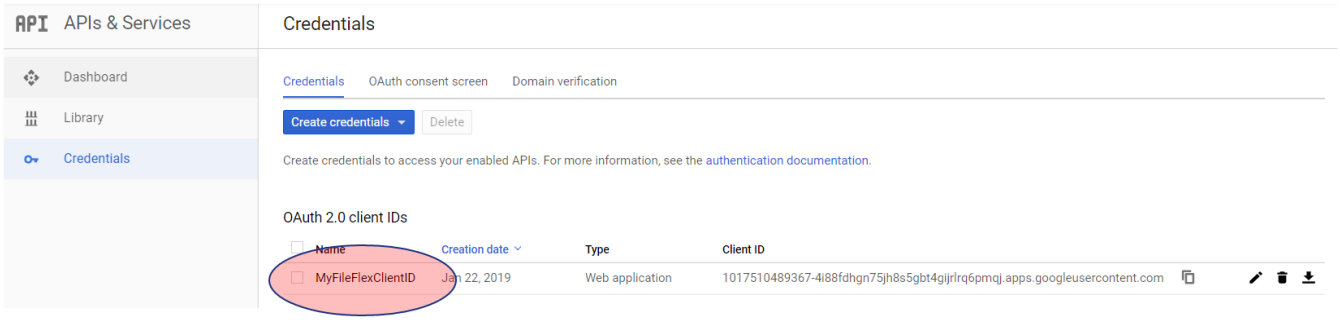


Click download to download your credentials file, and store this someplace safe.

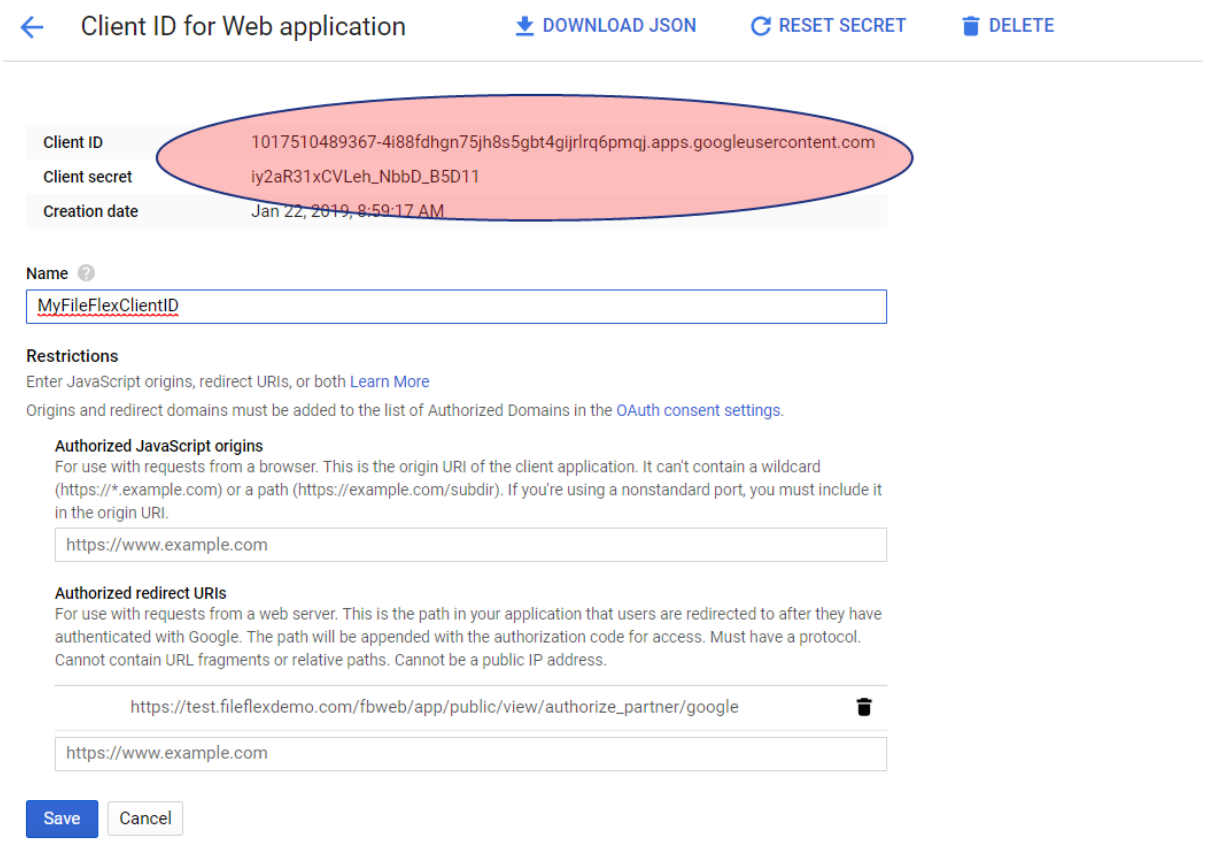
Click Done to proceed. You will be redirected to the credentials screen:



Select your OAuth 2.0 client IDs:

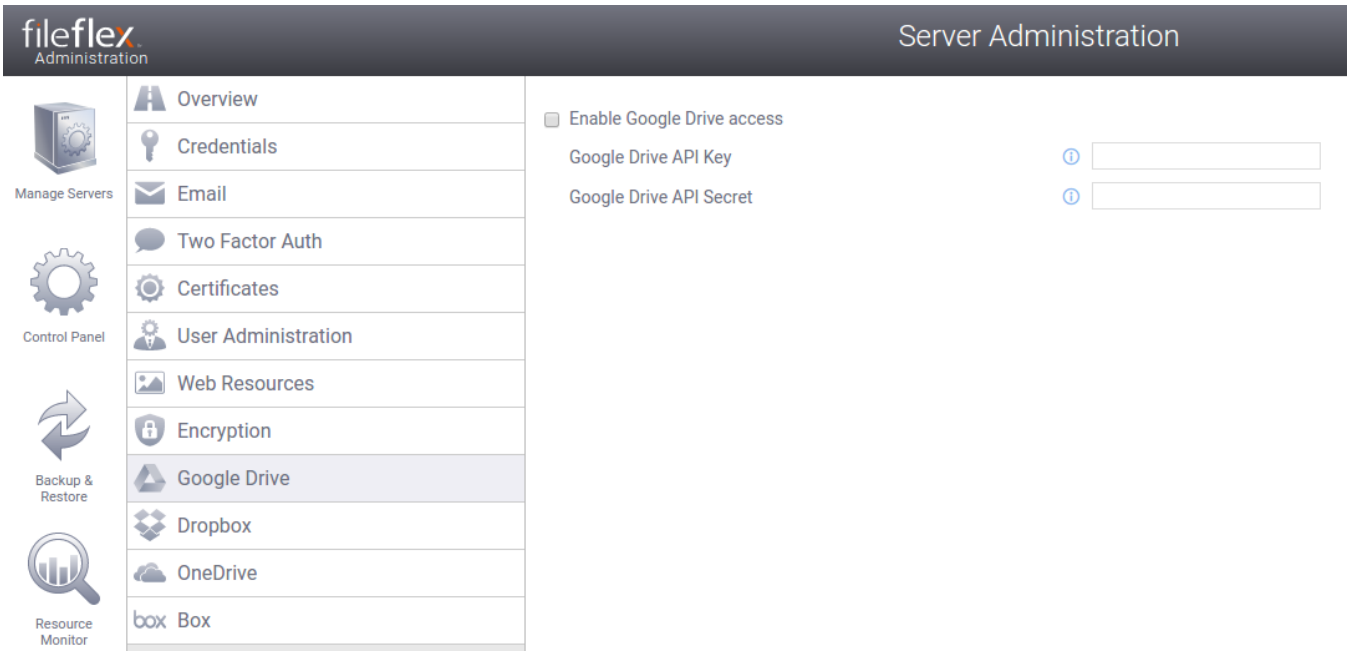


You will then see your credentials:

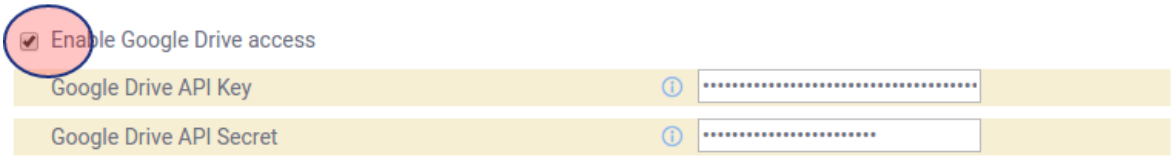


Using your clipboard (select and right click), copy the "Client ID" and "Client secret" into a temporary storage area (e.g. notepad) for use in the following steps.

The next step is to enable Google Drive from within FileFlex Server Administration. Open FileFlex Enterprise, and navigate to the "Google Drive" tab of the control panel:



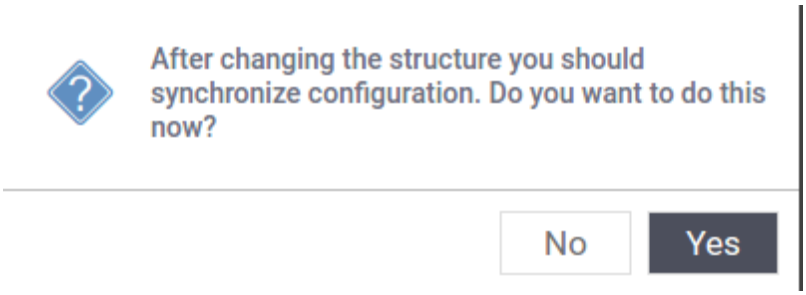
Click to enable google drive access:



You will then need to enter the API Key (Client ID) and Secret (Client Secret) provided earlier by Google.

Click the Apply button at the bottom of your screen:

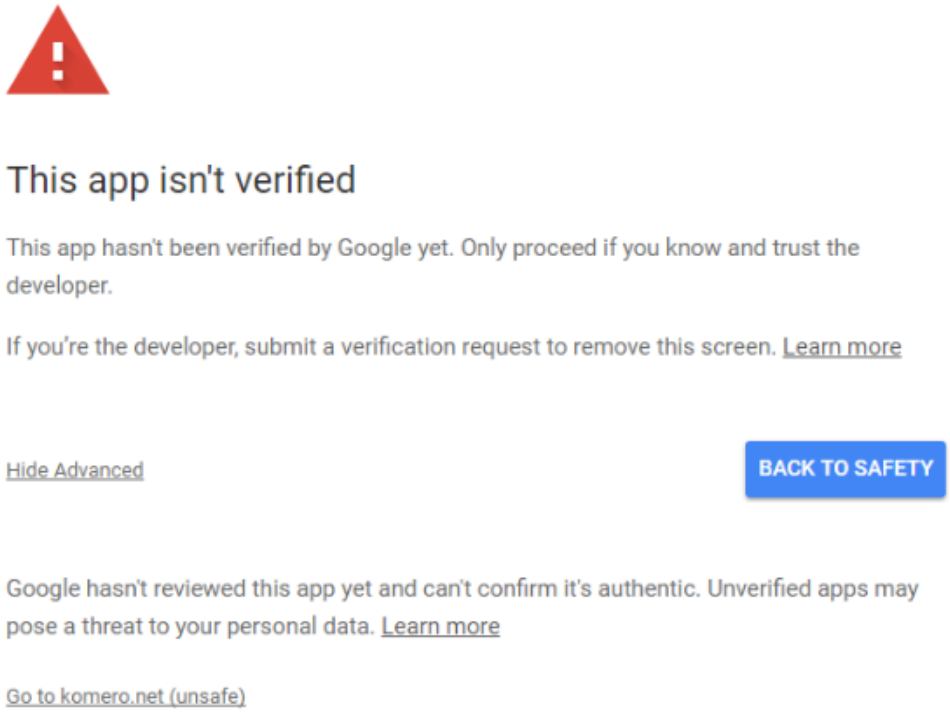
You will be presented with a confirmation to restart:



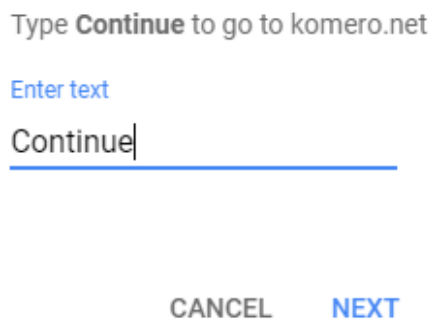
Select "Yes". Congratulations - you are now ready to start using Google Drive from within FileFlex Enterprise!

8.11.2. Unverified Applications

When using the Google Drive content source as described above, you will see a warning message similar to the following:



This warning is shown to your users because you have not yet been validated as a "developer" and must go through the developer verification steps for this domain. You may proceed by clicking on "Go to domain (unsafe)". You will then be presented with a screen similar to the following.



Enter "Continue" followed by clicking on "Next", and you may continue using the application normally. The steps that follow describe the method you must use to become a validated developer, so that your users will no longer see this warning.

> ⚠ **Temporary Verification Workaround**
>
> If you'd like to validate that your deployment works end-to-end skipping the developer verification delays, you can follow these short-term instructions.
>
> 1. Log in to Google using the account you'd like to test Drive with.
> 2. Join the 'risky access' Google Group by navigating to this link.
> 3. Click on "Join Group"
>
> This user will no longer see the warning. This temporary workaround is only useful for one user at a time!

8.11.2.1. Preparing for Application Verification

The next step is to verify the application with Google. A few preparations are needed:

1. An email address from the same domain that is used for the Google Drive application is needed. In the sample above we registered a callback URL at "https://www.fileflexdemo.com/fbweb/partner/google/authorized". This means an email at fileflexdemo.com would be needed.
2. A working and externally addressable URL for the FIleFlex solution. External access is required for the Google team to verify your application. You can later close external access if your deployment doesn't require it.
3. You must have access to the DNS records of the domain being worked with.
4. A privacy policy that is publicly accessible by HTTP at a domain related to that hosting the FileFlex solution.
    a. A generic privacy policy is supplied if you do not want to provide a custom one.
    b. It is available on your FileFlex server at (substituting your own domain name) https://fileflexdemo.com/fbweb/static/docs/privacy.txt

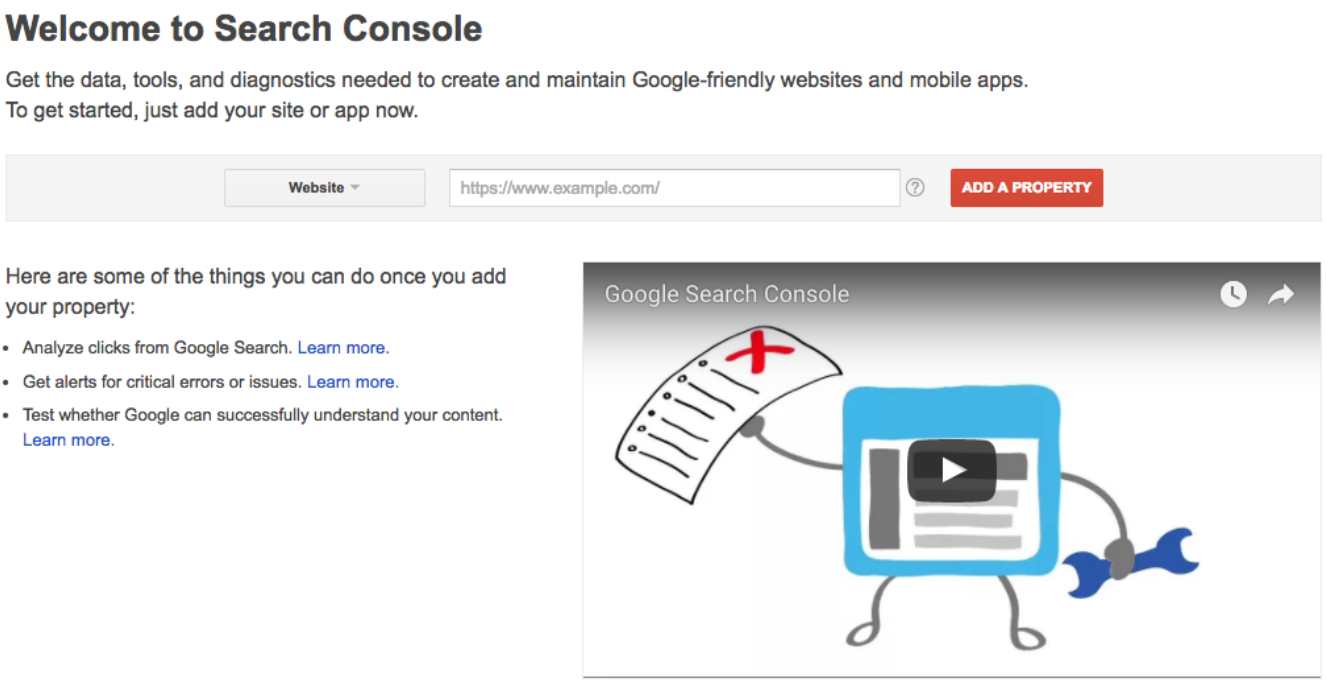
> ⚠ If you have not already done so, follow the steps in this manual under "Control Panel and Configuration / Updating Web Resources" to update your privacy policy.

8.11.2.2. Domain Verification

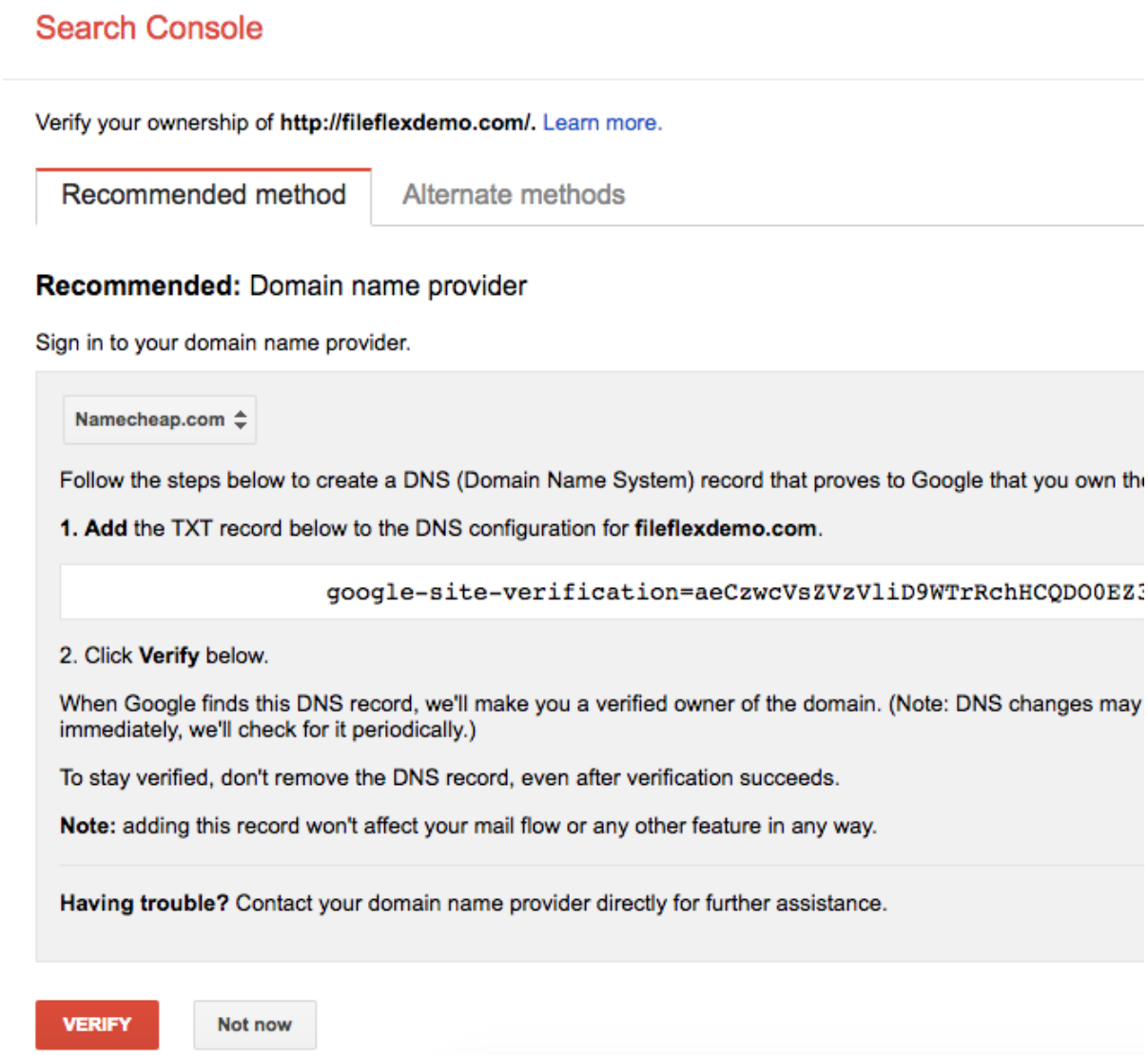
Google requires you to verify your ownership of the domain that's being used to run FileFlex Enterprise. For reference consult this link.

> ⚠ You must verify your domain with a Google account that is either a *Project Owner* or a *Project Editor* on your (Google Drive API) Project.

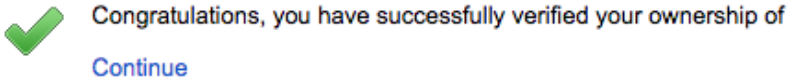
- Log in to Google using an appropriate account that is either the owner of, or an editor of, the API Project.
- Navigate to https://www.google.com/webmasters/tools/home to proceed with validation. You will be presented with a screen similar to the following:



- Enter the URL of the FileFlex Enterprise solution being deployed in the "website" field, and click "Add Property". In this case we entered "fileflexdemo.com". You will see a screen similar to the following:



- Select your DNS provider from the dropdown for instructions on how to proceed with them.
- If you host your own DNS, then select "Other" and follow the instructions there.
- You will need to add a TXT or CNAME entry to validate your domain ownership.
- Follow the instructions, and then click the "verify" button.
- Once validated you will see a screen similar to:



8.11.2.3. Proceed with Application Verification

Once your domain ownership has been validated you can proceed to application verification.

- To proceed with application verification navigate to the following URL:

```
https://support.google.com/code/contact/oauth_app_verification?authuser=0
```

- You will be presented with a screen similar to:

OAuth Developer Verification Form

To protect our users, publicly available apps that need access to certain user data must first be approved.

Who needs to fill out this form?

Submit a review request if you answer yes to all of the following:

1. You're building a web app that requires an OAuth web client or creating an AppScript add on which accesses data using
2. You are seeing the **unverified app screen** associated with your app and would like to remove it.
3. You intend to make your app **available to the public**.

Who doesn't need to fill out this form?

Don't submit a review request if either of the following applies to you:

- You'll only request OAuth tokens for your own accounts and **not from external users**.
- You're using the app to send emails through Wordpress Plugins or similar single-account SMTP usage.

You don't need to fill out this form or go through the verification process. We recommend that you continue to use your app
more details. However, if you want to remove the unverified app screen, you will need to submit your app for approval.

- Complete the contact information. For example:

Contact Info

Full name *

George Mattoge

Your phone number *

Canada (+1) 416-123-4567

Homepage URL for your app *

http://www.fileflexdemo.com

Company name *

File Flex Demo

Company website

http://www.fileflexdemo.com

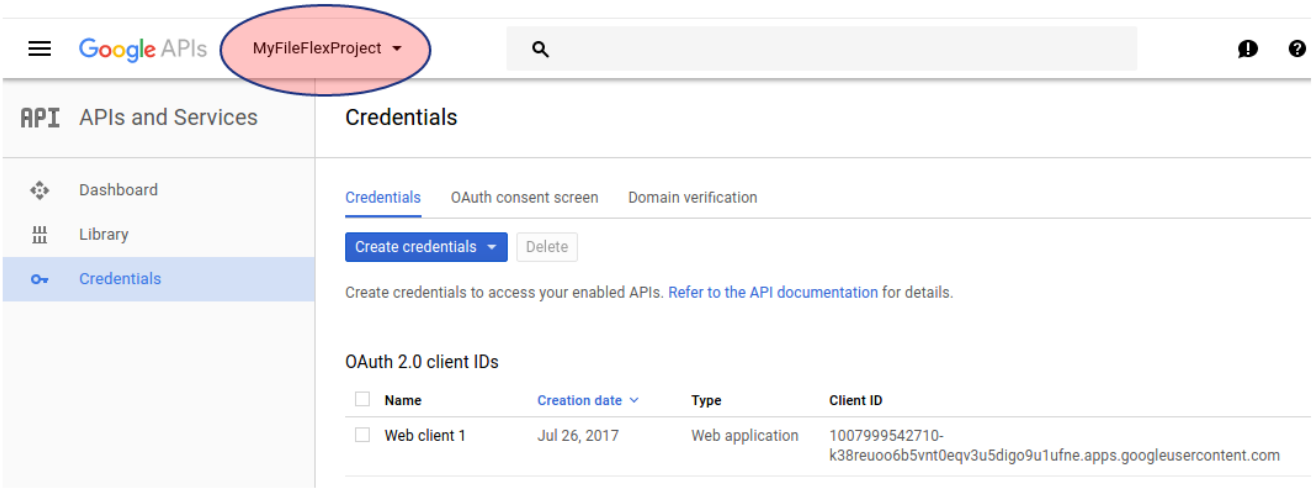
Your email address on your company domain *

george@fileflexdemo.com

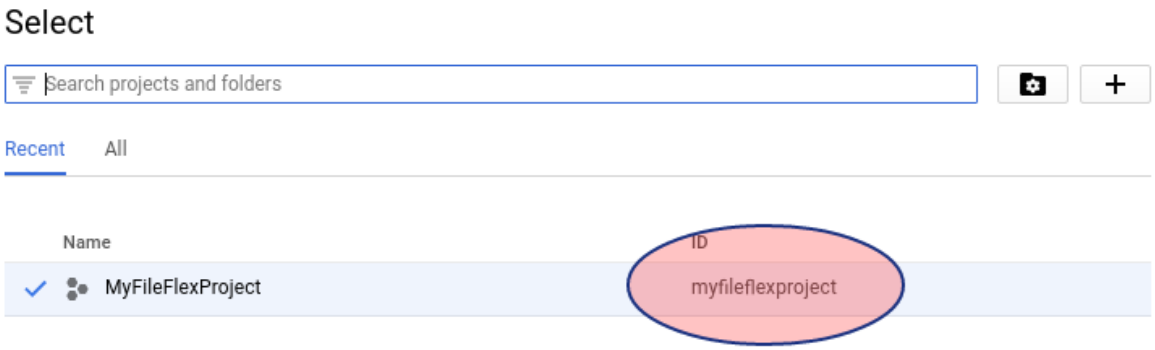
- Without closing your verification page tab, the next step is to locate your project ID for the Google Drive API. Navigate to the Google developer console:

```
https://console.developers.google.com/apis/credentials
```

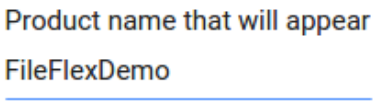
- Click on the project drop down to open the project selection dialog:



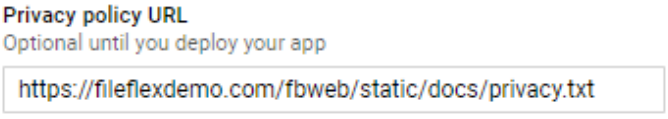
- From the dialog copy the project ID to the clipboard:



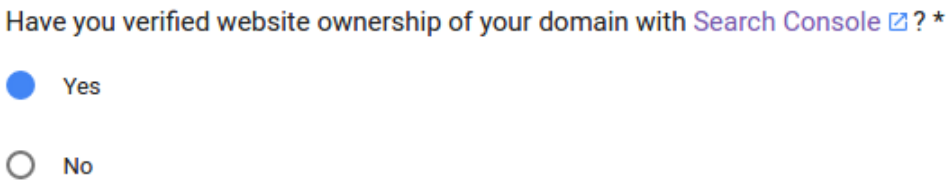
- In the verification page tab, scroll down to the product details and enter the product name:



- Enter the project ID and Client IDs which you previously retrieved:
- Enter your privacy policy URL (substitute your own domain name):

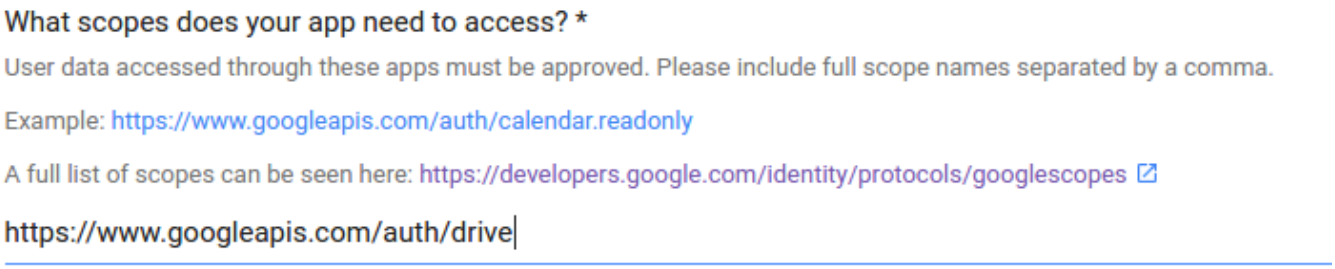


- Inform Google that you've verified your website/domain:



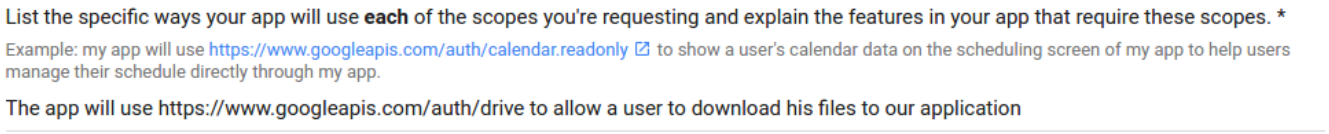
- Under the "What scope does your app need to access?" question, enter the following:

```
https://www.googleapis.com/auth/drive
```

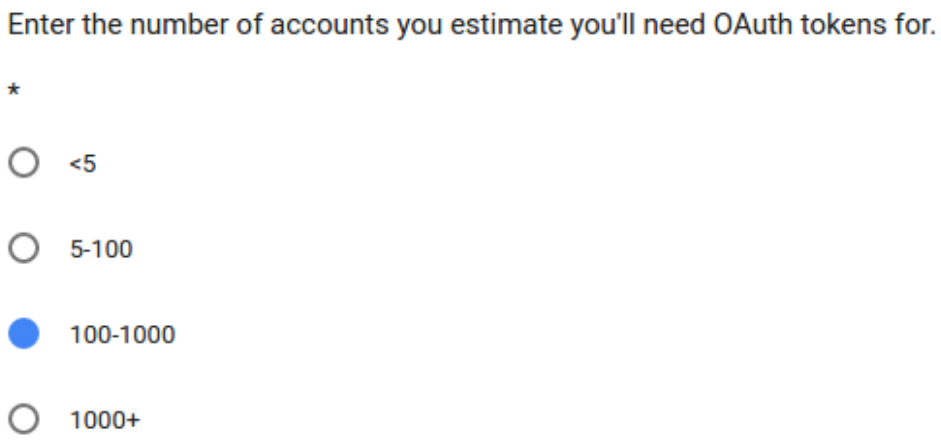


- Under the next field, requesting the ways in which your app will use the scopes, we suggest the following:

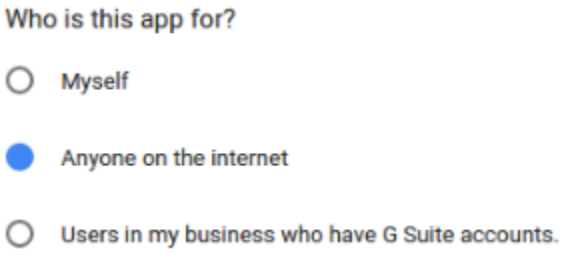
```
The app will use https://www.googleapis.com/auth/drive to allow a user to list, download and synchronize his existing Google Drive files through our application
```



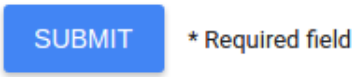
- Select the number of accounts you estimate will use the Google Drive feature within your FileFlex deployment. For example, we have selected 100-1000 in this case:



- Inform Google that this app is for anybody on the internet (unless this is false):



- You can skip the question asking you if you are a play store developer.
- You can skip the question asking if there is any other information that would be useful.
- When you've finished, click the submit button:



- You will be presented with a screen informing you it takes between 3 and 7 business days for them to review the application.

Thank you for submitting the verification request. A member of our team will review your submission and get back to you as soon as possible. This typically takes between 3 and 7 business days, but in some cases it may take longer.

In the meantime, you can continue to test your application with the unverified app screen intact. Please note that the unverified app screen will disappear only after the verification process is complete.

Sincerely,

Google Cloud Platform/API Trust & Safety

8.12. Configure Microsoft OneDrive Access

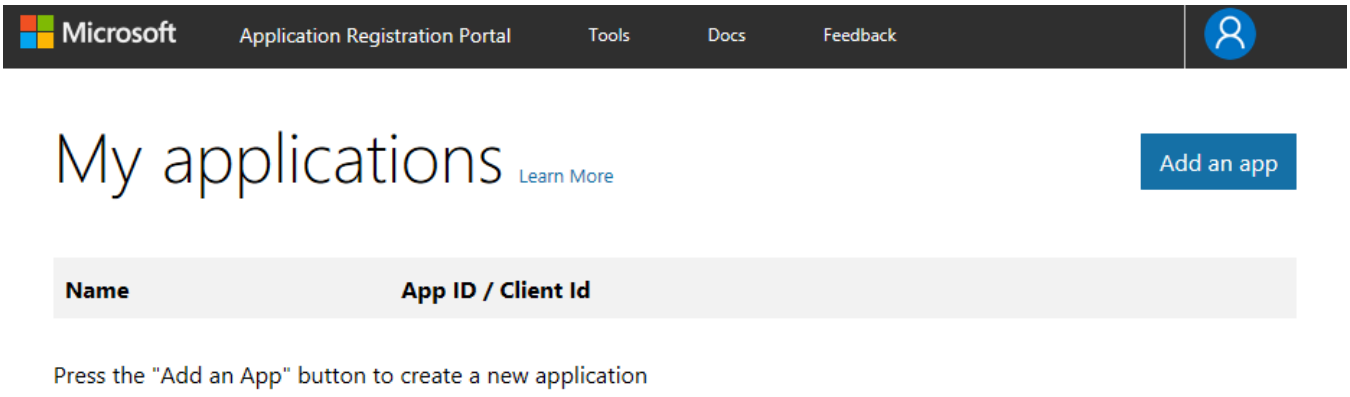
8.12.1. Registering for Microsoft OneDrive API Credentials

⚠ It's important to complete the "Supplying an SSL Certificate" steps prior to configuring OneDrive Access.

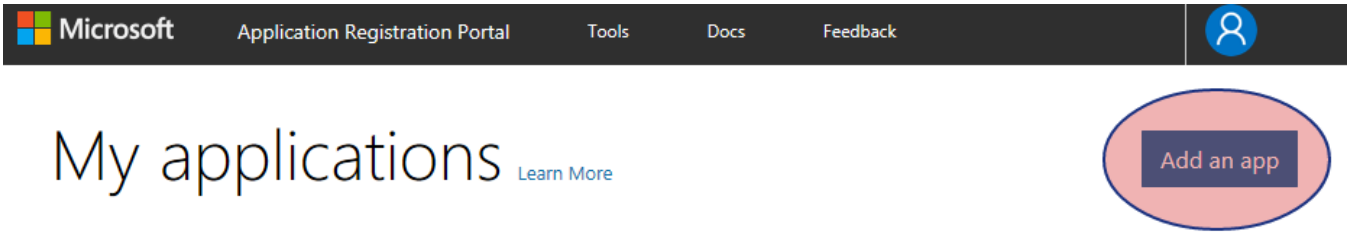
In order to configure OneDrive access from within FileFlex Enterprise, you must obtain a OneDrive Key and Secret from Microsoft. Sign in to your Microsoft Live account, and navigate to the following Microsoft URL which is used to configure their APIs:

```
https://apps.dev.microsoft.com
```

You will be presented with a screen similar to the following:

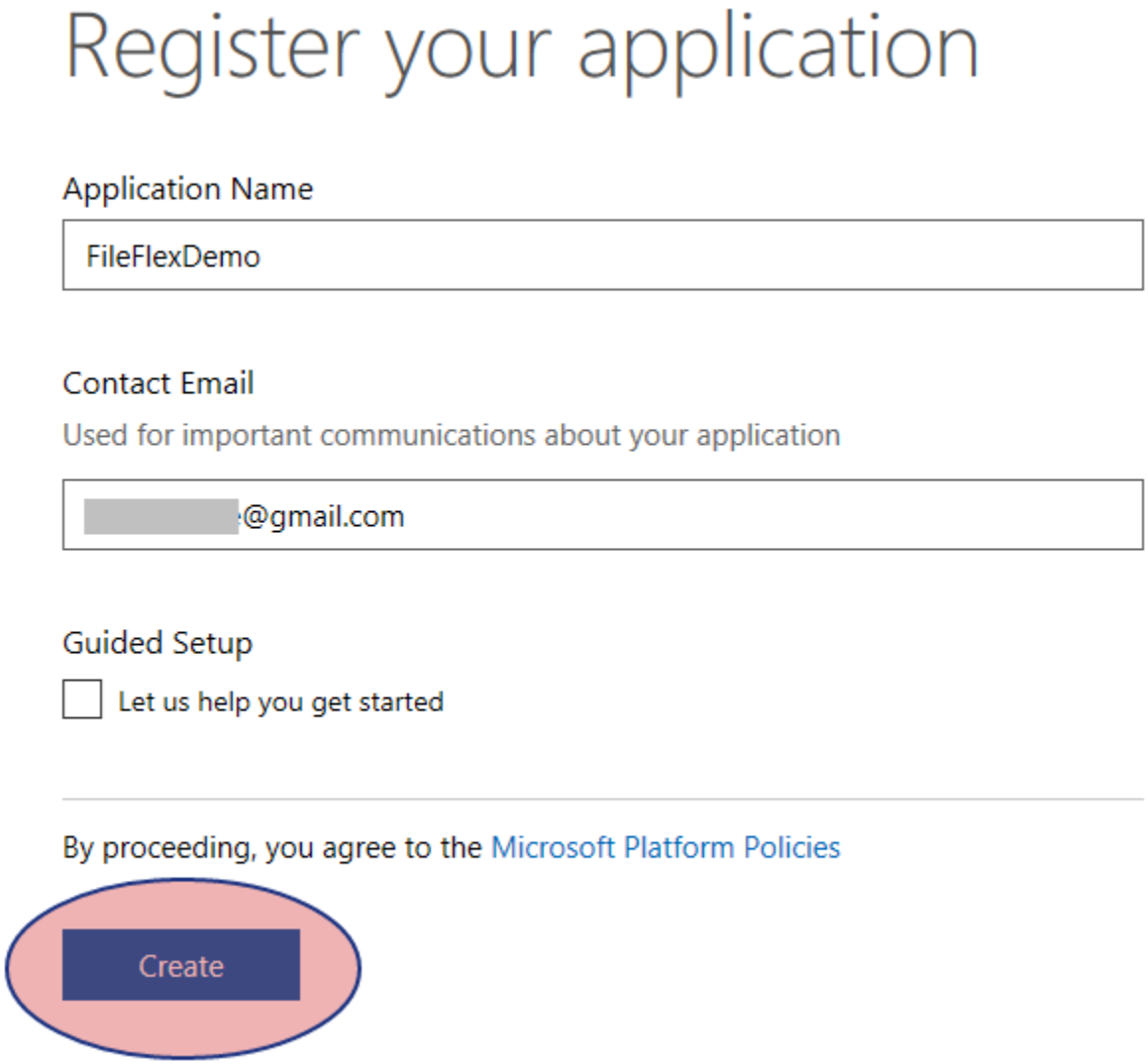


First you must create a project by clicking on the "Add an app" button:



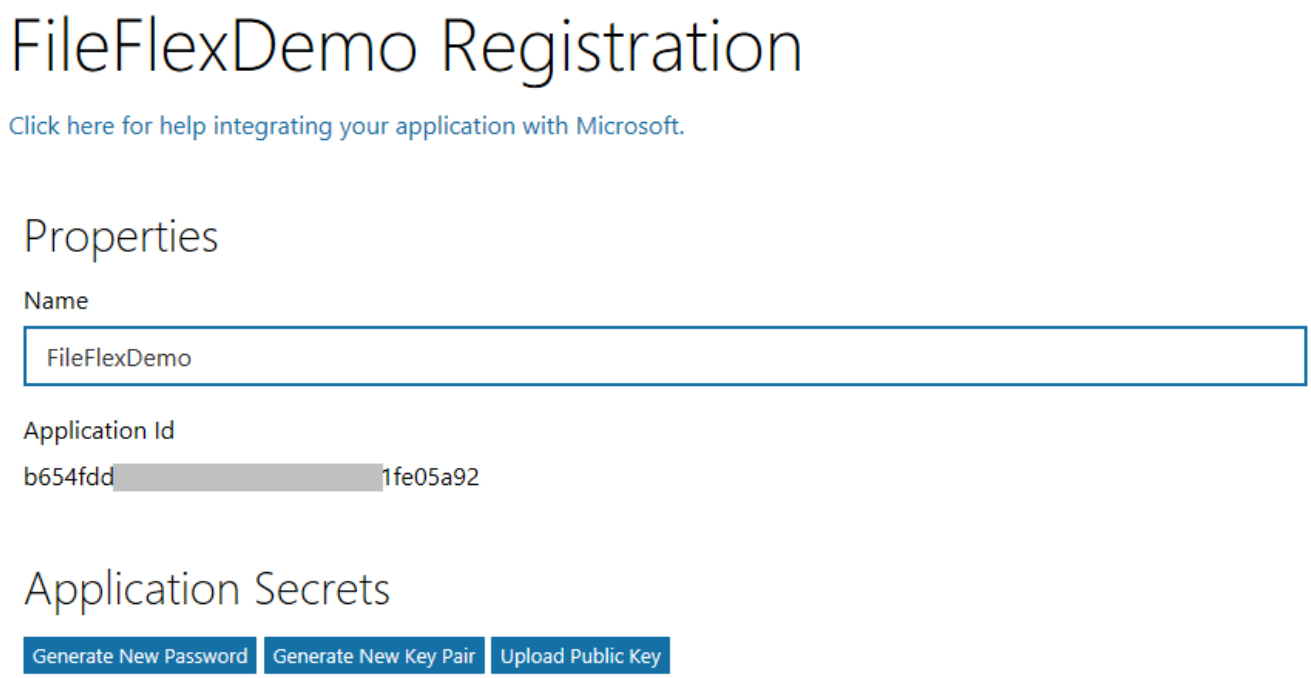
You will be presented with an application registration screen.

Enter your application name (FileFlexDemo in this example), and your contact email address for important communications:

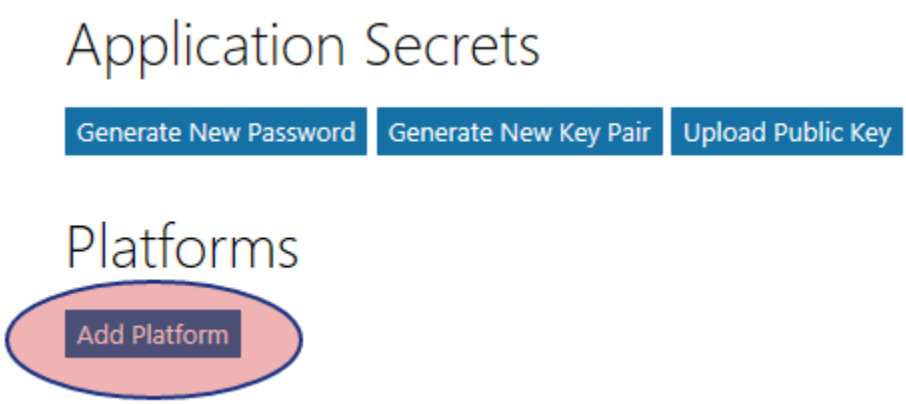


Ensure that the "guided setup" checkbox is **not** selected, and then click the 'create' button.

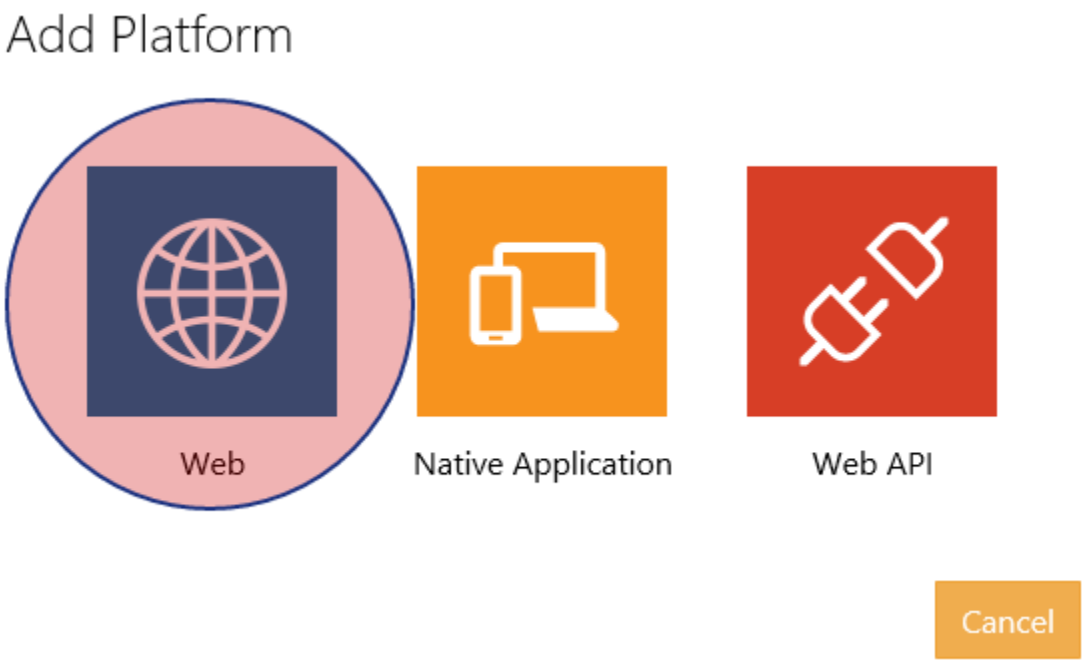
You will then be presented with the application registration screen:



Scroll down and click on "Add Platform":



From the dialog that pops up, select "web":



A new "web" section is added under the "Platforms" heading.

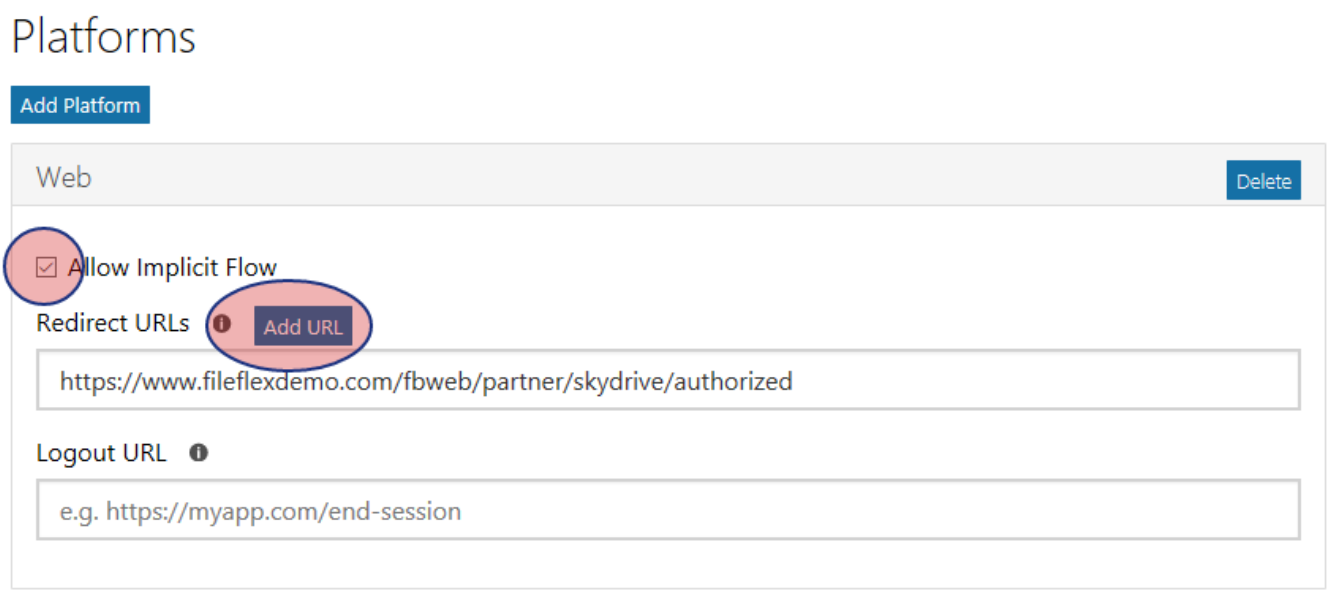
The formatting of the redirection URL (which is how OneDrive sends users back to FileFlex) is very important. Use the following format, substituting 'www.fileflexdemo.com' for your domain name:

```
https://www.fileflexdemo.com/fbweb/app/public/view/authorize_partner/skydrive
```

> **SkyDrive vs OneDrive**
>
> It's important the the redirect URL include the "skydrive" URL segment, which is a legacy name for Microsoft's OneDrive product

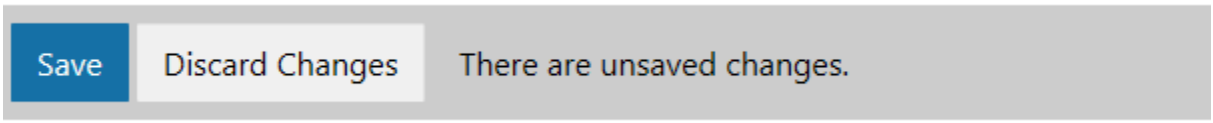
Enter the redirect URL using the example provided above.

Ensure that the "Implicit" flow option is selected, and then click on "Add URL":

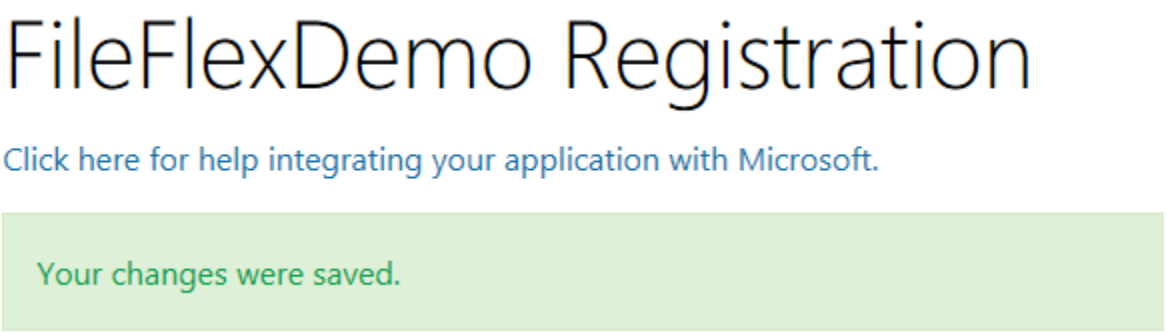


Scroll down to the "Profile" section and enter your application host name under "Home page URL":

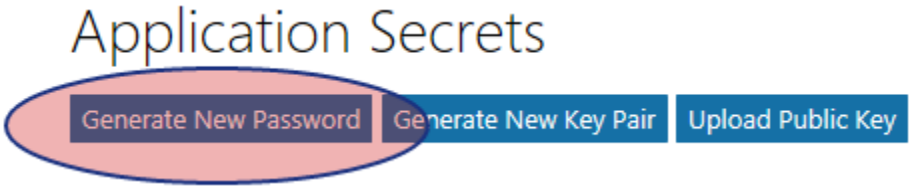
Scroll down to the end of the page, and click "save":



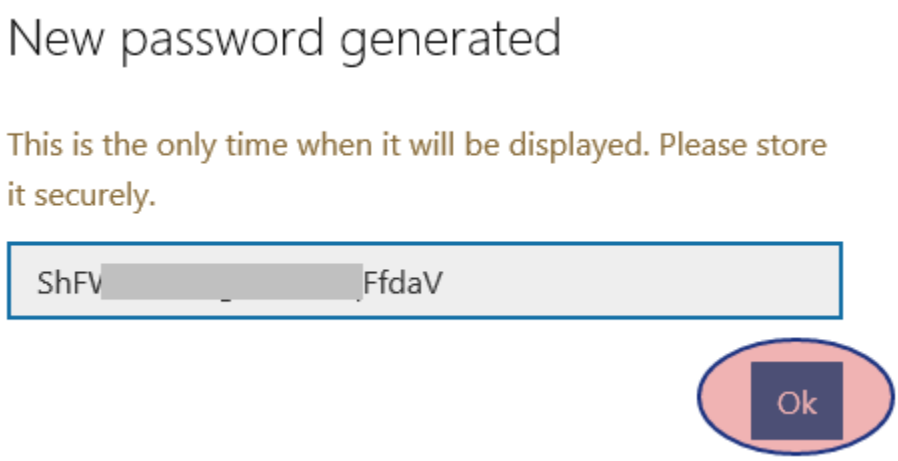
You will see a confirmation that your changes were saved:



Under "Application Secrets", click on "Generate New Password":

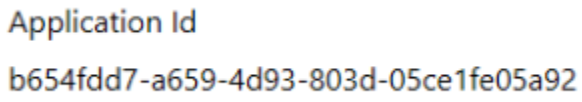


A dialog box will be shown showing you your application password. It will not be shown again, so ensure you copy it to your clipboard and store it somewhere temporarily:

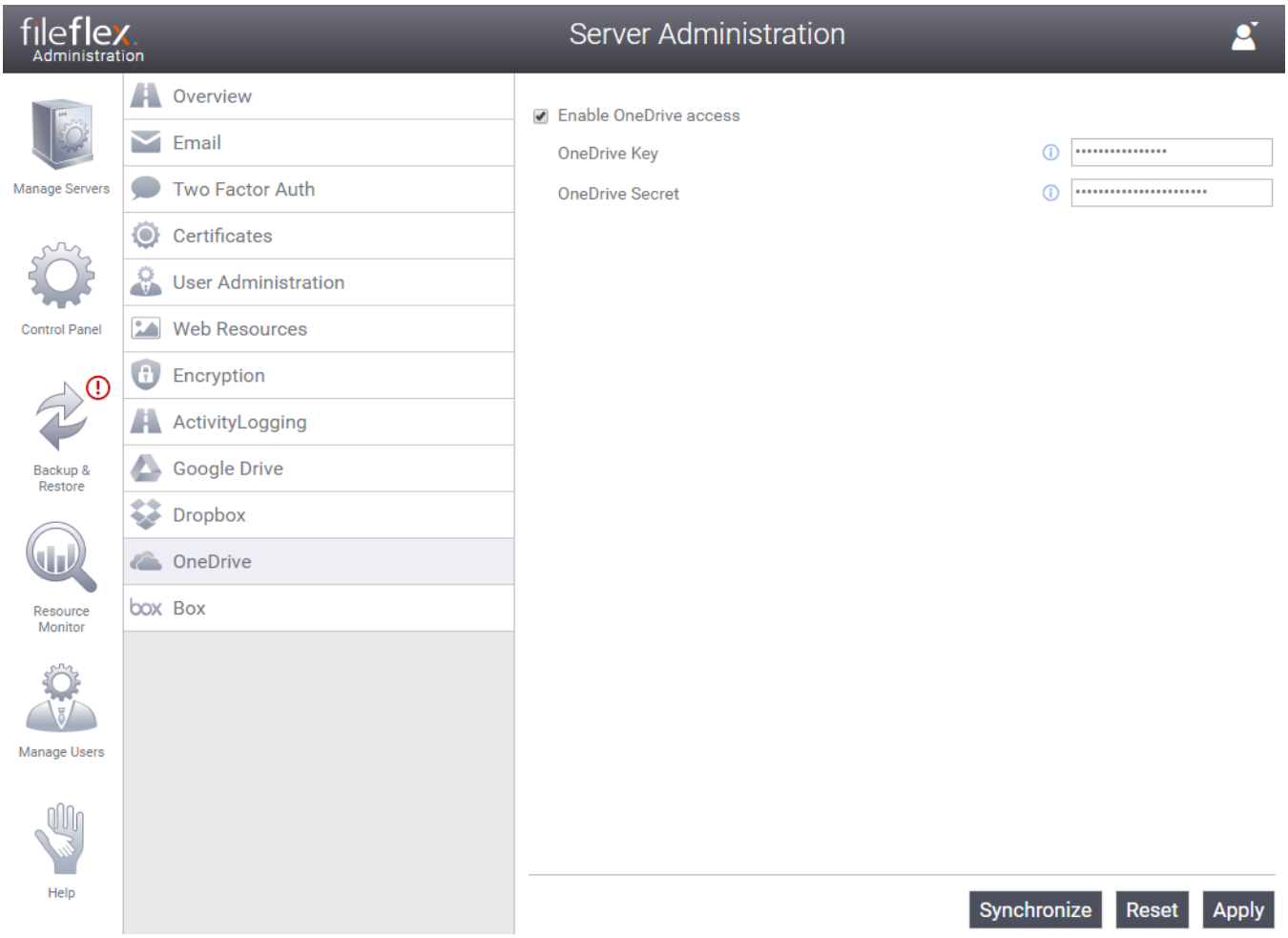


Click the OK button to close the dialog.

Near the top under "Properties" locate the "Application Id" and copy if to your clipboard to store it somewhere temporarily:



Open FileFlex Enterprise, and navigate to the "OneDrive" tab of the control panel:

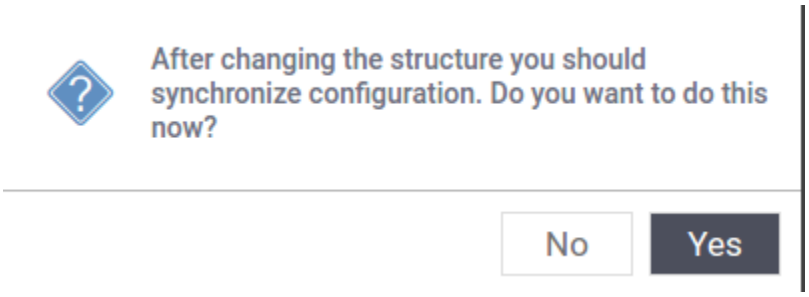


Enable the checkbox to enable OneDrive access:

- In the "OneDrive Key" field, enter the "Application Id" located earlier.
- In the "OneDrive Secret" field, enter the password located earlier.

Click the Apply button at the bottom of your screen:

You will be presented with a confirmation to restart:



Select "yes". Congrulations - you are now ready to start using OneDrive from within FileFlex Enterprise!

8.13. Configure DropBox Access

8.13.1. Registering for DropBox API Credentials

> ⚠ It's important to complete the "Supplying an SSL Certificate" steps prior to configuring DropBox Drive Access.

In order to configure DropBox access from within FileFlex Enterprise, you must obtain a DropBox App Key and App Secret from Dropbox. Sign in to your Dropbox account, and navigate to the following URL which is used to configure their APIs:

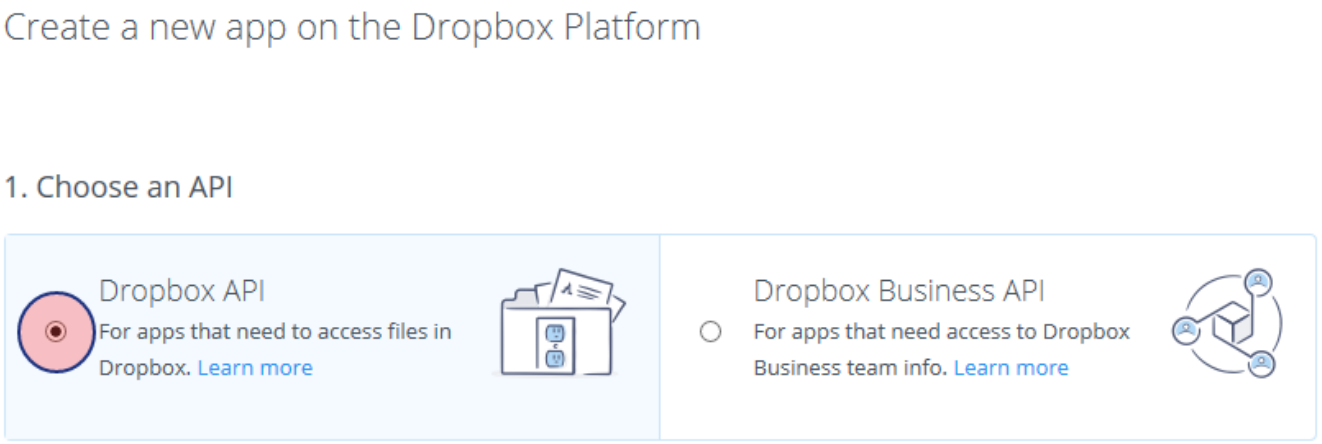
```
https://www.dropbox.com/developers/apps
```

You will be presented with a screen similar to the following:

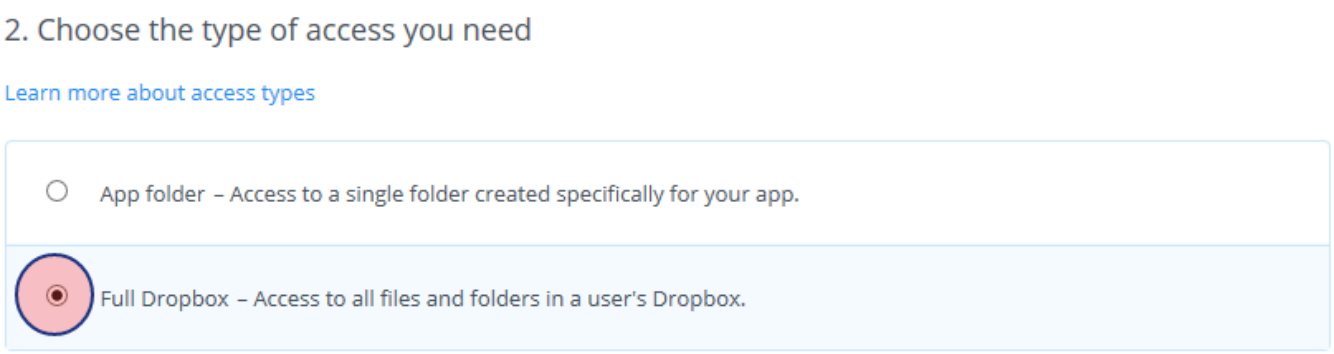
First you must create a project by clicking on the "Create app" button:

You will be presented with an application creation screen.

The first step is to select your API type.



Choose "Dropbox API" as indicated above. You will then be prompted to select the access you need:

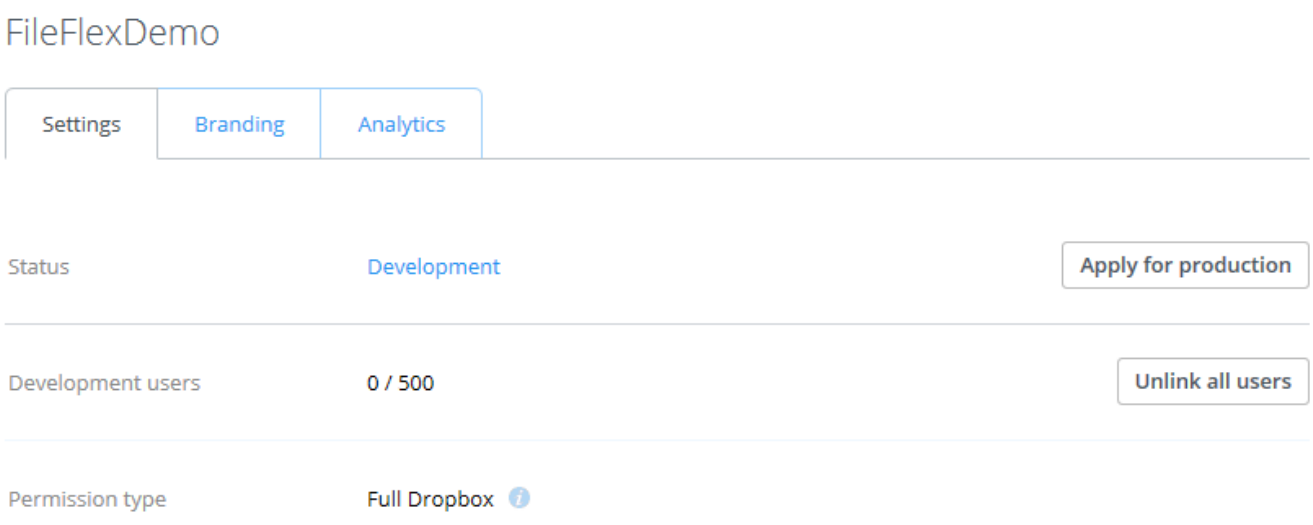


Select "Full Dropbox" from the list. You will then be asked for your app name:

Enter your app name ("FileFlexDemo" in this case).

Select the box to agree to the Dropbox API terms.

Finally, click on the "Create app" button. You will be presented with a success message, and the primary application settings screen; similar to the following:

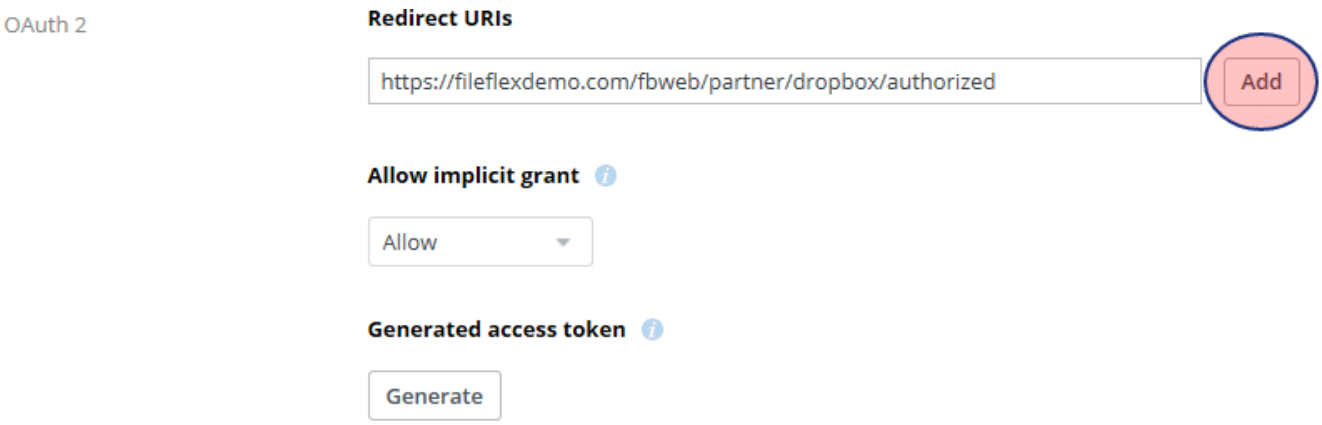


Following this section are your application credentials:

Click on "show" to reveal your app secret. The app secret will then be revealed:

Write down both values temporarily for later entry into FileFlex.

Scroll down to the "OAuth 2" section:



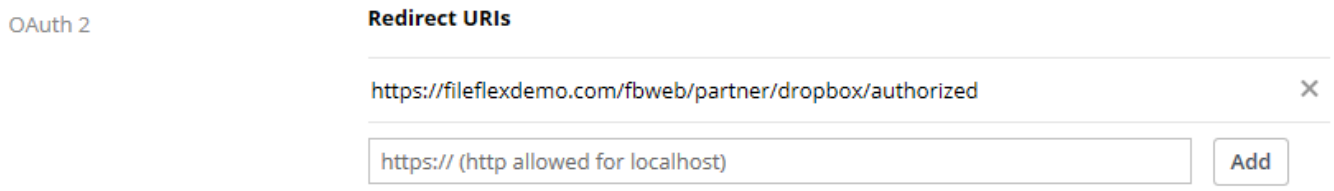
The formatting of the redirection URL (which is how DropBox sends users back to FileFlex) is very important. Use the following format, substituting 'fileflexdemo.com' for your domain name:

```
https://fileflexdemo.com/fbweb/app/public/view/authorize_partner/dropbox
```

Enter the redirect URL using the example provided above.

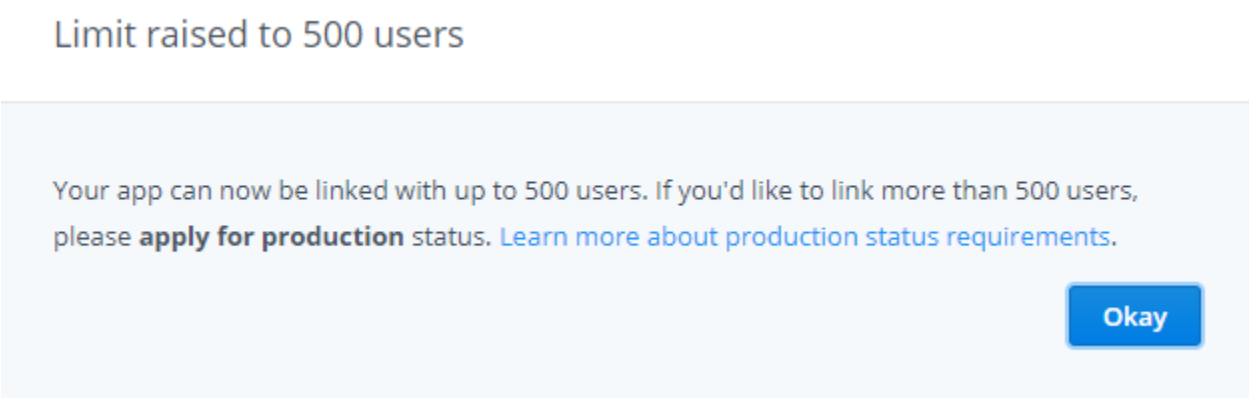
Ensure that the "Implicit" grant option is selected, and then click the 'add' button.

You will then see your new URL listed:



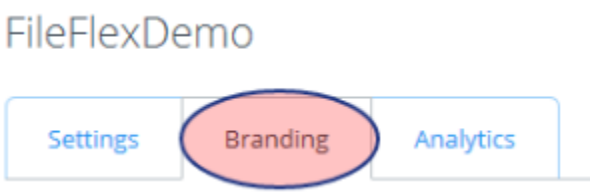
Near the top locate the "Development users" section and change it from "Only you" to the 500 users you're allowed while testing:

Click on "Enable additional users" and you will be presented with the following confirmation dialog:

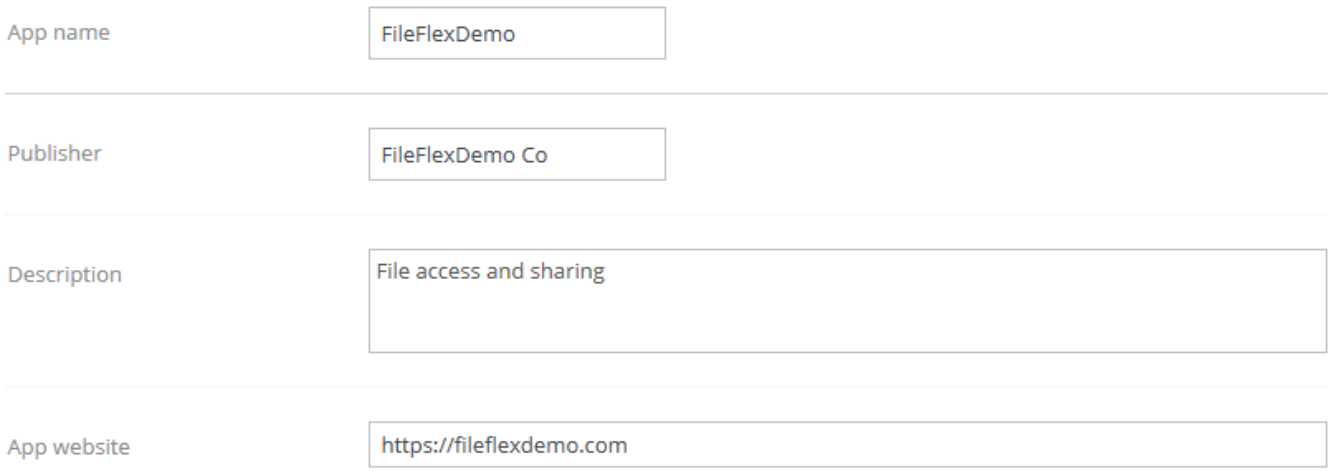


Click "Okay". You should now see that 500 users are allowable:

Click on the "branding" tab at the top:



You will be presented with a screen in which you will enter your application and company information:



Your app name will already have been entered.

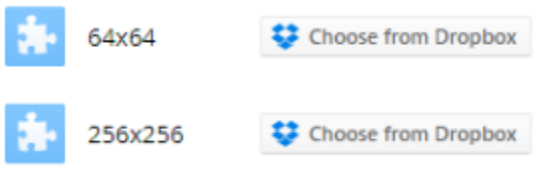
Enter your company name under publisher.

Enter a description. A suggestion is: "File access and sharing".

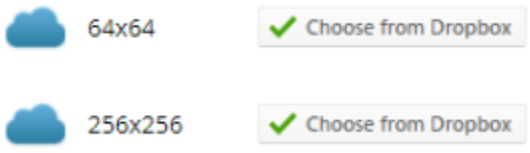
Enter your application host name as a URL under "App website". As an example:

```
https://fileflexdemo.com
```

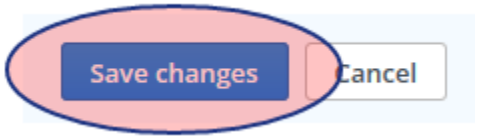
You must then supply a branding icon if you wish to apply for production:



Click on "Choose from Dropbox" and upload an icon for the application. You should provide a 64x64 and 256x256 variant, though DropBox will rescale a larger image down to the smaller size on your behalf automatically. Once complete you will see your icon as follows:

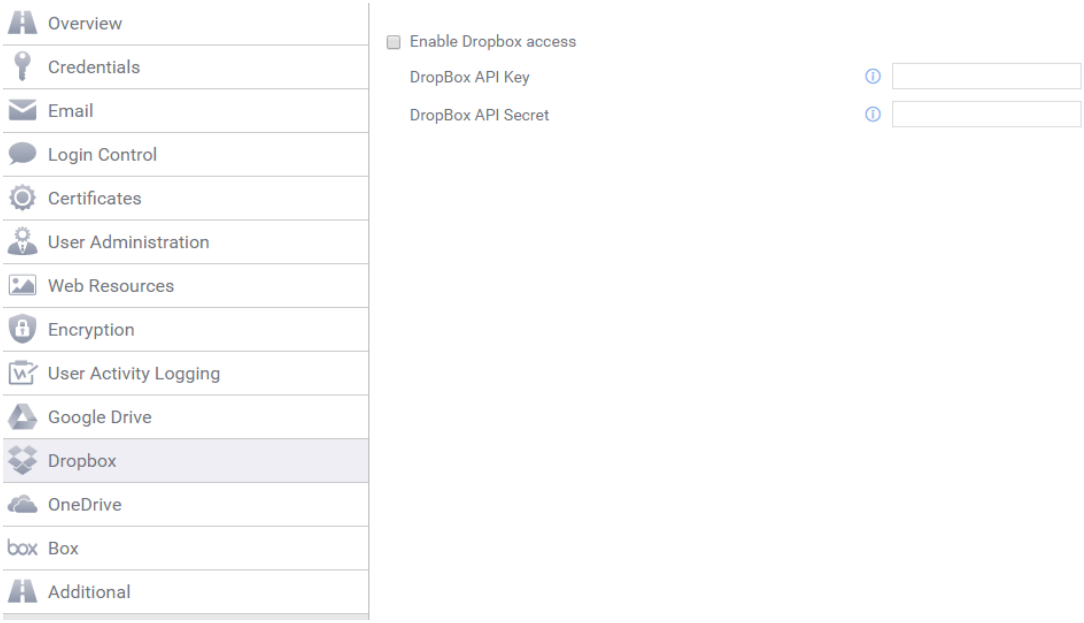


Scroll down to the end of the page and click on "save changes".



Congratulations - you are now ready to start using Dropbox from within FileFlex Enterprise!

Open FileFlex Enterprise, and navigate to the "Dropbox" tab of the control panel:



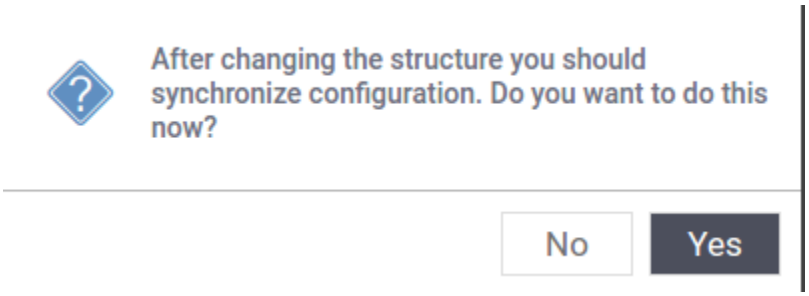
Click to enable Dropbox access:

8.13.1.1.

You will then need to enter the API Key and Secret provided earlier by Dropbox.

Click the Apply button at the bottom of your screen:

You will be presented with a confirmation to restart:



Select "Yes". Congratulations - you are now ready to start using Dropbox from within FileFlex Enterprise!

8.13.1.2. Proceeding with a Production Request

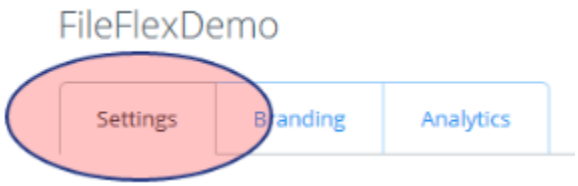
Application Testing

You still have a 500 user limit at this point until you apply for production status. Prior to being allowed to apply for production, you must have tested your application with at least one user! If you do not need more than 500 DropBox users on your system, it is not mandatory to apply for production.

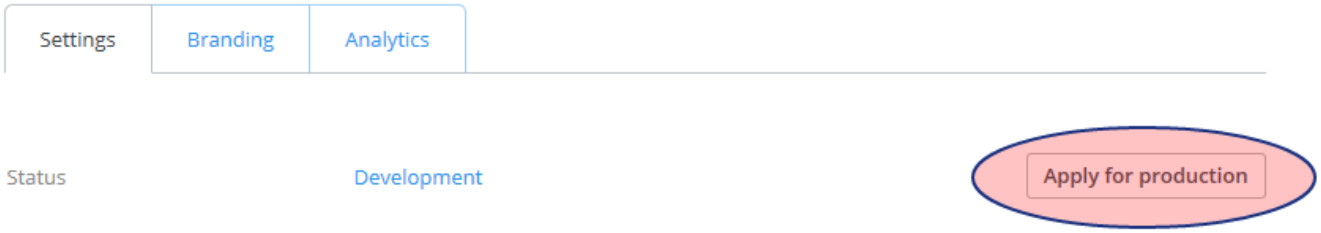
Before proceeding with these steps, you must have created a user with which the DropBox team will conduct it's testing of the solution. That user must have "Manage Content Source" privileges, so that they can add their own Dropbox content source!

It's a good idea to create a new test company to house your test user whose credentials you will provide to DropBox for validation. Once validation has been complete, you can remove that user so that they do not take up a seat.

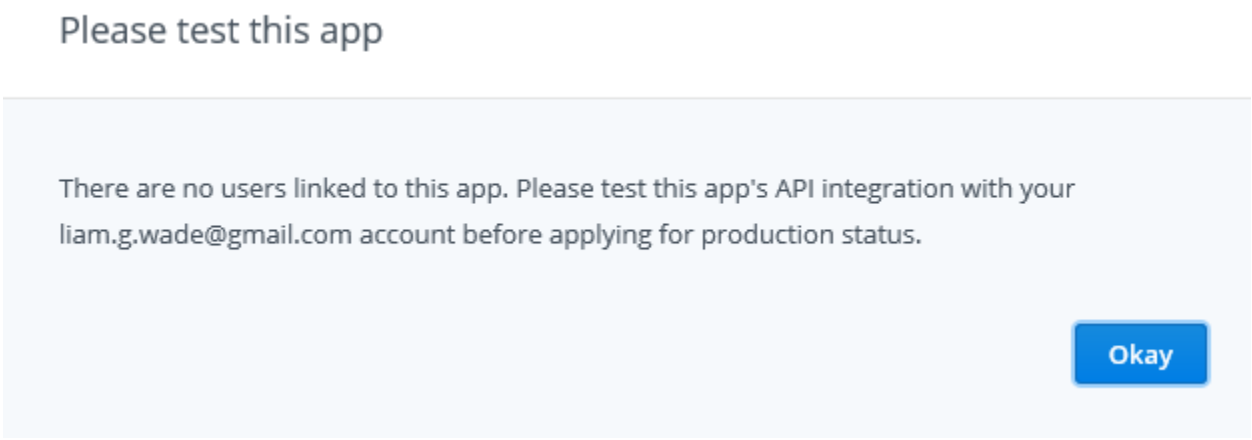
Click into the "settings tab":



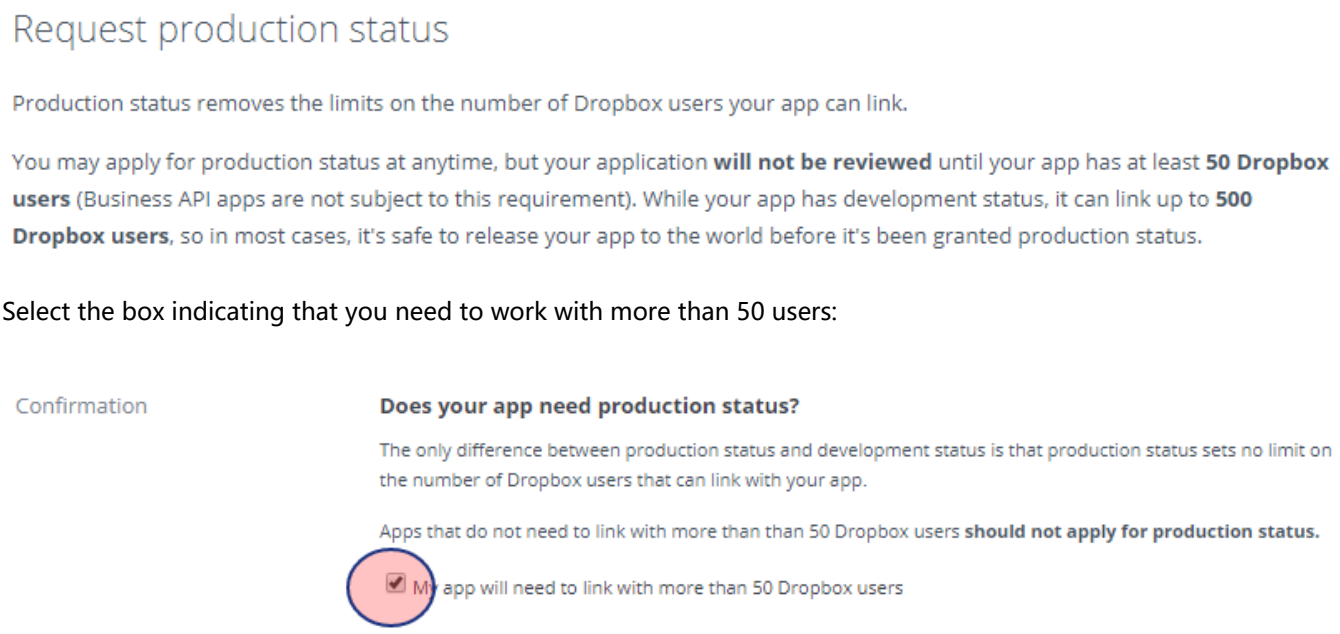
Click on "Apply for production":



If you have not yet tested the application you will be presented with the following message:



You will be taken to a new screen with some text to read and a form to fill out:



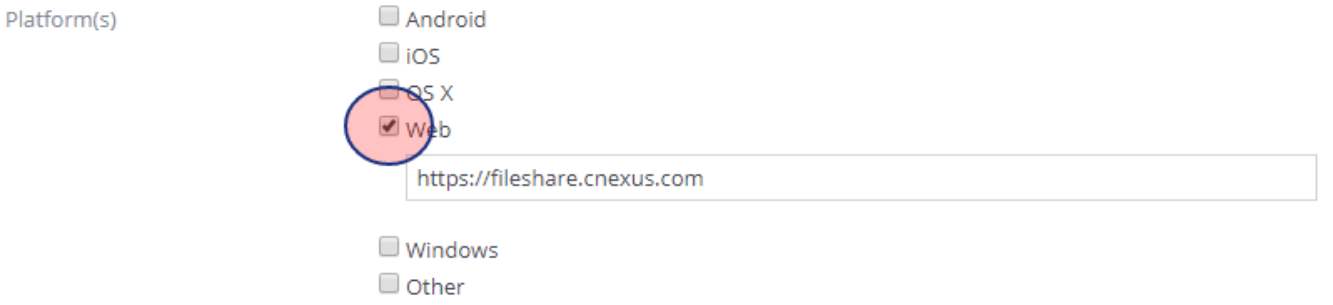
Select the box indicating that you need to work with more than 50 users:

Scroll down to "Dropbox integration":

Enter the following suggested text:

```
The app will use the DropBox API to allow a user to list, download and synchronize his existing DropBox files through our application
```

Scroll down to "Platforms":



Select the "Web" checkbox" and then enter your hostname as a URL similar to the following:

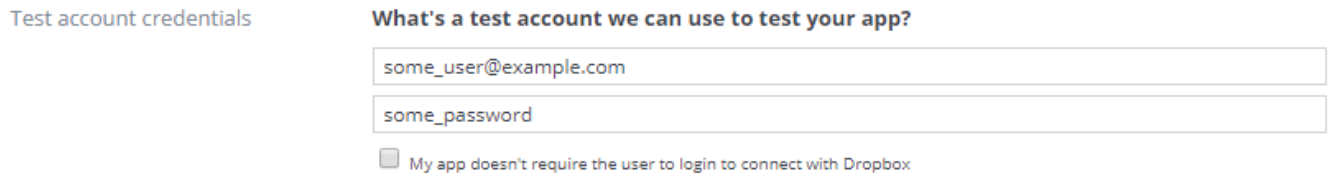
```
https://fileflexdemo.com
```

Under "Testing instructions", enter the following instructions:

Instructions for the DropBox Team

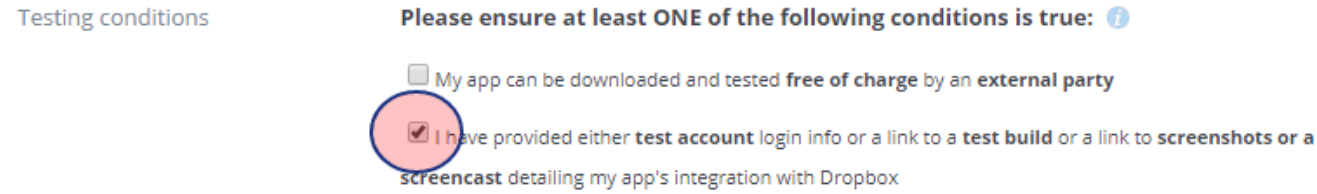
```
1. Log in to the web platform URL specified earlier using the provided credentials.

2. Add a DropBox content source by following the instructions contained in http://help.
fileflex.com/en/how-to-connect-to-dropbox.

3. Navigate the folders presented and download any existing user file.
```

Under "Test account credentials" enter the username and password you generated for the DropBox testing team:



Ensure that the "My app doesn't require the user to login" check box is **not** selected.

Under "Testing conditions", check the "I have provided a test account" box:

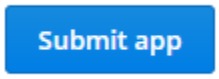


Under "Request early review" enter the following example text (adjust accordingly if it is not accurate, or if you do not want an early review):

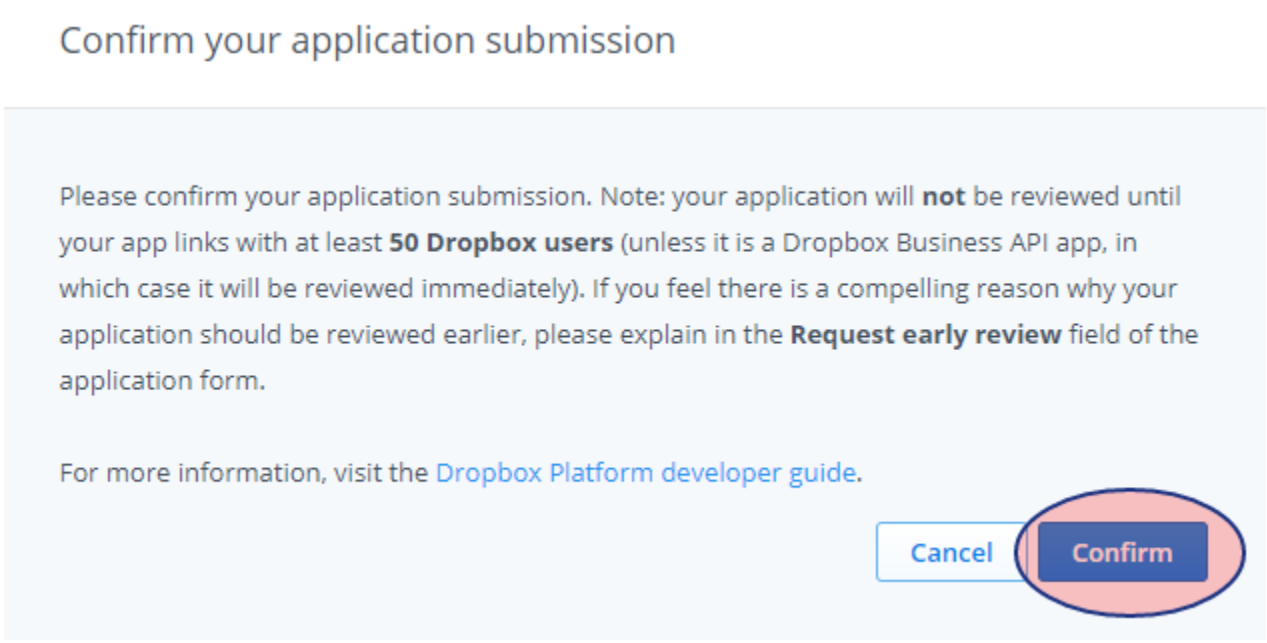
Early Review Reason

Once activated, it's expected that more than the maximum number of allowable users may come online suddenly, possibly causing service outages for us.

Click on the "Submit app" button:



You will then be prompted to confirm your application submission:



You must now wait for the review process to be completed by the DropBox team.

8.14. Configuring Box.net Access

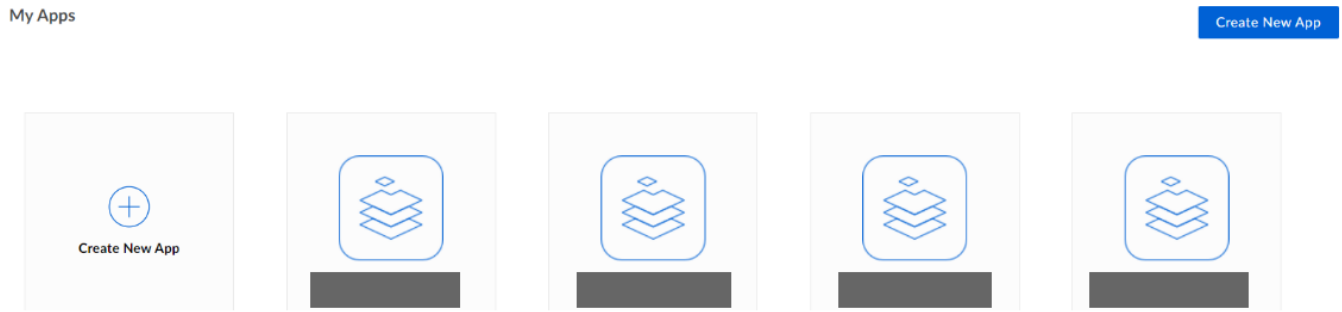
8.14.1. Registering for Box.net Credentials

> ⚠ It's important to complete the "Supplying an SSL Certificate" steps prior to configuring Box.net access.

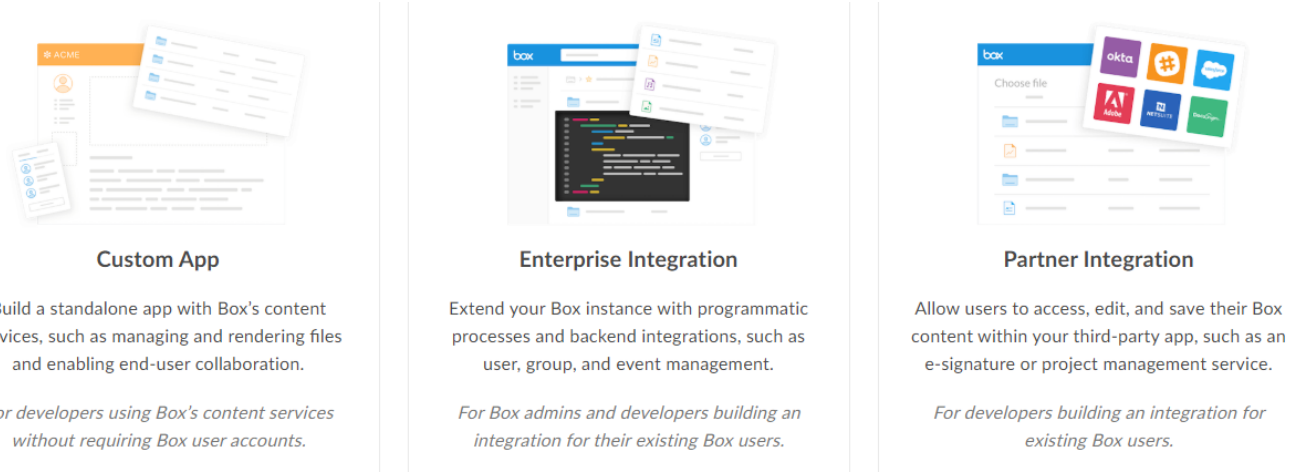
In order to configure Box.net from within FileFlex Enterprise, you must obtain a Client ID and Secret from Box.net. Sign in to your Box.net account, and navigate to the following URL which is used to configure their APIs:

```
https://app.box.com/developers/console
```

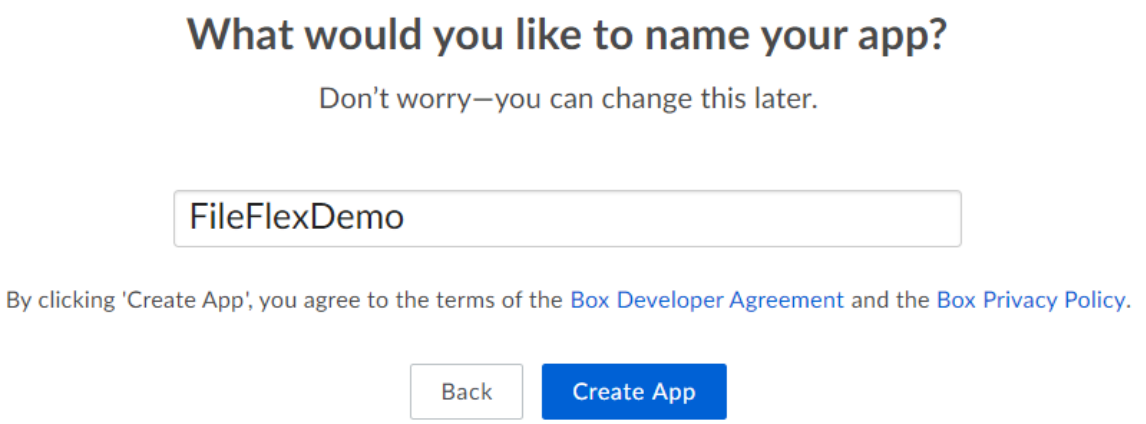
You will be presented with a screen called "My Apps", listing any apps you may already have configured with Box.net:



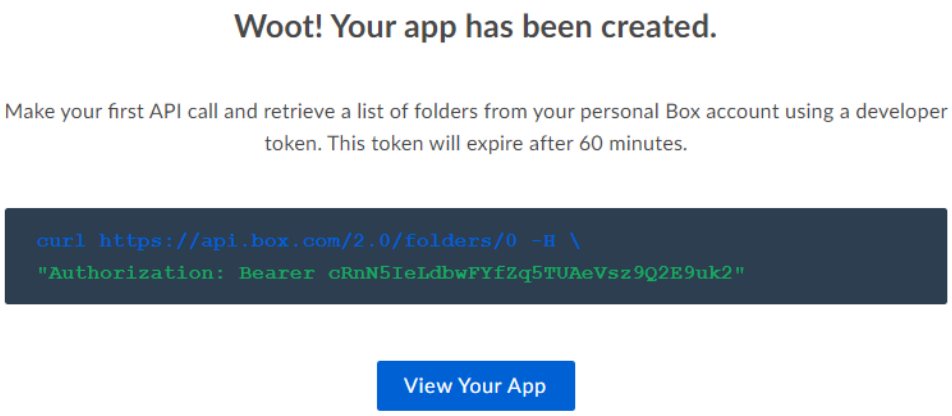
Click on the "Create new app" button at the top right. You will be presented with a choice of application type to build:



Select "custom app" and click the "Next" button. You will be asked to name your app:

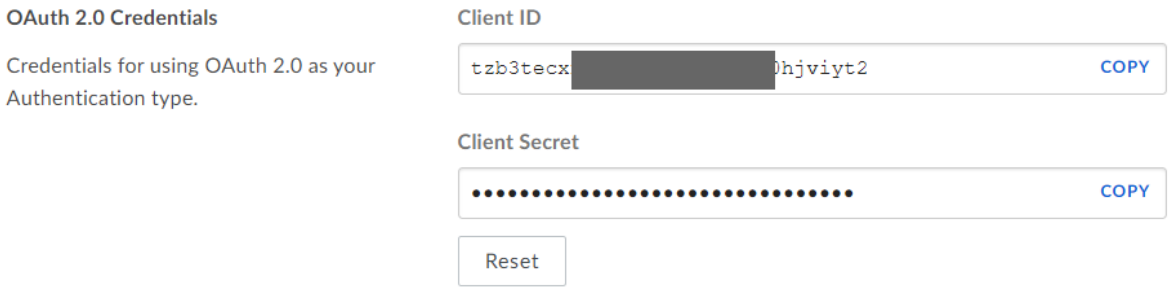


Enter a name for your application (FileFlexDemo in this case), and click "Create App". You will be presented with a confirmation screen:



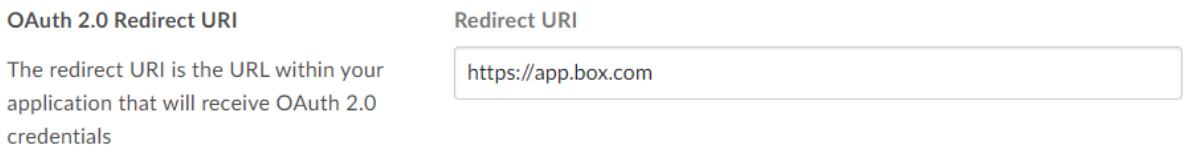
Click "View Your App" to proceed with some necessary configuration steps.

Scroll down to your "OAuth 2.0 Credentials" and take note of your Client ID. You can click the "copy" link in the edit box to copy it into the clipboard and store it for later use.



Do the same for the client secret which is not yet visible. Once "copy" is clicked, it will be revealed, and in your clipboard. Store it for later use as well.

Scroll down to the "OAuth 2.0 Redirect URI" section:

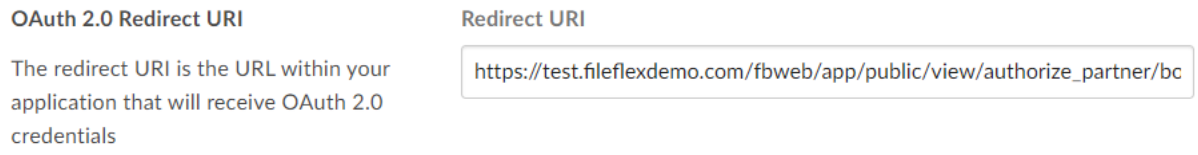


You will need to enter a new redirect URI, which Box.net uses to send users back to the FIleFlex application after authorization.

The formatting of the redirection URL is very important. Use the following format, substituting 'www.fileflexdemo.com' with your FileFlex domain name:

```
https://www.fileflexdemo.com/fbweb/app/public/view/authorize_partner/box
```

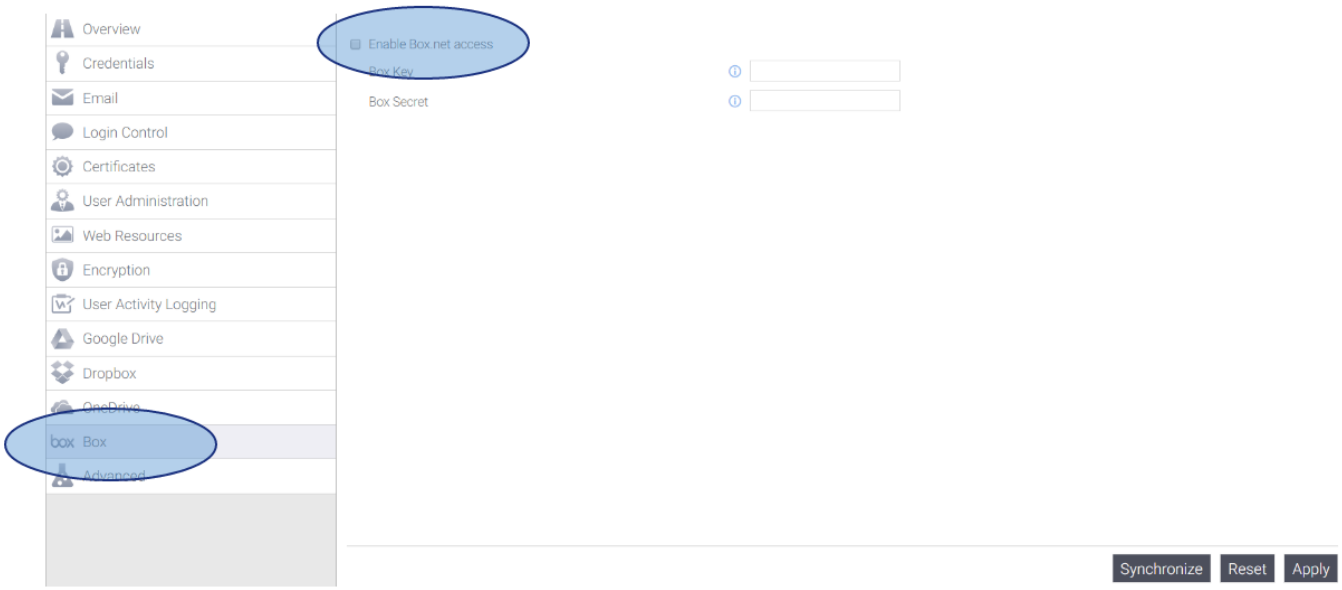
It should look something like the following:



Click the "Save Changes" at the top right:

You should be presented with a success message:

Open FileFlex Enterprise, and navigate to the "Box" tab of the control panel:

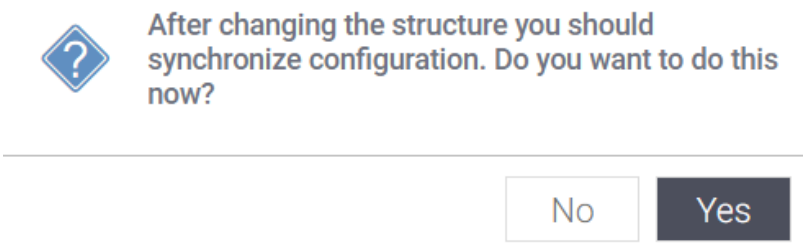


Choose to enable Box.net access:

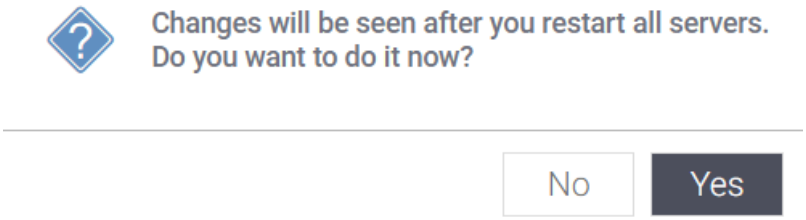
You will then need to enter the Key and Secret provided by Box.net earlier.

Click the apply button at the bottom of your screen:

You will be presented with a confirmation to restart:



Select "Yes". You will then be prompted to restart all servers:



Select "Yes". Wait a few moments while the servers restart.

Once the servers have restarted, you will see in the control panel overview that Box.net has been configured:

Congratulations - you are now ready to start using Box.net from within FileFlex Enterprise!

8.15. Configuring Amazon S3 Access

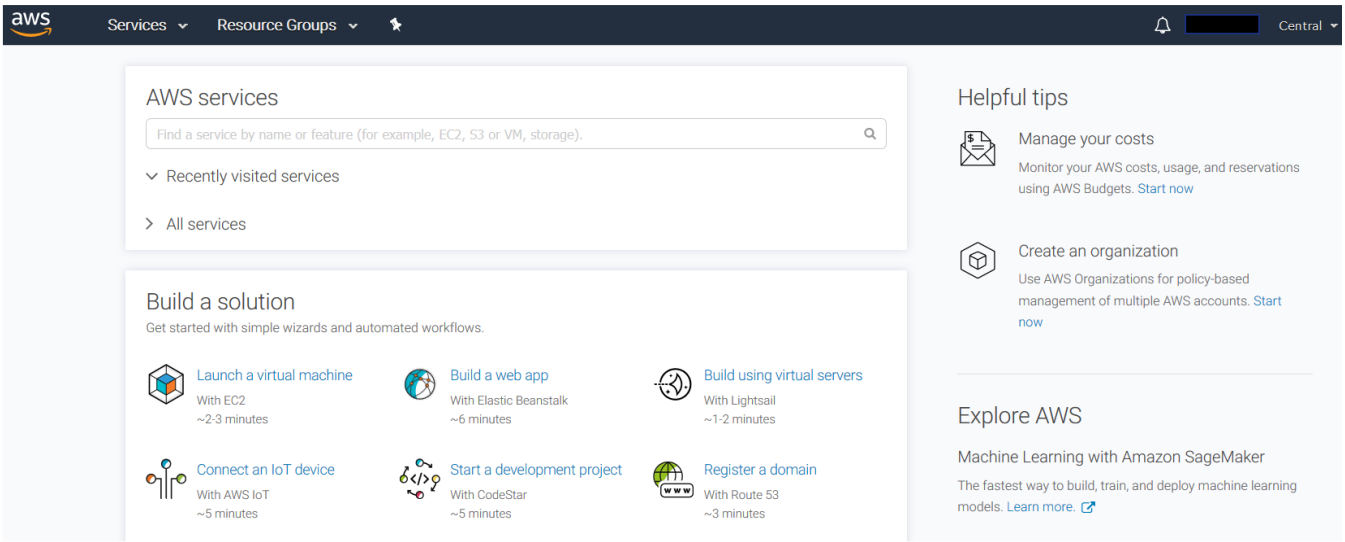
In order to configure Amazon S3 for access from within FileFlex Enterprise, you must first have an S3 bucket to which FileFlex can be connected. This guide is in three parts - creating an S3 bucket, enabling S3 access, following by adding an S3 content source.

8.15.1. Creating an S3 Bucket

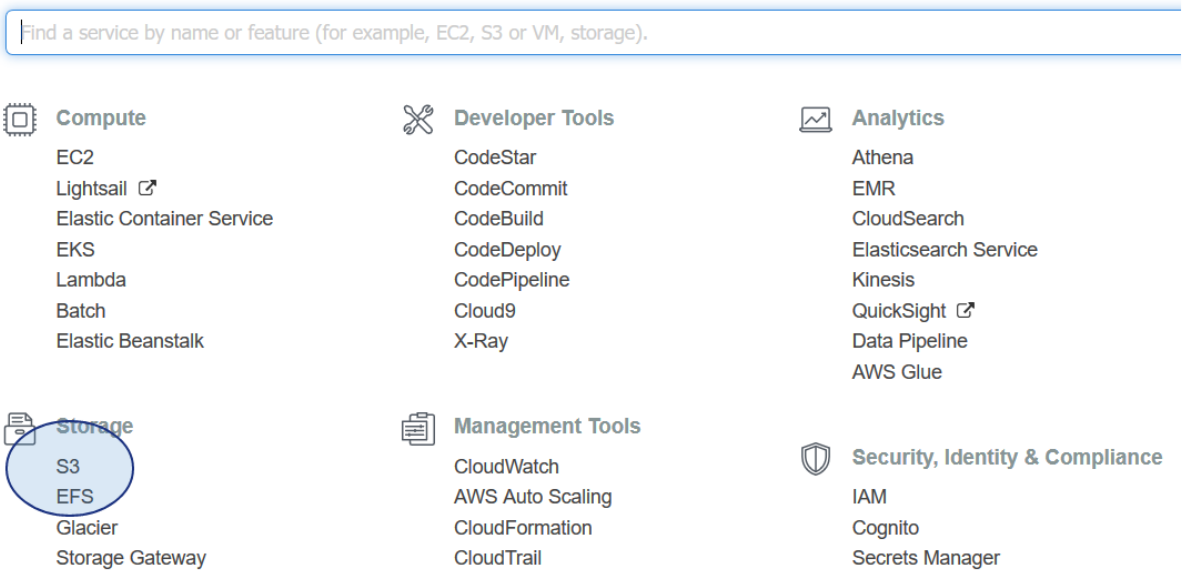
Log in to the amazon AWS console:

```
https://console.aws.amazon.com/console/home
```

Once logged in you should be at your Amazon AWS console, similar to the following:

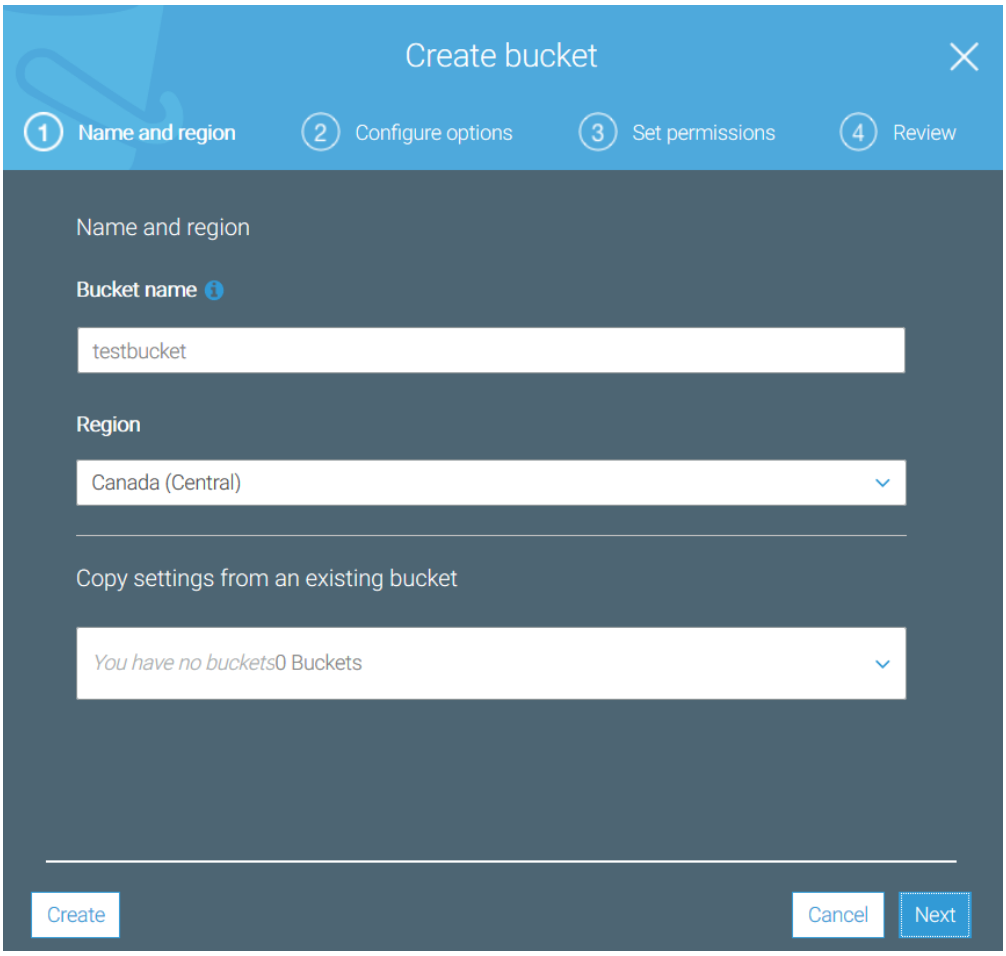


Click on the services dropdown at the top left, and from it select S3:



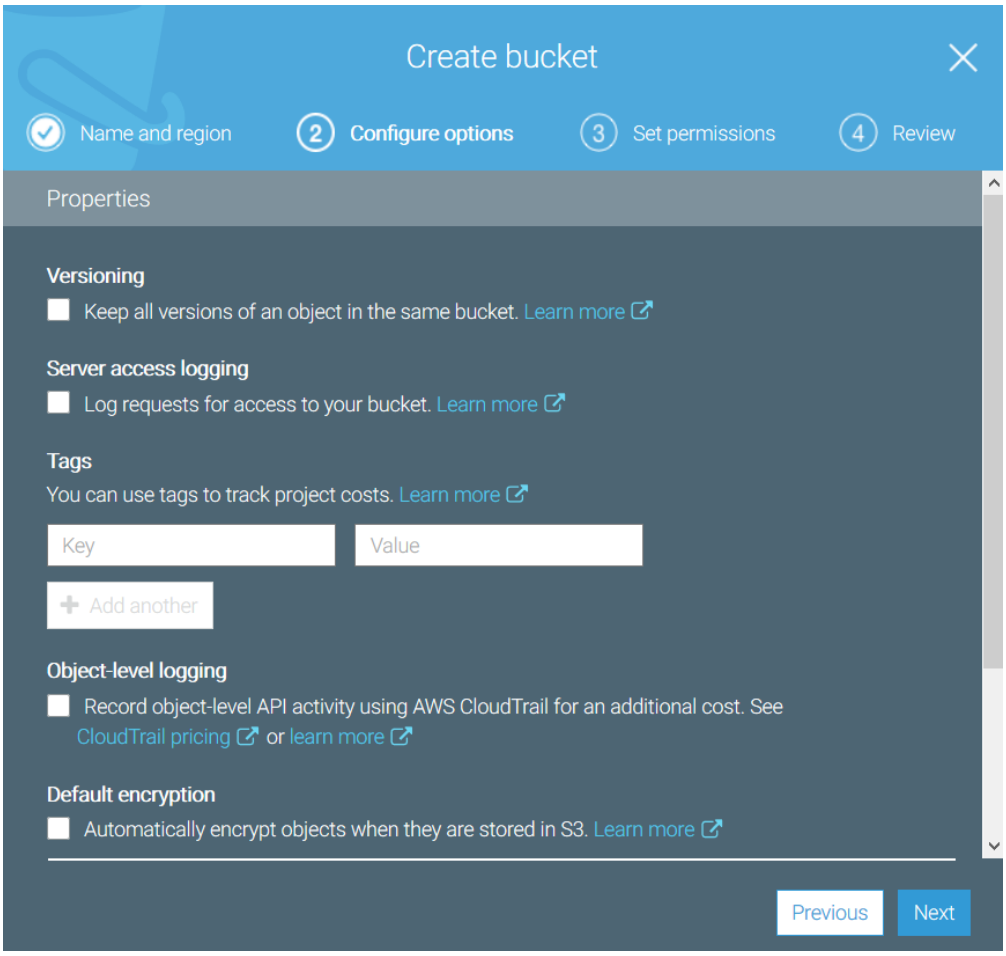
Click on the "Create bucket" button:

Enter a bucket name, and click next:

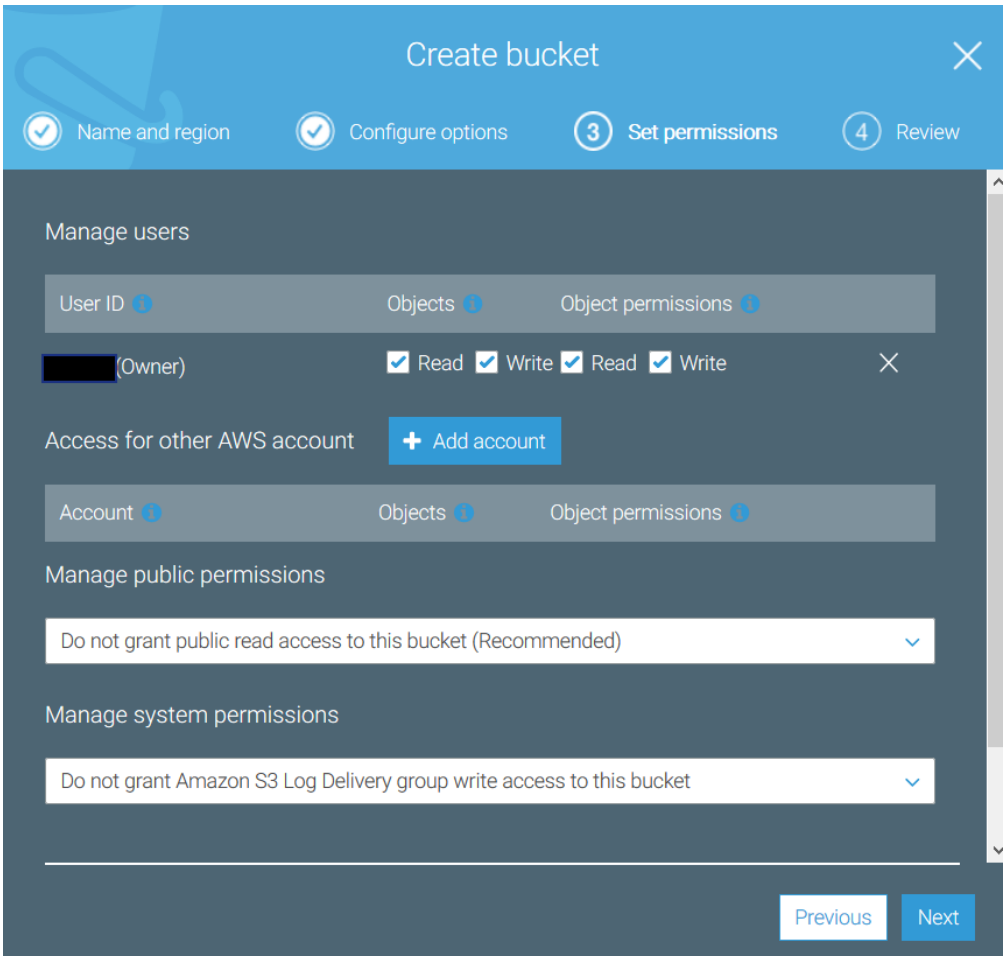


In this case the bucket is named "testbucket". Substitute a more appropriate name for your bucket. Click next.

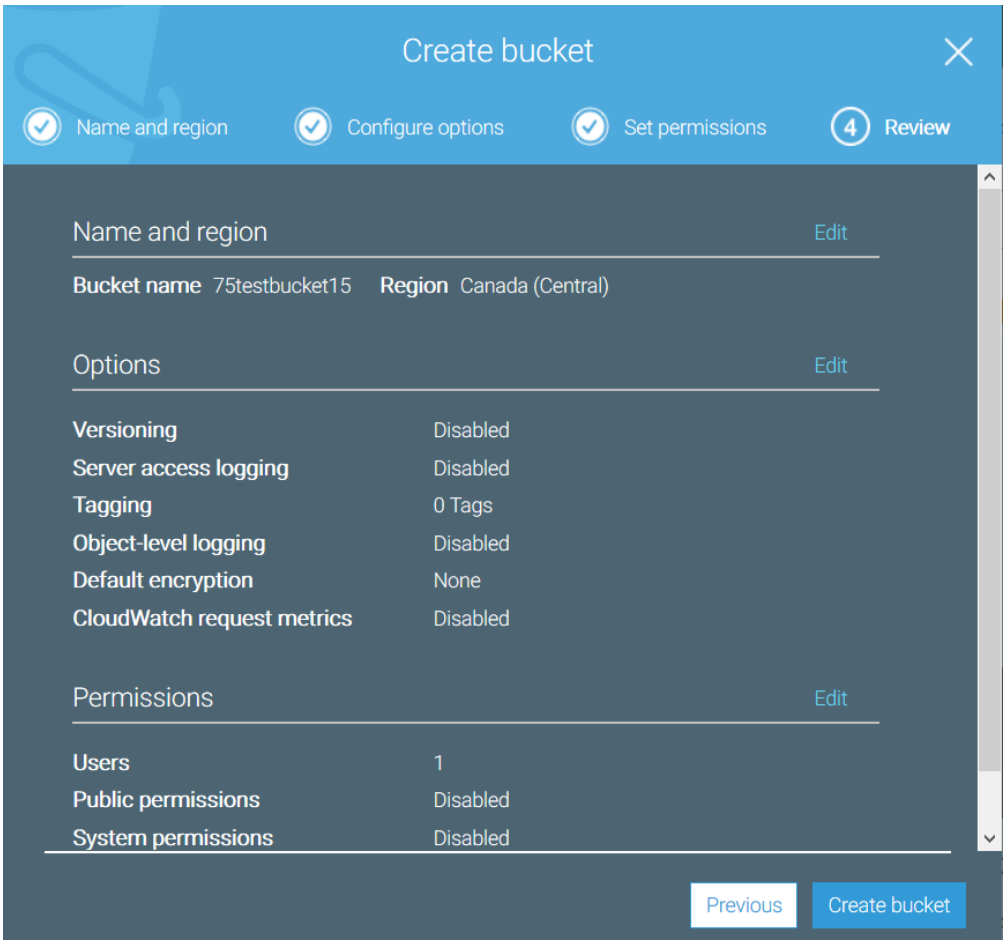
> Bucket names must be globally unique. You will likely need to add numbers or characters around your bucket name to ensure it is unique.



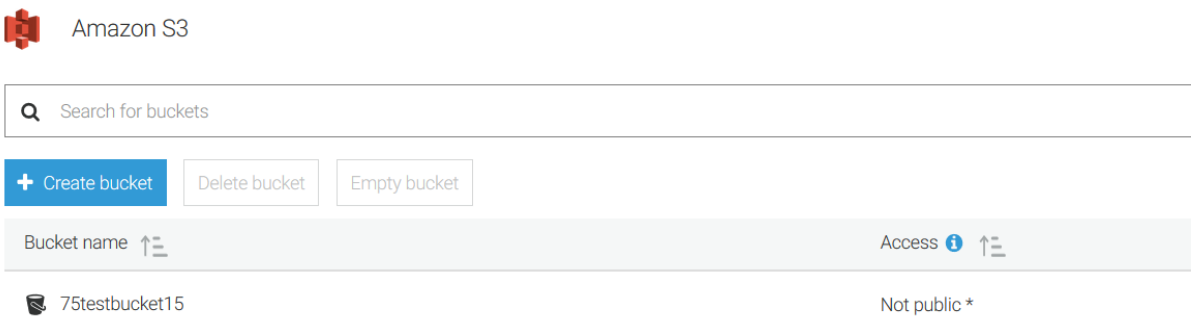
Nothing needs to be changed on this screen unless specific changes are desired. Click next.



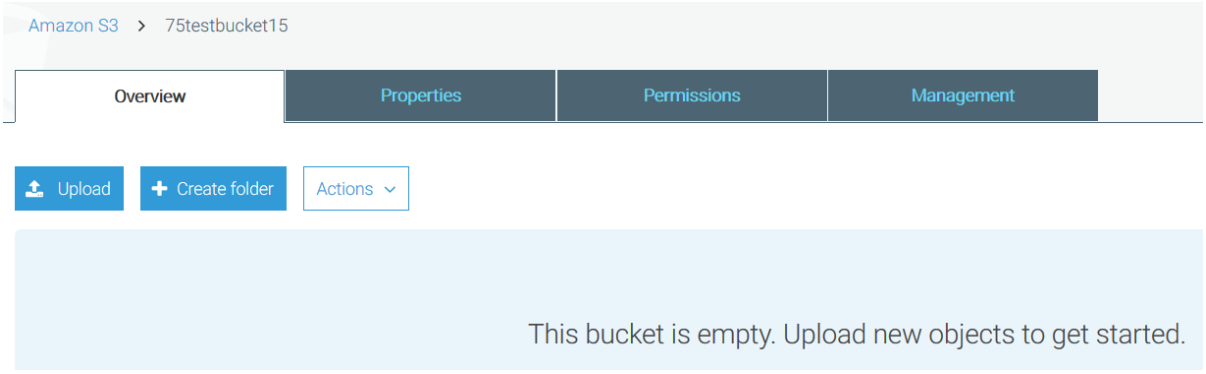
Change permissions if needed, but otherwise click next.



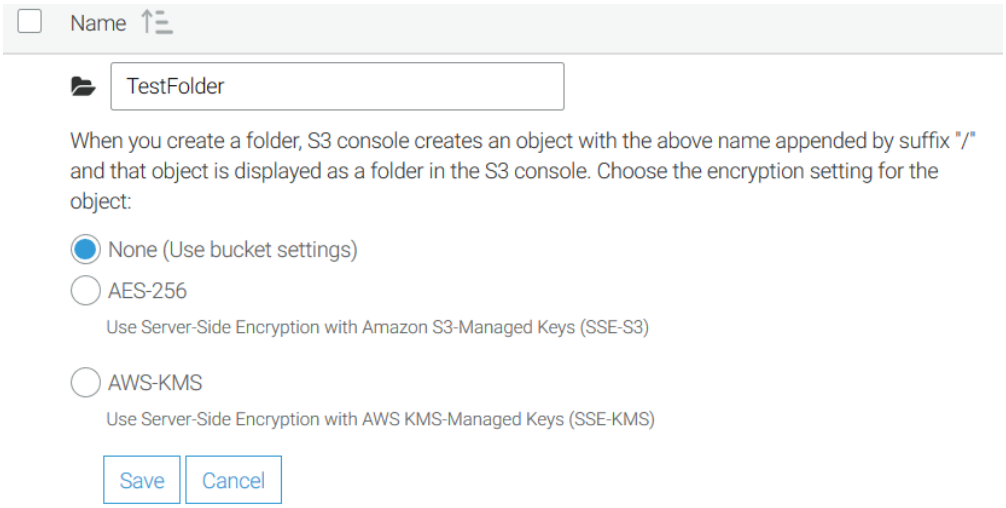
Click 'create bucket' to finish. You should now see your bucket listed:



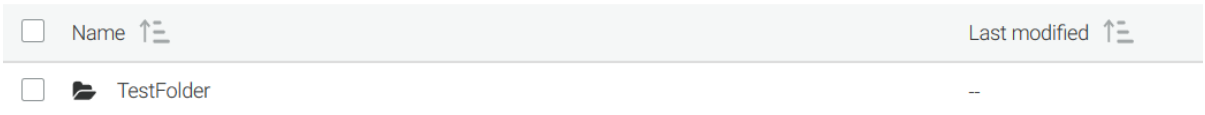
Let's create a bit of content so we can access it from FileFlex. Click on the bucket in the list and you will see an empty bucket screen:



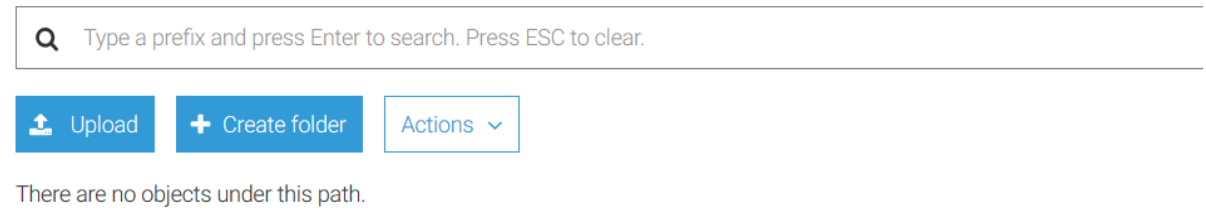
Click on "Create folder" to create a new folder:



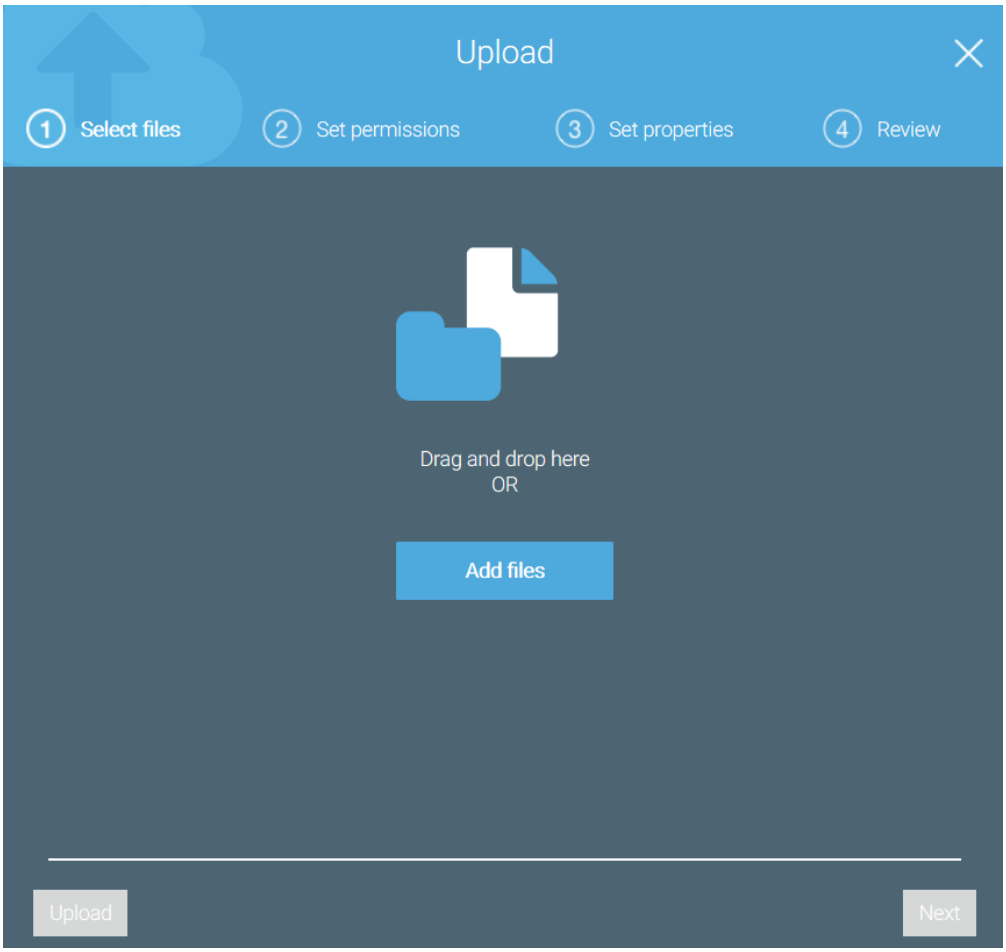
Enter a folder name ('TestFolder' in this case), then click save. You will then see it listed:



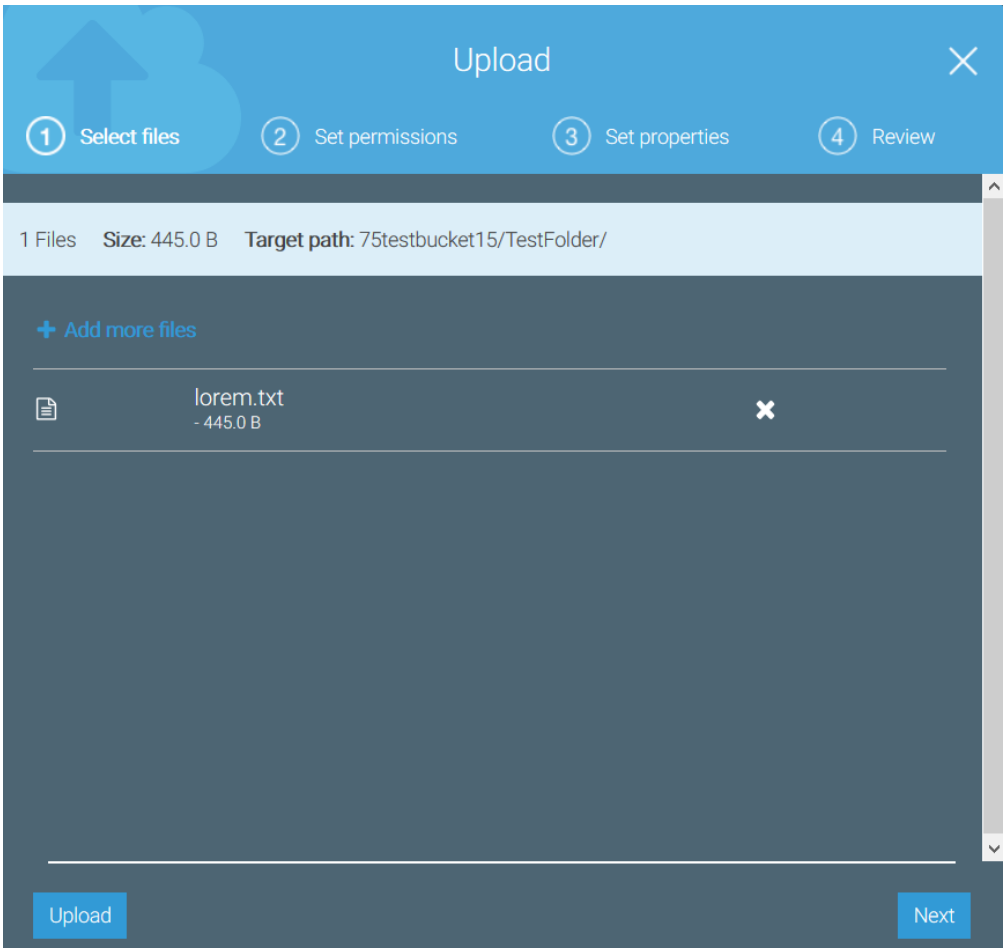
Click the folder to enter it. Click the upload button:



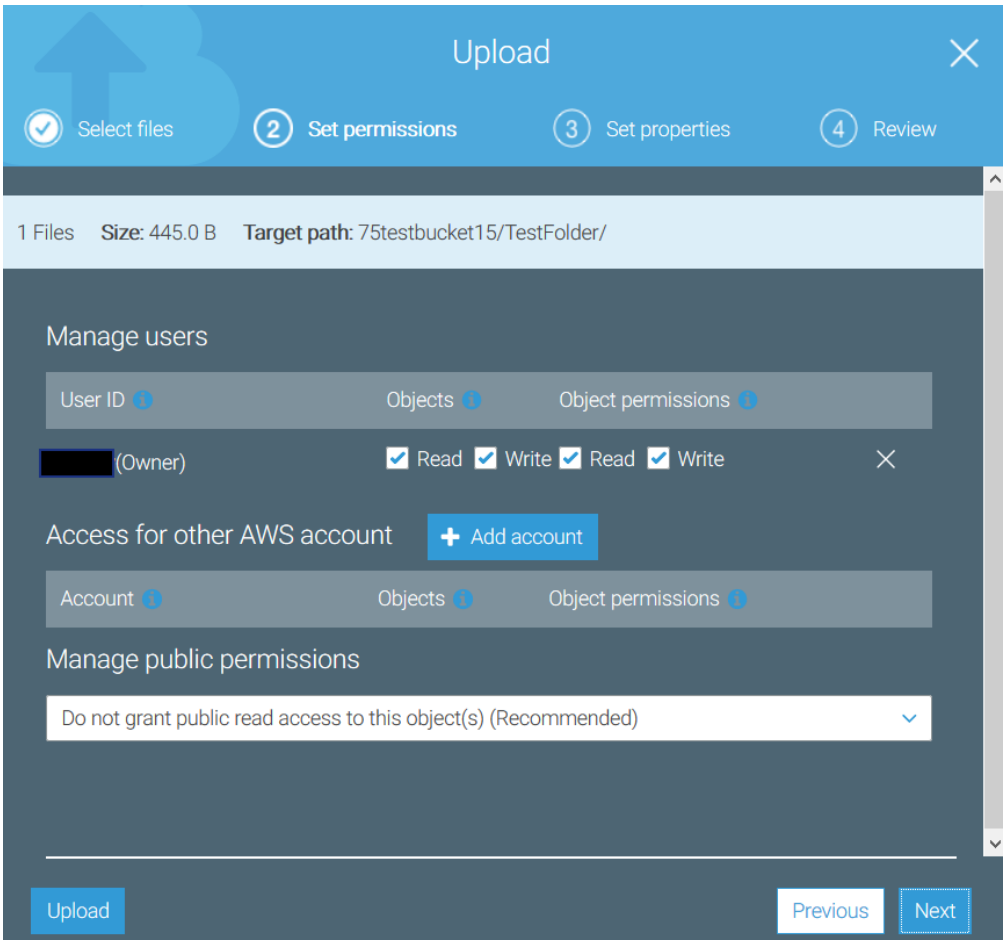
You will be presented with a dialog to upload files:



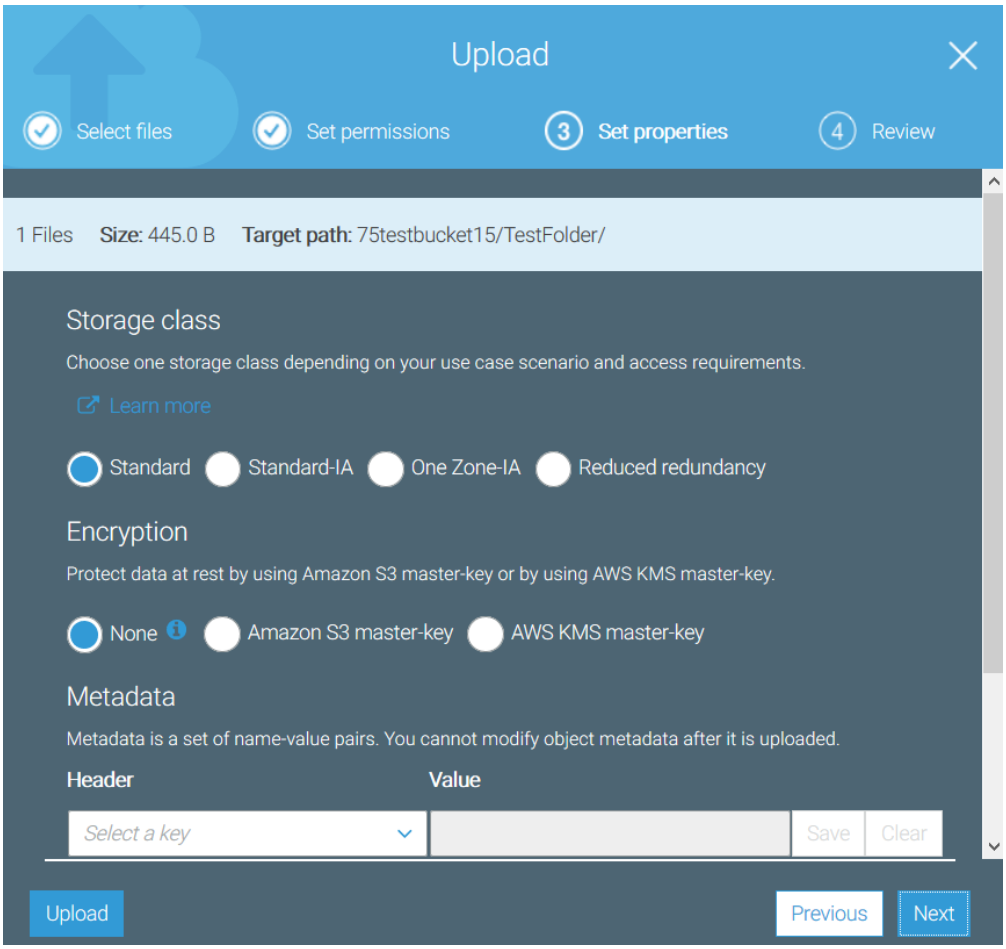
Drag a file into the indicated area:



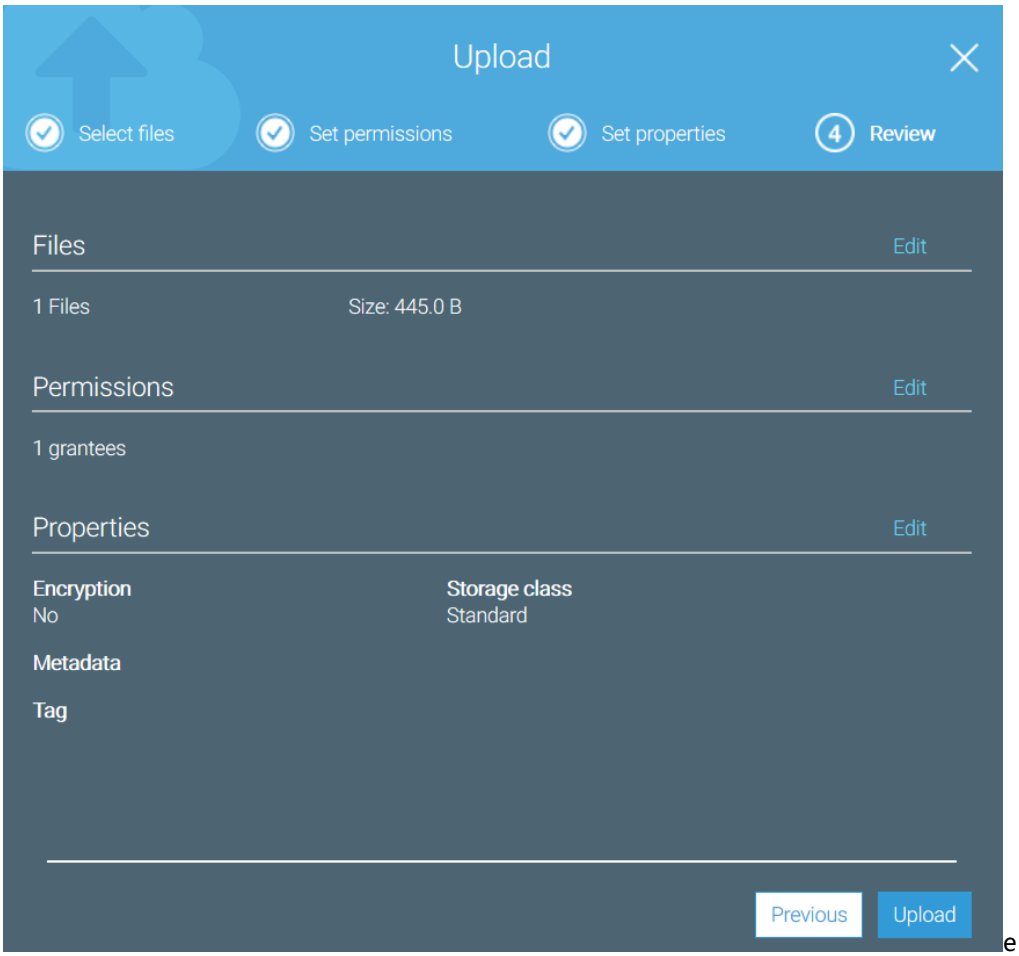
Click Next. You will see a screen in which you can set permissions:



If you want to change something in the permissions do so now, otherwise click next.

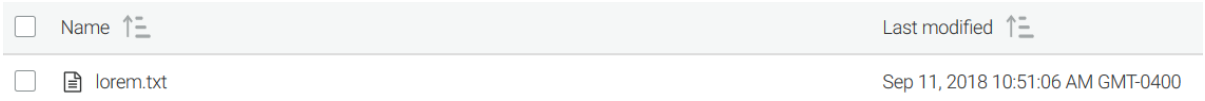


You will see a screen where you can set file properties. Unless you want to change something click next.



e

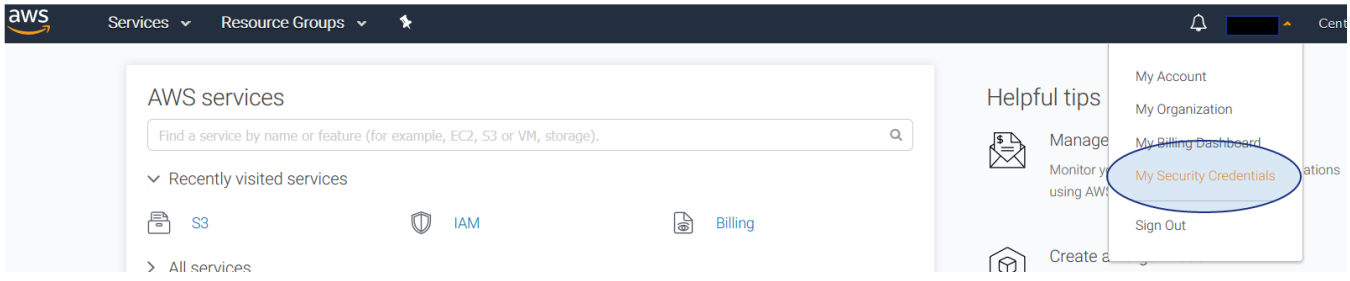
To complete the process, click upload. You will see the file listed:



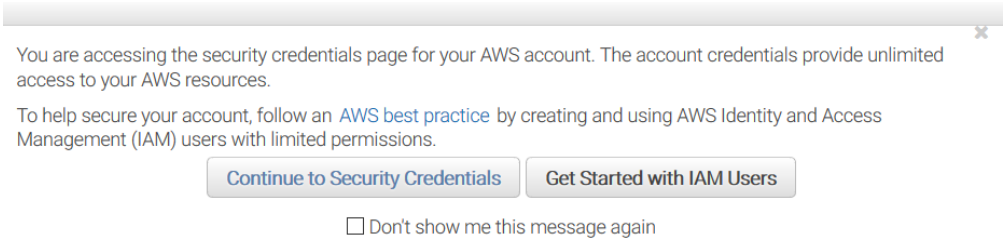
Now it's time to get your Amazon credentials if you have not already done so.

8.15.2. Getting Your Amazon Credentials

In order to connect a FileFlex account with Amazon S3, you will require your Amazon AWS security credentials. To access them, navigate to "My Security Credentials" from the account dropdown menu at the top right:

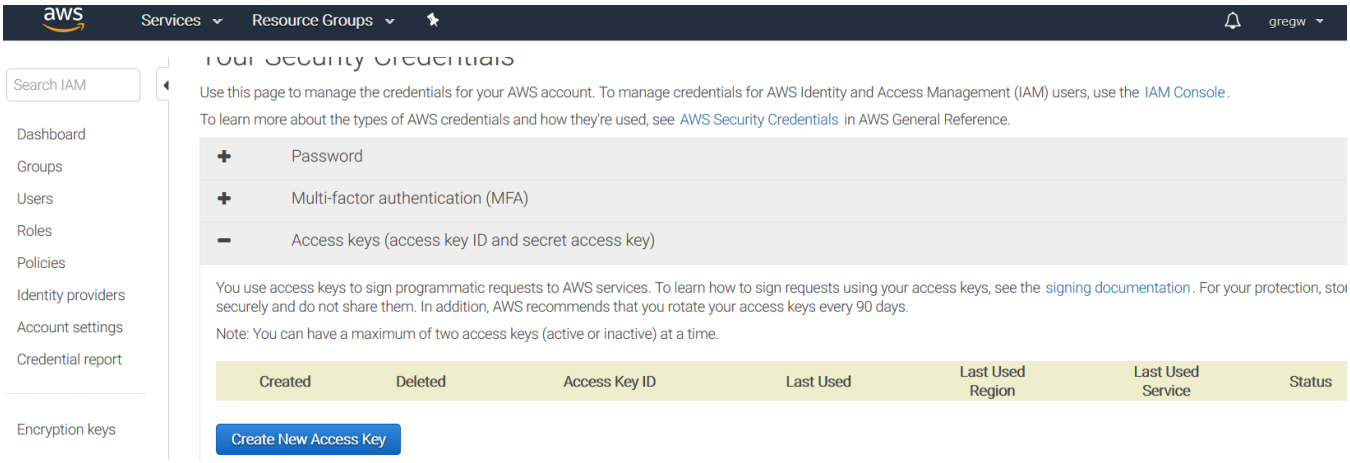


You may be presented with a warning about about using AWS Identity and Access to create a limited-permission user to access AWS. You can do that, but this guide assumes we bypass that for the sake of simplicity. Click "Continue to Security Credentials".

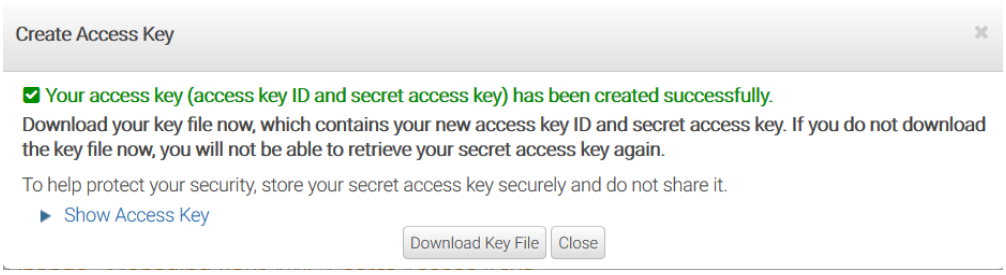


It is recommended that you follow Amazon's advice for any production accounts - but the remainder of this tutorial applies either way.

Expand the "Access keys" section of the security credentials panel:



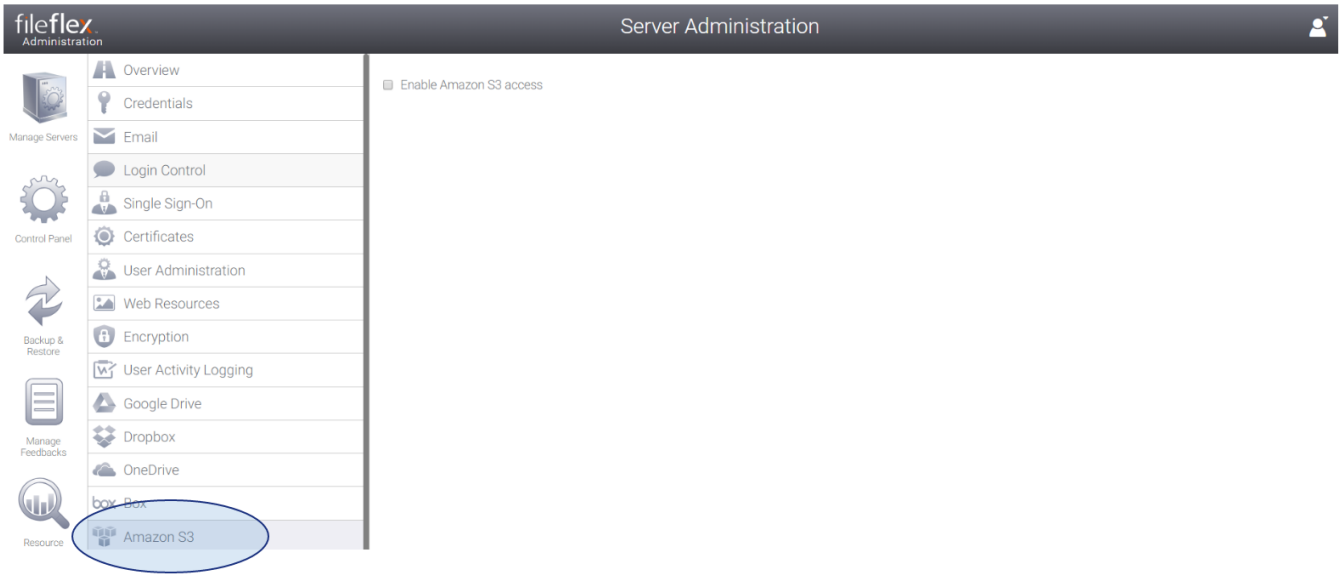
Continue by clicking on "Create New Access Key". You will see the following confirmation:



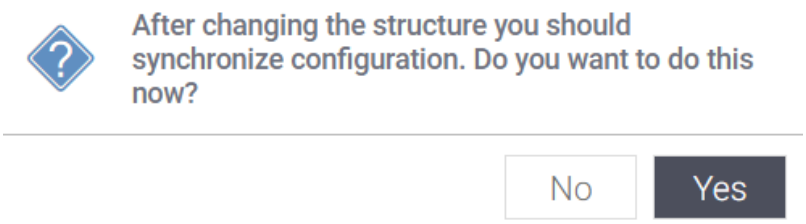
Click "Show Access Key" and write down the access key and secret access key that are revealed. You will need these in the next section.

8.15.3. Enabling S3 Access

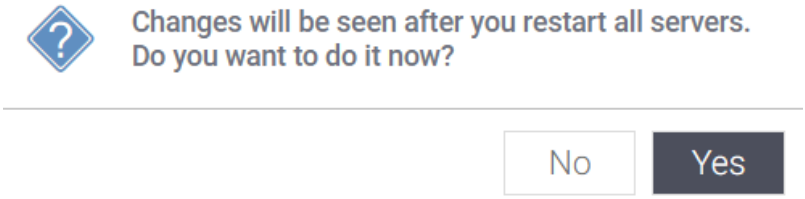
Open FileFlex Server Administration, and open the control panel tab. From there, open the "Amazon S3" panel:



Select the "Enable Amazon S3 access" checkbox, followed by the apply button at the bottom right. You will see the following dialog:



Click "yes". After a few seconds, another dialog will be shown:

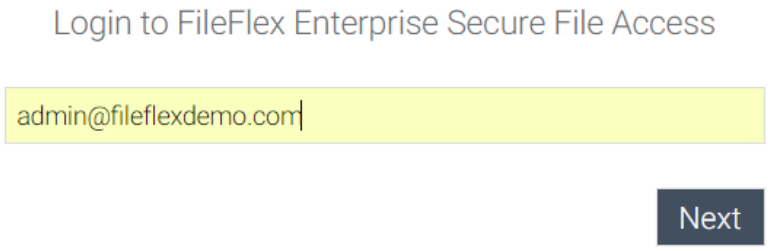


Click yes to restart the servers. After a few minutes, the server list will appear indicating that your servers are running normally. Click the control panel tab to verify that S3 has been configured:

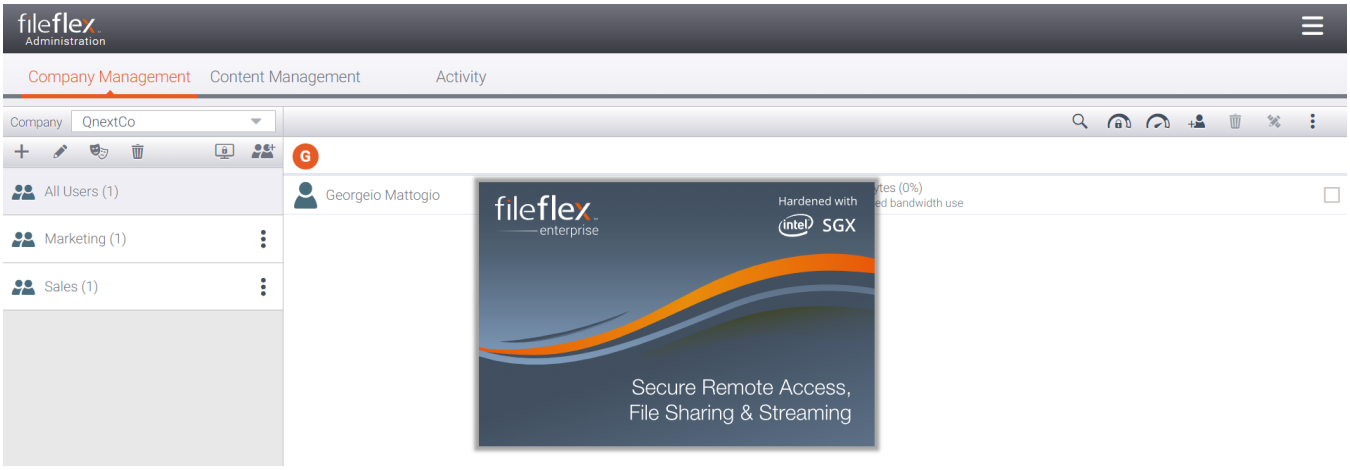
8.15.4. Connecting FileFlex to an S3 Bucket

The connection between FileFlex and Amazon S3 is made from user administration, or as an end user when given permission to define content sources. This guide assumes that the content provider will be configured from user administration.

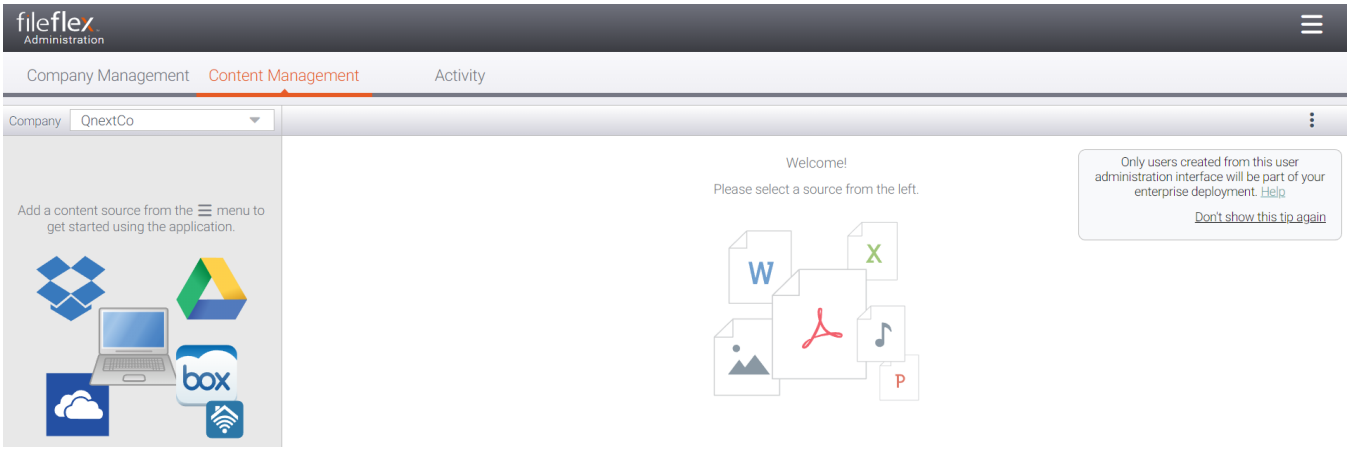
From Server Administration, click on the "Manage Users" tab from the left hand side. This will open User Administration in a new browser tab:



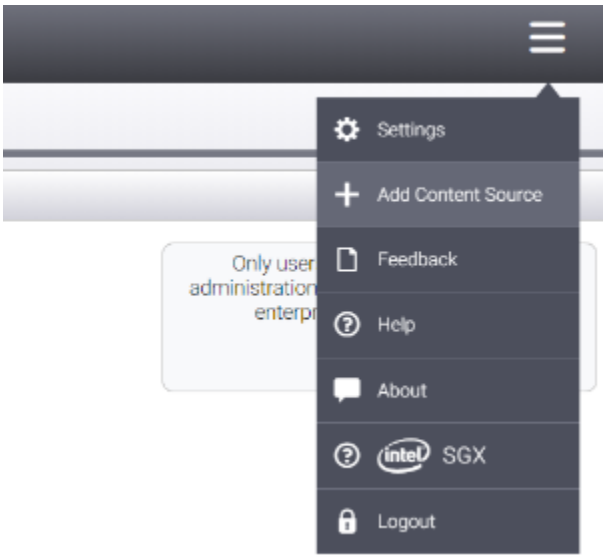
Enter your user administrator email address, followed by clicking on the Next button. Enter the password, followed by clicking on "Login" to complete the login. Once in, you will see the user administration application:



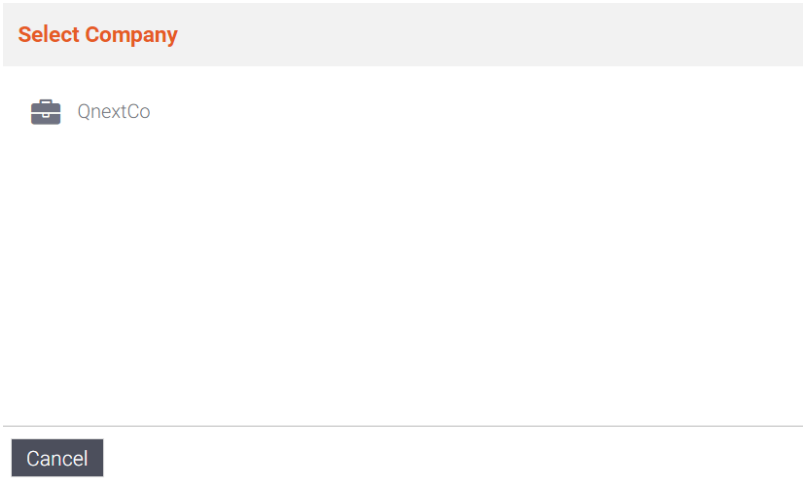
Click the "Content Management" tab:



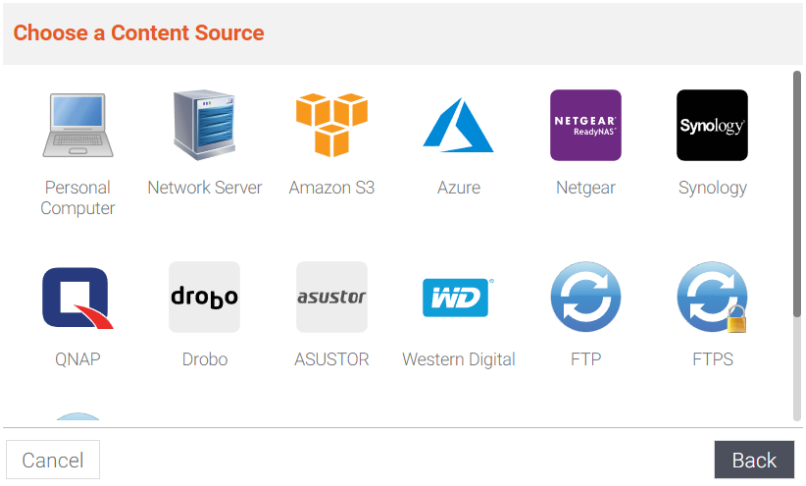
From the right hand menu, select "Add Content Source":



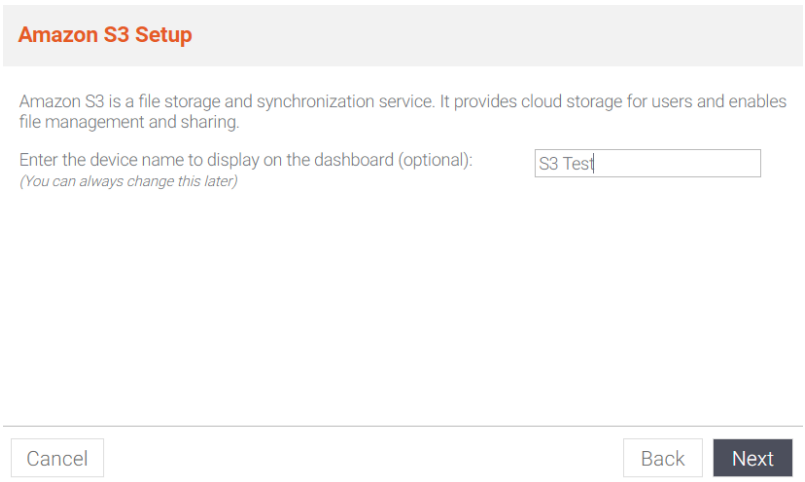
Select the company which will receive the Amazon S3 content source:



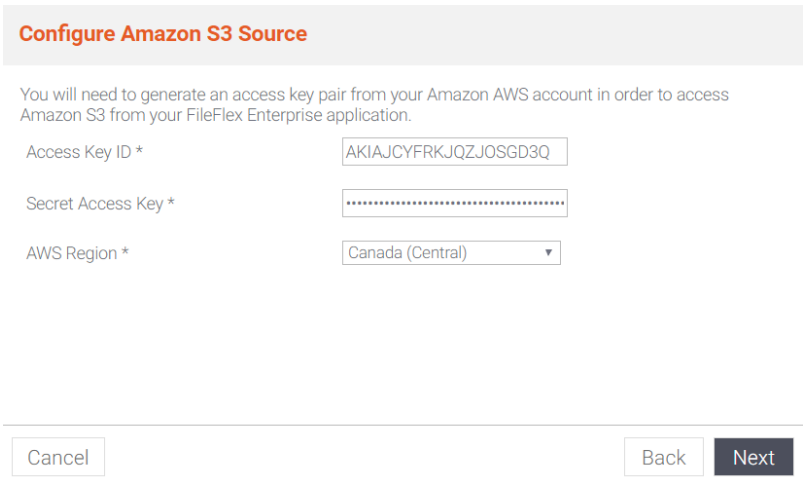
Select "Amazon S3" as the content source:



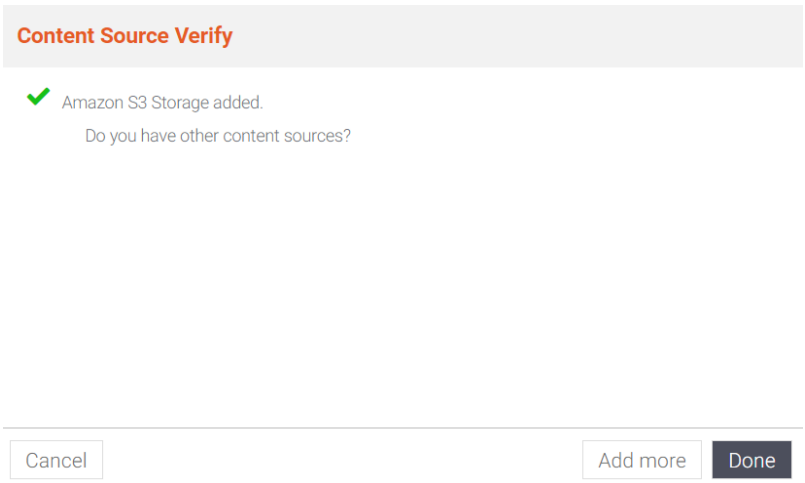
Enter a name for the content source. In this example we'll call it "S3 Test":



Click Next to continue. There you will see a screen asking you to enter your Amazon AWS Access Key ID and Secret Key. You will also need to know the region in which the S3 bucket was created. Enter that information. For example:



Click Next. If the information you entered was correct, you will be presented with a confirmation screen as follows:



Congratulations - your Amazon S3 bucket is now accessible from FileFlex!

8.16. Configuring Microsoft Azure Access

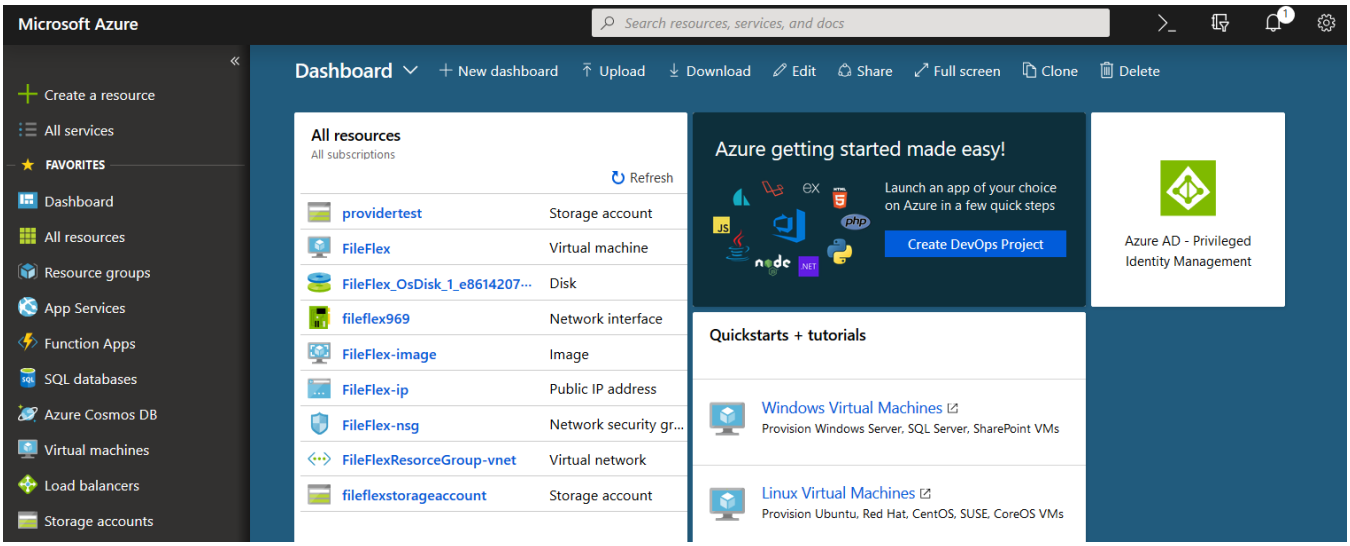
In order to configure Microsoft Azure for access from within FileFlex Enterprise, you must first have an Azure storage bucket to which FileFlex can be connected. This guide is in three parts - creating an Azure storage account, then enabling Azure access, followed by adding an Azure content source.

8.16.1. Creating an Azure Storage Account

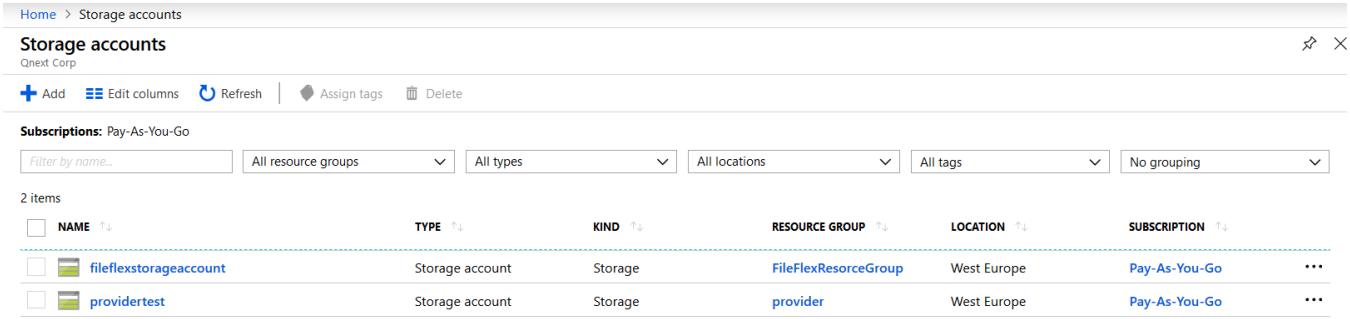
Log in to the Microsoft Azure portal:

```
https://portal.azure.com
```

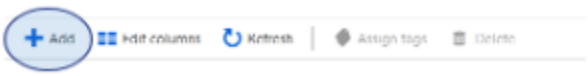
Once logged in you should be at your Azure console, similar to the following:



From the left hand side, select "Storage Accounts". You should see a screen similar to the following:



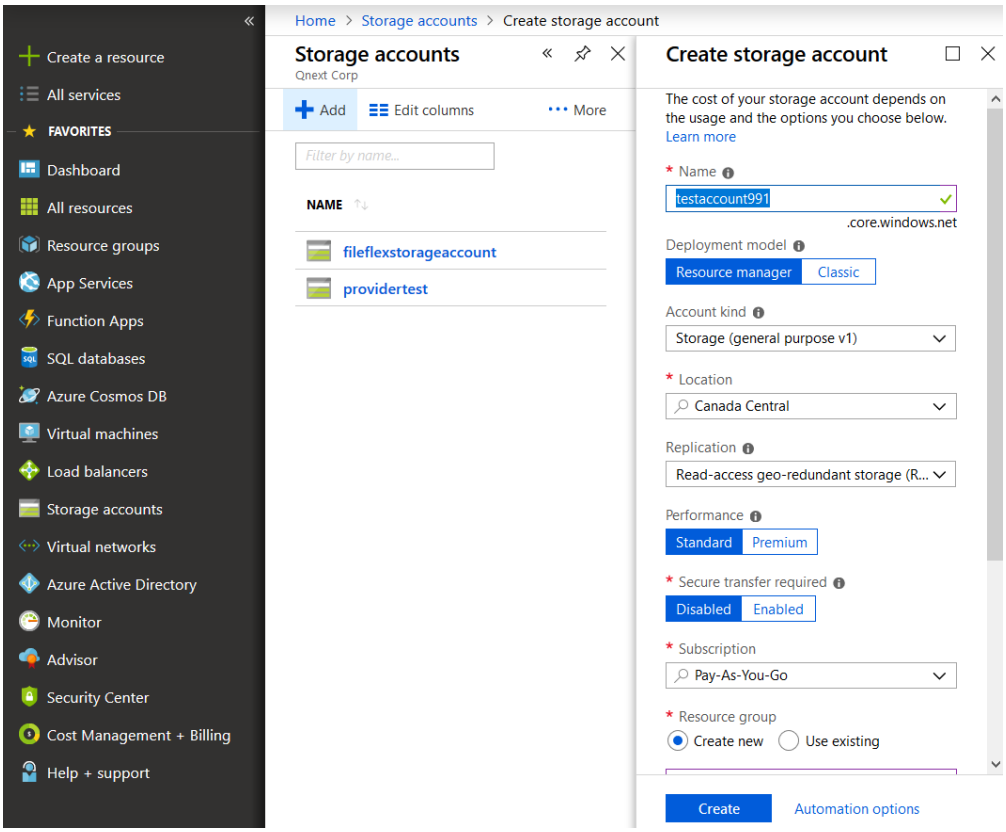
Click the "Add" button:



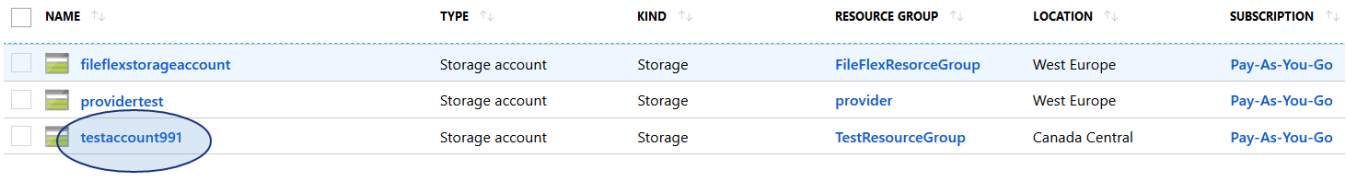
You will then be presented with a "Create storage account" panel where you can enter details for your new storage account. Fill out the information as appropriate, but the defaults should be fine in most cases. You will need to enter a resource group name (or select one that was already defined).

> Bucket names must be globally unique. You will likely need to add numbers or characters around your bucket name to ensure it is unique.

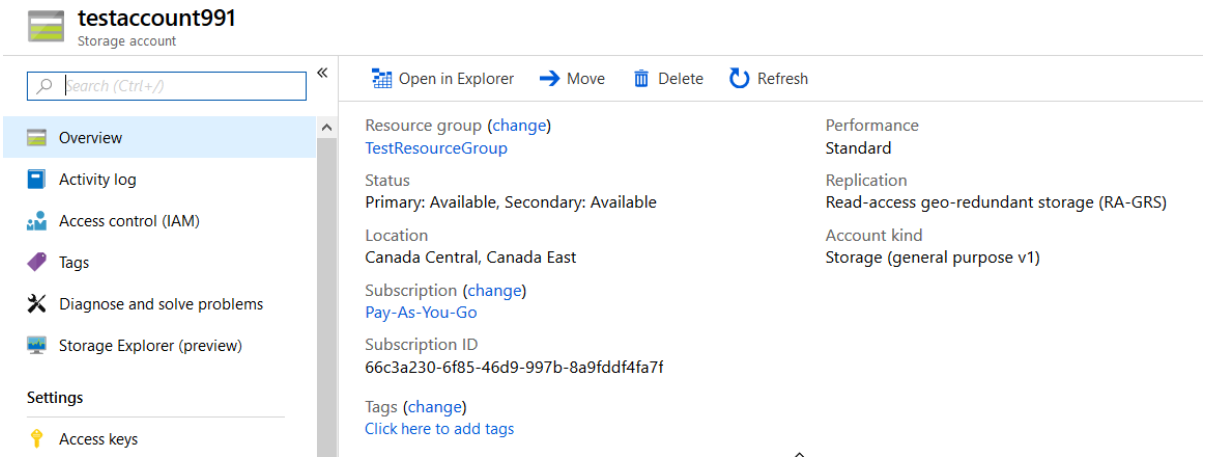
For example:



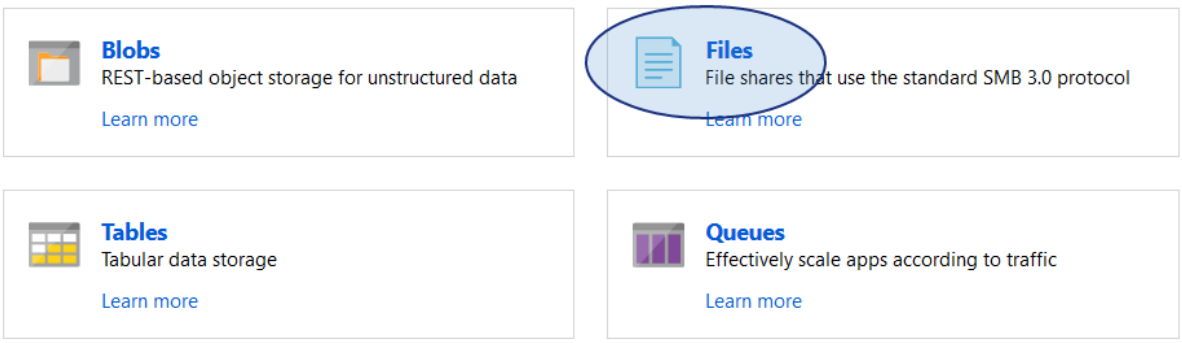
Click the create button at the bottom when complete. Wait a few minutes, and then refresh your browser. You should then see your storage account listed:



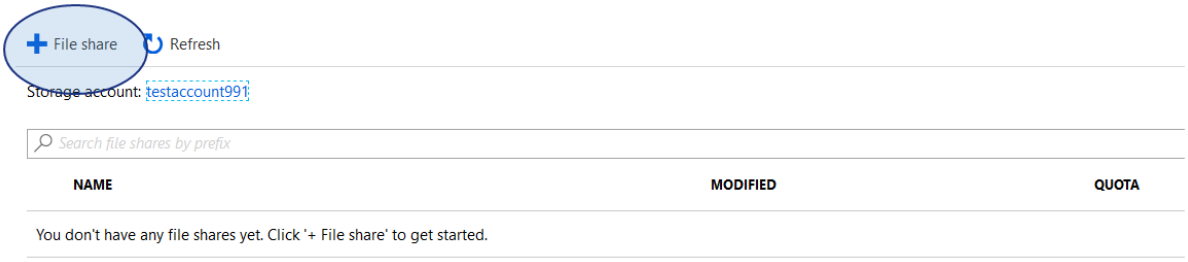
Let's create a bit of content so we can access it from FileFlex. Click the storage account to continue (testaccount991 in this case). You will see a panel similar to the following:



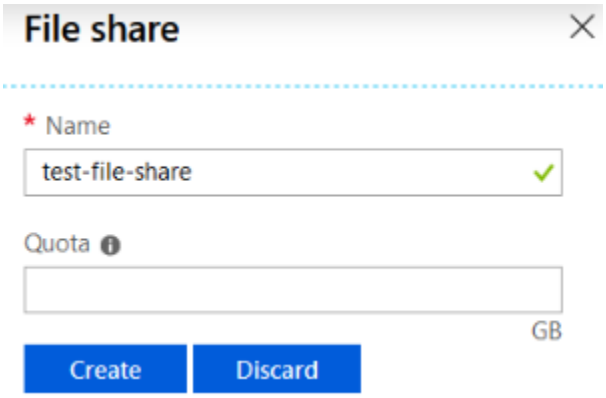
From the overview panel (where you are presently), click on the "Files" service box:



This will open a new panel listing the file shares in your storage account. Click the "+ File share" icon to add a share:

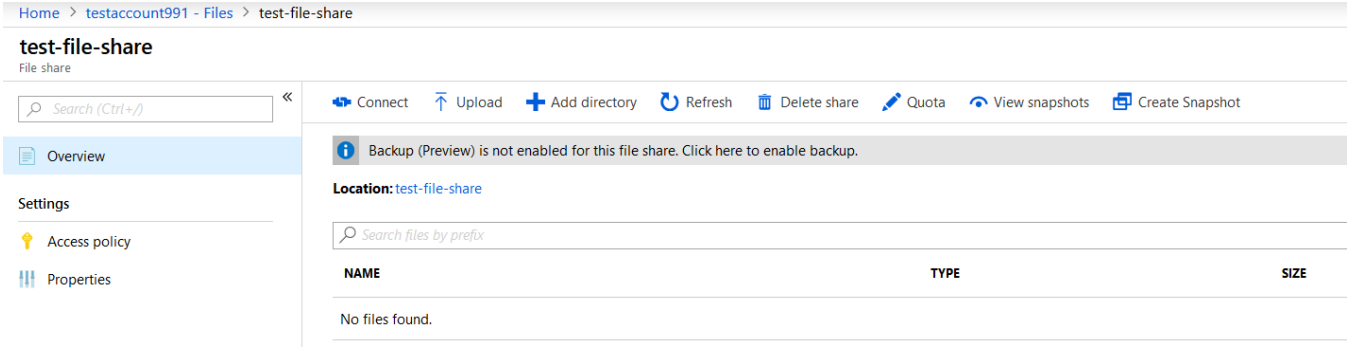


This will open a new panel in which you must enter the share name:

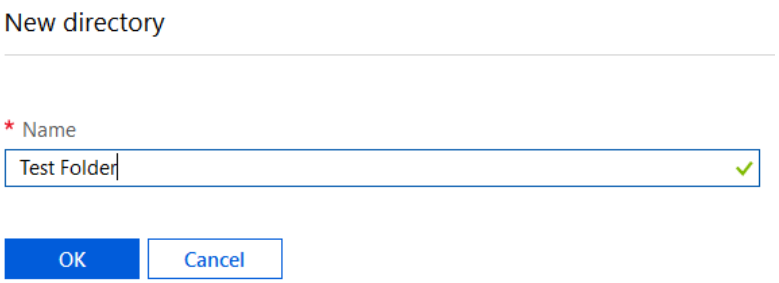


Enter your name, then click the "Create" button. Your share will then be listed:

Click the name of the share to enter it. You will see an empty file listing similar to:

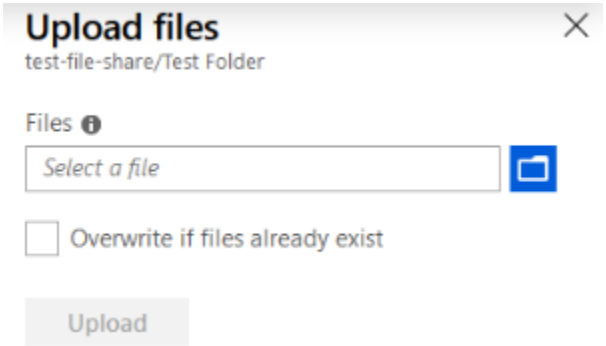


Let's create a directory. Click "Add directory". A dialog box will be shown. Enter a name similar to:

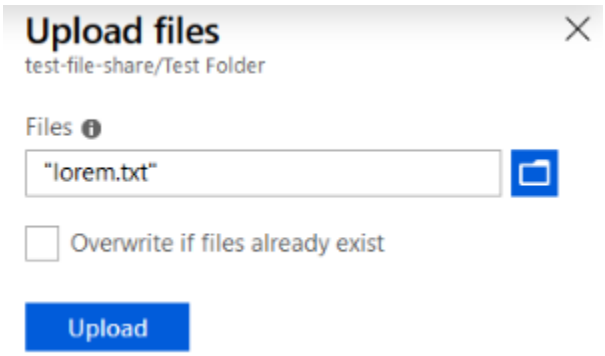


Click OK and you will be presented with a list of files that now includes your new folder. Click the folder to enter it:

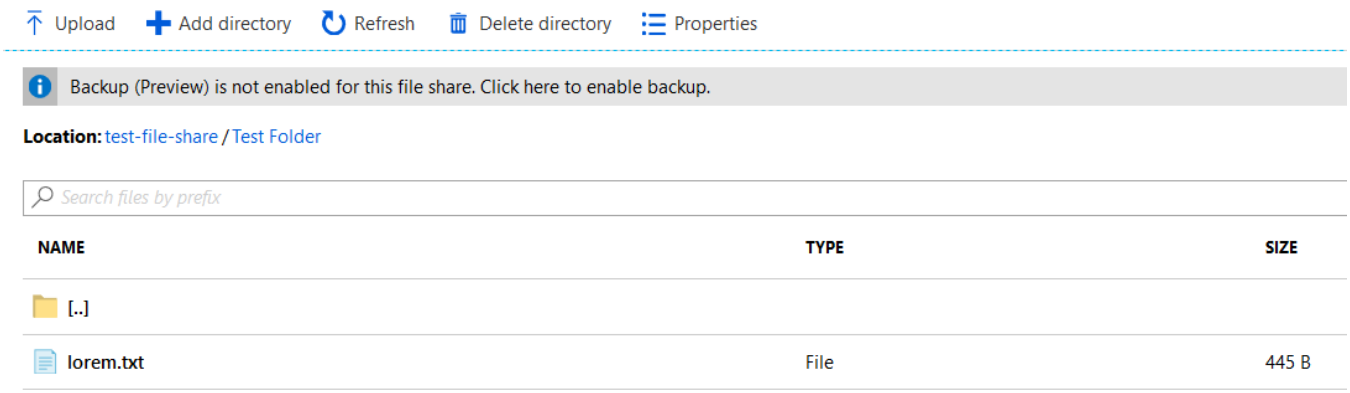
Once in the new folder, we can upload a test file. Click the "Upload" action and you will be presented with an upload file panel:



Click the blue folder icon to bring up a file browser. Select a file. The Upload action will be highlighted:

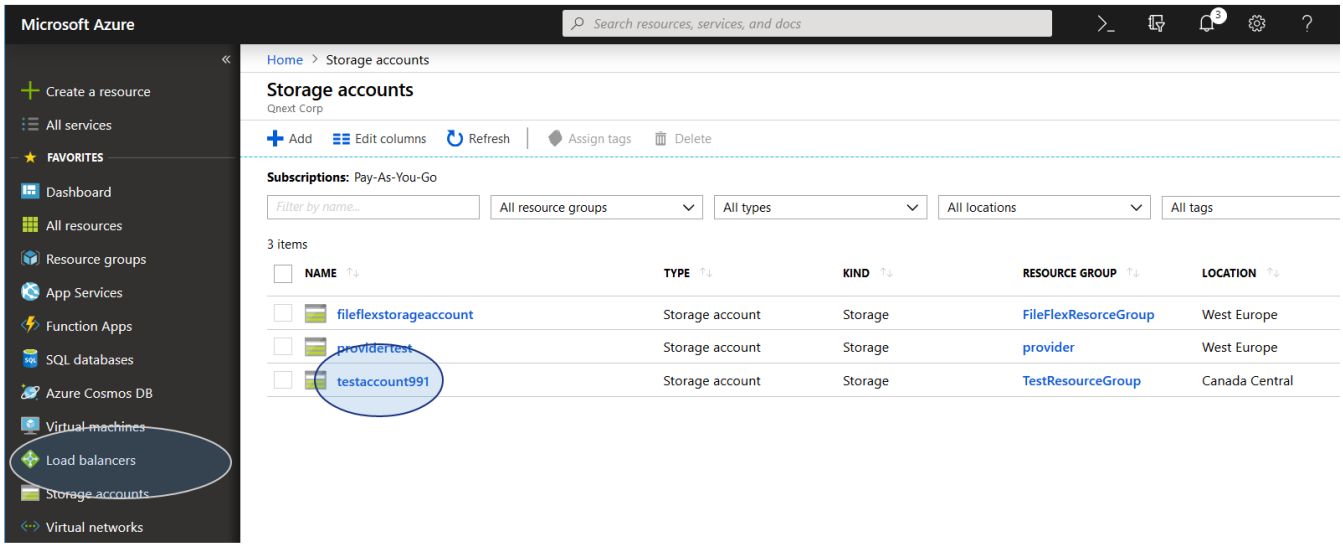


Click upload to proceed. Your file will now be listed:

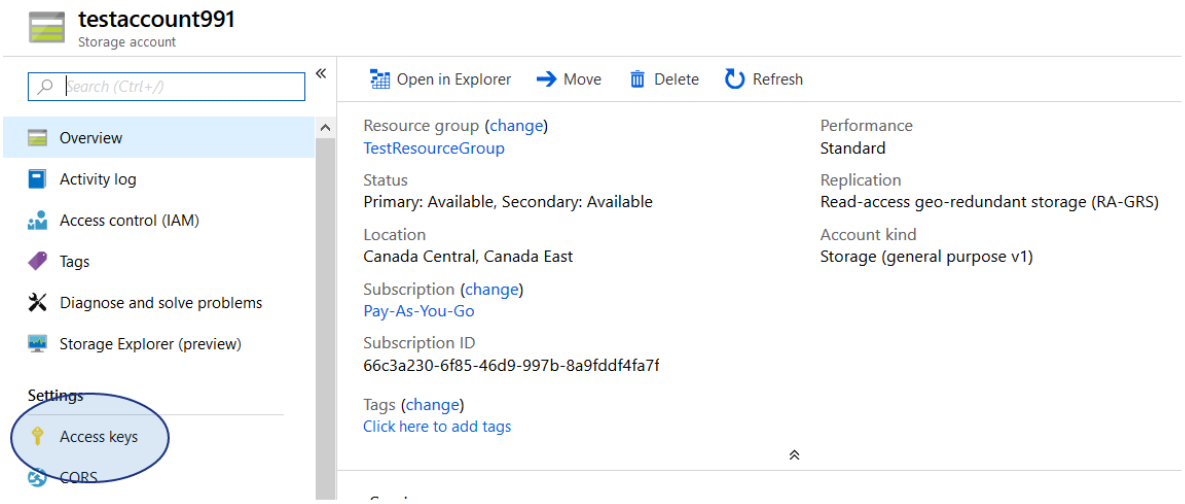


8.16.2. Getting Your Azure Credentials

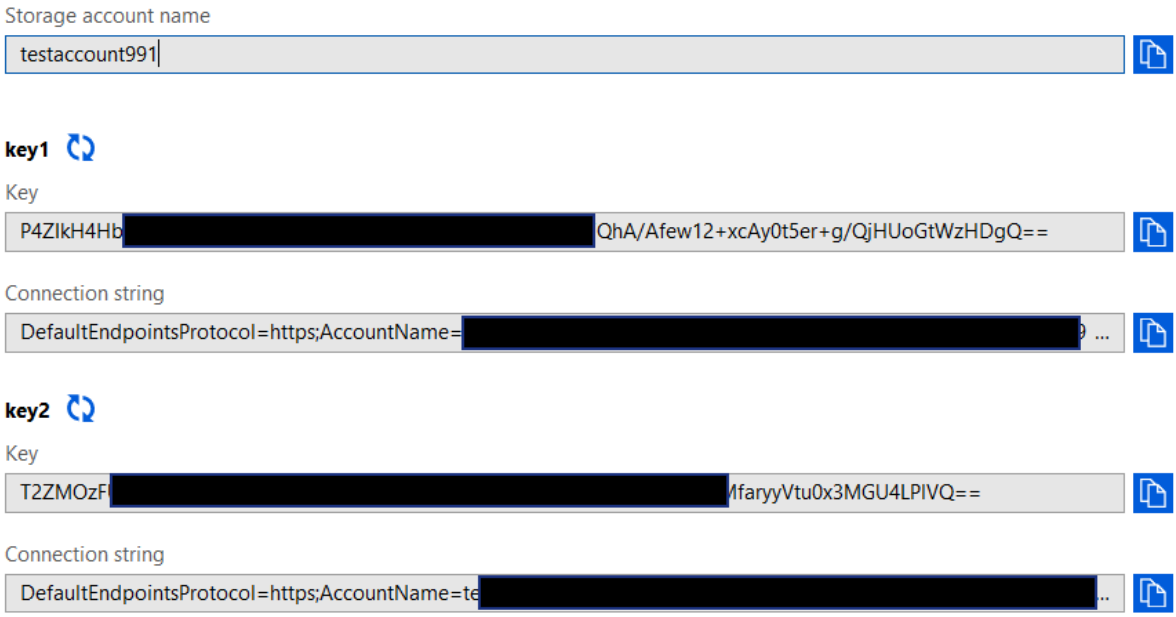
In order to connect a FileFlex account with Microsoft Azure Storage, you will require your Azure Storage access keys. To get them, go your Azure control panel, and go to your storage accounts by clicking on storage accounts on the left hand side:



Click your storage account to enter it (testaccount991 here). You will then be presented with your storage account details screen.



From there, select "Access keys":

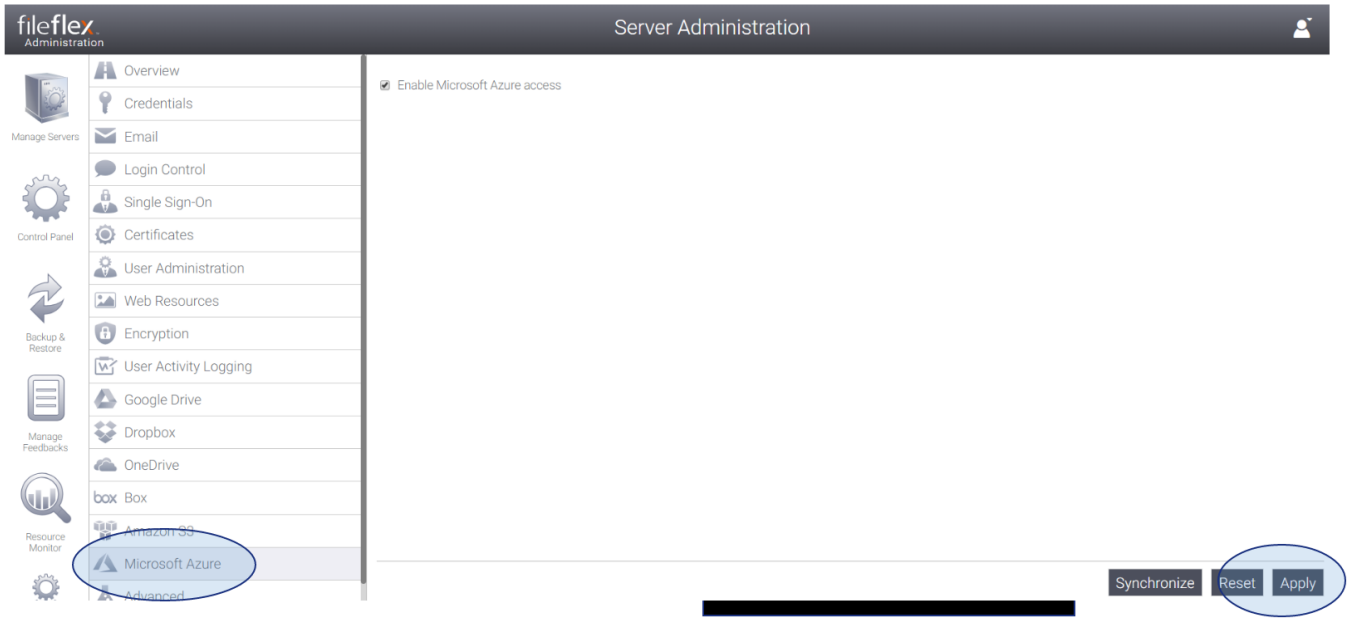


You will need the storage account name (testaccount991 here), and the first available key (94Zxxxxxxx here). Write these values down since you'll need them in the next section.

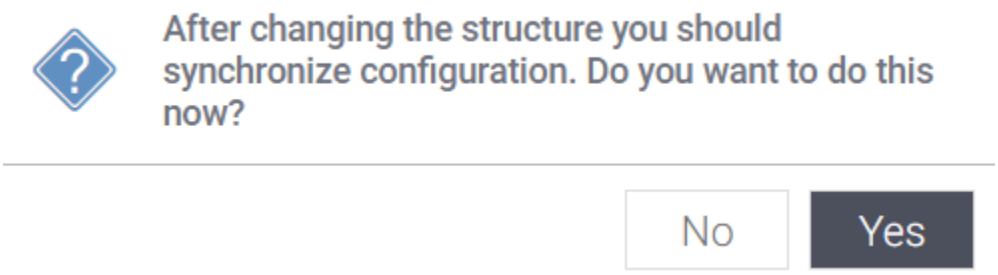
> Hint: Use the blue copy-to-clipboard icons on the right hand side to make this easier.

8.16.3. Enabling Azure Access

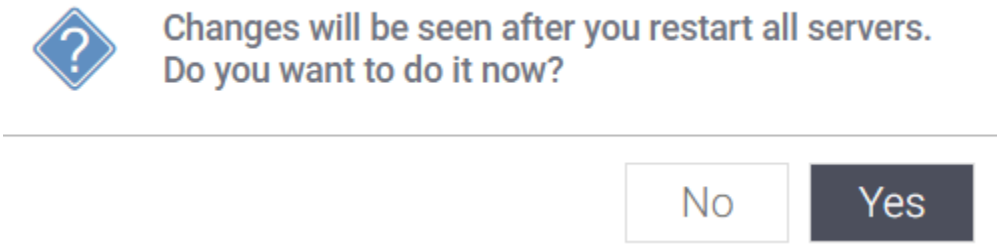
Open FileFlex Server Administration, and open the control panel tab. From there, open the "Microsoft Azure" panel:



Select the "Enable Microsoft Azure access" checkbox, followed by the apply button at the bottom right. You will see the following dialog:



Click "yes". After a few seconds, another dialog will be shown:



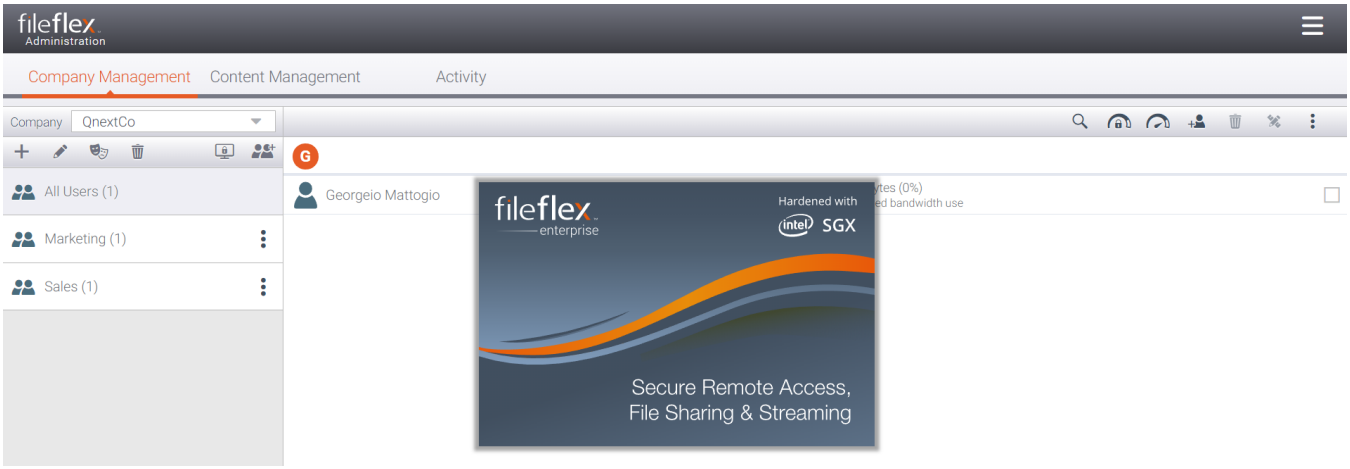
Click yes to restart the servers. After a few minutes, the server list will appear indicating that your servers are running normally. Click the control panel tab to verify that S3 has been configured:

8.16.4. Connecting FileFlex to an Azure Storage Share

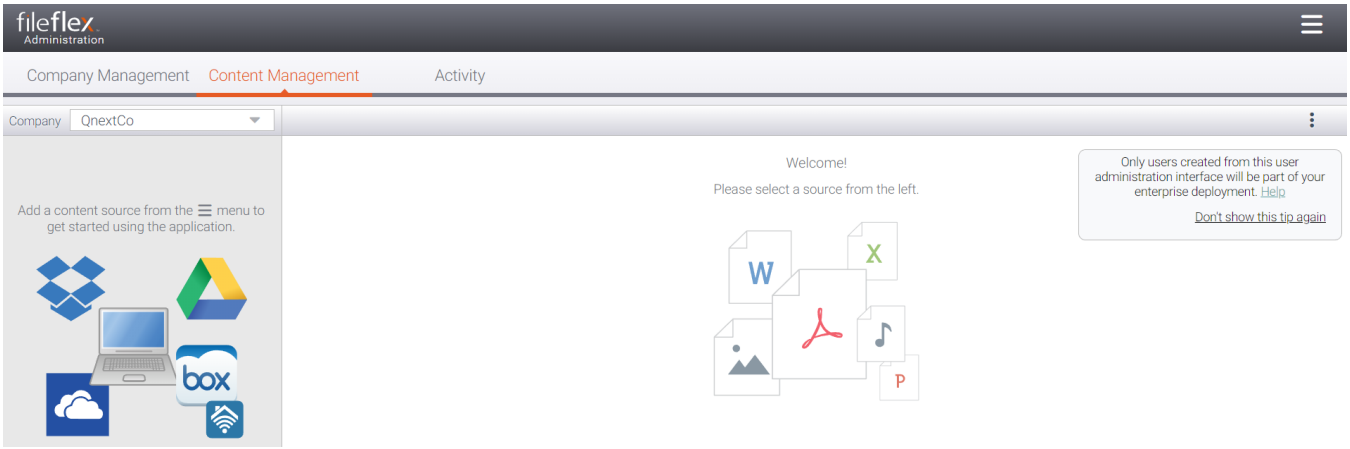
The connection between FileFlex and Azure is made from user administration, or as an end user when given permission to define content sources. This guide assumes that the content provider will be configured from user administration.

From Server Administration, click on the "Manage Users" tab from the left hand side. This will open User Administration in a new browser tab:

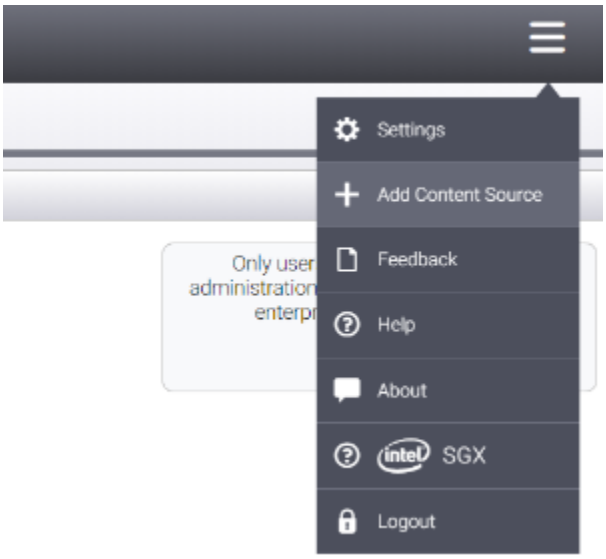
Enter your user administrator email address, followed by clicking on the Next button. Enter the password, followed by clicking on "Login" to complete the login. Once in, you will see the user administration application:



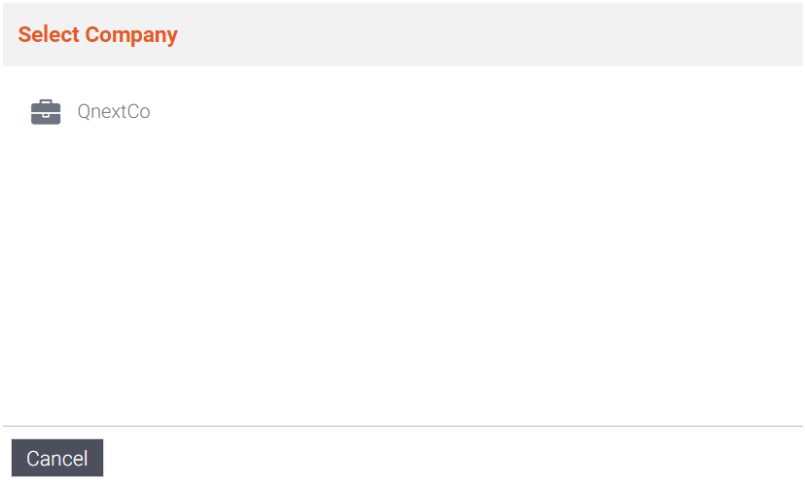
Click the "Content Management" tab:



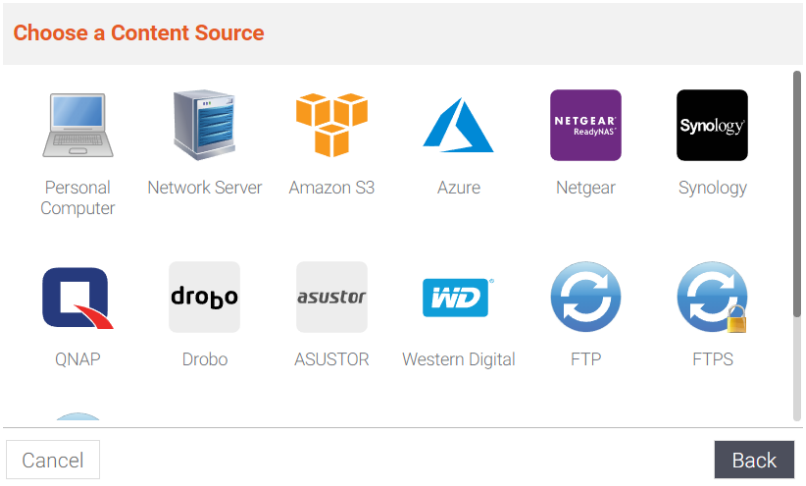
From the right hand menu, select "Add Content Source":



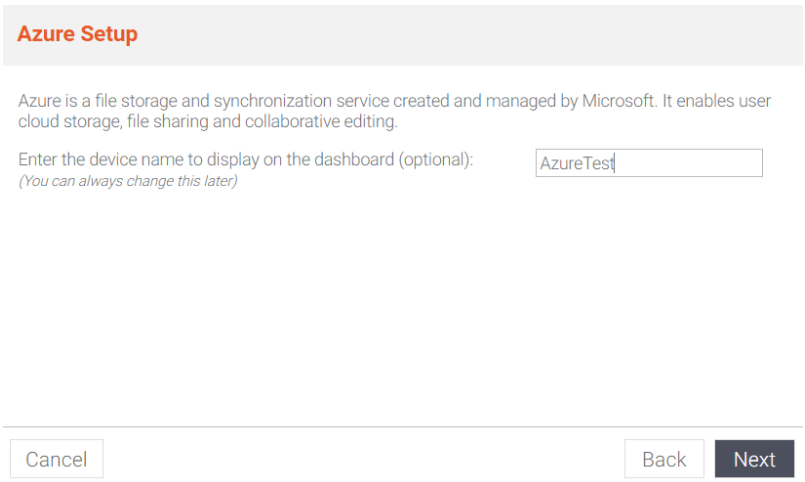
Select the company which will receive the Azure content source:



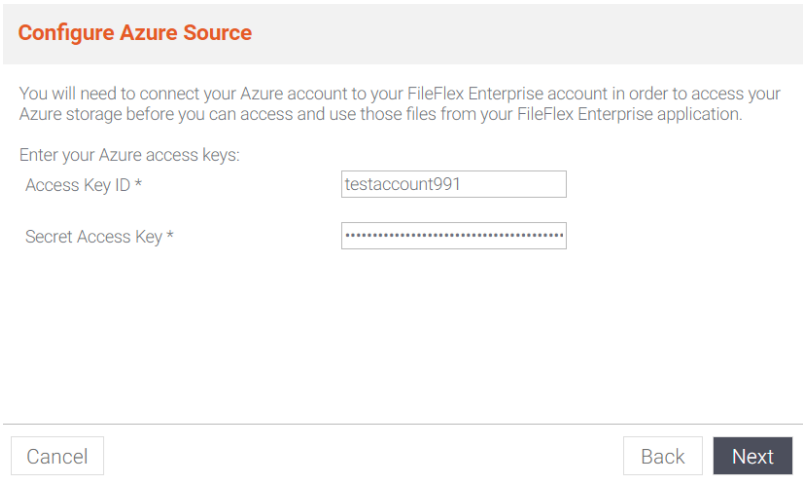
Select "Azure" as the content source:



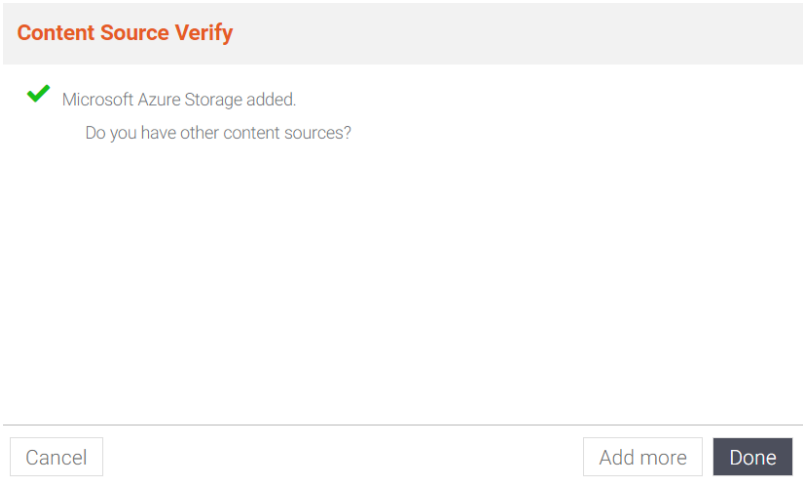
Enter a name for the content source. In this example we'll call it "Azure Test":



Click Next to continue. There you will see a screen asking you to enter your Azure Access Key ID and Access Key. The "Access Key ID" corresponds to the "storage account name" you wrote down earlier, while the "Secret Access Key" corresponds to the key you wrote down earlier (e.g. 94Zxxxxxxx).



Click Next. If the information you entered was correct, you will be presented with a confirmation screen as follows:



Congratulations - your Microsoft Azure Storage share is now accessible from FileFlex!

8.17. Configuring Google Cloud Access

In order to configure Google Cloud Storage for access from within FileFlex Enterprise, you must have a Storage bucket created under a project using Google Cloud Platform (GCP) Console. The project needs to have a Service Account created which has the required permissions to edit the bucket. You would then provide service account details to FileFlex so that you can start accessing Google Cloud from within FileFlex. This guide is in three parts - creating a bucket in GCP, creating a service account in GCP and configuring FileFlex.

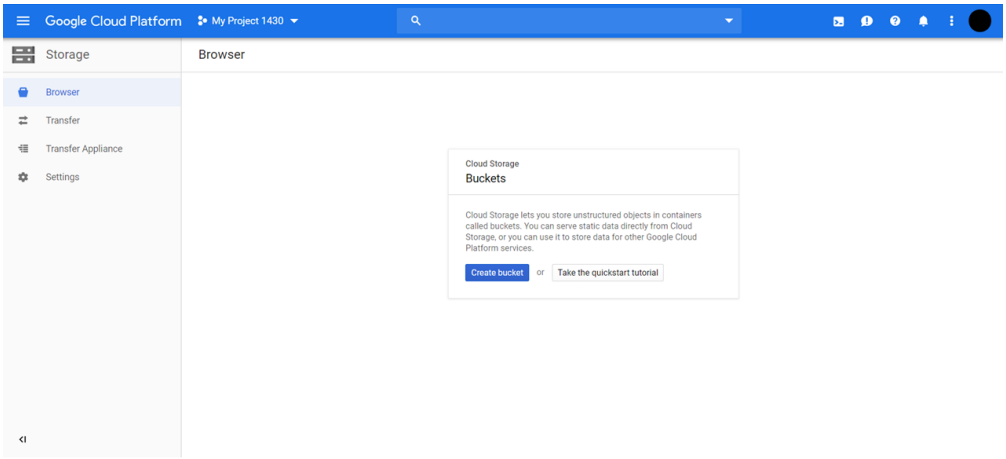
8.17.1. Creating a GCP bucket in a project

If you already have your bucket created, you can skip this section and proceed to the next section focussing on the creation of service account.

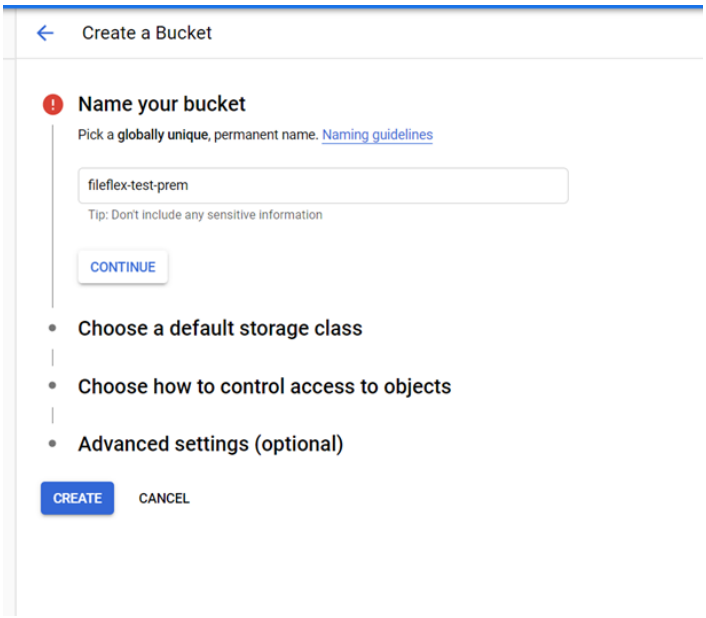
Login to the GCP console :

```
https://console.cloud.google.com/
```

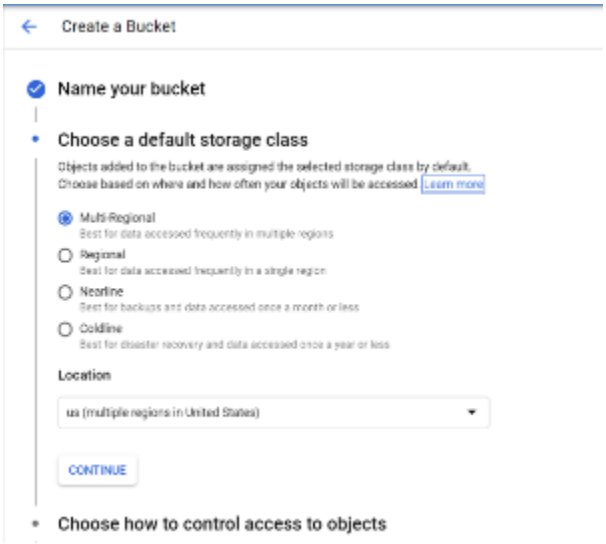
Once logged in it should look similar to as below. You should be logged into your default project if no project was created earlier.



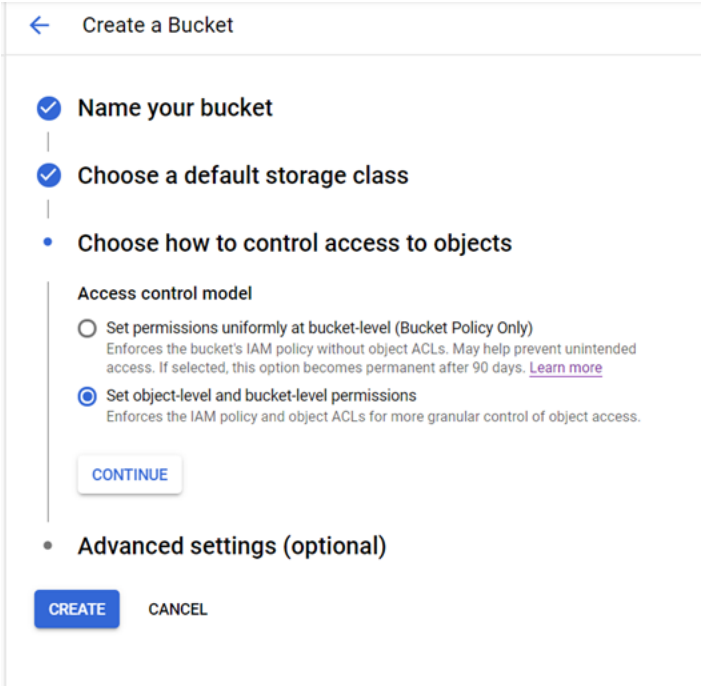
Click on "Create Bucket" and then provide a name to the bucket.



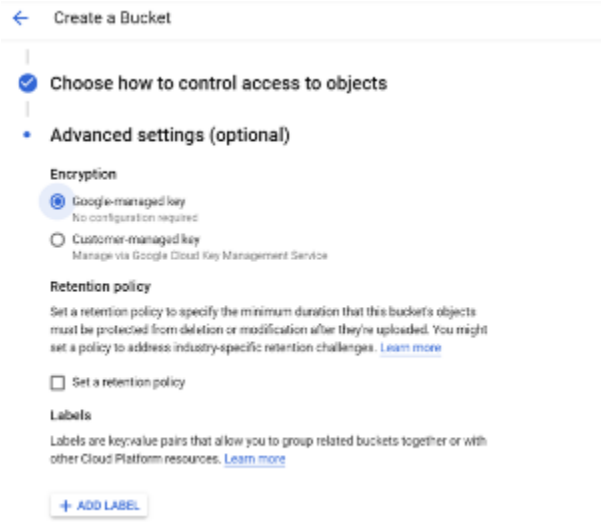
Select the storage class based on your need and location depending upon where you believe content will be mostly consumed from.



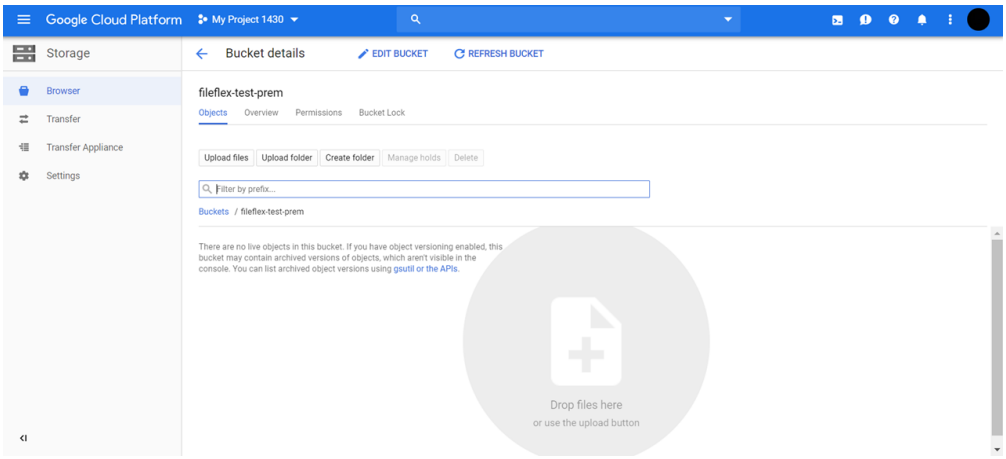
Select the access control model. Depending upon the access policy you want to create, you can select any of the models.



You can keep the default values in advanced settings or change it as per your requirements.



This completes the bucket creation process and you should see a similar screen as shown below.

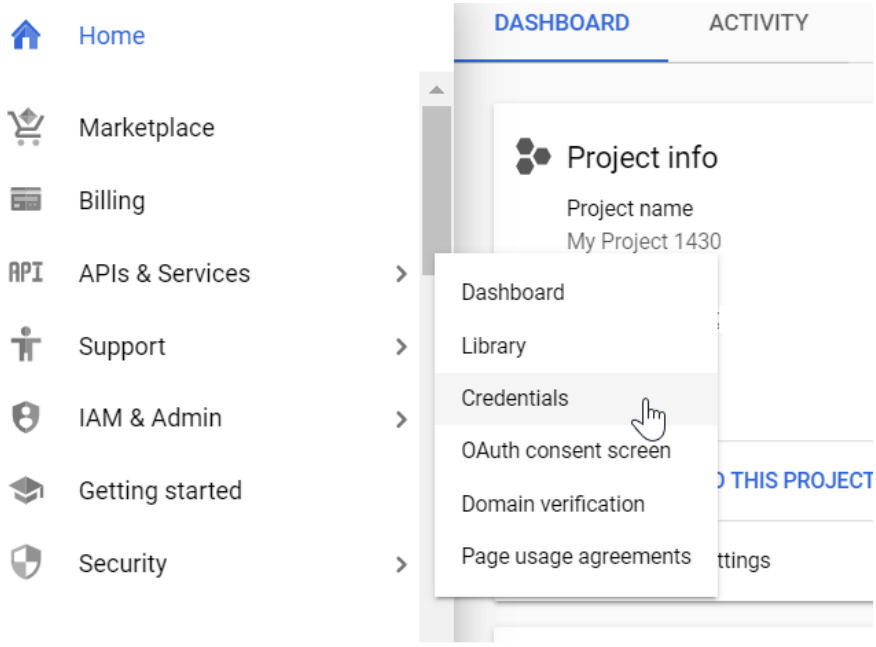


8.17.2. Creating OAuth-Credentials

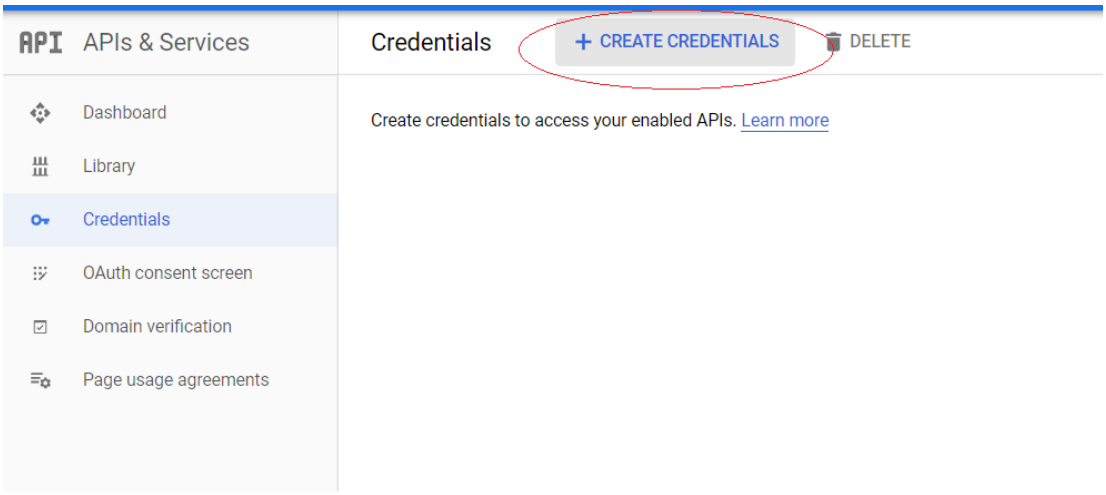
Once the bucket is created, you would need to create and publish an OAuth Client application whose details will be provided to FileFlex so that integration with Google Cloud can be completed.

This is also the place where you would provide the FileFlex Server URL in Google Console.

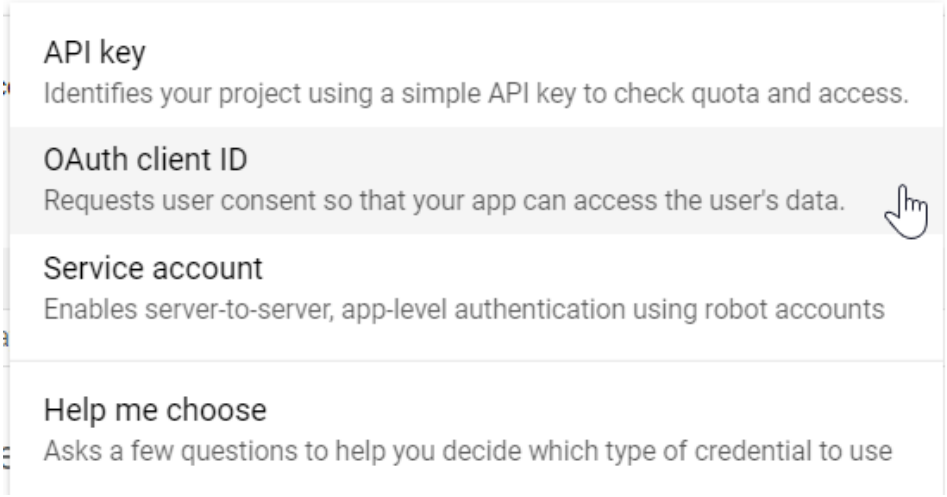
From the side-bar menu, select API & Services and then select Credentials



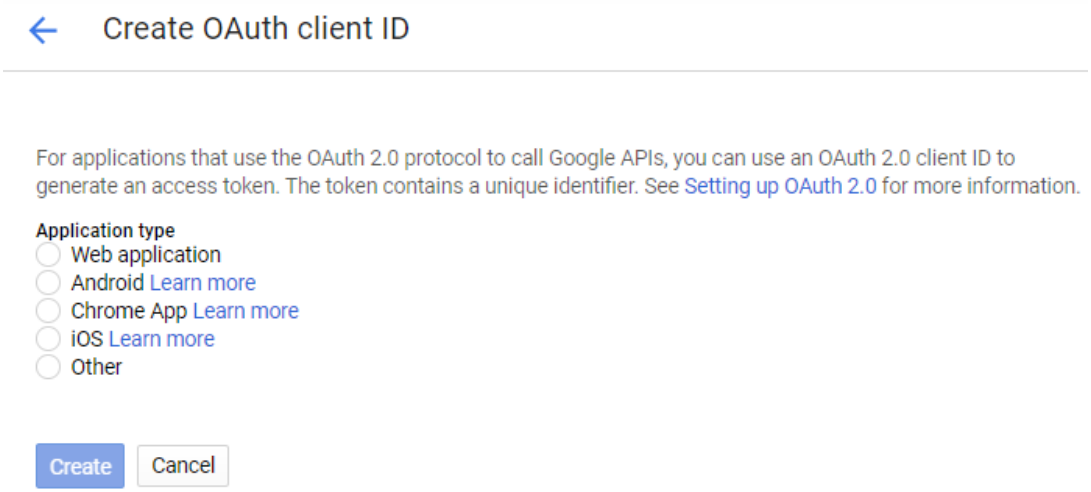
Click "CREATE CREDENTIALS"



Select "OAuth client ID"



Select "Web application"

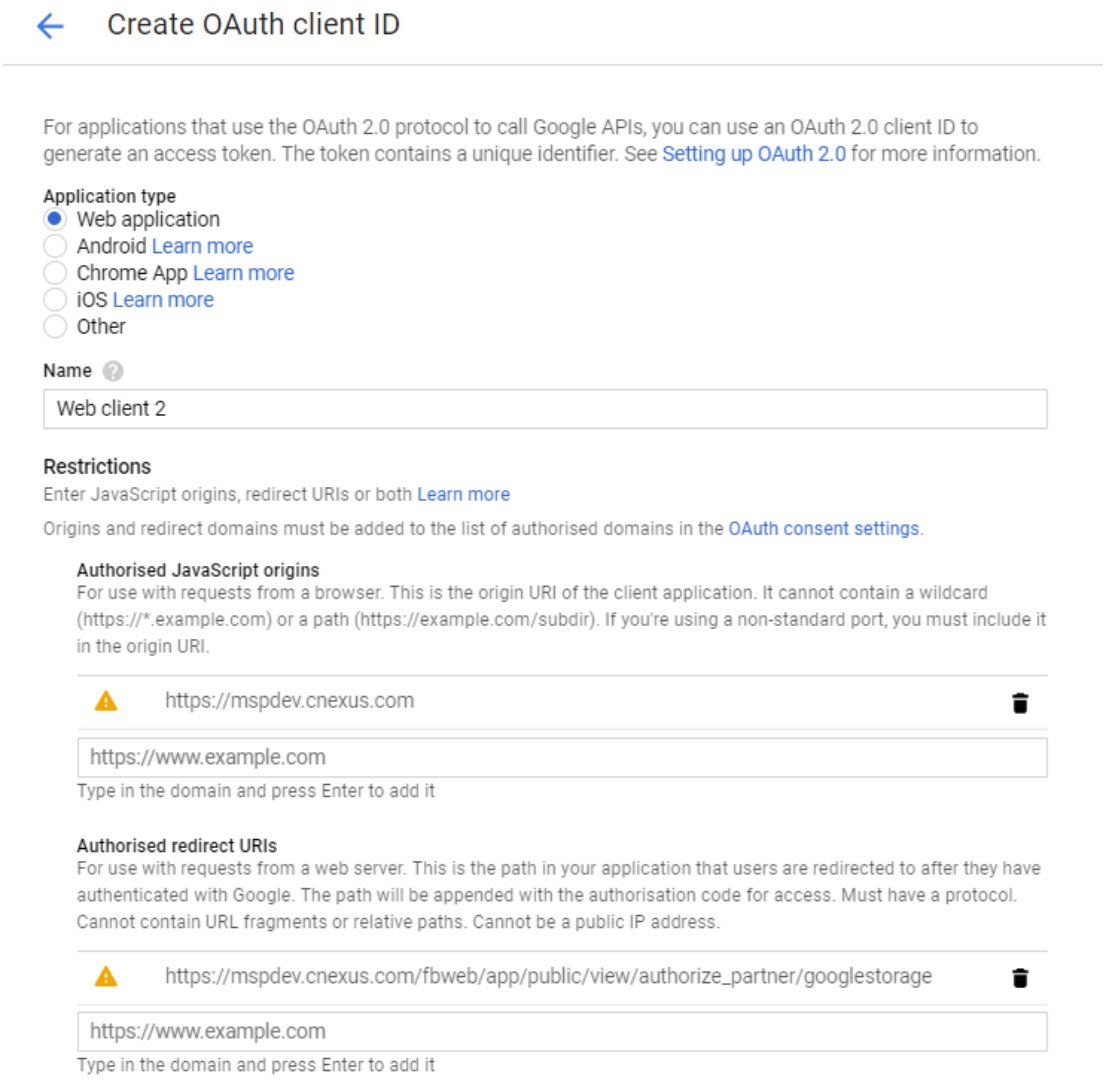


Provide your FileFlex server URL in authorized javascript origin as shown in example below:

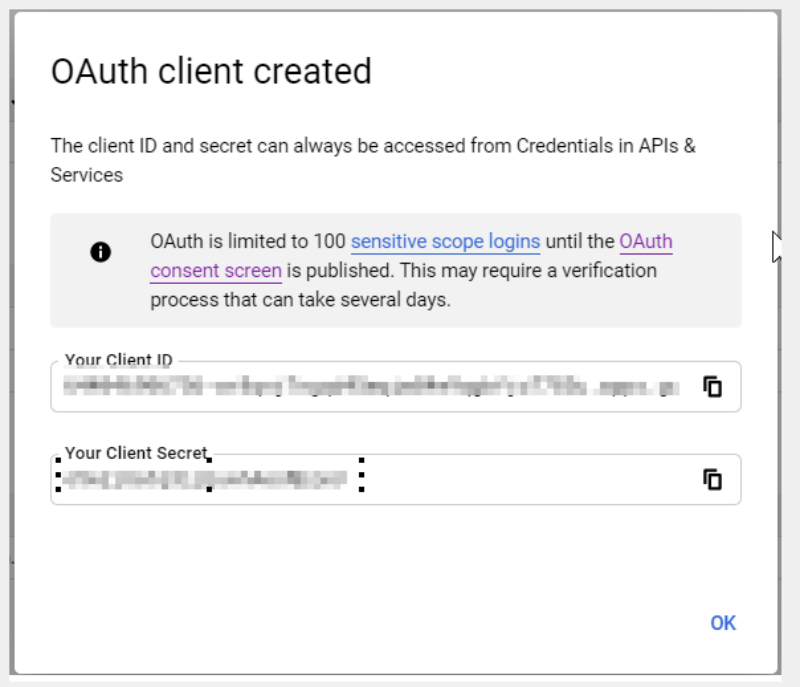
Authorized Javascript origin URI : <Fileflex server domain>

Authorized redirect URIs to include URI in below format

<Fileflex server domain>/fbweb/app/public/view/authorize_partner/googlestorage



Click Create.



Save the Client ID and Client secret in a text file as that would be required later when we need to provide the details of the newly created web client to FileFlex.

Click OK.

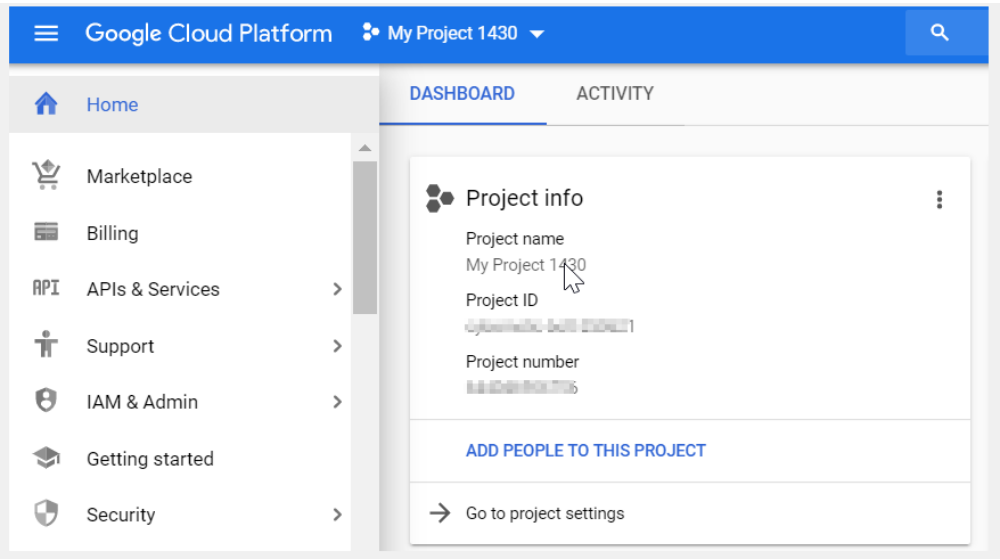
As a next step, you would need to ensure OAuth Consent includes the domain of Fileflex server.

Click the "OAuth consent screen" from the GCP Sidebar and complete the requested application.

Capturing Project ID

Click HOME from the side-bar of GCP console and identify your project tile.

Copy the project ID from the same and save it to Text File as shown in from a sample project below.

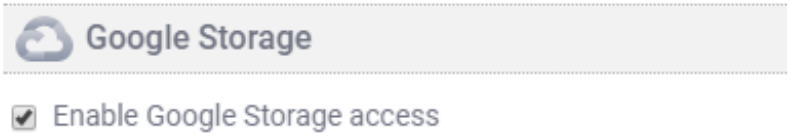


You can now move to FileFlex Server where the above-captured details will be provided.

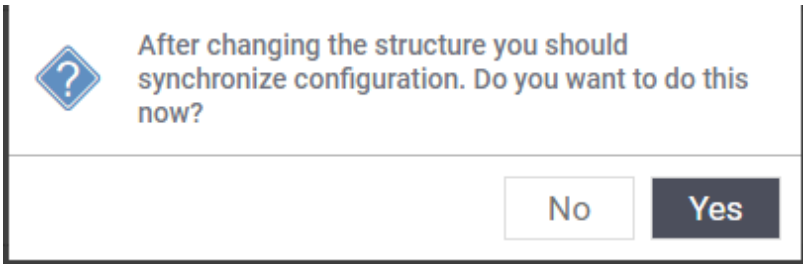
8.17.3. Enabling Google Cloud Access

Open FileFlex Server Administration, and open the control panel tab. From there, click "Cloud Storage" and scroll down to the section "Google Storage".

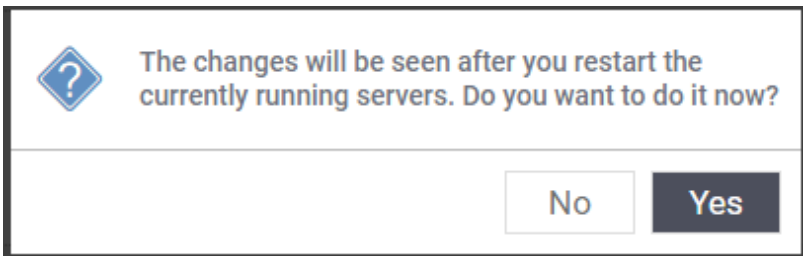
Select the checkbox to enable Goole Cloud access.



You will see the following dialog:



Click "Yes". After a few seconds, another dialog will be shown:

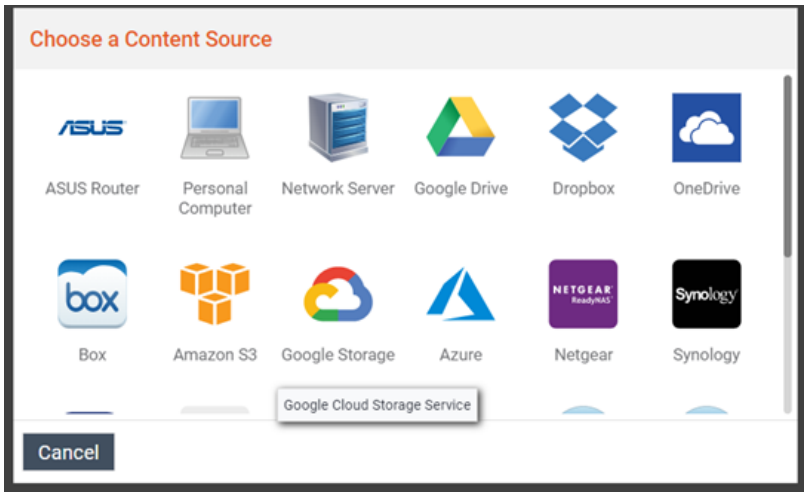


Click "Yes" to restart the servers. After a few minutes, the server list will appear indicating that your servers are running normally. Click the control panel tab to verify that Google Cloud has been configured.

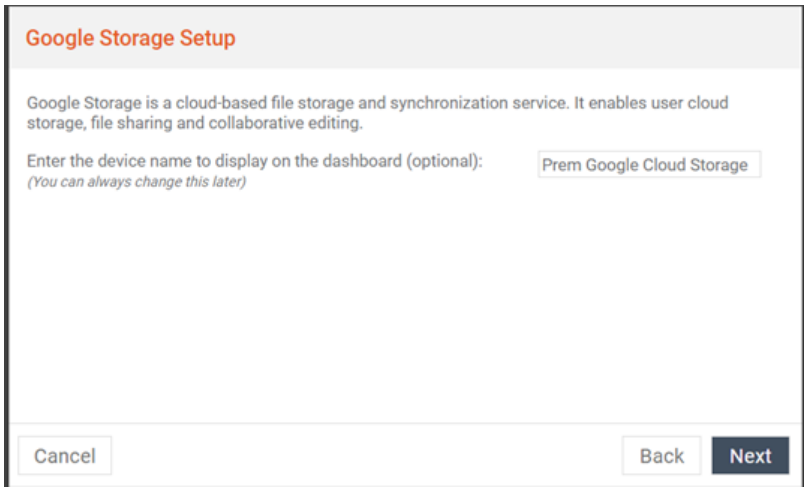
8.17.4. Configuring FileFlex

We now need to provide the details of the OAuth web client created above to FileFlex so that it can connect to the bucket created.

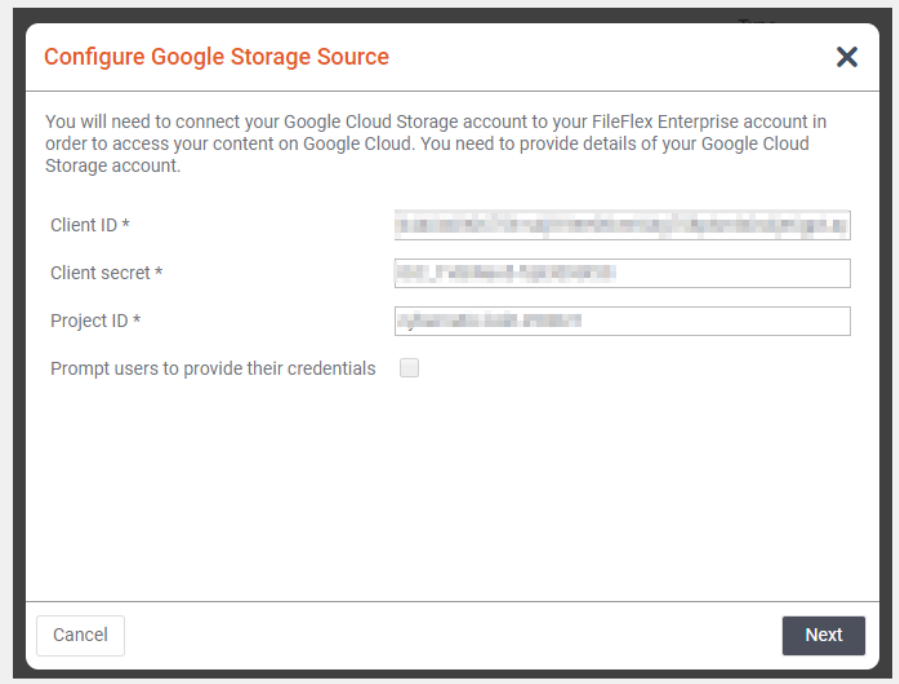
Login to FileFle and click on "Add content source"



Select Google Storage and in next step provide a nick-name (optional)

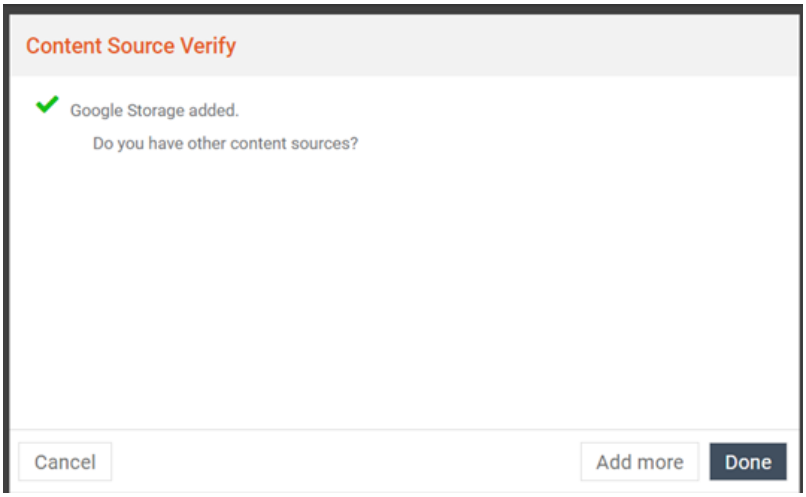


In the below screen, provide the values that were captured in previous section.



"Prompt user to provide their credentials": In the setup where all end users have their own credentials to GCP, you can check this option. In case your Google Organisation is not setup and only access id is used by the end-users, you can keep it unchecked.

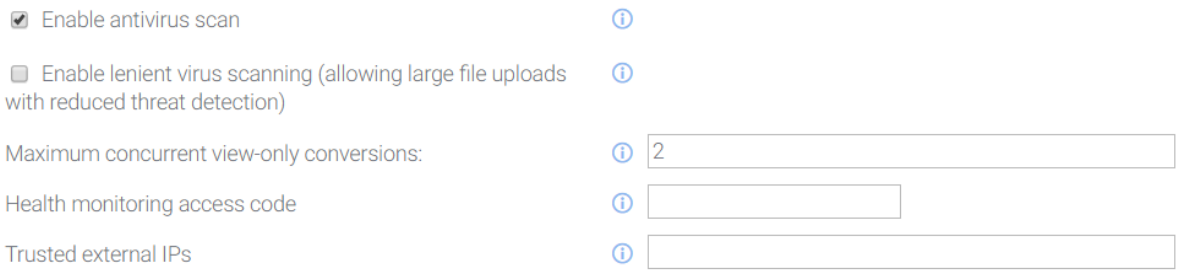
Click Next and FF setup with google cloud setup is now complete.



You can now access the content in google storage directly from FileFlex.

8.18. Advanced Settings

Clicking on the 'Advanced' panel of the Control Panel will reveal some configuration properties:



8.18.1. Enable Antivirus Scan

This enables or disables the integrated antivirus scanning for files uploaded to remote repositories that are not based on the FileFlex Connector Agent. More specifically, if enabled, files will be scanned while on their way to third party repositories such as Dropbox, Google Drive, or FTP servers. The content sources that are affected by this property are:

- Google Drive
- Dropbox
- Box.net
- Amazon S4
- Microsoft Azure
- Microsoft OneDrive
- FTP
- FTPS
- SFTP

All other content sources which are based on the FileFlex Connector Agent (e.g. PC and NAS devices) rely on local host-system based antivirus scanning, and are therefore not affected by this property.

> It's recommended that antivirus scanning remain active for security purposes. The most likely reason for wanting to disable it would be if the specific content being triggered is resulting in false positive detections.

8.18.2. Enable Lenient Virus Scanning

By default FileFlex is strict when it comes to the types of files that it will scan, to avoid the possibility of malware getting past the scanner. More specifically, it will not allow the following files to be uploaded:

- Files larger than 25mb cannot be uploaded.
- Archives (e.g. zip, tar, tgz, etc) cannot be uploaded.

If lenient virus scanning is enabled, these restrictions will be lifted, with the following known limitations when it comes to threat detection:

- Only the first 25mb of any file will be scanned for threats.
- Portions of an archive exceeding 100mb after expansion will not be scanned for threats.
- Only the first 25mb of any file contained within an archive will be scanned for threats.

8.18.3. Maximum Concurrent View-Only Conversions

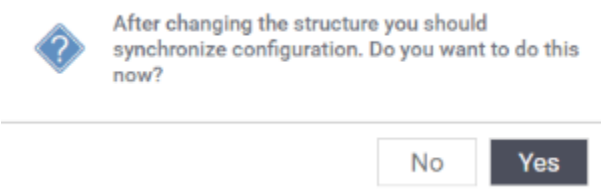
This defines the maximum number of view-only conversions that may execute at the same time. When a user chooses to view an office document within the application, a conversion is necessary. When this number of concurrent conversions is reached (e.g. 2 users are current waiting on a conversion), further users will wait in a queue until the conversions have completed. Depending on the frequency with which conversions are requested, you may need to increase this value.

The number of conversions that can happen at the same time is directly connected to the amount of CPU and RAM allocated to the server. Each "concurrent view-only conversion" requires 1 dedicated CPU core, and 1gb of RAM.

We recommend adding 1 CPU core and 1gb of RAM for each additional 1,000 users added to the system, depending on the frequency with which they are viewing documents within the application, and the size of the documents they are viewing.

Set the value to the desired value (in this example, 3):

Click the Apply button at the bottom, and you will be presented with a confirmation dialog:



Click "Yes" to proceed with the synchronization, and your change will be made immediately.

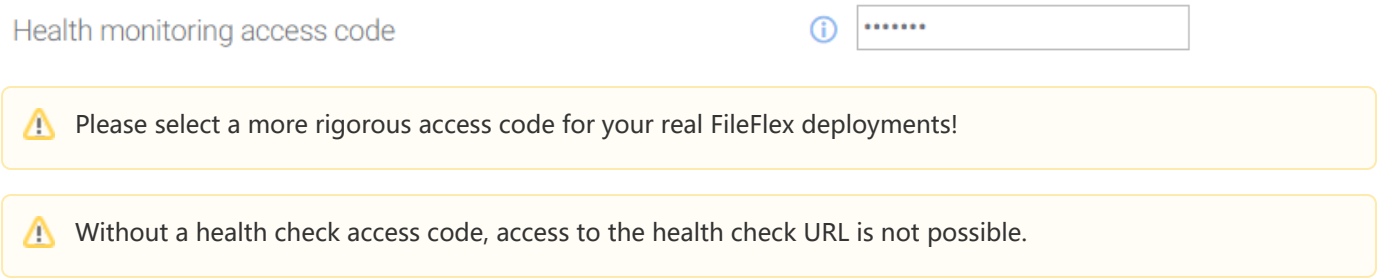
8.18.4. Health Check Monitoring

The remaining two properties (health monitoring access code and trusted external IPs) work together to allow third party server monioring solutions to keep an eye on your FileFlex deployment. For example, Nagios can be used to monitor the health of one or FileFlex deployments from a single monitoring control panel. Any monitoring system that supports HTTPS-based requests for health checks can be used.

Access to the health check URL is protected by an IP limitation and a secret monitoring access code.

8.18.4.1. Health Monitoring Access Code

Enter a secret monitoring access code (e.g. an access token) into the health monitoring access code field to ensure that only people with knowledge of this code can access the status of your FileFlex deployment. For example, entering "test123" results in a field similar to the following:



8.18.4.2. Trusted External IPs

You can limit access to only a specific set of externally visible IP addresses. For the common case of a single monitoring server, enter the monitoring server's IP. You can also use a wildcard as follows:

More specifically, the field is a regular expression, so any valid regular expression may be used here to allow an arbitrary set of IP addresses.

8.18.4.3. Health Check URL

The URL that must be used for a health check is the following:

Health Check URL Format

```
https://<HOSTNAME_OR_IP>/fbweb/internal/ajax/health?secret=<HEALTH_CHECK_ACCESS_CODE>
```

For example:

Example Health Check URL

```
https://192.168.2.241/fbweb/internal/ajax/health?secret=test123
```

8.18.4.4. Health Check Format

A successful health check will respond with a standard HTTP response code of 200, making basic health checks simple in most monitoring cases. Any system failure will result in a standard HTTP exception (400, 500 series). So long as your monitoring solution relies on these codes (most do), there should be no problem.

It is possible to extract more information from the health check response for a more detailed analysis (e.g. to ensure specific versions are deployed everywhere), but that is beyond the scope of this manual. The format of the response is JSON. An example follows:

Example Health Check Response

```
{
        "properties": {
                "version": "3.3.63",
                "date": "2017.06.13 14:17:28:753 UTC",
                "date_post": "2017.06.19 11:55:56:837 GMT",
                "date_start": "2017.06.21 16:31:18:330 GMT"
        },
        "performance": {
                "time": 84473,
                "cpu": 1.13,
                "memory_used": 153646048,
                "threads_live": 99,
                "load_system": 0.0
        },
        "storage": {
                "version": 13,
                "maintain": false
        },
        "messages": {
                "countSent": 1,
                "countReceived": 1
        }
}
```

8.18.4.5. Example Health Check with Nagios

A detailed description of deploying Nagios is beyond the scope of this manual. This example makes a few assumptions:

- Nagios 4 has been installed on a separated machine on the same local network.
- The Nagios check_http plugin has been deployed and is available.
- The reader is familiar with SSH access and the Nagios system.
- The reader has sudo access to the Nagios server.

These instructions where generated on a Ubuntu 16.04 Server deployment hosting Nagios 4 built from source. More specifically:

- The host operating system is Ubuntu 16.04
- Nagios version is: 4.3.4

In this example, the connectivity information is:

- Nagios monitoring server is on 192.168.2.236
- FileFlex is installed in a single machine deployment on 192.168.2.241
- The health check access code is "test123"

Start by ensuring that the access code is "test123" and that the Nagios monitoring server's IP is entered into the appropriate fields:

Log in to your Nagios monitoring server by SSH, and create a new server deployment file:

Creating the FileFlex Server in Nagios

```
cd /usr/local/nagios/etc/servers
sudo pico fileflex.cfg
```

Paste the following code into the editor:

```
define host {
        use                             linux-server
        host_name                       fileflexdemo
        alias                           FileFlex Deployment
        address                         192.168.2.241
        max_check_attempts              5
        check_period                    24x7
        notification_interval           30
        notification_period             24x7
}

define service {
        use                             generic-service
        host_name                       fileflex
        service_description             HTTPS Health Check
        check_command                   check_http!-H 192.168.2.241 -S -p 443 -u https://192.168.2.241/fbweb
/internal/ajax/health?secret=test123
        notification_interval           10
        notification_interval           60
        retry_interval                  5
        max_check_attempts              3
        check_interval                  10
        check_period                    24x7
        notification_period             24x7
        notifications_enabled           1
}
```

Ensure that the address field reflects the IP of your FileFlex deployment.

Ensure that your check_command statement uses your FileFlex IP, and the secret access code entered earlier.

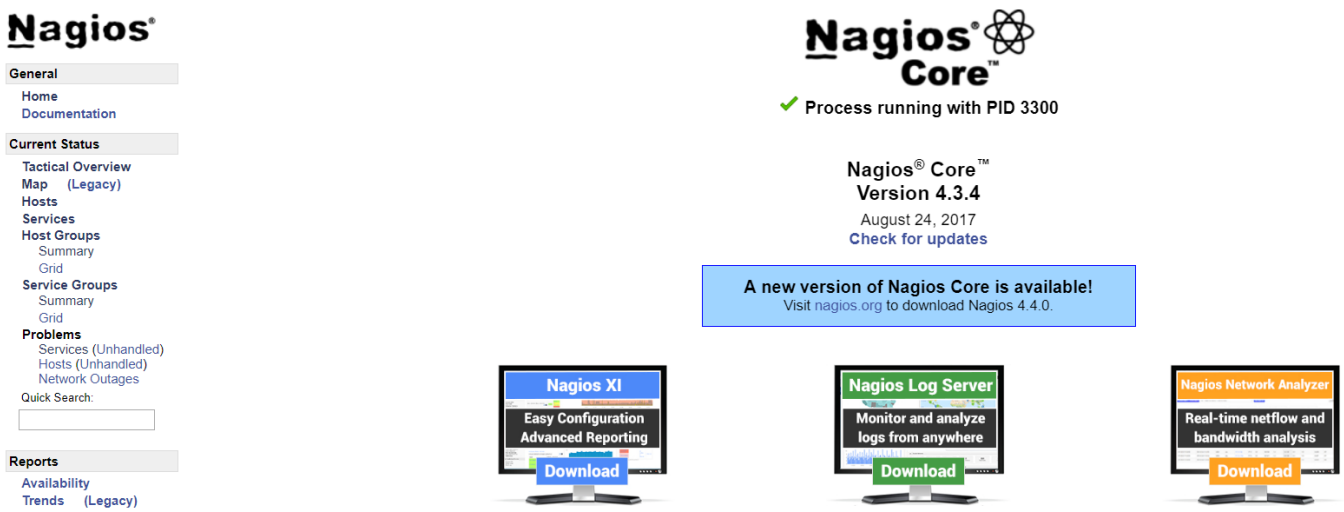
Save the file and exit the editor.

Restart Nagios:

Restarting Nagios

```
sudo /etc/init.d/nagios restart
```

Open your browser to the Nagios server's IP:



Click "services" from the left hand menu. After a few minutes you should see the following:

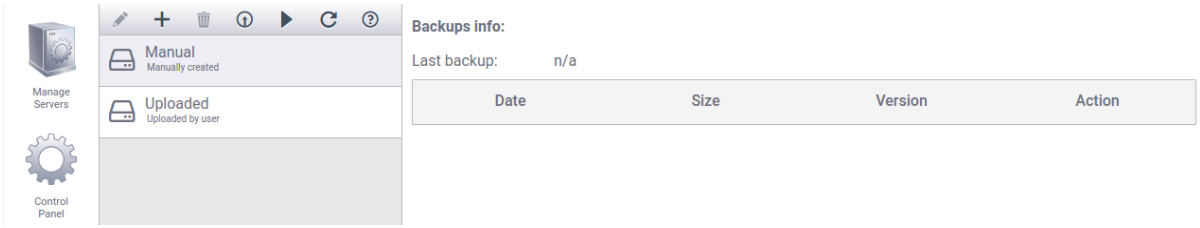
Your FileFlex server is now being monitored by Nagios.

9. Backup and Restore

This section describes the backup and restoration features available within the server administration module.

9.1. Backup and Restore Overview

Clicking on the "Backup & Restore" tab will reveal the following panel:

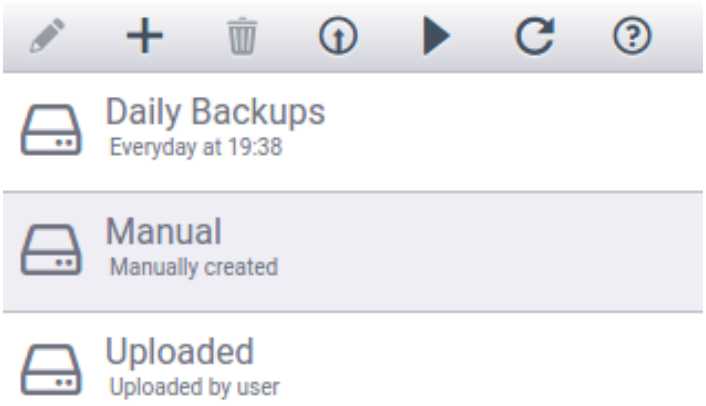


The screen is divided into two columns:

- The left hand side represents backup tasks and schedules.
- The right hand side lists all the backups performed according to the associated task.

9.1.1. Backup Task Panel

The backup task panel contains a toolbar of backup and restoration actions, along with a list of backup tasks:



The backup and restoration tools available are defined as follows:

	Edit the selected backup task. Use for example to change a daily backup to a weekly backup schedule.
	Add a new backup task. Use for example to start backing up files daily.
	Delete the selected backup task. Used to stop executing backups.
	Upload a backup from the administrator's local machine. Used to immediately restore data that you have locally available.
	Perform an immediate backup if the "manual" or "uploaded" rows are selected. If a configured backup task is selected, executes it immediately including it's associated offsite backup.
	Refresh the backup list. This is used in case the list is ever out of date because of a background backup task that happened while the panel was already opened.
	Open context-specific help relating to backup and restoration.

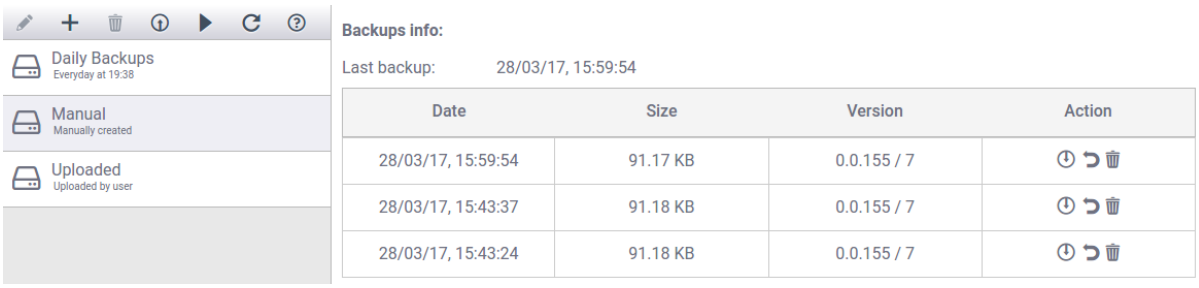
Below the toolbar is a list of backup tasks. Two items are permanently displayed:

Manual	List all manually backed up datasets (e.g. backup immediately)
Uploaded	List all manually uploaded datasets (e.g. uploaded by the administrator)

The other items in the list (for example 'daily' in the example above) are backup tasks that have been configured by the administrator to execute automatically. For instance daily backups, weekly backups, etc. Selecting a row from the list will visualize a filtered list in the backup task listing on the right hand side.

9.1.2. Backup Listing

Every backup task has a set of backup files associated with it (which could be empty). Selecting a backup task on the left will show a filtered list of backups on the right:



Each backup row shows it's date, size, version and a set of actions available to be performed with that particular backup. Consult the following table for more details:

Backup Column	Example	Meaning
Date	22/03/17, 12:41:47	The backup was taken on March 22, 2017 at 12:41:47
Size	8.63 MB	The backup occupies 8.63 MB of space
Version	0.0.153 / 7	The configuration that was backed up has version 0.0.153 The data that was backed up has version 7
Action		Download, Restore and Delete operations on that backup

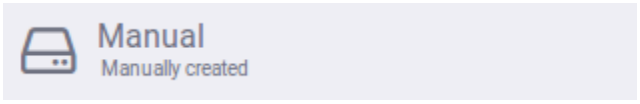
Backup Data or Configuration?

Configuration and data backups are handled separately. The reason for this is that you might want to back up your data when upgrading to a clustered deployment. Doing so would require radically different configuration, but the same underlying data. In that situation you would only restore the data.

9.1.3. Manual Backup

There are two kinds of backups which can be executed. The first and simplest is a manual back, which we'll describe here. A manual backup is executed immediately, and the data is stored within the VM. This is likely not where you'll want to store the backup files long term, so it's assumed that you'll download a local copy and store it someplace safe outside of the virtual image.

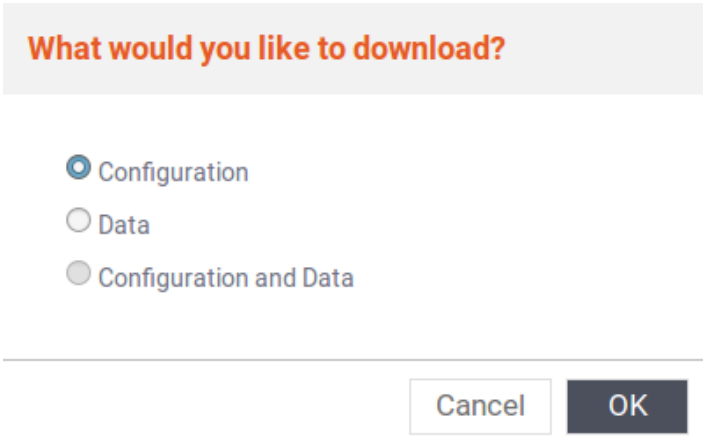
Select the 'manual' entry in the backup tasks on the left



Click on the backup now icon to initiate an immediate backup. After a moment you will see it listed on the right hand side:

Your backup is now complete, but unfortunately it's stored within your VM which isn't ideal. You should download a copy to your local device and then back it up somewhere of your choosing.

Click the backup tool of the backup set to download. You will be prompted if you want to download the configuration or data:



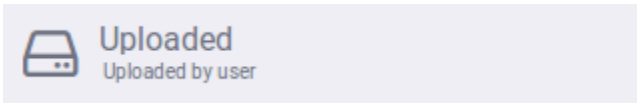
Select configuration followed by OK and the configuration data will be downloaded to your local machine. Repeat this procedure, downloading the data instead. You will now have two archives locally which you can use to restore configuration and/or data at any point in the future.

9.1.4. Restoring from Backups

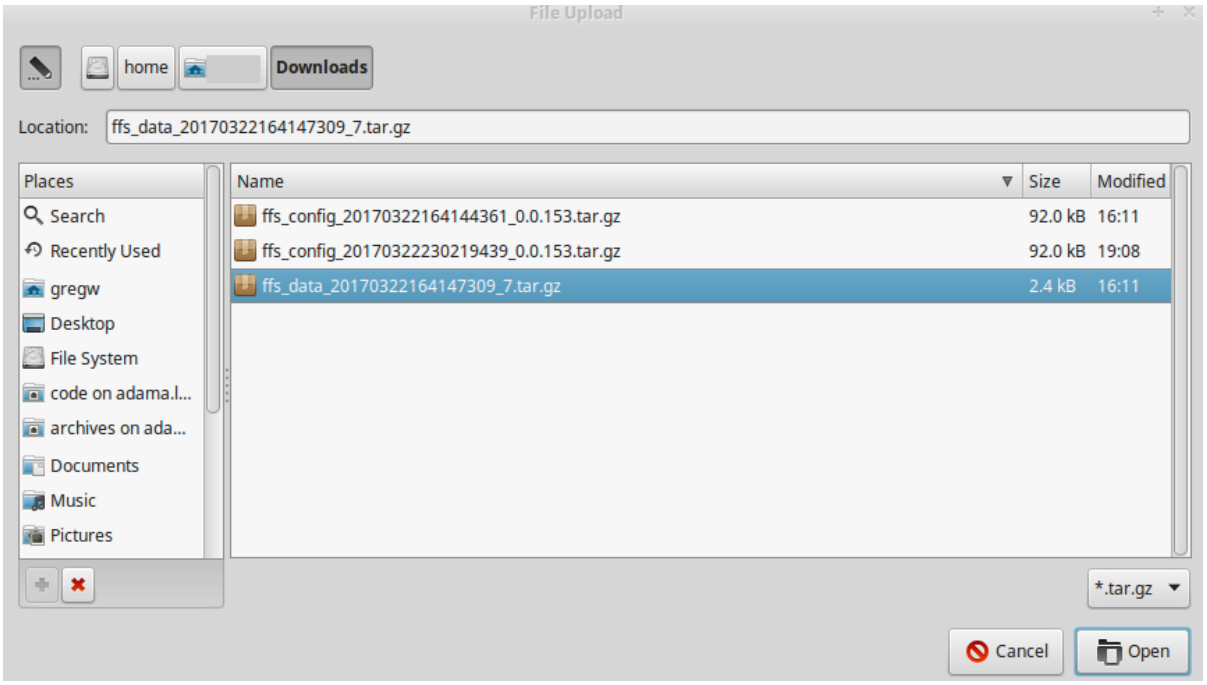
Once you have a backup you must be able to restore it. If the data is already contained in your VM as a backup set, you can restore it directly from there without uploading it in to your VM. If however you backed up your data somewhere manually (as suggested above), you'll need to upload your archives into the VM first.

9.1.4.1. Uploading Backups to the VM

Select the Uploaded row from the backup tasks on the left hand side to see all uploaded backup sets:



Ensure that your backup is not listed on the right hand side. This document assumes that it is not listed there. Click the upload action from the backup toolbar. You will then be asked to select a file from your local machine.



You can select either configuration or data backups, and the upload will automatically detect which type was provided. Here we are assuming you selected a data backup set.

> ⚠ It's important to understand that uploading a backup set is not the same thing as restoring it. It has simply been copied into the virtual machine.

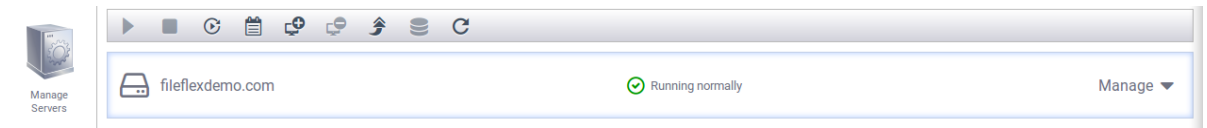
Once the upload is complete, you will see it listed on the right hand side:

9.1.4.2. Restoring Backups

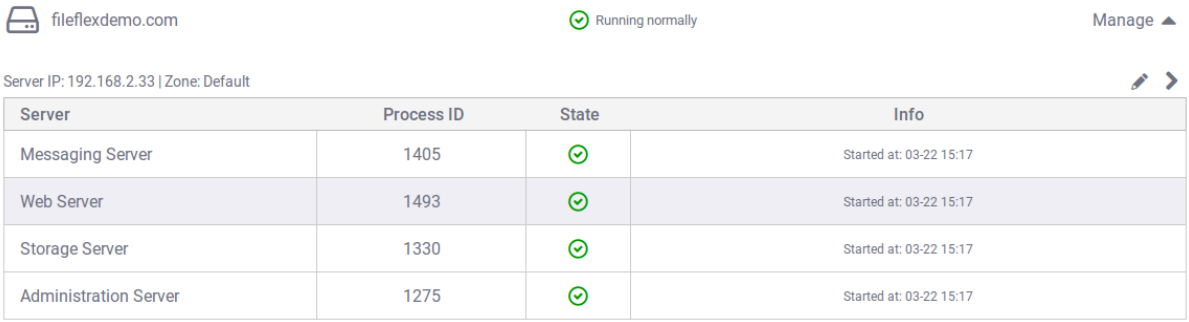
Once a backup set has been located within the VM (and it can be within any of the filters from the backup task list on the left), you can restore it.

> ⚠ A backup set may contain configuration information, or user data, or both

Prior to restoring a data set you must shut down the active processes. Click on manage servers on the left, and then select your active server:



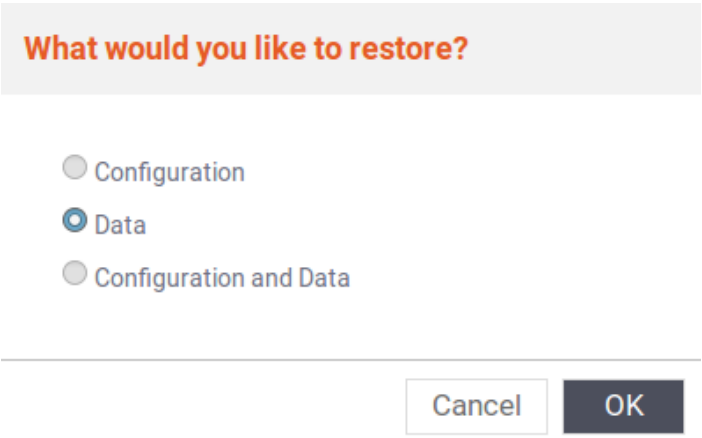
Click the manage button on the right to expand the server details:



Select the "web server" process followed by clicking the stop icon from the top menu. After a few moments you'll see the server listed with a warning that some processes are stopped:

Return to the backup and restore tab and select the "uploaded" backup task filter. Locate the backup set you wish to restore.

Once you identified backup set, click the restore action . You will then be asked if you want to restore configuration or data. Assuming you chose a backup set with data in it, select the data option (again, assuming that's what you're attempting to restore):



After clicking OK wait a few moment. When the operation completes, you will be returned to the backup set listing.

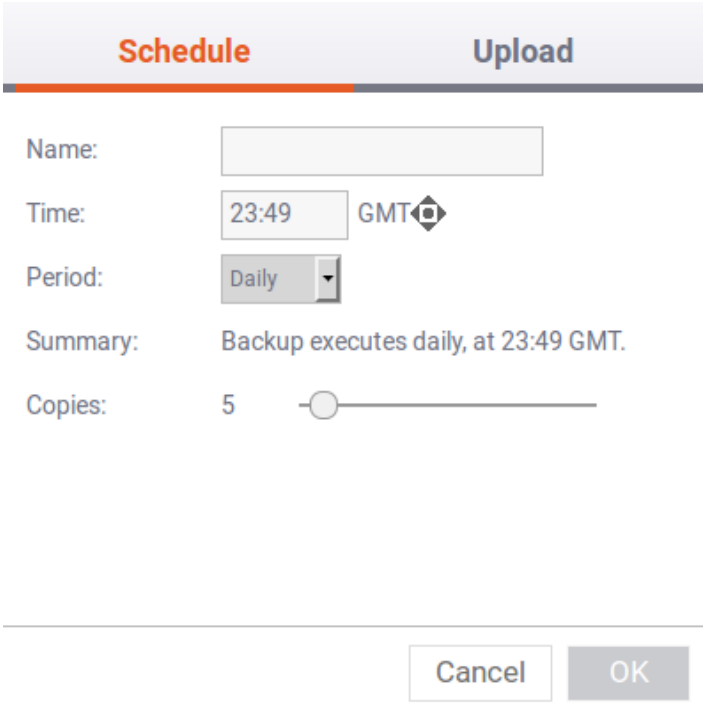
Congratulations - you've restored from backup!

9.1.5. Scheduling Backups

Scheduling automated backups is an important component of any backup strategy. You can configure FileFlex to automate backups on a variety of schedules, but something similar to a daily and weekly combination is recommended.

9.1.5.1. Creating an Automated Backup Task

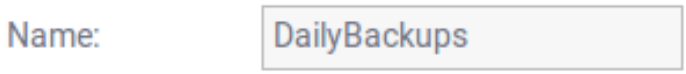
Start by clicking the new backup task button from the backup toolbar. You will then be presented with a scheduling dialog box:



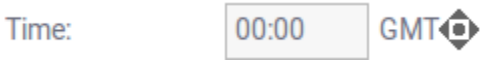
This is where you control exactly when the backups will be executed for this particular backup task.

> You may have any number of concurrently configured independent backup tasks. For example you can have daily backups, weekly backups, and first of the month backups.

Start by entering a name for your backup task:



Select a backup start time (defined in Greenwich Mean Time - GMT) for the backup set. For example, we will select midnight GMT:



> You can optionally use the diamond shaped control to the right of the time selection to increment the minutes and hours.

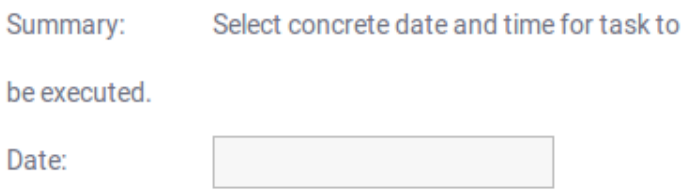
The next step is to select the time period for the backups.

9.1.5.1.1. One Time Backups

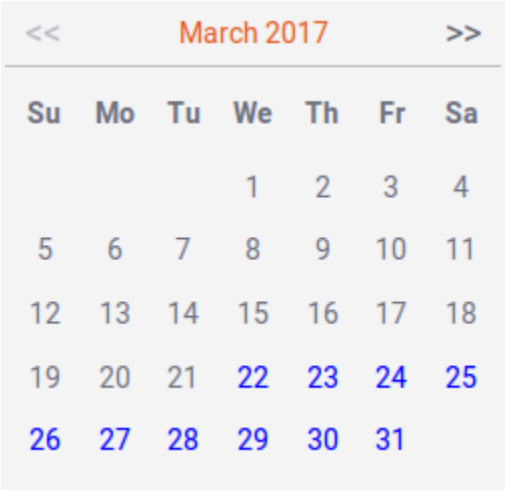
One time backups allow you to backup on a specific day at a specific time one time.

Select "Once" from the period dropdown:

A summary will be shown along with an empty date field.



Click in the date field to reveal the date picker:



Select the date you want the backup performed.

9.1.5.1.2. Daily Backups

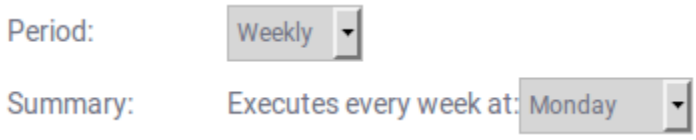
Daily backups allow you to backup every day at the specified time.

Select "Daily" from the period dropdown:

9.1.5.1.3. Weekly Backups

Weekly backups allow you to backup once a week on a selected day of the week at the specified time.

Select "Weekly" from the period dropdown:



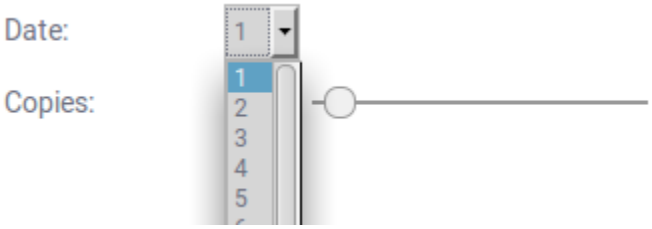
Select the day of the week you'd like to have the backups performed:

9.1.5.1.4. Monthly Backups

Monthly backups allow you to backup once a month on a selected day of the month at the specified time.

Select "Monthly" from the period dropdown:

Select the date (day of the month) you'd like to have the backups performed:



⚠ Only 28 days are allowed in the monthly backup schedule. It is not possible to select the 29th, 30th, or 31st of the month.

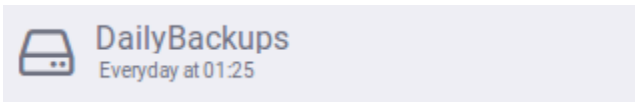
9.1.5.2. Number of Backup Copies

Since backups consume space within the virtual machine, it's important to limit the number of copies to retain for any backup task.

Drag the slider left or right to adjust the number copies. Values from 1 to 100 may be selected.

ⓘ It's a good idea to set the number of copies to a value that matches your time period. For example consider using 7 copies of a daily backup task, combined with 4 copies of a weekly backup task, combined with 12 copies of a monthly backup task to get a complete combination of backups from which to restore.

Once you're satisfied with your settings, click OK to confirm the backup schedule. You will then see your new entry in the list of backup tasks:



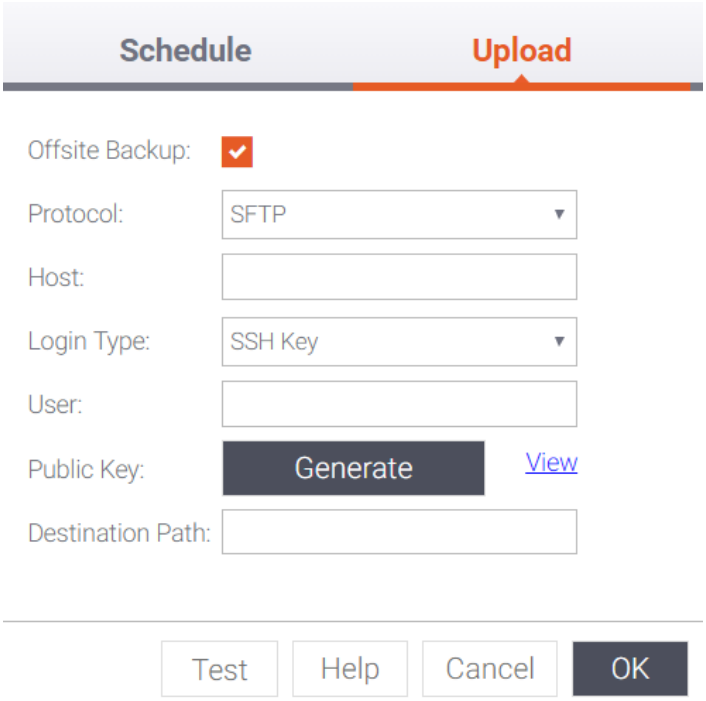
Congratulations - you've finished configuring your first backup schedule!

9.1.6. Offsite Backups

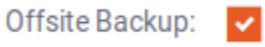
Offsite backups are a mechanism of automating the uploading of backup task results to a remote server. Keeping offsite copies allows you to automate the extraction of backup data from the FileFlex virtual machine and into your external servers for safe keeping.

> Offsite backups work with SFTP and rely on public/private keys to secure the transfers. Ensure that you have a public key enabled SFTP upload target before proceeding with this tutorial.

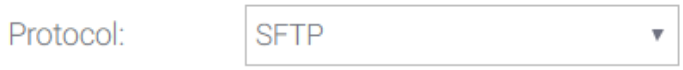
To enable offsite backups within your backup task, select the "Upload" tab in the backup task dialog:



You will then have to click the "Offsite Backup" check box to enable automated uploads of your backups:



From the "Protocol" dropdown, select the "SFTP" option:

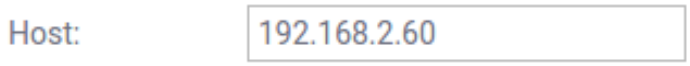


Advanced

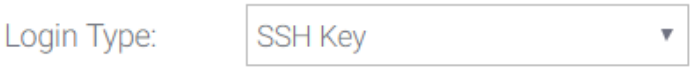
Although out of scope for this documentation, there is an advanced uploading mechanism allowed for. By selecting "Local Copy" from the "Protocol" dropdown, FileFlex will perform simple a local filesystem copy of the backups. Consider the following:

It is possible for you to SSH in to the virtual machine and configure (for example) an NFS mount point to a remote server of your choice. This would allow you to schedule the "copy" of backup sets to your NFS destination. Any mountable target is possible (for example, Samba, etc).

Enter a server/host you wish to connect to. In this example, we're connecting a local network IP:



Select the login type you wish to use. The options are "SSH Key" and "Password". This tutorial assumes that you will be using an SSH Key.

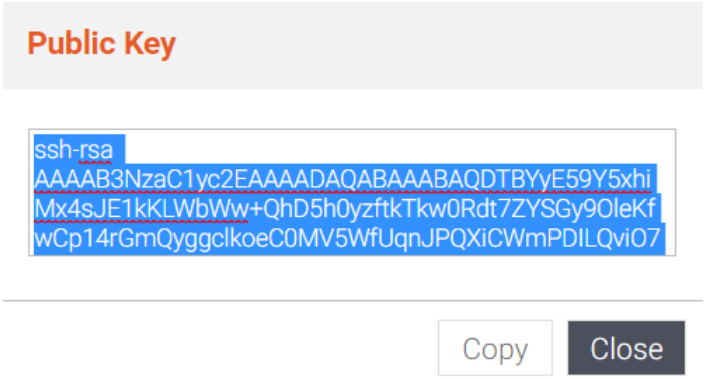


Using an SSH Key is more secure than using a password and is therefore the more desirable option.

Enter a username for your remote SSH connection:

Next, you will need to generate a public/private keypair. Click the "generate" button to do so:

Click the "view" link to show the public key contents:



Copy the key into your clipboard by clicking the copy button, and then close the dialog by clicking the close button.

Open a text editor, and paste the content of the key into it. Save the file somewhere in the file system of your current browser's operating system.

Uploading Your Public Key

In order to be allowed to upload into the remote SFTP server without a password being entered, you must upload your public key into that server. The specific instructions differ for varying destination server deployments, as well as for your current operating system. We assume you are using a desktop Linux (or Mac) system for this section of the documentation. If you are using windows, please adapt these instructions and use an application such as WinSCP.

For a typical Linux destination server, and assuming a user named "bkuser", the following steps will SCP the public key from the current host machine (containing your saved public key) to the remote machine using a password. From that point on, the public key will allow the backup process to upload remotely without a password. The example below assumes a remote host at 192.168.2.60, and a public key file named 'backup.pub'. Adjust your commands accordingly.

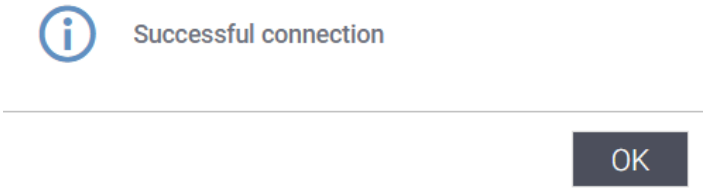
Run the following command, replacing the 'bkuser@192.168.2.60' with the appropriate user and IP for your backup destination.

```
awk 1 ~/backup.pub | ssh bkuser@192.168.2.60 "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys && chmod 600 ~/.ssh/authorized_keys"
```

Enter the password for the remote system when prompted. The remote system should now have your public key associated with the (example) bkuser account.

Enter a remote directory into which to place the backup files:

Click the test button to ensure everything is working. You should see a success message:



Click OK. Congratulations - when your backup task is executed your backups will be securely uploaded to the selected location using SFTP!

10. Managing Feedback

The feedback management of the control panel tab exposes your user's feedback messages to you. With those feebacks you are better able to provide support for your users with detailed information about what may have gone wrong. Additionally, you may (at your discretion) submit the information to the FileFlex team for further analysis and support.

When entering the panel you will see a list of feedback reports from your users:

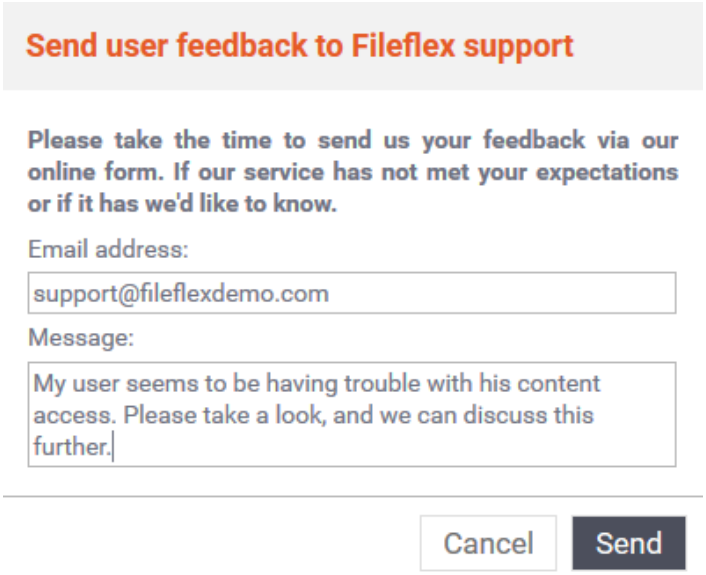
Date	Size	Server type	Hostname	Source	UserID	Reference ID	Action
Dec 11, 2017, 9...	5.48 KB	s.jetty	fileflexdemo.co...	main-client	QNadmin@filef...	node0cl1eqtgk...	
Dec 11, 2017, 9...	5.33 KB	s.jetty	fileflexdemo.co...	main-client	QNadmin@filef...	node0cl1eqtgk...	

Three operations are available for each user feedback item:

	Send to FileFlex Support
	Download Feedback
	Delete Feedback

10.1. Sending User Feedback to FileFlex Support

The "Send to FileFlex Support" option allows you to send a particular user's feedback to the FileFlex support team for further analysis. Clicking on the icon brings up a dialog in which you are prompted to enter a message for the FileFlex team along with your email address:



When you've completed that, click the send button to deliver the message and it's attachment to the FileFlex team for analysis. You will be contacted as soon as possible with a response.

10.2. Downloading User Feedback

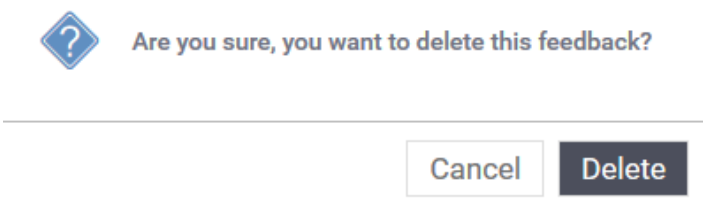
Clicking the download icon allows you to download the user feedback as a ZIP file. Within that file will be one or more text files relating to the user's situation. Opening that file will present you with detailed technical information, as well as the user name, time, date, and other criteria that may be relevant. For example:

```
Feedback received on: 2017.12.12 02:03:08:785 GMT
Date Sent: 2017.12.11 21:03:09:467
Received on: 10091@fileflexdemo.com
UID: QNadmin@fileflexdemo.com
Email: guy@notmyemail.com
Reference Number: node0cl1eqtgkppod43qmdherp2ti0
Address: 192.168.2.80
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
=====
Description: Why is there a button for feedback submission? I can't understand it's purpose.
```

Additional detailed technical information is present, but the intention is for that information to be analyzed by the FileFlex support team.

10.3. Deleting Feedback

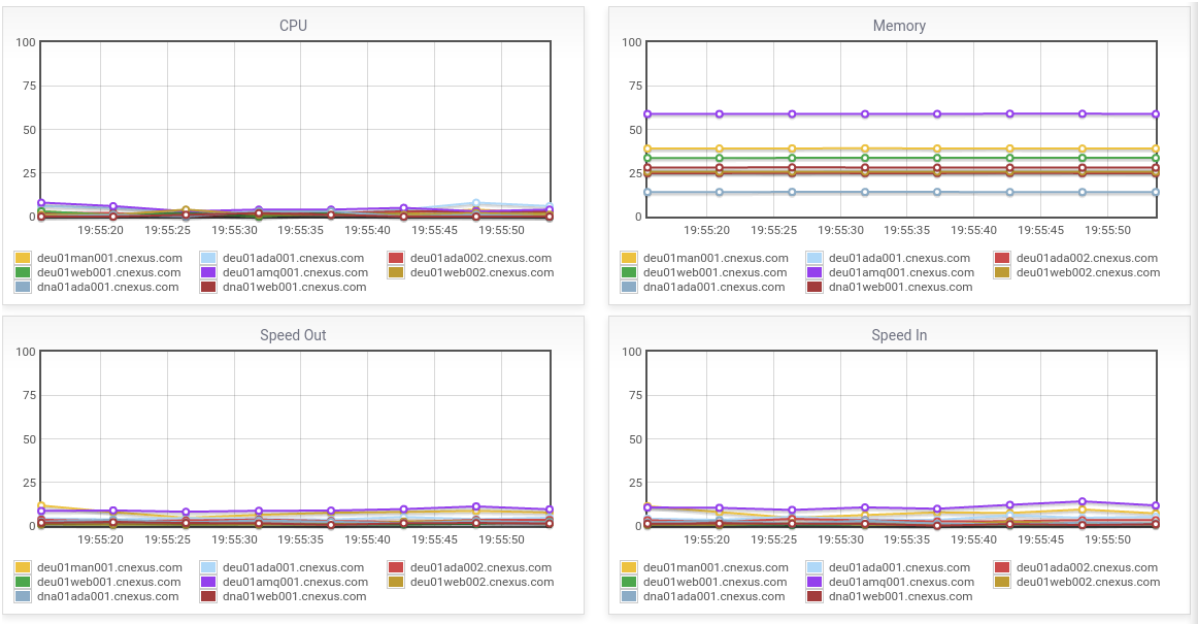
Over time you may accumulate many feedbacks from your users, and you can save space and clutter by periodically deleting items that are no longer of user. Clicking the "delete" icon will provide you with a prompt:



Click the delete button to permanently delete that user feedback item.

11. Resource Monitor

This section describes the resource monitor and the visualizations it provides to help you understand the resources available to your deployment. Clicking the "Resource Monitor" tab will reveal a set of graphs similar to the following:

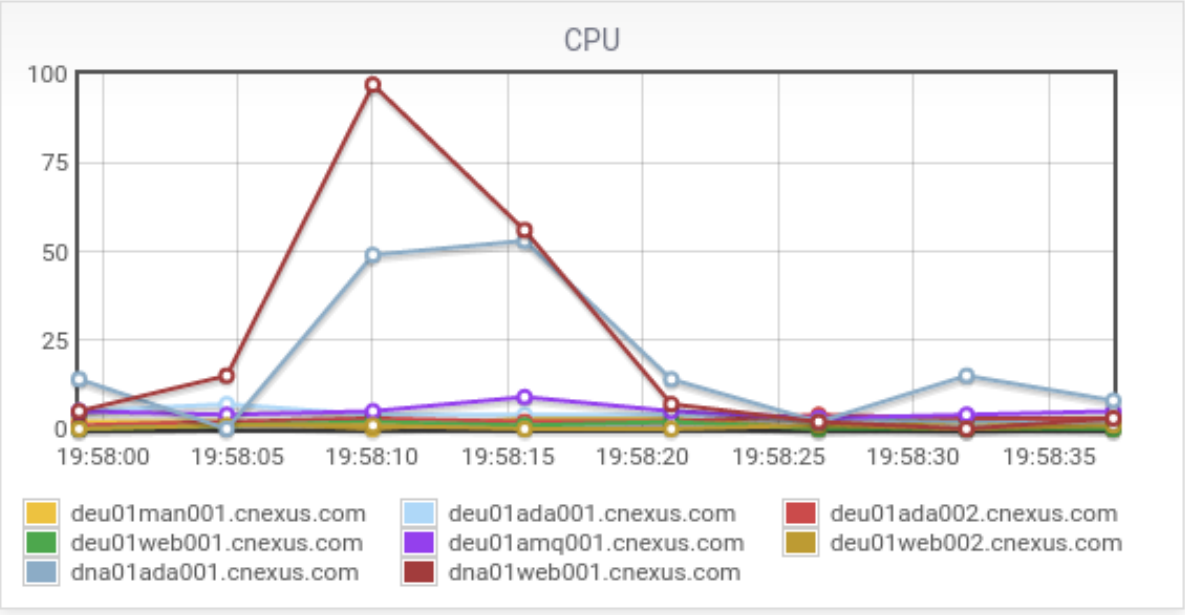


Each graph represents a different performance metric, while each colour of line represents a different machine within the clustered deployment.

⚠ SIngle machine deployments will only have single lines as shown in the image below.

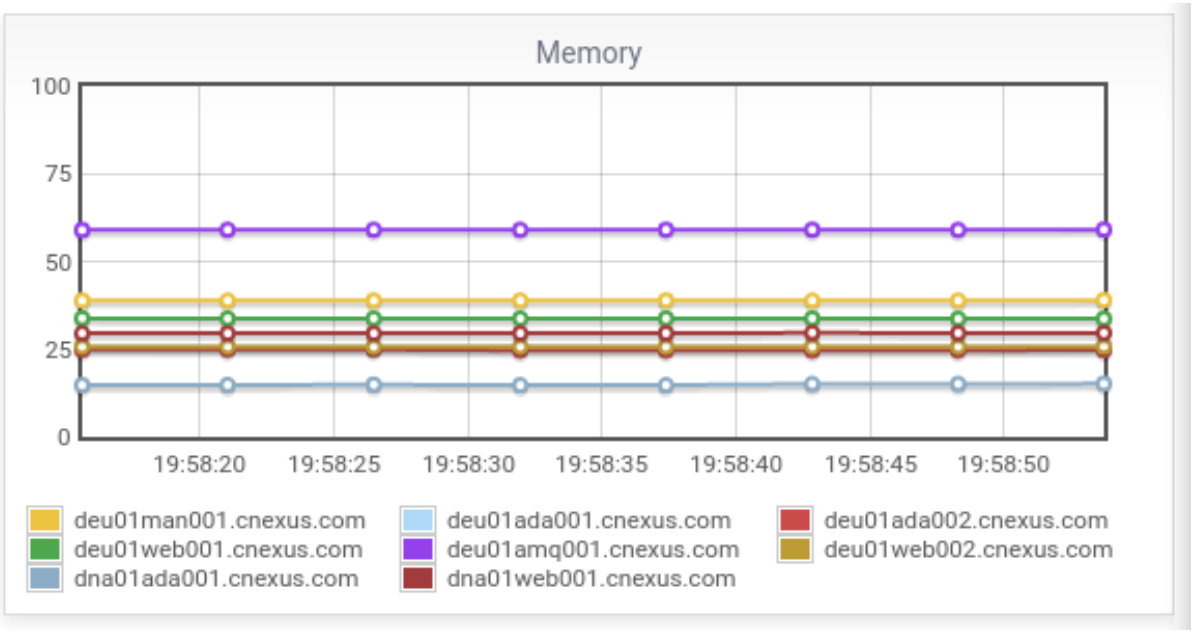
11.1. CPU Utilization

The CPU utilization represents the amount of CPU in use at a given time. It is relative to the total available CPU capacity available to the (virtual) machine.



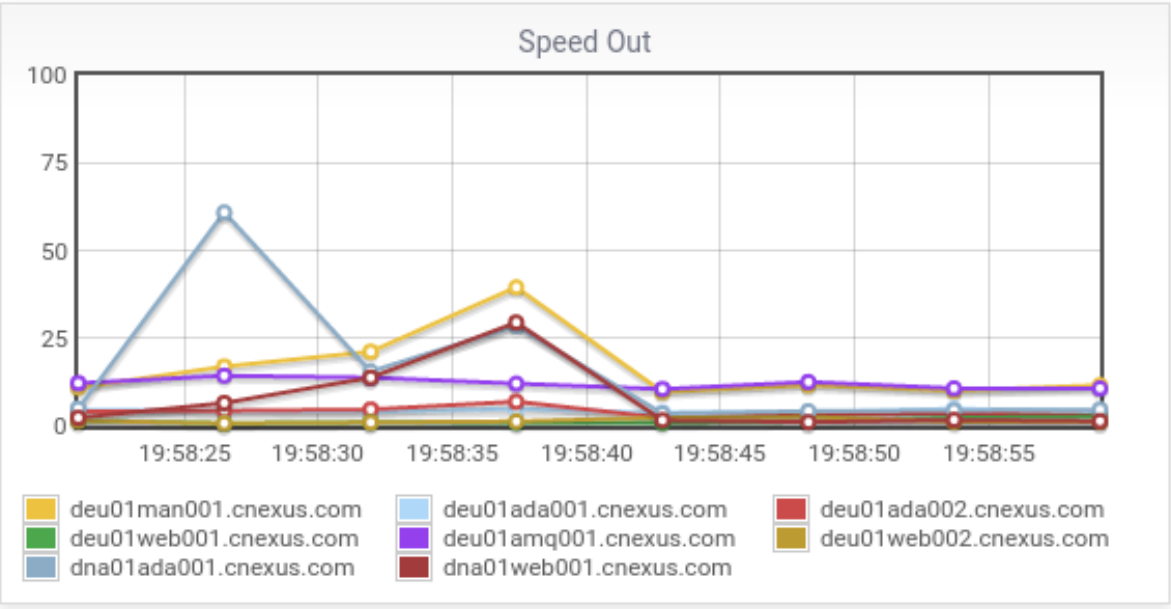
11.2. Memory Utilization

The memory utilization represents the total amount of memory in use on the system relative to the total amount available at a given time.



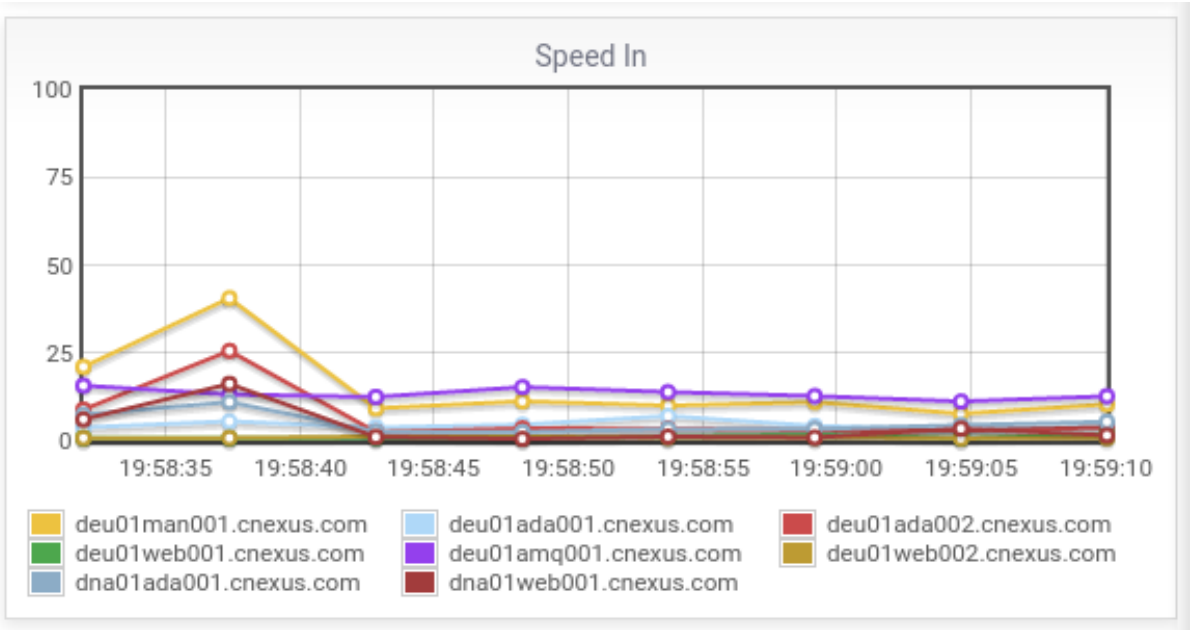
11.3. Speed Out

The speed out represents the proportional traffic egress relative to the maximum burst used on any machine in the cluster within the visualized time range.



11.4. Speed In

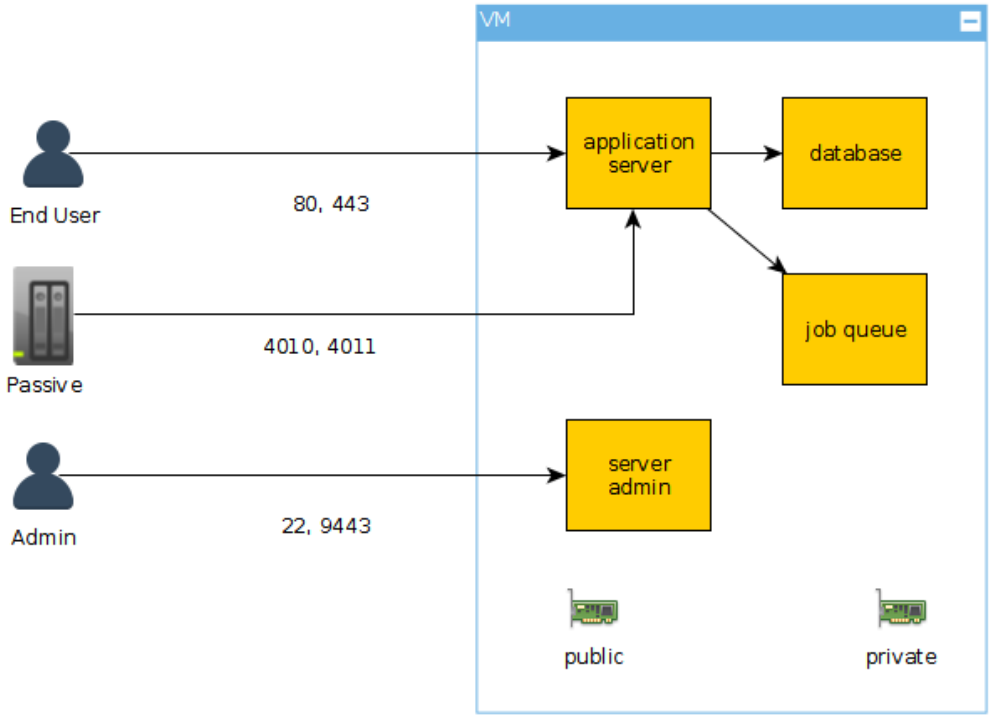
The speed in represents the proportional traffic ingress relative to the maximum burst used on any machine in the cluster within the visualized time range.



12. Appendix

12.1. Recommended Security Practices

The FileFlex Enterprise virtual machine includes a locally running firewall to help deter intrusions, however it's recommended that the solution be further protected within your enterprise by additional firewall devices to restrict administrative functions to specific IP addresses. The port assignments required by FileFlex are defined in the following diagram:



The following table lists the suggested accessibility for the relevant ports. Other non-listed ports are specifically blocked by the VM firewall, but should also be blocked by any additional appliances in front of FileFlex. Within the table, public and private access are defined as follows:

- Public access: Scope of IP addresses that will need access to the solution as end users.
  - Typically open to the outside world depending on the specific needs of the customer based primarily on their potential need to share outside the organization.
  - It is recommended that when global access is not required, that geo-location aware firewall rules be put in place to restrict access from unauthorized countries.
- Private access: Scope of IP addresses that will need access to FileFlex administration.
  - It is recommended that access to these ports be restricted to specifically authorized administrative IP addresses.

Ports	Purpose	Public Access	Private Access
80, 443	Web access	Yes	Yes
4010, 4011	Connector access	Yes	Yes
22	SSH access	No	Yes
9443	Server admin access	No	Yes

> ⚠ **SSH Notes**
>
> FileFlex is configured to use SSHv2 exclusively, and does not allow SSHv1 connections. Ensure that your clients are appropriately configured to use this version. Version 2 is is certified under the FIPS 140-1 and 140-2 NIST /U.S government cryptographic standards, and brings additional security features including improved crytographic cyphers (such as 3DES and AES), the use of sound cryptographic Message Authentication Code (MAC) algorithms for integrity checking, and support for public key certificates.

12.2. Obtaining a Certificate

If you need help obtaining a certificate for your server, some guidance is presented here. Please note that this guide is general only - all certificate providers differ from one another in the methods they use to validate your identify, and the exact processes needed to finally obtain the certificate.

12.2.1. Choosing a Certificate

There are many types and suppliers of certificates on the market. Some example suppliers are:

- Comodo (https://comodosslstore.com)
- DigiCert (https://www.digicert.com)
- GeoTrust (https://www.geotrust.com)
- And many others

Certificates are available in different scopes:

- Single site certificates (for securing a single site, such as www.mysite.com
- Multi-Domain certificates (for securing a few sites, such as www.mysite.com, and www.myothersite.com)
- Wildcart certificates (for securing all subdomains under a domain, such as www.mysite.com, ftp.mysite.com, something.mysite.com, etc)

Any of these certificiate types may be used, but the lowest cost option is the single site certificate. Certificates are also available in differing validation levels. For example:

- Domain validated (the lowest cost - these typically require you to validate your owership of the domain by uploading a file to your web server at that domain, or by updating values in your DNS records). These are often issued instantly.
- Business validated (these cost a little more but validate your domain ownership as above, and also authenticate your business identity)
- Extended validation (these are the most expensive, but validate the domain ownership, the not just the business identity but the legal and physical operational existence of the business entity). These typically require more time to issue. These have the benefit of displaying a full green bar in browsers for additional end-user trust.

FileFlex will work with any of the certificate validations mentioned above.

12.2.2. Generating a CSR

You should follow the instructions provided by your certificate provider. These are guidelines and general instructions only. The first step in obtaining most certificates is to provide a CSR (Certificate Signing Request). You can do that from the FileFlex console by logging in (as sadmin) and entering the following command. This example is suitable for a single-site certificate, rather than for a wildcard or multi-domain certificate.

```
openssl req -nodes -newkey rsa:2048 -keyout myserver.key -out server.csr
```

You will then be asked to enter some information on the command line. Many of the fields can be left empty by hitting enter to answer the following question. Here is an example operation:

```
Generating a 2048 bit RSA private key
...........+++
...+++
writing new private key to 'myserver.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CA
State or Province Name (full name) [Some-State]:ON
Locality Name (eg, city) []:Toronto
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company Name Ltd
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:fileflexdemo.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Be sure to enter the fully qualified domain name for your FileFlex deployment, and that the password is empty. Two files will be generated:

- myserver.key - This is your private key. Ensure it stays backed up, and out of reach until required.
- server.csr - This is your certificate signing request.

12.2.3. Requesting a Certificate

Once you've chosen your certificate provider (for example, Comodo), you will have to select the type of certificate. Assuming you are selecting a domain-validation only certificate (such as PositiveSSL), you will then be asked to:

1. Provide them with your CSR.
2. Provide proof of domain ownership of the domain.

To fulfill the last step, you typically have two options:

1. You can upload a small file they provide to specific location of your domain's web server.
2. You can update your DNS records with a special entry they provide.

Since you may have already pointed your DNS to the FileFlex server, and it's not possible to upload a random file to the specified location, the DNS method is usually simpler. If you cannot do that you must update your DNS records to point the domain in question to a web server you control, and then upload the supplied file to it. Once validated, you can then re-point your DNS records to the FileFlex server if using that method.

Once the validation step has been completed you will receive the certificate. As mentioned elsewhere in this document, when submitting the certificate to FileFlex you will need to combine it with any intermediate certificates provided by your certificate issuer.