

Server Administration User Manual

Document Version 1.3

1. Table of Contents

- 1. Table of Contents
- 2. Introduction and Preparation
 - 2.1. Introduction
 - 2.2. Preparation
 - 2.3. Considering External Access
- 3. Virtualization and Hardware
 - 3.1. Server Hardware Allocation Requirements
 - 3.2. Deploying With Oracle VirtualBox
 - 3.3. Deploying with VMware Workstation
 - 3.4. Deploying the Virtual Machine
 - 3.5. Deploying With VMware vSphere
 - 3.6. Deploying the Virtual Machine
 - 3.7. Deploying on Amazon EC2
- 4. Installing FileFlex Enterprise
- 5. Initial Configuration Wizard
 - 5.1. Local Network Access
 - 5.2. Logging in to FileFlex Server Administration
- 6. User Interface Overview
 - 6.1. Functionality by Section
 - 6.2. Global Notifications
- 7. Managing Servers
 - 7.1. The Server List
 - 7.2. Server Action Toolbar
 - 7.3. Managing a Machine's Processes
 - 7.4. Adding and Editing Machine Server Processes
 - 7.5. Upgrading a Virtual Machine
- 8. Control Panel and Configuration
 - 8.1. Configuration Overview
 - 8.2. Your FileFlex Enterprise Credentials
 - 8.3. Configuring Email Delivery
 - 8.4. Setting up Login Control
 - 8.5. Configuring Single Sign-On
 - 8.6. Supplying an SSL Certificate
 - 8.7. User Administration Credentials
 - 8.8. Updating Web Resources
 - 8.9. Encryption Settings
 - 8.10. User Activity Logging
 - 8.11. Configure Google Drive Access
 - 8.12. Configure Microsoft OneDrive Access
 - 8.13. Configure DropBox Access
 - 8.14. Configuring Box.net Access
 - 8.15. Configuring Amazon S3 Access
 - 8.16. Configuring Microsoft Azure Access
 - 8.17. Configuring Google Cloud Access
 - 8.18. Advanced Settings
- 9. Backup and Restore
 - 9.1. Backup and Restore Overview
- 10. Managing Feedback
 - 10.1. Sending User Feedback to FileFlex Support
 - 10.2. Downloading User Feedback
 - 10.3. Deleting Feedback

- 11. Resource Monitor
 - 11.1. CPU Utilization
 - 11.2. Memory Utilization
 - 11.3. Speed Out
 - 11.4. Speed In
- 12. Appendix
 - 12.1. Recommended Security Practices
 - 12.2. Obtaining a Certificate

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

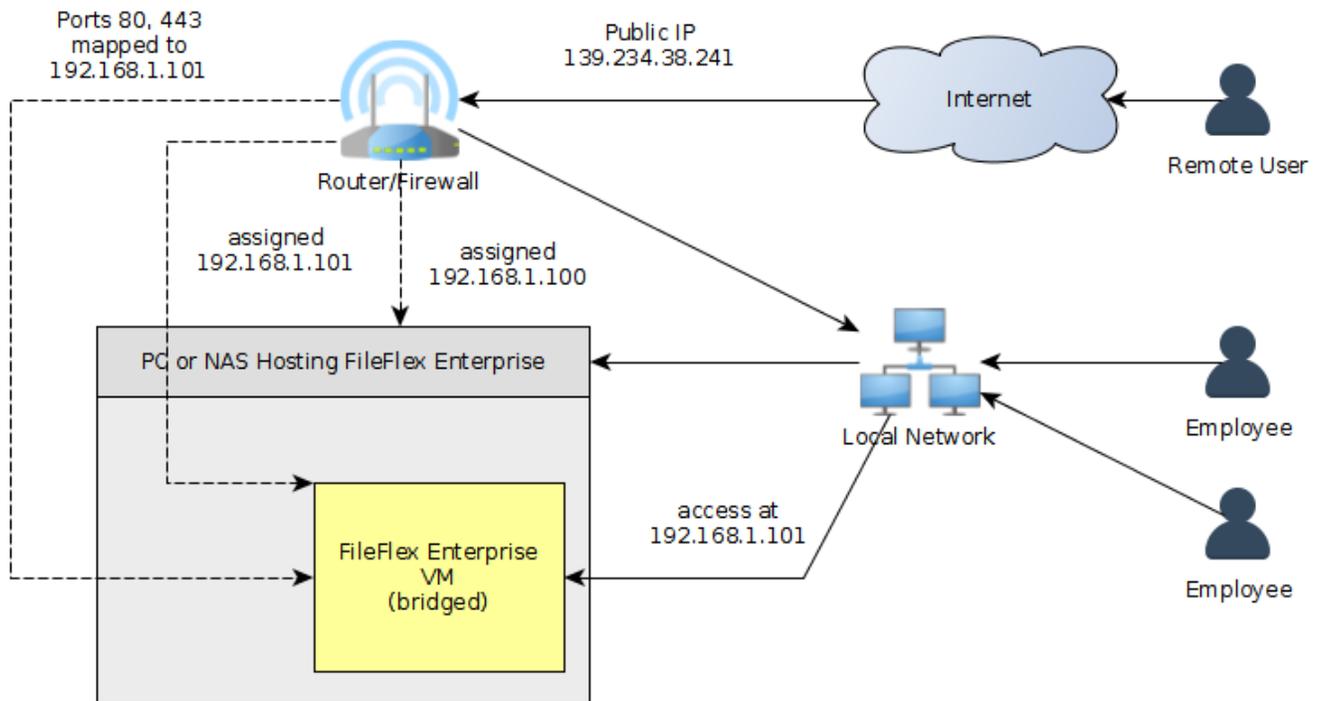
This document is intended to aid the reader in configuring a working FileFlex Enterprise virtualized environment. That environment will be available within the local network in which it is deployed, but it's expected that external public access will also be desired. The method of external access should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

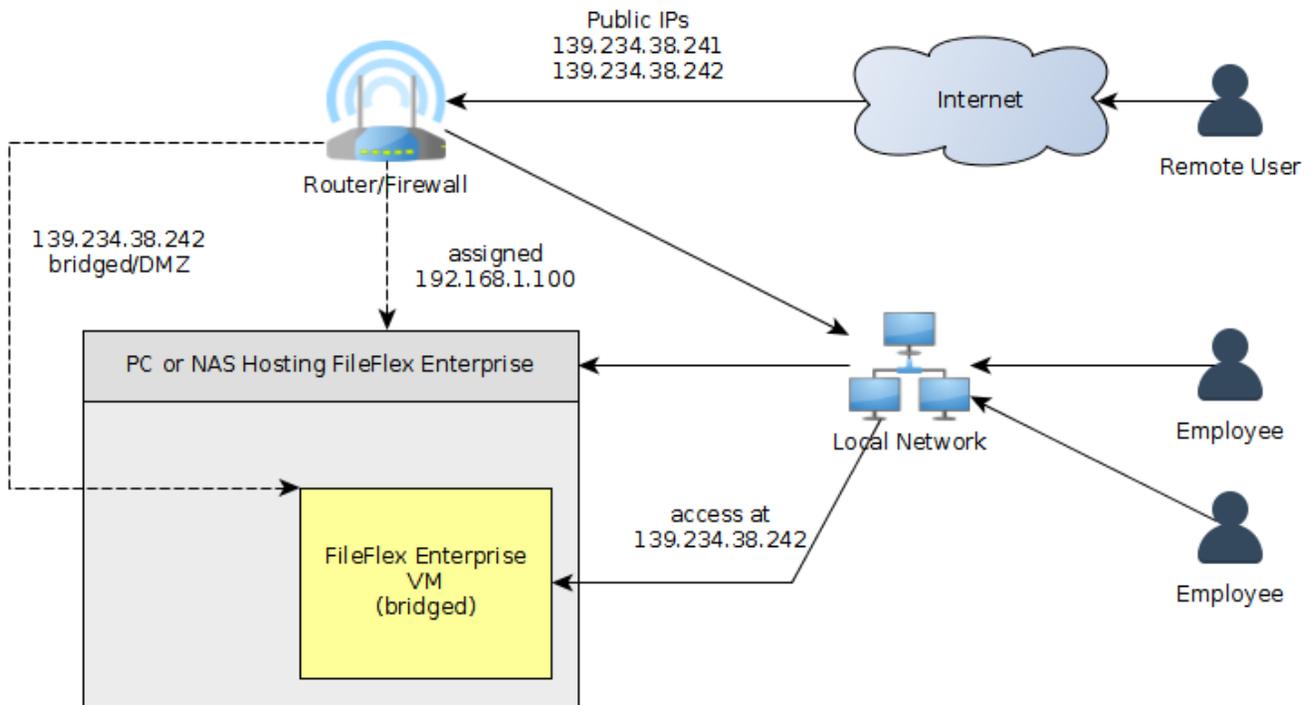
This documentation assumes that the VM will be given an IP using DHCP from the local network's router (or other DHCP server). This is made possible by using bridge mode networking at the VM level, and because of this, obtaining the privileged ports 80 and 443 should not be a problem. This means that 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



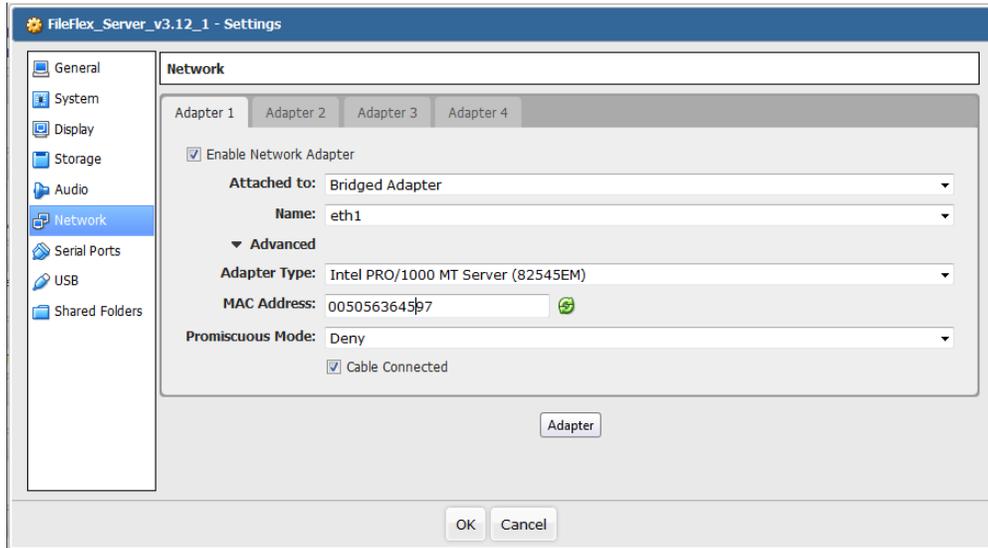
In this NAT scenario, local network users ("employees") are able to access the FileFlex Enterprise VM using the router-assigned local network IP on the default ports. Remote users going through the internet are able to access the FileFlex services by accessing the router's public IP address. The router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

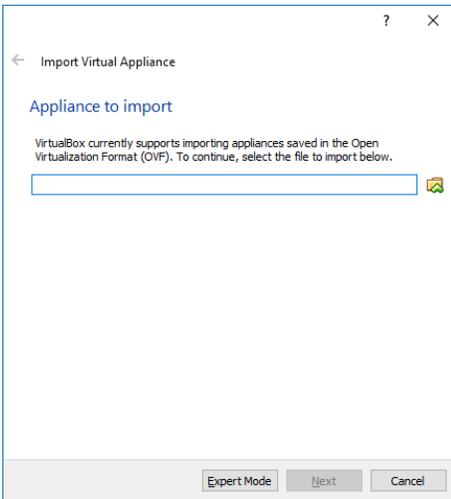
This section describes the process of installing FileFlex Enterprise on Oracle VirtualBox. The following versions of Oracle Virtualbox are supported:

- Oracle VirtualBox 5.x

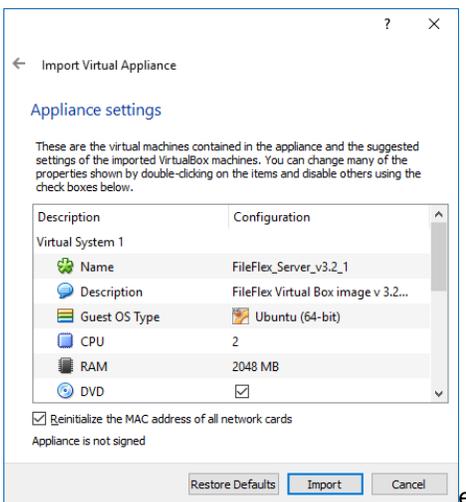
3.2.1. Deploying the Virtual Machine

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.

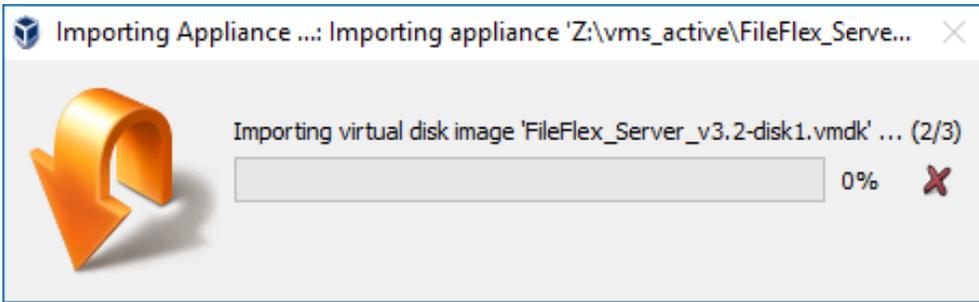
From VirtualBox's File menu, select Import Appliance. The following window will appear:



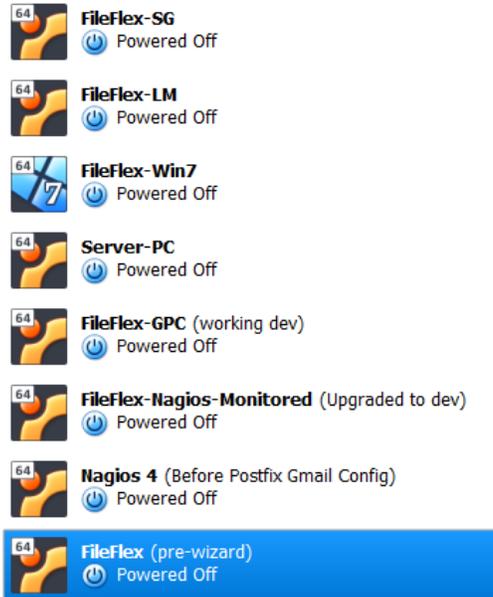
Select the OVA file you downloaded earlier and click the 'next' button. Check the "Reinitialize the MAC address of all network cards" box.



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



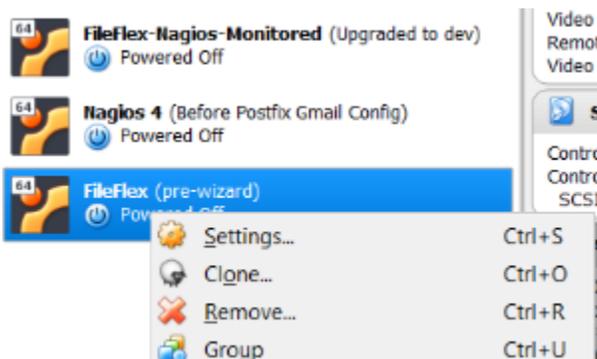
After a few moments you will see the virtual machine in your list of available VMs:



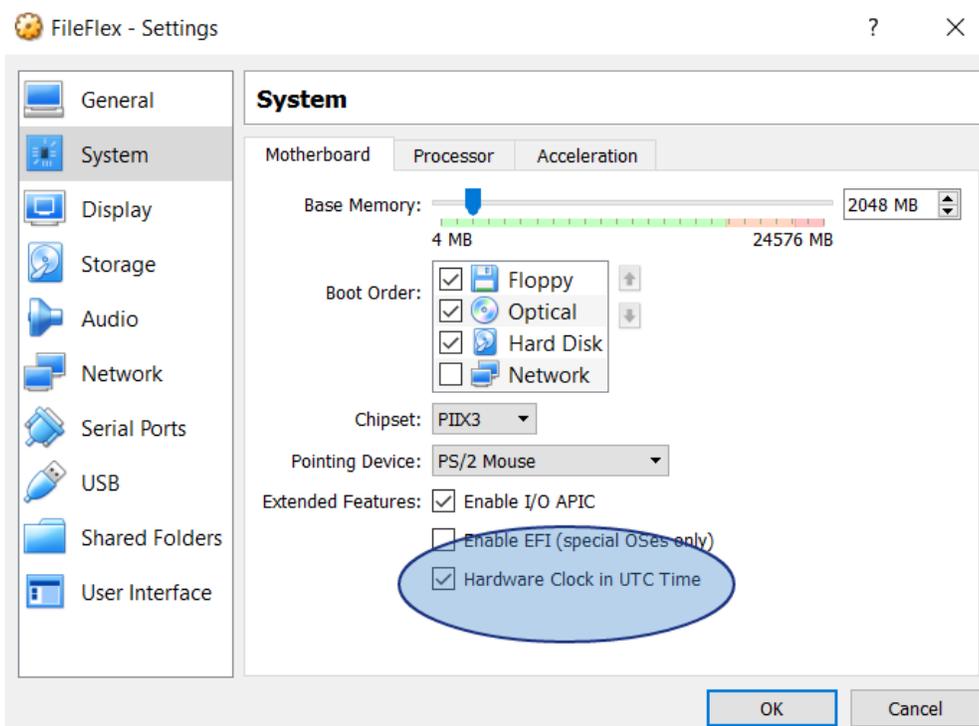
Right click on the new machine:

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:



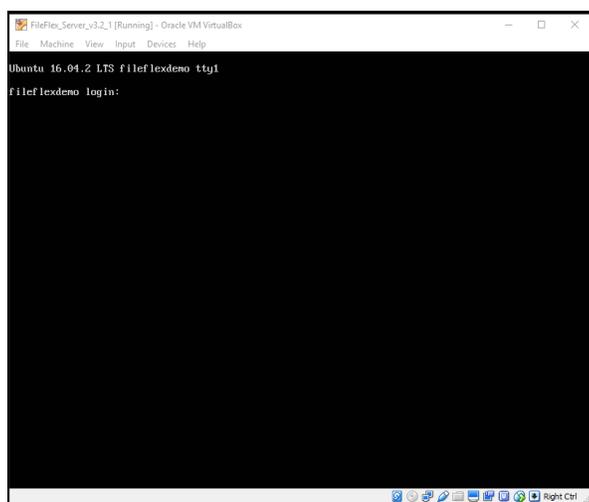
Ensure that the "Hardware Clock in UTC Time" checkbox is selected. Click OK.

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:



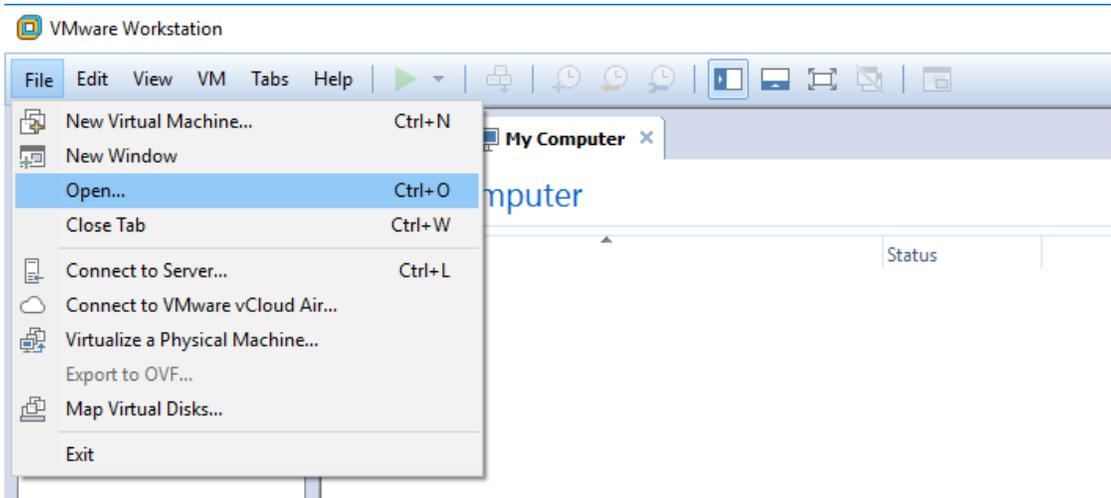
3.3. Deploying with VMware Workstation

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

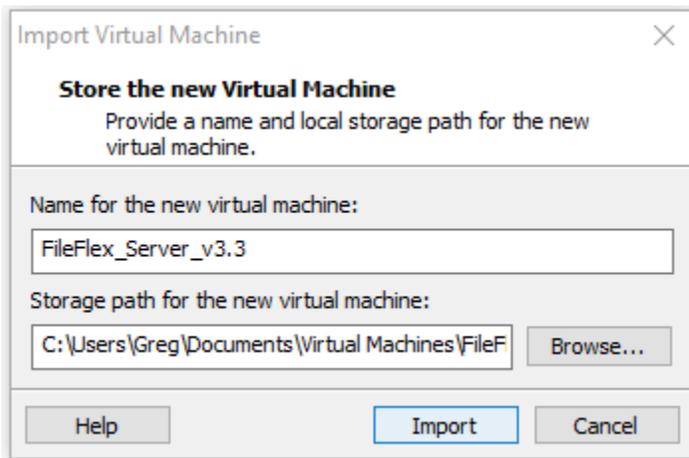
- VMware Workstation 11
- VMware Workstation 12
- VMware Workstation 12.5

3.4. Deploying the Virtual Machine

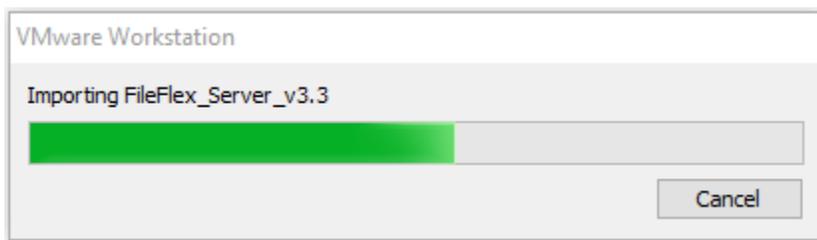
Open VMware Workstation, and select File/Open:



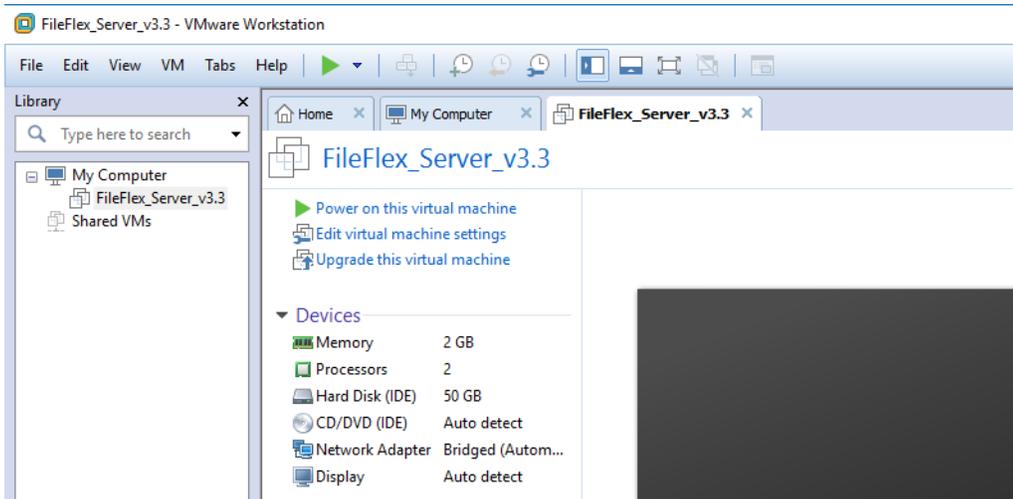
Navigate to your copy of the FileFlex_Server_v3_X.ova file, and select it.



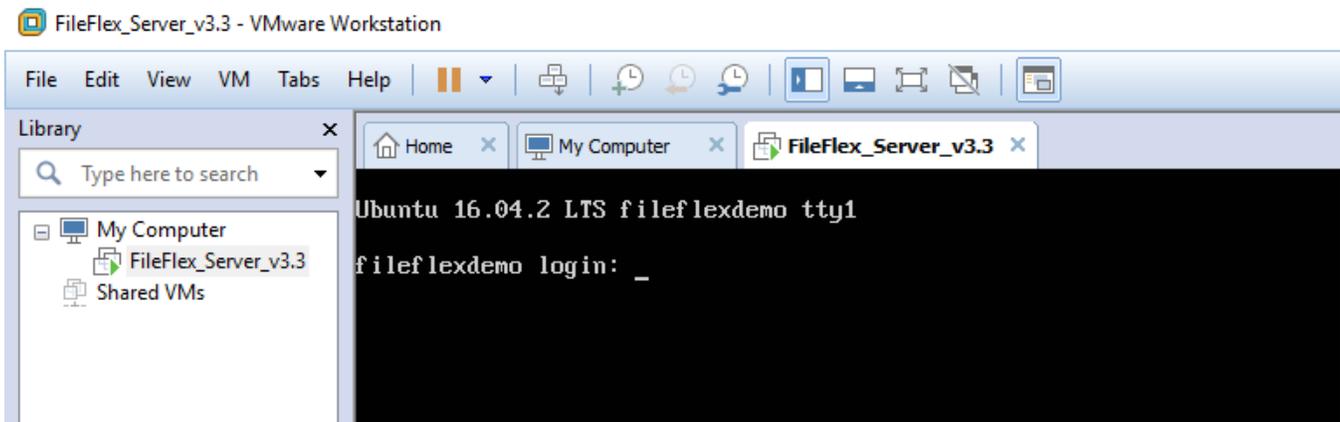
Choose to import the file, then wait a few minutes while it imports:



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.

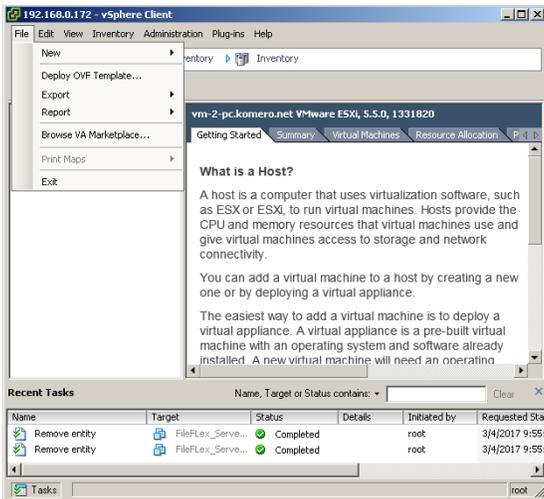
3.5. Deploying With VMware vSphere

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:

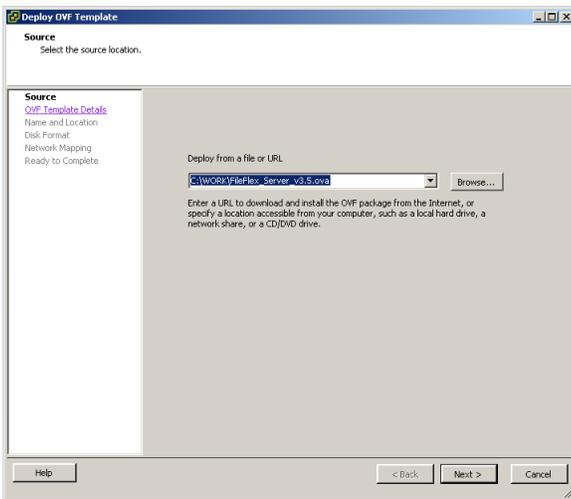
- VMware ESXi 5.5 (vSphere)
- VMware ESXi 6.0 (vSphere)
- VMware ESXi 6.5 (vSphere)

3.6. Deploying the Virtual Machine

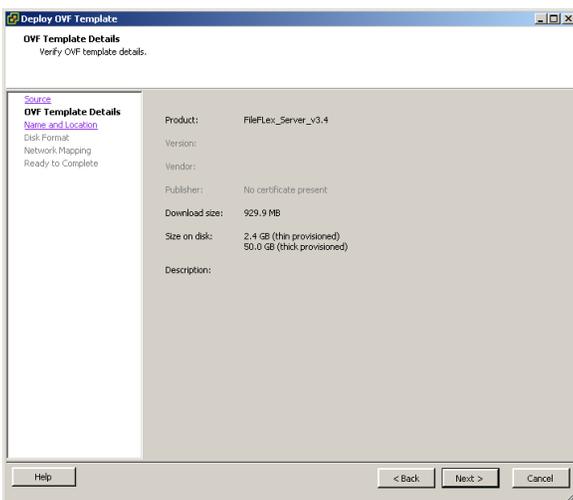
Open the vSphere client, and from the File menu select "Deploy OVF Template:



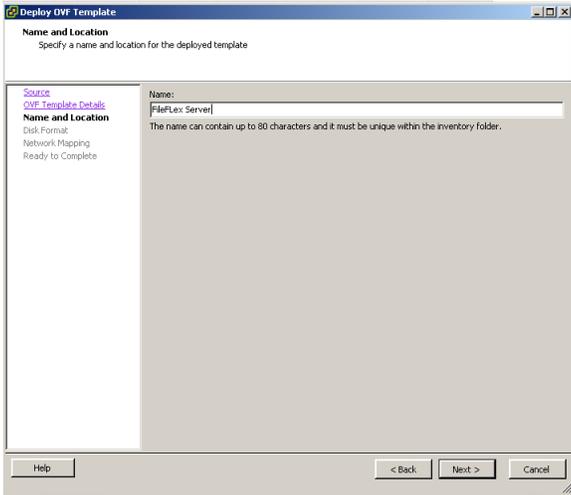
In the "Source" panel of VMware, click "browse" to locate your (previously downloaded) FileFlex_server OVA image:



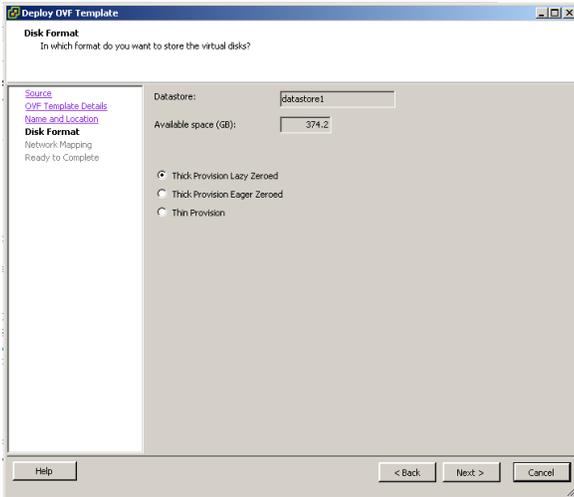
Click the "next" to enter the "OVF Template Details" panel which reveals information about the image:



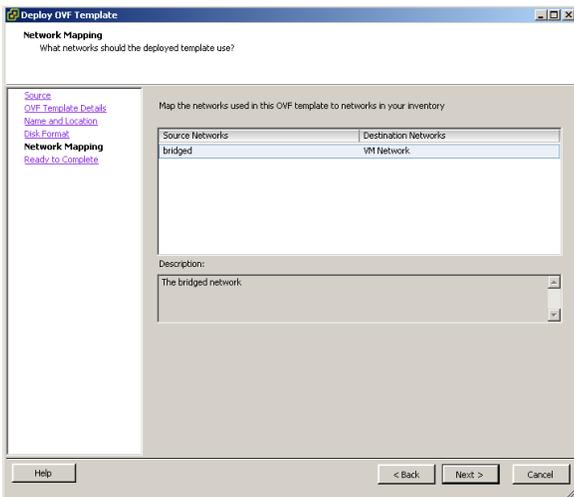
Click "next" to reveal the "Name and Location" panel. There you will be able to enter a new name (if you wish to override the default) for the deployed image:



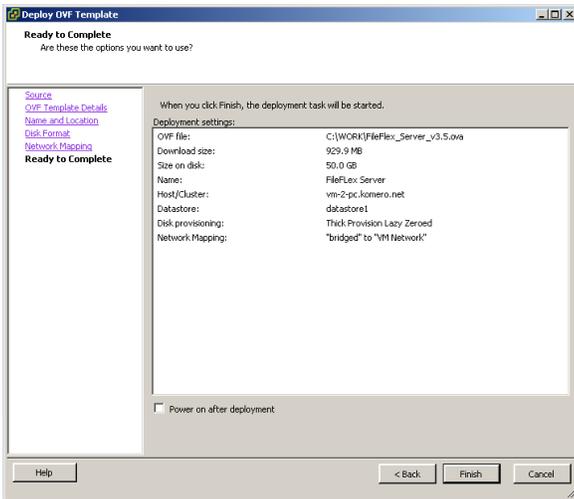
Click "next" to reveal the "Disk Format" panel:



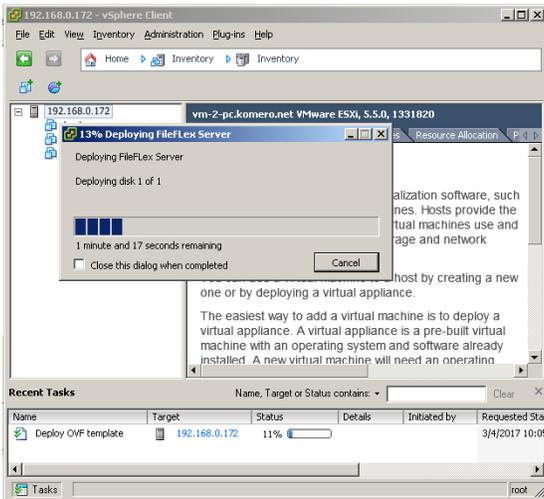
Select the "Thick Provision Lazy Zeroed" option, then click the "next" button to reveal the "Network Mapping" panel:



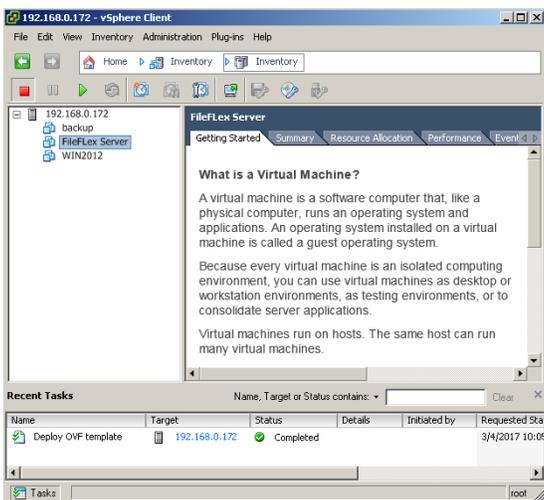
Select the bridged network entry for your VM network, then click the "next" button to reveal the confirmation panel:



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

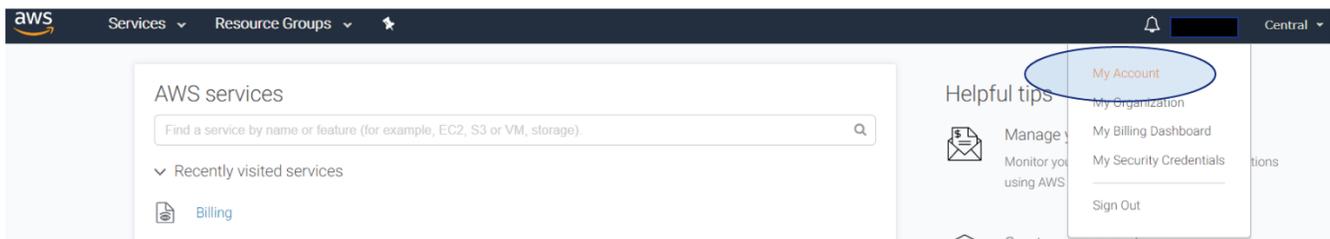
FileFlex provides an Amazon Machine Image (AMI), though it is not publicly available. In order to be able to use the image, you must provide our Enterprise Portal with your Amazon AWS Account ID.

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:

Account Settings [Edit](#)

Account Id: 17[REDACTED]732
Seller: AWS Inc.
Account Name: [REDACTED]
Password: *****

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:



Username and/or Password is empty.

USERNAME OR EMAIL ADDRESS

customer

PASSWORD



REMEMBER ME

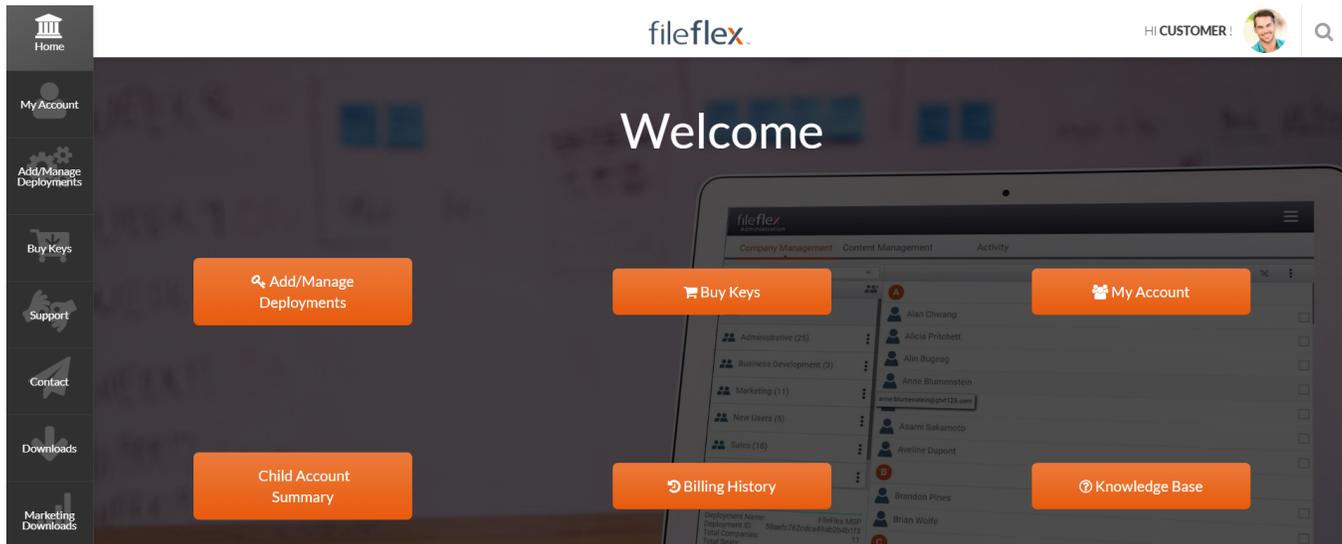
[Forgot Password](#)

[LOGIN](#)

You can request an MSP Account by filling out everything on this application form, and await a moderator to validate all info and approve your account for use.

[APPLY TO BECOME A FILEFLEX PARTNER](#)

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:

Add/Manage Deployments

Connect Web Service Accounts

New Server Deployment Name

URL

PKI URL (Optional, Windows Only)

Email

Help

Add Server Deployment

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

Connected Web Service Accounts

Amazon AWS ID

Amazon ID

Allow

Close

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

Notice

Amazon ID 17[REDACTED]2 is allowed.

Close

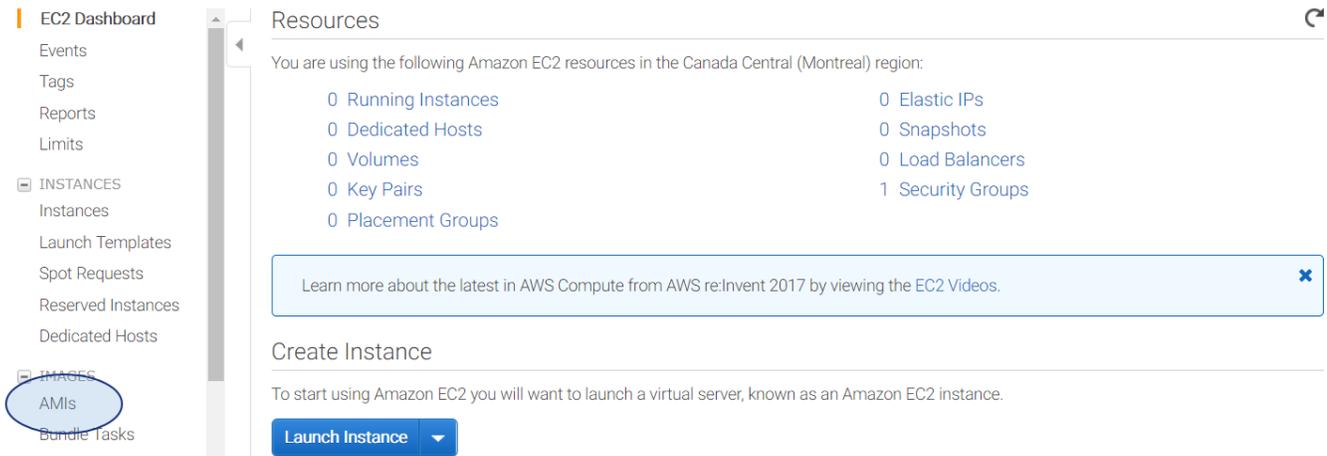
Click the "Close" button.

3.7.1.3. Deploying an EC2 Instance

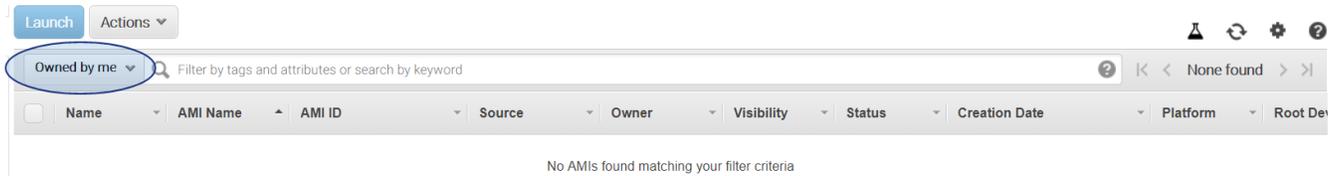
Turning our attention to deploying an EC2 instance, the first step is to log in to your EC2 console. Once logged in, expand the "Services" menu from the top left of the screen:



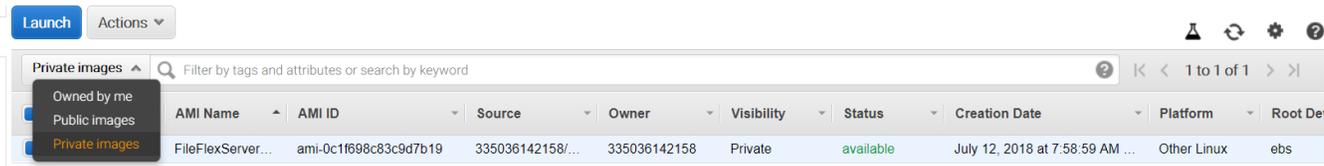
Click the EC2 menu item. You will see a screen similar to the following:



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". Because we linked the account, you will 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:

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t3.medium (Variable ECUs, 2 vCPUs, 2.5 GHz, Intel Skylake P-8175, 4 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes

i 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).

<input checked="" type="checkbox"/>	General purpose	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5d.large	2	8	1 x 75 (SSD)	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5d.xlarge	4	16	1 x 150 (SSD)	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5d.2xlarge	8	32	1 x 300 (SSD)	Yes	Up to 10 Gigabit	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

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

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details [Edit AMI](#)

FileFlexServer v.1 - ami-0c1f698c83c9d7b19
FileFlex Server
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t3.medium	Variable	2	4	EBS only	Yes	Up to 5 Gigabit

Security Groups [Edit security groups](#)

Security group name: launch-wizard-1
Description: launch-wizard-1 created 2018-09-12T11:10:52.484-04:00

Type	Protocol	Port Range	Source	Description
This security group has no rules				

Cancel Previous **Launch**

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:

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair ▼
Select a key pair
No key pairs found ▼

 **No key pairs found**
You don't have any key pairs. Please create a new key pair by selecting the **Create a new key pair** option above to continue.

[Cancel](#) [Launch Instances](#)

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:

Create a new key pair ▼
Key pair name
FileFlexDemo
[Download Key Pair](#)

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:

Launch Status

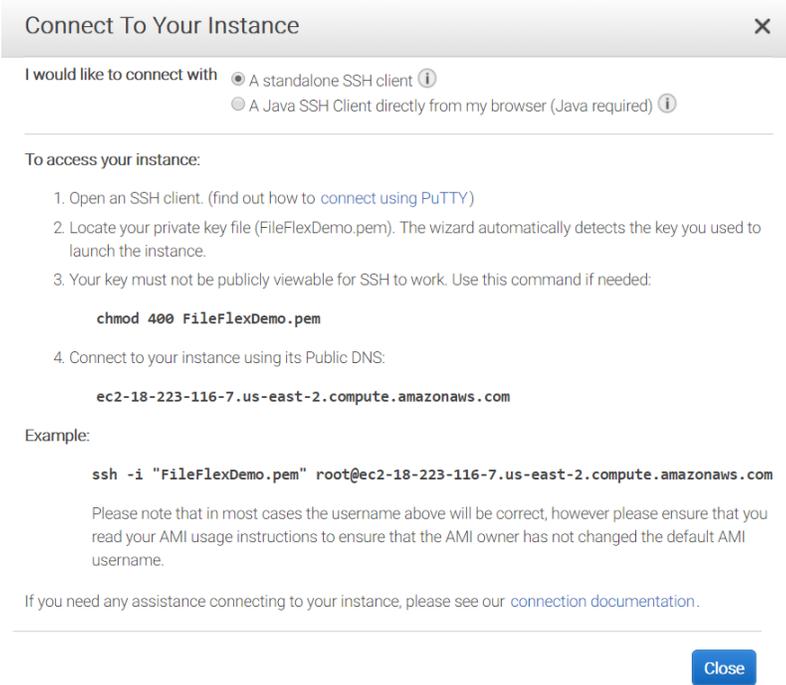
 **Your instances are now launching**
The following instance launches have been initiated: i-08f74[redacted]7d3 [View launch log](#)

 **Get notified of estimated charges**
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

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:



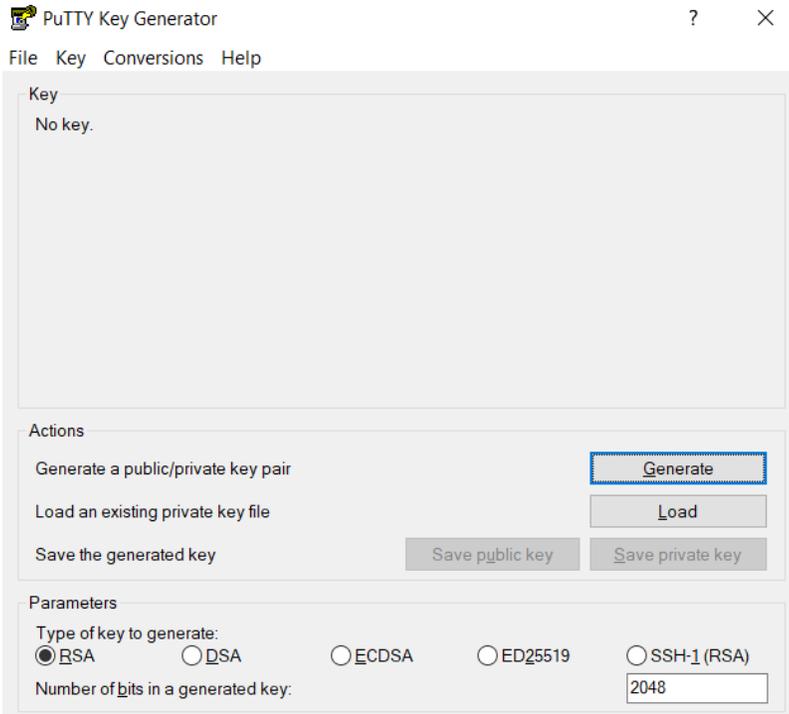
Select "A standalone SSH client" from the list of connection options (it should be the default). Follow the instructions provided for your SSH client of choice.

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

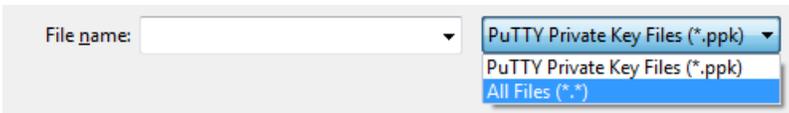
In this example, we will use Putty on Windows to connect to our virtual machine. We must now convert the key provided by Amazon into a format that's compatible with Putty.

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.



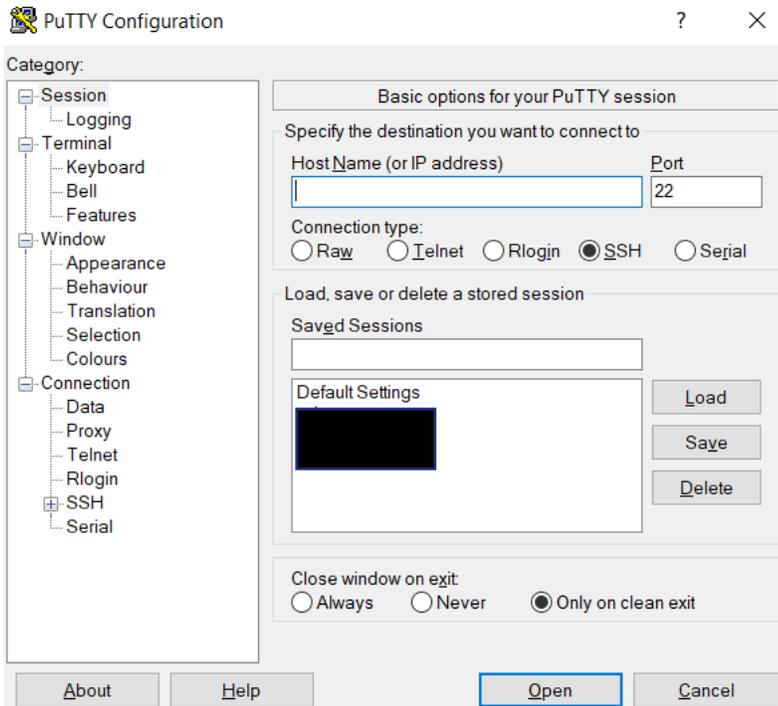
Select your `.pem` file for the key pair that you specified when you launched your instance, and then choose "Open". Choose "OK" to dismiss the confirmation dialog box.

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".

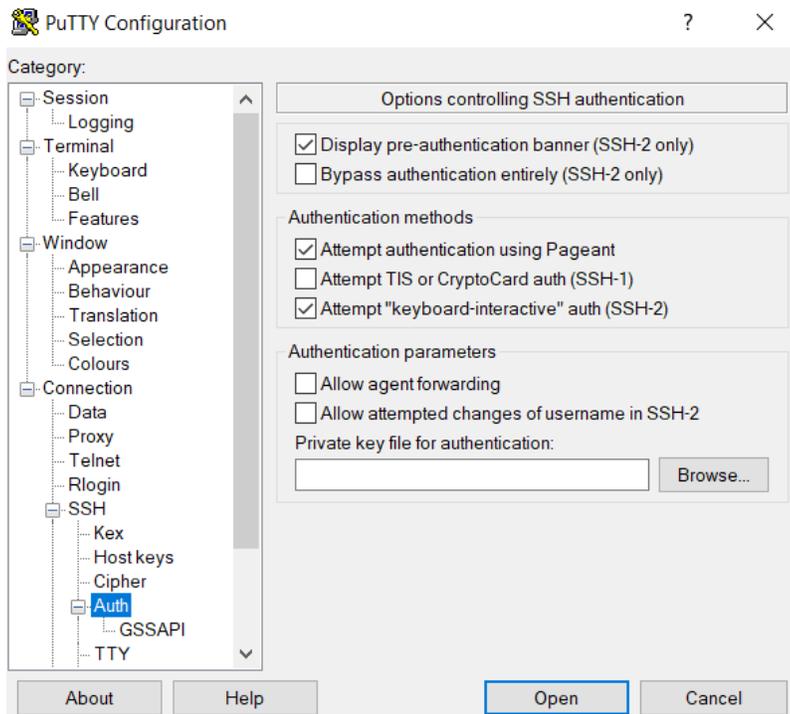
 A passphrase on a private key is an extra layer of protection, so even if your private key is discovered, it can't be used without the passphrase. The downside to using a passphrase is that it makes automation harder because human intervention is needed to log on to an instance, or copy files to an instance.

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:

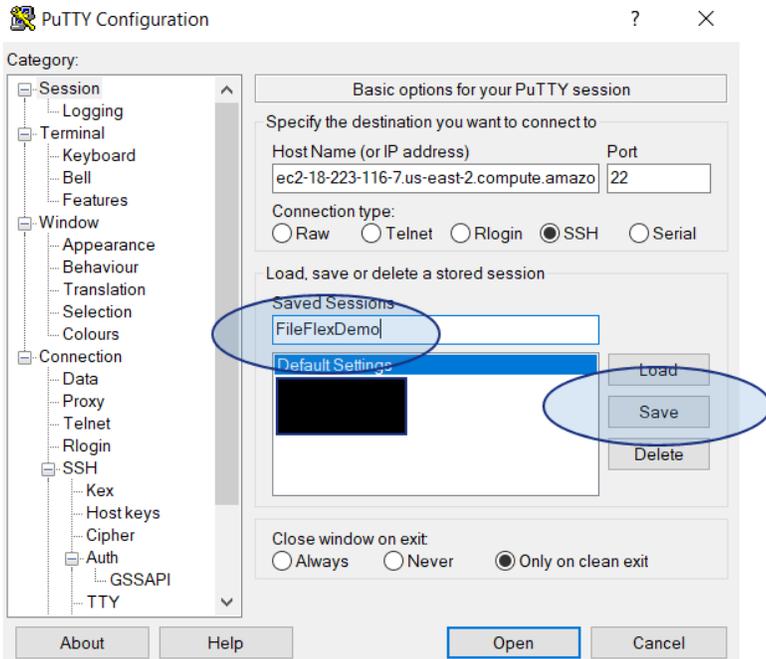


Enter the "Public DNS" URL you wrote down earlier in Putty's "Host Name" field. Next, we need to provide the private key to PuTTY. Do so by expanding the "Connection" node from the left panel, then the SSH node as well. You will then be able to select the "Auth" note:



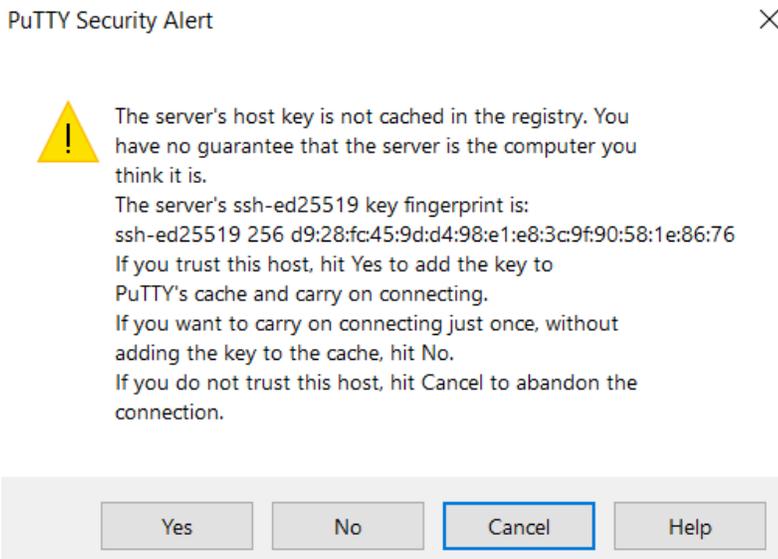
Click "Browse" and locate the key you recently generated with PuTTYgen.

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:

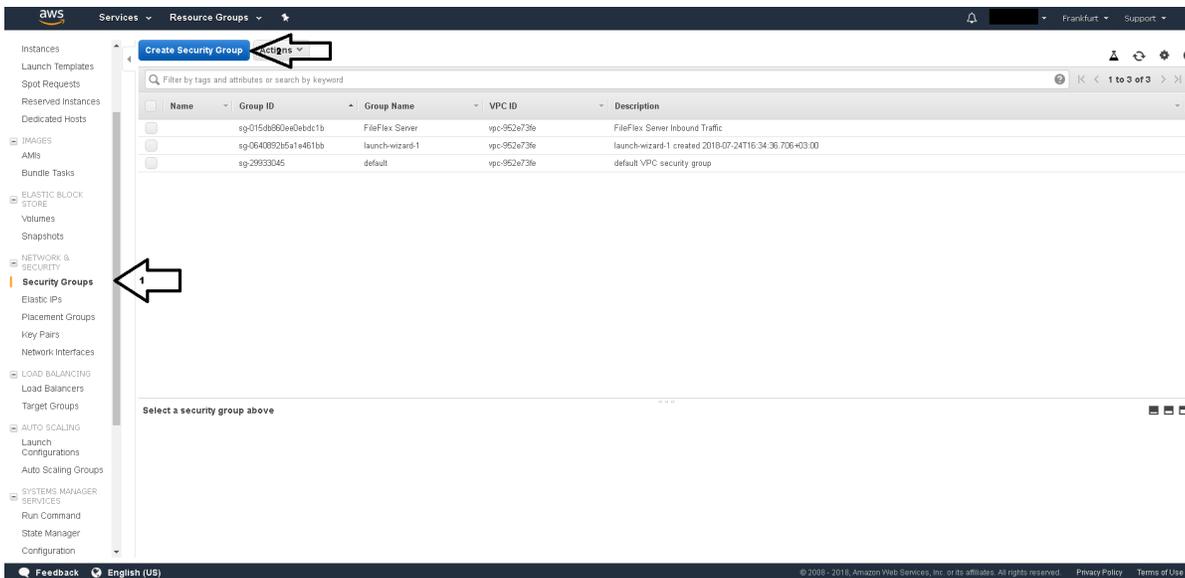


Your machine is now accessible by SSH!

3.7.1.5. Creating a Security Group

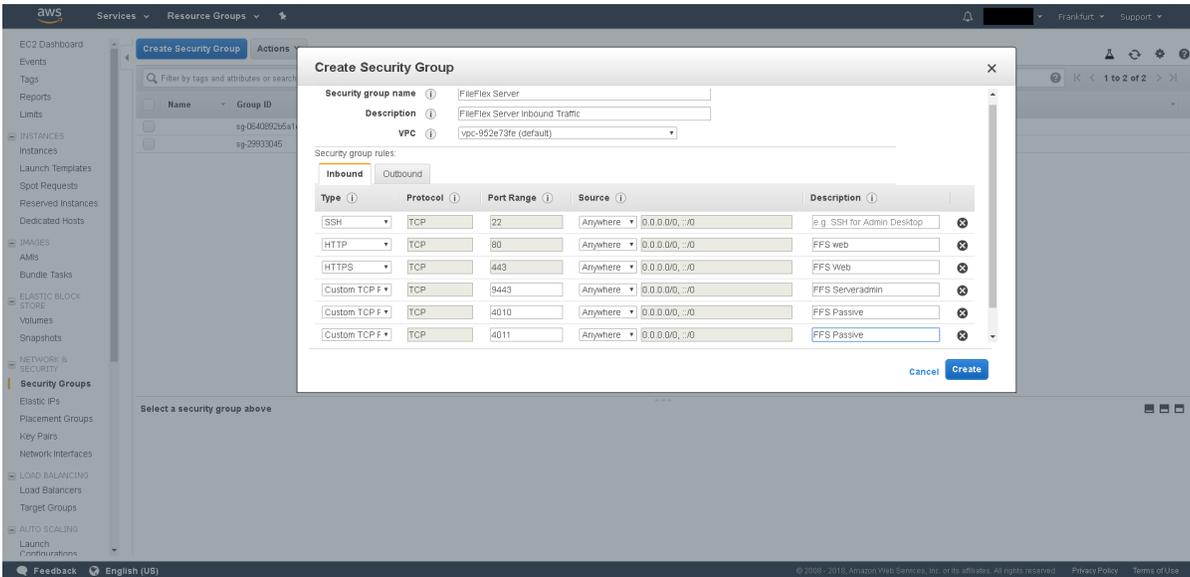
By default a new instance that's been created isn't allowed to receive any inbound external traffic other than on the SSH port 22. To resolve that we must create or modify an existing security group and apply it to our instance.

Navigate to security groups on the Amazon Dashboard:



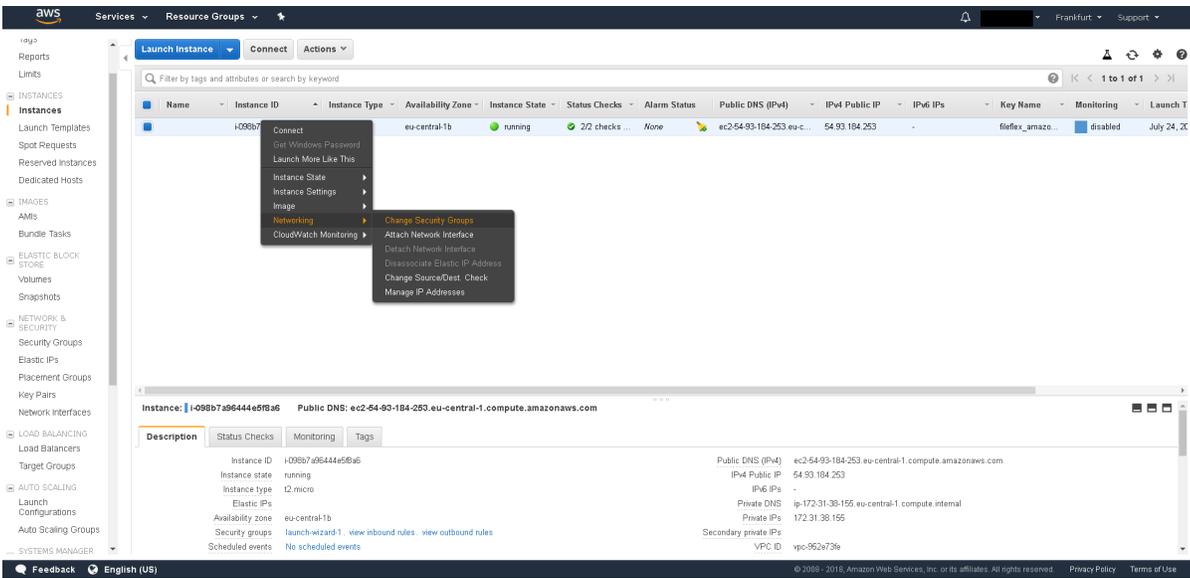
Create a security group. Name it "FileFlex", and ensure that the following TCP ports are allowed from "anywhere":

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

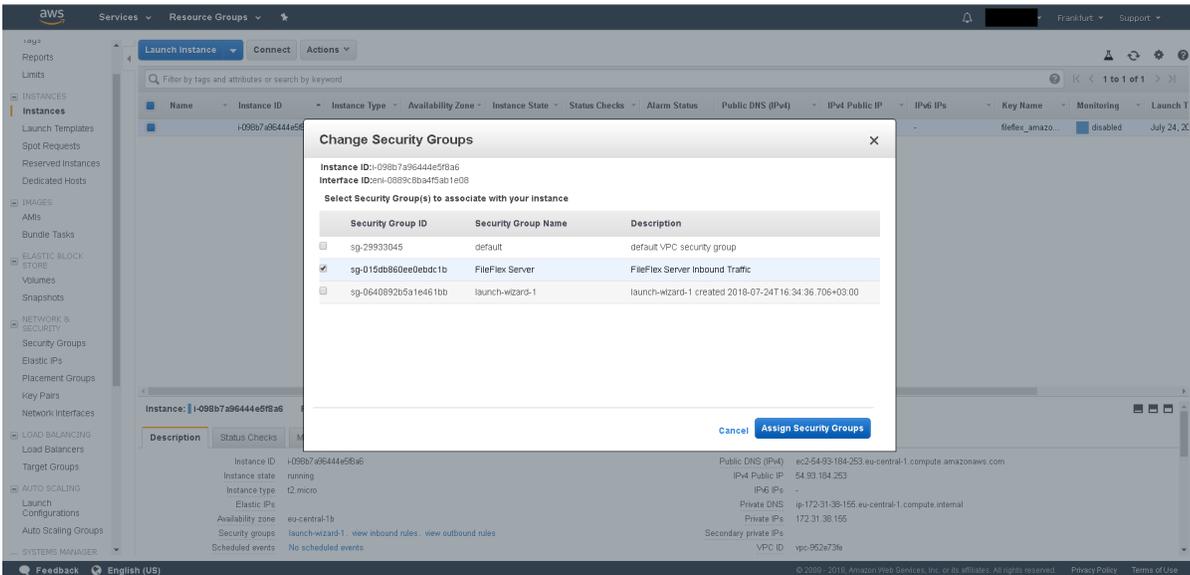


Click create to finish this and close the dialog.

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:

```

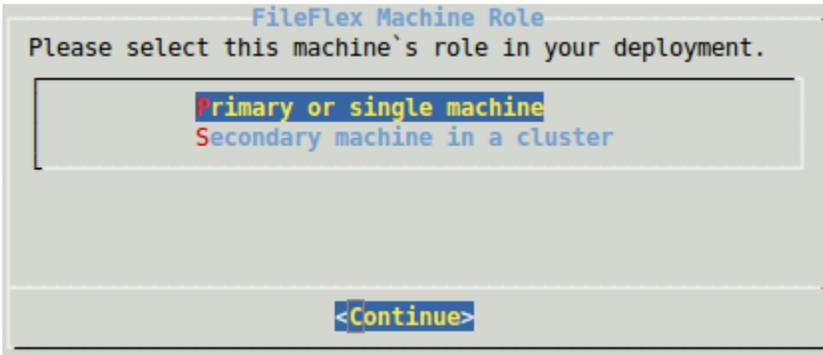
Ubuntu 16.04.2 LTS fileflexdemo.com tty1
fileflexdemo login: sadmin
Password:
  
```

Login using the default credentials:

Default FileFlex Enterprise OS credentials:

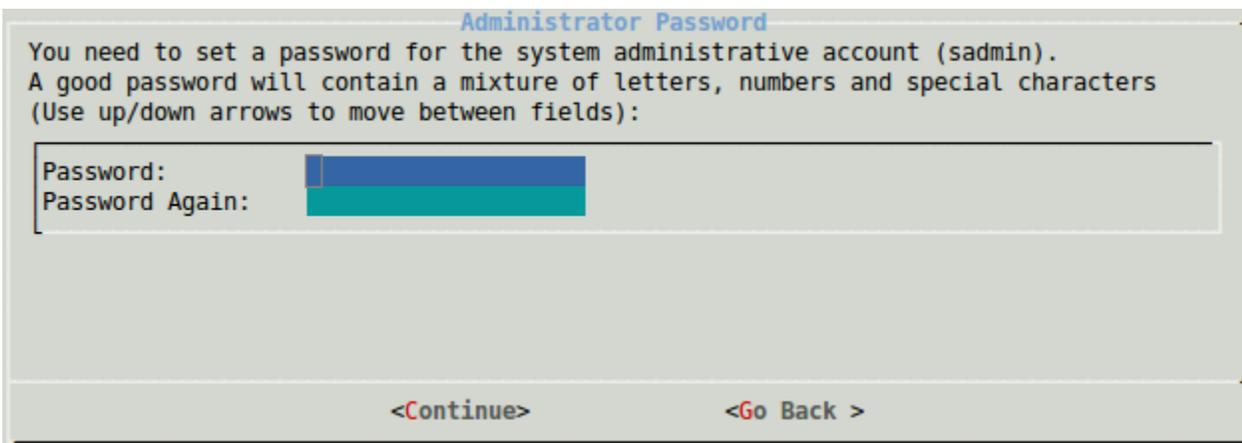
Username	sadmin
Password	Q!w2e3r4

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



i 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.



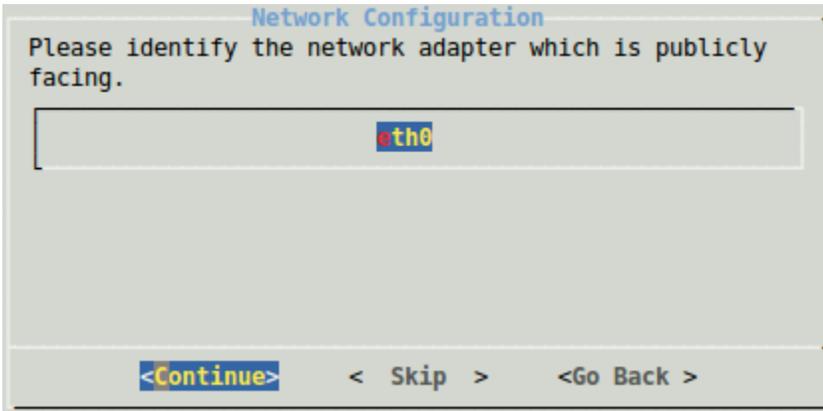
You must now enter a password for the "sadmin" user which you'll use for logging in to the VM and to the server administration application.

- i** 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.

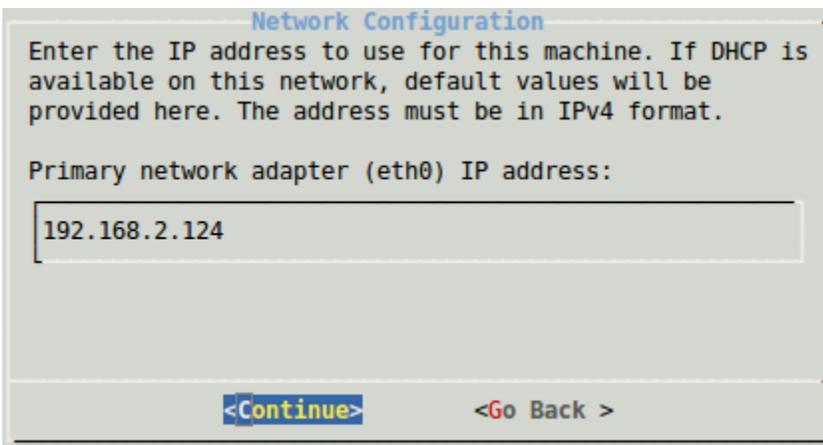
! You must use the arrow keys to navigate between the password fields!

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



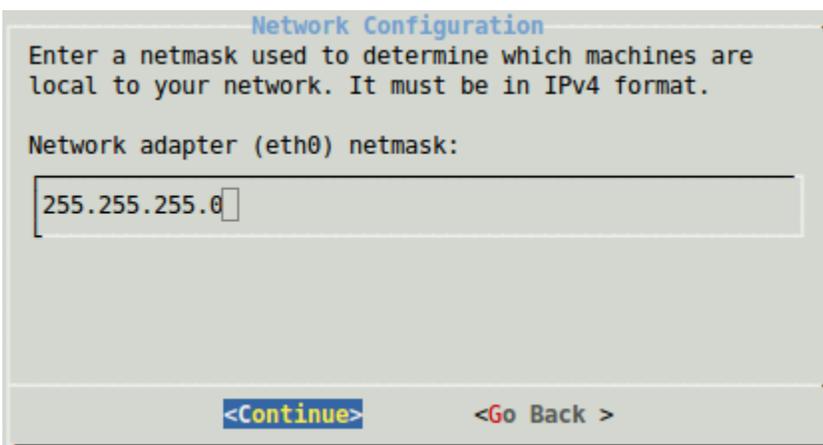
In this case (a single machine deployment) there should be only one, so hit enter to continue.

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:

Network Configuration

Enter the network gateway's IP address that indicates the gateway router on your network. It must be in IPv4 format.

Network adapter (eth0) gateway:

<Continue> **<Go Back >**

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:

Network Configuration

Enter the name servers (DNS) used to look up host names on this network. Please enter IP addresses (not host names) of up to 3 name servers separated by spaces.

Network adapter (eth0) DNS servers:

<Continue> **<Go Back >**

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:

Network Configuration

Enter this machine's hostname. The hostname must be the same as the Deployment URL you selected for this server.

Valid characters are ASCII letters 'a' through 'z', digits '0' through '9', and the hipen '-'.

Machine hostname:

<Continue> **<Go Back >**

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.

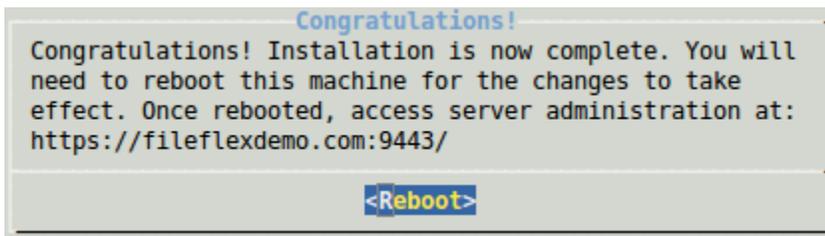
Hostname and Deployment URL

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:

```
net.core.rmem_max = 524288
net.core.wmem_max = 524288
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_rmem = 4096 65536 524288
net.ipv4.tcp_wmem = 4096 65536 524288
net.core.netdev_max_backlog = 250000
net.ipv4.tcp_no_metrics_save = 1
Ign:1 http://apt.cnexus.com/prod production InRelease
Hit:2 http://apt.cnexus.com/prod production Release
Reading package lists... Done
W: http://fileflex:kpLb27x9@apt.cnexus.com/prod/dists/production/Release.gpg:
0606573F633EA02C3A6791EA0945FCA6461 uses weak digest algorithm (SHA1)
Apt source updated
```

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.

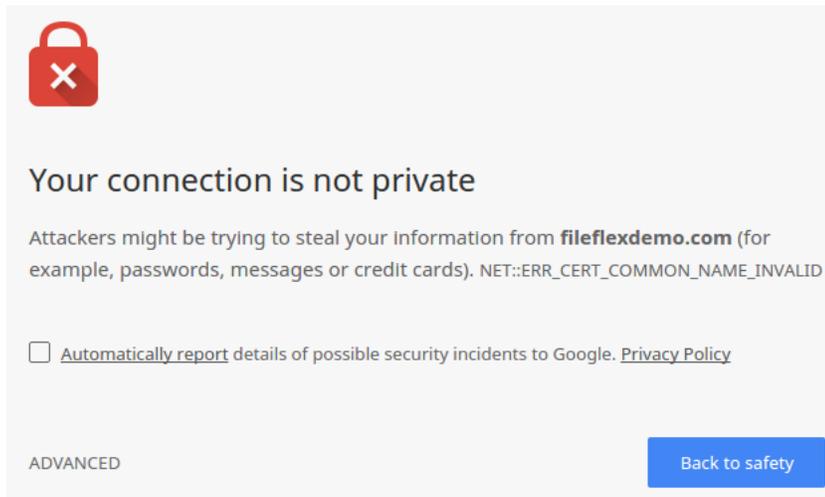
Your DNS servers (or hosts files) must be correctly configured to point the configured host names to the IP given to the VM, and your fire walls must not block port 9443 for local network access to that VM.

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:

Authentication Required

https://fileflexdemo.com:9443 requires a username and password.

User Name:

Password:

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):

FileFlex Deployment ID

1

FileFlex Deployment Key

2

MSP Company Name

3

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.

Initial Configuration Wizard

Welcome to the initial configuration wizard.
Before proceeding you must verify your FileFlex MSP credentials.

FileFlex Deployment ID

596e12a02cdca87137ae

FileFlex Deployment Key

.....

MSP Company Name

GregMSP1



Verify

Done

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.

Initial Configuration Wizard

Would you like to deploy a standard single-machine configuration?
You can always re-configure manually.

- Yes, deploy a single-machine configuration.
- No, I will configure multiple machines manually.

Would you like to enable double-encryption in this deployment through the use of a PKI server?

- Yes, install PKI server and enable double encryption
- No, I don't need double encryption or will configure PKI server later

Next

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:

Initial Configuration Wizard

Would you like to deploy a standard single-machine configuration?
You can always re-configure manually.

- Yes, deploy a single-machine configuration.
- No, I will configure multiple machines manually.

Would you like to enable double-encryption in this deployment through the use of a PKI server?

- Yes, install PKI server and enable double encryption.
- No, I don't need double encryption.

Installing modules - this may take several minutes. Please wait.

Next

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

Initial Configuration Wizard

Name

Email

Password
Password strength: Strong

Confirm Password

Back

Add

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:

Initial Configuration Wizard

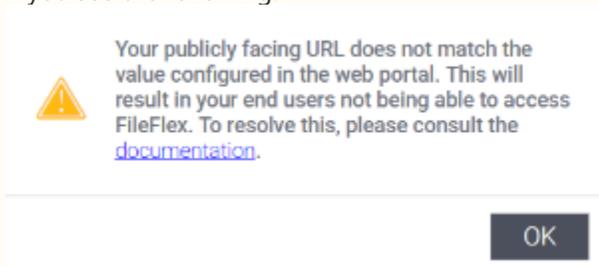
Your detected hostname:
fileflexdemo.com

Your settings are ready to synchronize. Your publicly accessible URL will also be validated against that which was entered in the portal to ensure accessibility.

Done

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

 If you see the following:



 Your publicly facing URL does not match the value configured in the web portal. This will result in your end users not being able to access FileFlex. To resolve this, please consult the [documentation](#).

OK

... 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:

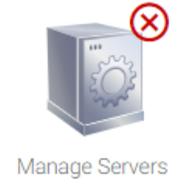
 Changes will be seen after you restart all servers.
Do you want to do it now?

No

Yes

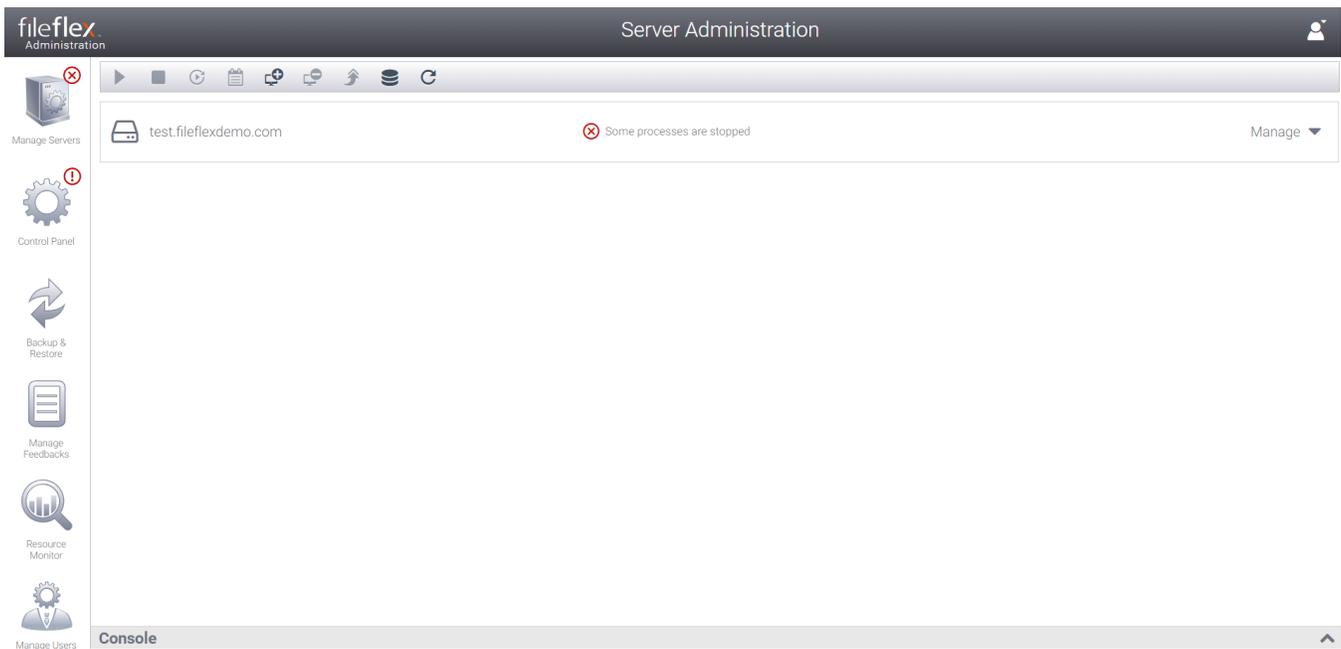
Click "yes" to proceed. Wait about 30 seconds and you will be presented with the Server Administration web application.

i 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 overlaid 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	Manage Servers Attention Required	Indicates that your attention is required in the "manage servers" section. Typically indicates that updates are available.
 Manage Servers	Manage Servers Execution Failure	Indicates that one more more server processes did not start as expected.
 Control Panel	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.

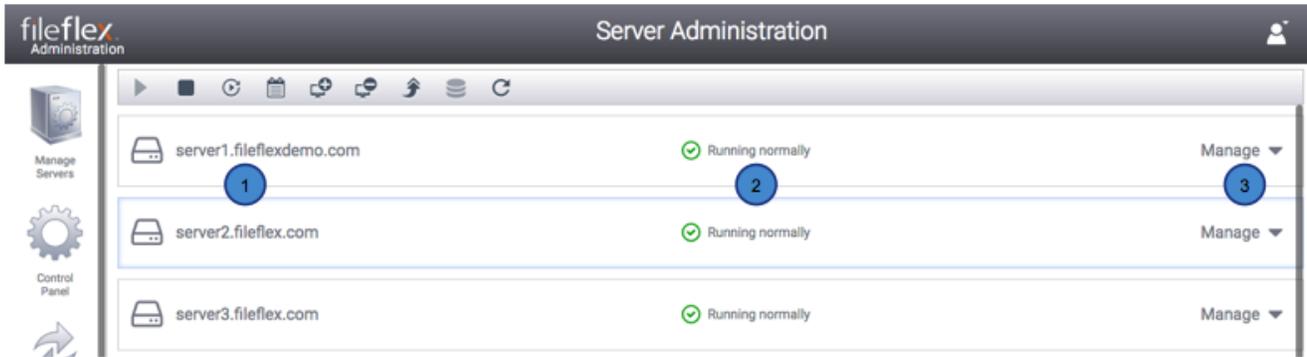
 <p>Backup & Restore</p>	<p>Backup & Restore</p> <p>Urgent Notification</p>	<p>Indicates that a backup failure occurred.</p>
---	--	--

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.

i 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:

fileflexdemo.com
🟢 Running normally
Manage ▲

Server IP: 10.0.2.5 | Zone: Default

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.

i 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:

Server	Process ID	State	Info
Messaging Ser 1	2	3	Started 4 19:54
Web Server	1493	🟢	Started at: 03-13 19:54
Storage Server	1340	🟢	Started at: 03-13 19:54
Administration Server	1286	🟢	Started at: 03-13 19:54

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



Module
activemq (0.0.9)
adapter (0.0.136)
fbweb (0.0.138)
mongo (0.0.13)
serveradmin (0.0.150)

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.

Web Server	1493		Started at: 03-13 19:54	adapter (0.0.136) fbweb (0.0.138)
------------	------	---	-------------------------	--------------------------------------

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.

Edit Machine

Hostname:

IP:

Zone:

Module name	Inst
Server Administration	<input checked="" type="checkbox"/>
Web Application	<input checked="" type="checkbox"/>
Adapter	<input checked="" type="checkbox"/>
Mongo	<input checked="" type="checkbox"/>
ActiveMQ	<input checked="" type="checkbox"/>
Document conversion	<input checked="" type="checkbox"/>
General language pack	<input checked="" type="checkbox"/>
Admin language pack	<input checked="" type="checkbox"/>
Load balancer	<input type="checkbox"/>
PKI	<input checked="" type="checkbox"/>
AntiVirus	<input checked="" type="checkbox"/>

Field	Explanation
Host name	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

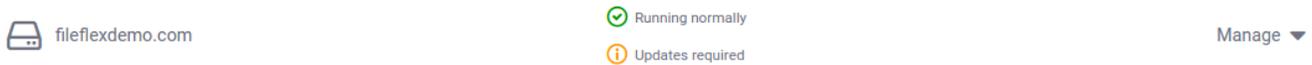
7.4.1. Deployable Modules

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.

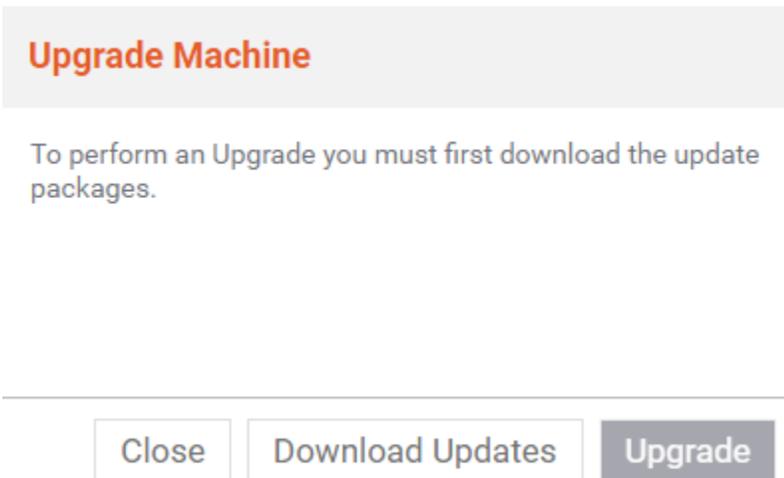
Document Conversion	Document visualization package.
General language pack	The primary application's internationalization files.
Admin language pack	The server administration internationalization files.
Load balancer	A load balancer used when deploying cluster configurations.
PKI	Public key infrastructure 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 its 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:

Upgrade Machine

To perform an Upgrade you must first download the update packages.

Close

Download Updates

Upgrade

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



You cannot upgrade while servers are running. Do you want to continue and STOP all selected servers?

No

Yes

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



The servers are stopped. Do you want to upgrade the selected machines?

No

Yes

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:



Some of the servers are not running. Do you want to START all servers?

No

Yes

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:

	Overview
	Credentials
	Email
	Login Control
	Single Sign-On
	Certificates
	User Administration
	Web Resources
	Encryption
	User Activity Logging
	Google Drive
	Dropbox
	OneDrive
	Box
	Amazon S3
	Microsoft Azure
	Advanced

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 credentials have been verified.
-  Email delivery has not been configured.
-  Two factor authentication has not been configured.
-  Single sign one has not been configured.
-  A custom certificate has not been provided.
-  A User Administration account has not been created.
-  A customized splash screen has not been provided.
-  Google Drive access has not been configured.
-  Dropbox access has not been configured.
-  OneDrive access has not been configured.
-  Box access has not been configured.
-  Amazon S3 access has not been configured.
-  Microsoft Azure access has not been configured.
-  All advanced properties have been configured.

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.

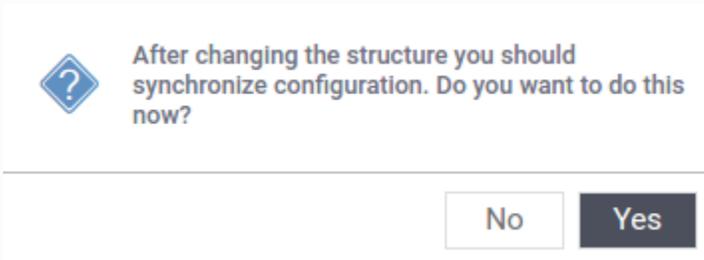
i Applying Configuration Changes

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:

The screenshot shows the FileFlex configuration interface. On the left is a navigation menu with items: Overview, Credentials, Email (highlighted), Login Control, Certificates, User Administration, Web Resources, Encryption, User Activity Logging, Google Drive, Dropbox, OneDrive, Box, and Advanced. The main area is titled "Email" and contains the following fields:

- Sender email: admin@fileflexdemo.com
- Sender name: Administrator
- SMTP Server: smtp.fileflexdemo.com
- SMTP Port: 587
- Authentication required:
- Username: postmaster@fileflexdemo.com
- Password: [masked]
- Secure connection (TLS) is required:
- Notification address: admin@fileflexdemo.com

At the bottom of the main area is a "Send a test Email" button and a "Send to:" input field. At the bottom right of the configuration area are three buttons: "Synchronize", "Reset", and "Apply".

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

i The default sender 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: <code>johnsmith@place.com</code> .
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: <code>smtp.mycompany.com</code>
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: <code>johnsmith@place.com</code>
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	<code>admin@fileflexdemo.com</code>
Sender Name	FileFlex Demo
SMTP Server	<code>smtp.mailgun.org</code>
SMTP Port	587
Authentication Required	True
Authentication Username	<code>postmaster@fileflexdemo.com</code>

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

Notification Emails

Although optional, it's a good idea to configure a notification email address. The system will inform you when resource limits are reached or when users experience problems by sending you a notification email. Click the  symbol next to "Notification address" to add an email address for notification delivery. Several recipient emails may be configured.

Notification address



admin@fileflexdemo.com



8.3.3. Testing Email Delivery

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

Send a test Email

Send to:

example_person@gmail.com

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):



me

Test Email - Test sending Email

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 the 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:

- ✔ Your FileFlex credentials have been verified.
- ✔ Email delivery have been configured.
- ⓘ Two factor authentication has not been configured.
- ⓘ A custom certificate has not been provided.
- ✔ A User Administration account has been created.
- ⓘ A customized splash screen has not been provided.
- ⓘ Google Drive access has not been configured.
- ⓘ DropBox access has not been configured.
- ⓘ OneDrive access has not been configured.
- ⓘ BoxNet access has not been configured.

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.

Allow cookie-based login (remember me). ⓘ

Enable two-factor authentication ⓘ

Two-factor authentication is mandatory for all users.

Use SMS delivery for authentication

Sms Provider ⓘ

Expertexting

Twilio

Plivo

Account SID ⓘ

Auth Token ⓘ

From ⓘ

Send to:

⚠ 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 ExpertTexting delivery has been selected.
Password	This is ExpertTexting's account password used for accessing their services. Only available when ExpertTexting delivery has been selected.
API Key	This is ExpertTexting's API key used for accessing their services. Only available when ExpertTexting 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:

The screenshot shows a user interface for configuring two-factor authentication (TFA). At the top, there are three tabs: 'General', 'Profile', and 'Security', with 'Security' being the active tab. Below the tabs, there is a checkbox labeled 'Enable two factor authentication' which is checked. To the right of this checkbox is a help icon '[?]'. Below the checkbox, there is a 'Phone:' label followed by a dropdown menu showing a US flag and the phone number '+11234567890', and a 'Verify' button. Below this, there is a text block: 'It's a good idea to have a means of recovery in case you lose your two factor authentication device. Print out your recovery codes and/or specify an alternate recovery device.' Below this text, there is a section titled 'My recovery codes' with an 'Alternate:' label, a dropdown menu showing a US flag and the phone number '+1 201-555-5555', and another 'Verify' button. At the bottom of the form, there are two buttons: 'Cancel' and 'Save'.

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

i 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:

Login to FileFlex Enterprise Secure File Access

george@fileflexdemo.com

.....

If you do not receive confirmation code in 5 minutes please repeat the login procedure. You can enter the code being delivered to your device, or one of your recovery codes.

Code

Cancel

Login

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.

Sign up for free

George

Mattoge

FileFlexDemo

george@twilio.com

.....

.....

 Strong

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

WHICH PRODUCT DO YOU PLAN TO USE FIRST?

SMS 

WHAT ARE YOU BUILDING?

Two Factor Authentication 

CHOOSE YOUR LANGUAGE

I'm not a developer 

[Get Started](#)

By clicking the button, you agree to our [legal policies](#).

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

We need to verify you're a human.

  [Verify via SMS](#)

We will send a verification code via **SMS** to number above

Or, we [call you instead](#).

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

Console Dashboard

Account Summary

ACCOUNT SID AC45e9bd6b9ef9e1afde0f50c6e1ae1743
AUTH TOKEN 

[Account Details](#)

News & Tips

Looking up a phone number

Ever curious who you are making calls and sending messages to? You can do a [lookup](#) on a non-Twilio number to learn more about that number and who it belongs to.



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

Programmable SMS Dashboard

[Show API Credentials](#) >

Programmatically send and receive SMS worldwide. Route text messages globally to and from your application over local, mobile, toll-free, and short code numbers.

- [Get Started](#)
- [Tutorial Docs ↗](#)
- [Features & Pricing](#)

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

Get Started with SMS

[Show API Credentials](#) >

1. First let's get a Twilio phone number

[Get your first Twilio number](#)

2. Send a message

Now let's learn how sending a message works on Twilio. Input your information above to auto-generate the code needed to send a message from your phone number and account.

3. Let's send a message to your Twilio phone number and see what happens

Learn about our markup language, TwiML, and how it can be used to respond to SMS messages sent to your Twilio number.

4. Go to the SMS Tutorials

Ready to start learning how to build your SMS App?

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

Your first Twilio Phone Number



(647) 560-8821

Don't like this one? [Search for a different number](#)

This Canada phone number has the following capabilities:

Voice: This number can receive incoming calls and make outgoing calls.

SMS: This number can send and receive text messages to and from mobile numbers.

MMS: This number can send and receive multi media messages to and from mobile numbers.

Cancel

Choose this Number

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:

Congratulations!



Your new Phone Number is **+16475608821**

For help building your Twilio application, check out the resources on the getting started page. Once you've built your application, you can configure this phone number to send and receive calls and messages.

Done

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:

Get Started with SMS

[Show API Credentials](#) >

1. First let's get a Twilio phone number

2. Send a message

Now let's learn how sending a message works on Twilio. Input your information above to auto-generate the code needed to send a message from your phone number and account.

TO

You can only send messages to verified numbers in trial. [Upgrade](#) or [verify another number](#).

FROM

You will send this message from your new Twilio phone number.

BODY

Enter the message you want to send. ⓘ

[Show Request Code](#)

Make Request

3. Let's send a message to your Twilio phone number and see what happens

Learn about our markup language, TwiML, and how it can be used to respond to SMS messages sent to your Twilio number.

4. Go to the SMS Tutorials

Ready to start learning how to build your SMS App?

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:

Success! The message was successfully sent from your Twilio phone number to the verified phone number.

Did you receive the message? (You may need to wait for a few seconds for the message to come through.)

Yes

No

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:

Phone Numbers

Phone Numbers

Number Voice URL [Filter](#)

NUMBER	FRIENDLY NAME	CAPABILITIES			CONFIGURATION
		VOICE	SMS	MMS	
+1 647-560-8821 Toronto, ON	(647) 560-8821				Voice URL: https://demo.twilio.com/welcome/voice/ Messaging URL: https://demo.twilio.com/welcome/sms/reply/

* Can send/receive calls to domestic numbers only
† Can send/receive sms to domestic numbers only
‡ This number does NOT support SIP Trunking
(beta) This number is new to the Twilio Platform

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:

CREDIT CARD PAYPAL

CREDIT CARD NUMBER:

EXPIRES:

CVV :

CARDHOLDER NAME:

STREET ADDRESS:

ZIP CODE:

COUNTRY:

COMPANY/PROJECT URL:

PHONE NUMBER:

optional optional

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:

AMOUNT TO ADD TO YOUR ACCOUNT NOW

\$20.00 

Turn on automatic recharge

When your balance falls below **\$10.00**, we will recharge your balance to **\$20.00**.

Upgrade Account

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

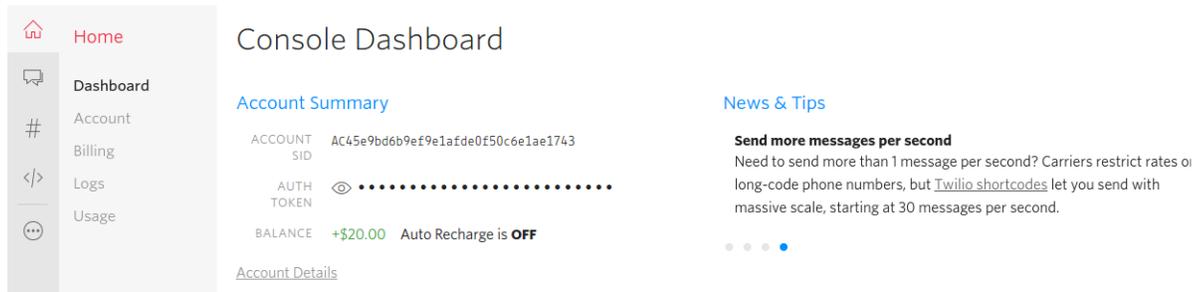
Congratulations! We've upgraded your account and charged your selected payment method **\$20.00**.

The next time you'd like to add funds to your account, click the "Add Funds" link on your account balance page to make a payment.

Your trial number, (647) 560-8821, is now yours to keep for \$1.00 per month, which we will automatically deduct from your account balance starting on April 20th. You can release your numbers at any time from the [Numbers page](#).

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:



The screenshot shows the Twilio Console Dashboard. On the left is a navigation sidebar with links for Home, Dashboard, Account, Billing, Logs, and Usage. The main content area is titled "Console Dashboard" and contains an "Account Summary" section with the following details:

- ACCOUNT SID: AC45e9bd6b9ef9e1afde0f50c6e1ae1743
- AUTH TOKEN: [REDACTED]
- BALANCE: +\$20.00
- Auto Recharge is OFF

Below the account summary is a link for "Account Details". To the right of the account summary is a "News & Tips" section with a sub-heading "Send more messages per second" and a paragraph explaining carrier restrictions and Twilio shortcodes.

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

Account Summary

ACCOUNT SID AC45e9bd6b9ef9e1afde0f50c6e1ae1743

AUTH TOKEN  4ad87[REDACTED]9c81a0f

BALANCE +\$20.00

Account Details

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 Enterprise 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:

Allow cookie-based login (remember me). 

Enable two-factor authentication 

Two-factor authentication is mandatory for all users.

Use SMS delivery for authentication

Sms Provider  Expertexting
 Twilio
 Plivo

Account SID 

Auth Token 

From 

Send to:  +1 201-555-5555

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:

Sms Provider

- Experttexting
 Twilio
 Plivo

Account SID	<input type="text" value="....."/>
Auth Token	<input type="text" value="....."/>
From	<input type="text" value="Phone:(647)123-4567"/>

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:

Send to:

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

 After changing the structure you should synchronize configuration. Do you want to do this now?

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:

- Your FileFlex credentials have been verified.
- Email delivery have been configured.
- Two factor authentication have been configured.

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:

Enable single sign-on with Onelogin

Issuer URL

Service URL

Logout service URL

Certificate











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:

onelogin DEVELOPERS

DOCS

API REFERENCE

SUPPORT

GET A DEVELOPER ACCOUNT

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

Get a Free Developer Account

First name	Last name
Work email	
Work phone	
Company name	
Your sitename	.onelogin.com
Number of users	

Fill 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:

Find Applications

🔍 search...

- | | | |
|------------------|--------------------|--------------------------------------|
| Accounting (306) | Entertainment (17) | Product Management (8) |
| Advertising (29) | ERP (28) | Professional Services Automation (7) |

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:



SAML Test Connector (IdP)
OneLogin, Inc.

SAML2.0

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

Display Name

Visible in portal



Rectangular Icon



Upload an icon with an aspect-ratio of 2.6:1 as either a transparent .PNG or .SVG

Square Icon



Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

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:



Portal

Display Name

Tab

Visible in portal



Rectangular Icon



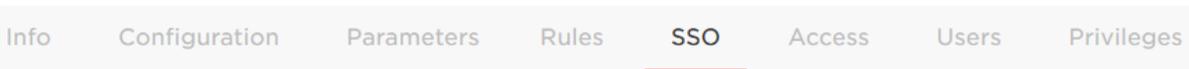
Upload an icon with an aspect-ratio of 2.6:1 as either a transparent .PNG or .SVG

Square Icon



Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

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:

Enable SAML2.0

Sign on method

SAML2.0

X.509 Certificate

Standard Strength Certificate (2048-bit)

[Change](#) | [View Details](#)

SAML Signature Algorithm

SHA-1

Issuer URL

<https://app.onelogin.com/saml/metadata/9fa9d3e1-a392-4c>



SAML 2.0 Endpoint (HTTP)

<https://qnext-dev.onelogin.com/trust/saml2/http-post/sso/ε>



SLO Endpoint (HTTP)

<https://qnext-dev.onelogin.com/trust/saml2/http-redirect/sl>



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:

X.509 Certificate

Standard Strength Certificate (2048-bit)

[Change](#) | [View Details](#)

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

X.509 Certificate

X.509 Certificate

```
-----BEGIN CERTIFICATE-----
MIIEETCCAvmgAwIBAgIUv4r4MkofANHP1k0R/6rUDpxrrVowDQYJKoZIhvcNAQEF
BQAwVjELMAkGA1UEBhMCVVMxDjAMBGNVBAoMBVfuZXh0MRUwEwYDVQQLDAXPbmVM
b2dpb1BJZFAXIDAeBgNVBAMMF09uZUxvZ21uIEFjY291bnQgMTMxNzk2MB4XDTE4
MDCzMDIwNTYyMFOxDTIzMDczMDIwNTYyMFOwVjELMAkGA1UEBhMCVVMxDjAMBGNV
BAoMBVfuZXh0MRUwEwYDVQQLDAXPbmVMb2dpb1BJZFAXIDAeBgNVBAMMF09uZUxv
Z21uIEFjY291bnQgMTMxNzk2MTMxNzk2MTMxNzk2MTMxNzk2MTMxNzk2MTMxNzk2

```

X.509 PEM ▼ DOWNLOAD

- 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:

← Standard Strength Certificate (2048-bit) DELETE SAVE

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

Info **Configuration** Parameters Rules SSO Access Users Privileges

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 preceding 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.

SAML Test Connector (IdP w/attr)

MORE ACTIONS

SAVE

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:

Enable single sign-on with Onelogin

Issuer URL

Service URL

Logout service URL

Certificate

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:

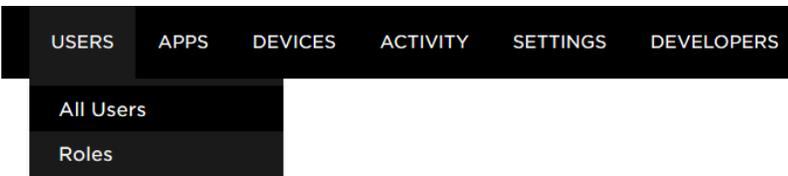
<input checked="" type="checkbox"/> Enable single sign-on with OneLogin	
Issuer URL	<code>https://app.onelogin.com/saml/metadata/9fa9d3e1-a3f</code>
Service URL	<code>https://qnext-dev.onelogin.com/trust/saml2/http-post/s</code>
Logout service URL	<code>https://qnext-dev.onelogin.com/trust/saml2/http-redirect</code>
Certificate	<pre>-----BEGIN CERTIFICATE----- MIIEETCCAvmgAwIBAgIUv4r4MkoFANHP1k0R/6rUDpxrrVowDQYJKoZIhvcNAQEF BQAwVjELMAkGA1UEBhMCVVMxZjAMBGNVBAoMBVfuZXh0MRUwEwYDQVQLDAsPbmVh b2dpbiBjZFAxIDAeBgNVBAMMF09uZUxvZ21uIEFjY291bnQMTMxNzk2MB4XDTE4 MDczMDIwNTYyMfoXDTIzMDczMDIwNTYyMfoVjELMAkGA1UEBhMCVVMxZjAMBGNV BAoMBVfuZXh0MRUwEwYDQVQLDAsPbmVhbn2dpbiBjZFAxIDAeBgNVBAMMF09uZUxv Z21uIEFjY291bnQMTMxNzk2MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgK CAQEAxBFHPh5CLqLDyF+M6kaofWZ3neLvNUmYM+zmf2F4suLpCQoUYiC6rUtDQN 8SSyN6PFsEFpSjzP68qOckRDR+KMF241V8FIN+B2JTjvnSToST3VBxHetnJyVwPeP /gzWn90Zn2qaFeIXe2rRmpupK0DANbJLE49j7omTSHZ9Jjbfyv6HPCIEZ2HFm8Y PqYHv7/9kam8ndGHvrtV93ScVkvPq1/cgYd37542egDCX1BbGu5pxjL22ke18YMo VV8NmB7Bfurkx1/hQDFR+x9MDFmi6RMHqtgPY7P7CvcuYvQ24h0JB04ZAH5+wcKm /G5KyBz8Mysp+cvfd+AtEeqHNwIDAQABO4HMMHTMAwGA1UdEwEB/wQCAAAwHQYD VR00BBYEFLSHV81oZwovmo5jfn5hCUIFUSZIMIGTbgNVHSMegYswgYiAFLSHV81o Zwovmo5jfn5hCUIFUSZIoVqkMdBWMQswCQYDVQGEwJVUzEOMAwGA1UECgwFUW51 eHQxFTATBgNVBAsMDE9uZUxvZ21uIE1kUDEgMB4GA1UEAwwXT251TG9naW4gQWwv b3VudCAxMzE3OTaCFFeK+DJKHwDRz9ZNEf+q1A6ca61aMA4GA1UdDwEB/wQEAwIH gDANBgkqhkiG9w0BAQEFAAOCAQEAHJ5p0b9D0HpicGgBORBQh3YLtL4gQq8IP03q 9+aTm03iUfvpz9eD+I0S/MzgFh/SYTKo6tK14im0nzuopvd3D4Mbb+f01EM8DmF7 KMKCUg8tu67cnjtJVB/q1NL/YdIAz8xaw5nm6AeM3K6eXotB0su0iP77spi sug wNE5pRGMwkNIjUxwUMvIh4e0VsZ1cTz7XNOzZSsh0A8ISHH5udxKbnNwMkKi1SfK bQo03Lah/m87kSzIEIjJ8E0rZ8+6pC7oQAGYg1Vj91C19Realj6iukJlq2fVer86 8nt+IbtHgwip1M3JpJYn7+P6Ylug6LMSCVM3RgAN1o9pTbURAvA== -----END CERTIFICATE-----</pre>

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.



Active



First Name *

George

Last Name *

Mattoge

Email



Username

Phone Number

Manager

Choose a manager

Company

Qnext

Department

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

George Mattoge

MORE ACTIONS

SAVE USER

User Info

Authentication

Applications

Activity

Assume User

Change Password

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:

User Info

Authentication

Applications

Activity

Roles

Default

Applications



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

Assign New Login To George Mattoge

This login will override any apps assigned via roles.

Select Application

FileFlexDemo

CANCEL

CONTINUE

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

Edit FileFlexDemo Login For George Mattoge

Enabled

Allow users to sign in

Email (SAML NameID)

[REDACTED]

E-mail (Attribute)

[REDACTED]

First Name (Attribute)

George

Last Name (Attribute)

Mattoge

Member of (Groups) (Attribute)

[REDACTED]

CANCEL

DELETE

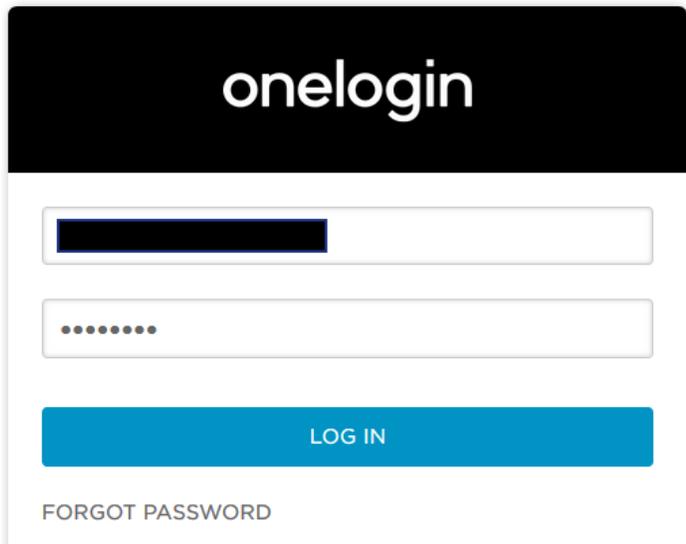
SAVE

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

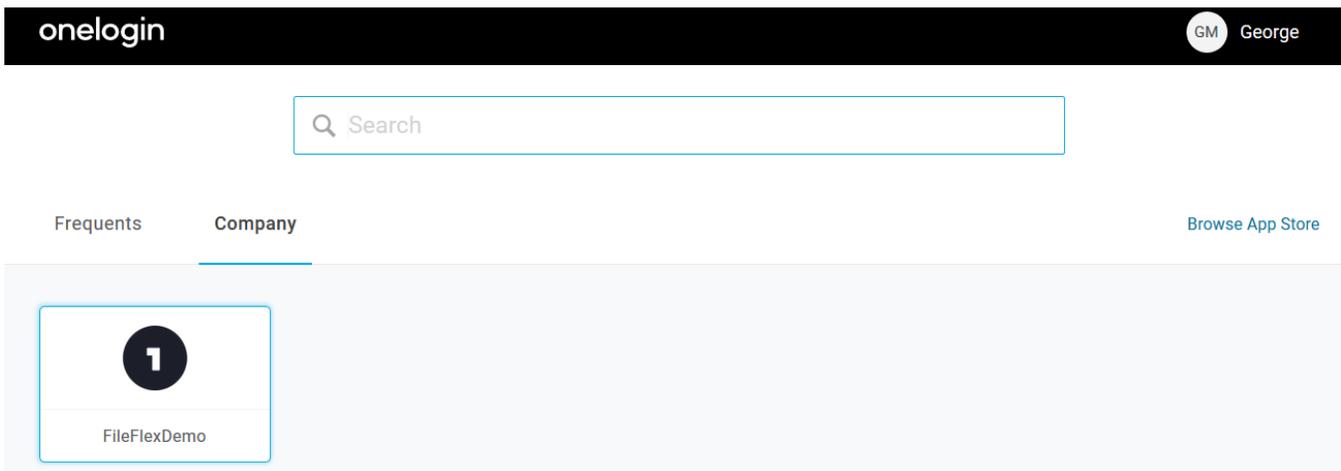
We must now ensure that the app appears to the user when logging in to the OneLogin portal. Navigate to the OneLogin portal. In this example case, it is at:

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

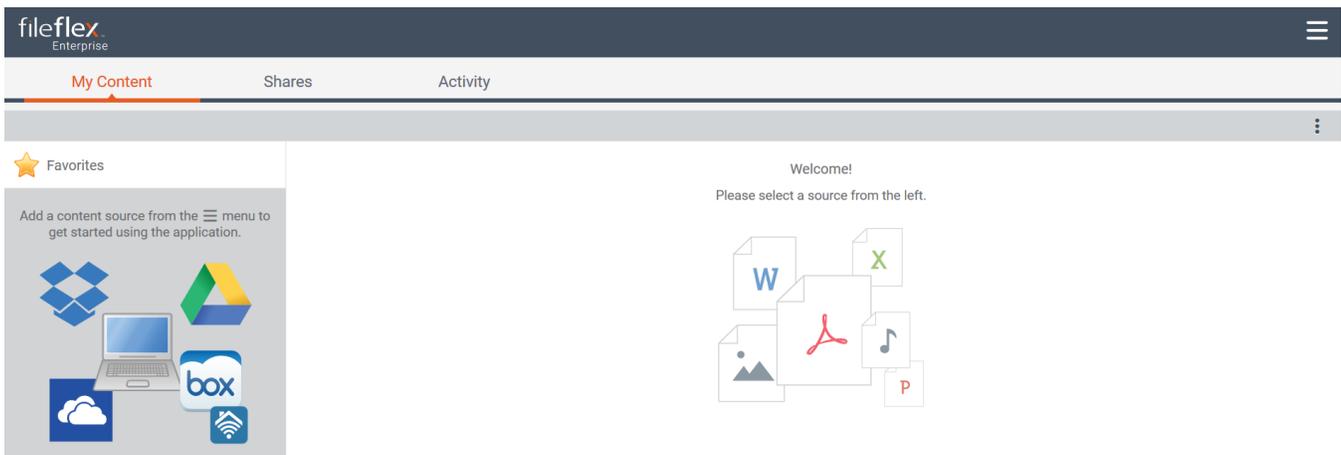
Enter the email and password for the user we just created:



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:

Login to FileFlex Enterprise Secure File Access

Next

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

Login to FileFlex Enterprise Secure File Access

Remember Me

[Reset Password](#)

Cancel Login

Login with OneLogin

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.

i 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.

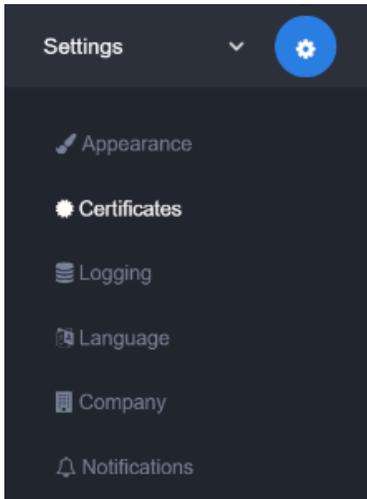
8.5.3.1. Creating a self-signed Certificate

Log in to the Admin Dashboard of HelloID.

i 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.

A web form titled 'GENERATE A SELF-SIGNED CERTIFICATE' with a breadcrumb 'HOME > CERTIFICATES > GENERATE A SELF-SIGNED CERTIFICATE'. It has 'Cancel' and 'Save' buttons. The form is divided into two sections: 'General information' with a 'NAME OF CERTIFICATE' input field, and 'Certificate information' with fields for 'COUNTRY NAME' (dropdown), 'LOCALITY NAME', 'STATE OR PROVINCE NAME', 'ORGANIZATION UNIT NAME', 'ORGANIZATION NAME', 'EMAIL ADDRESS', and 'COMMON NAME (DOMAIN)'. A blue envelope icon is in the bottom right corner.

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.

A web page titled 'CERTIFICATES' with a '+ Create Self-signed certificate' button. It features a search bar 'Search certificates' and a table with two columns: 'Name' and 'Actions'. The table lists four certificates: FileFlexDemo, HelloID-ActiveDirectoryIdP, QnextBG, and QnextDev. Each row has 'Details' and 'Delete' links in the Actions column.

Name	Actions
FileFlexDemo	Details Delete
HelloID-ActiveDirectoryIdP	Details Delete
QnextBG	Details Delete
QnextDev	Details Delete

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

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 screenshot shows a configuration page for an application. The top section contains various toggle and dropdown settings:

- Sign Assertion:
- Sign Response:
- Use DS Prefix:
- X509 Certificate: OneIDDev
- Override Audience:
- Extra audience: Initial value
- Encrypt Assertion:
- X509 Encryption Certificate: -- select certificate --
- Use Custom Digest and Signature methods:
- Custom Digest method:
 - http://www.w3.org/2009/09/untitledsha1
 - http://www.w3.org/2001/04/xmlmime#a256
- Custom Signature method:
 - http://www.w3.org/2009/09/untitledsha1
 - http://www.w3.org/2001/04/xmlmime#more#a256
- Send group membership attribute:
- Group membership attribute name: MemberOf
- Mapping Set: [#3 Configure Mapping Set](#)

The bottom section shows a table of configuration fields:

FIELD NAME	VALUE
Name ID format	emailaddress
Issuer	https://spdev.helloid.com
Endpoint/ACS URL	https://mplex.creus.com/flow/bagp/publicview/login_partner_saml
Wildcard and use ACS request URL	<input checked="" type="checkbox"/>
ACS validation list	https://mplex.creus.com/flow/bagp/publicview/login_partner_saml
Binding	HTTP-Post
SP-initiated URL	Initial value
Sign Assertion	<input checked="" type="checkbox"/>

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.

The screenshot shows the top right corner of the configuration page with the following buttons:

- Cancel
- Download metadata
- Save

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="_8F1C6575SDFG4563F23041EF3D485B382"
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>
            MIIDNDCCAhygAwIBAgI IHbg5V0hfOtkwDQYJxxxxxxxxx=
          </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>
```

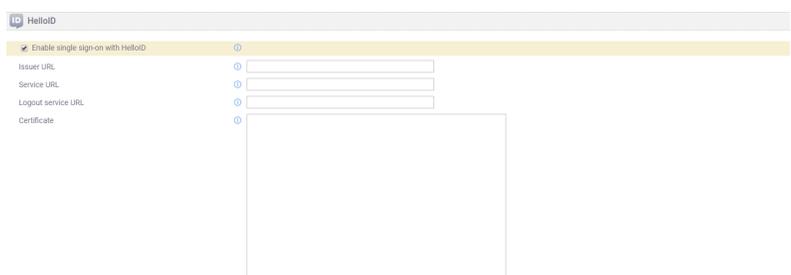
You need to search for two values from this metadata.

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-xxxxx"

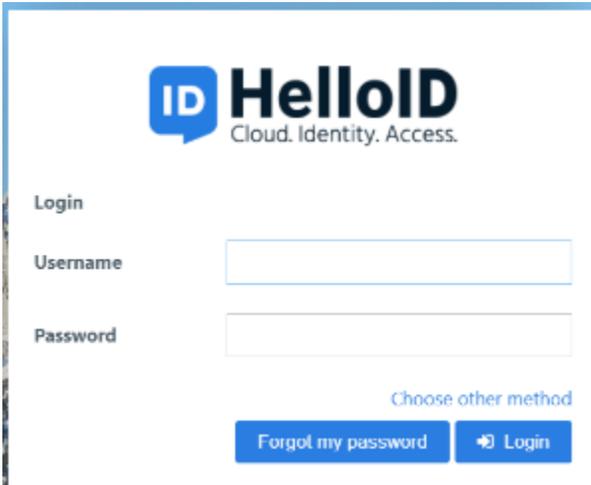
Save all the values in a text file and launch FileFlex Server Admin Page.

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.

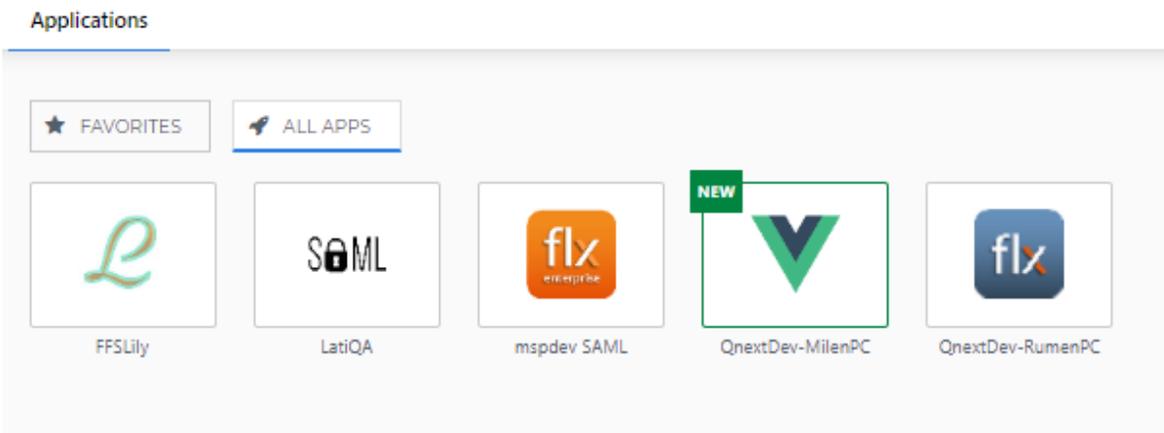


Once credentials are provided, the user is taken directly to FileFlex app and this completes our verification of HelloID Setup.

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.

i 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".

The screenshot shows the SmartLogin 'Company Apps' dashboard. On the left is a sidebar with the 'smartLogin' logo and a navigation menu including ADMIN, HOME, USERS, ROLES, APPS, CATEGORIES, GROUPS, POLICIES, NETWORKS, and DEVICES. The main content area is titled 'Company Apps' and includes a sub-header: 'You use the Apps page in Cloud Manager to assign web applications to users'. Below this are three buttons: 'ADD CAS APP', 'ADD FORM APP', and 'ADD SAML APP', with the last one circled in red. A search bar labeled 'Search for an app...' is positioned below the buttons. The dashboard displays two application cards: 'Amazon WS Administrative' (Cloud computing services, marked as 'DISABLED') and 'Dropbox Office' (File hosting service, marked as 'SAML'). At the bottom of each card, there are statistics for 'USERS' and 'GROUPS', both showing a count of 0.

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

ADD CAS APP ADD FORM APP ADD SAML APP

Configuration Description

< Back

*** Name:**
FileFlex_Test

Image:
Choose File No file chosen

*** Category:**
Systems

Admin URL:

If a URL is introduced, a link will be appear in the this app menu to easier access to this site

UUID:

Shareable:
If this option is enabled, it will allow users (with the right permissions) who have access to this application to share it with other users of the system. Refe

Created on:2020-01-20 18:59:04

Updated on:2020-03-23 11:16:13

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=SamISmartLogin

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:

Consumer service post:

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

Force IDP initialization?:

Relay state:

Discover attributes:

first_name
last_name
email
registration_id
username

Mapping:

Submit

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

The screenshot shows the FileFlex Admin console interface. On the left is a navigation sidebar with options like HOME, USERS, ROLES, APPS, CATEGORIES, GROUPS, POLICIES, NETWORKS, DEVICES, REPORTS, SETTINGS, RESTFUL, and BLACKLIST IPS. The top navigation bar contains icons for GENERAL, AUTH, PROVIDER (circled in red), SECURITY, NOTIFICATIONS, PERMISSIONS, and DEVICES. The main content area displays the configuration for a SAML Provider. The 'Enable' checkbox is checked. The 'Entityid' field contains the URL 'https://smartlogin.cnexus.com'. The 'Single sign_on' and 'Single logout' fields contain '/session/user/saml' and '/session/user/logout' respectively. The 'Valid for' field is set to 25 days. The 'Key file' and 'Cert file' fields have 'upload' and 'Delete' buttons. The 'Idp metadata' field contains 'idp.xml' and the 'Logging level' is set to 'INFO'.

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 :

i 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:

SSL Certificate

Enter a password to protect the keystore: i

Password strength: Very Weak

Enter your SSL certificate: i

Enter your SSL private key: i

The certificates panel is divided into 3 sections:

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 admin user. You should then see a green bar under the password entry indicating that the password is of sufficient strength:

Enter a password to protect the keystore: i

Password strength: Strong

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:

Enter your SSL certificate: i

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):

Name	Date modified	Type	Size
524daaa823ca8e28.crt	5/15/2018 12:49 PM	Security Certificate	3 KB
gd_bundle-g2-g1.crt	5/15/2018 12:49 PM	Security Certificate	5 KB

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

Enter your SSL certificate: ?

1. 524daaa823ca8e28.crt
2. gd_bundle-g2-g1.crt

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

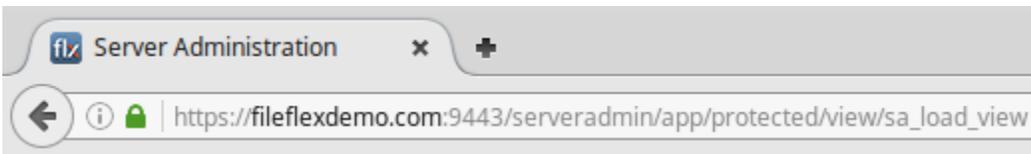
Enter your SSL private key: ?

1. test.fileflexdemo.com.key

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:

 **Changes will be seen after you restart all servers.**
Do you want to do it now?

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:

-  Your FileFlex credentials have been verified.
-  Email delivery have been configured.
-  Two factor authentication have been configured.
-  A custom certificate have been provided.

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 is the account which can be used to log in to user administration.

Name	<input type="text" value="Administrator"/>
Email	<input type="text" value="greg.r.wade@gmail.com"/>
Password	<input type="password" value=""/> Password strength: Very Weak
Confirm Password	<input type="password"/>



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:

Enter an email address and a password (twice) that will be used to log in to user administration once your deployment is ready.

Name	<input type="text" value="Admin"/>
Email	<input type="text" value="admin@fileflexmsp.com"/>
Password	<input type="password" value="*****"/> Password strength: Strong
Confirm Password	<input type="password" value="*****"/>

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:

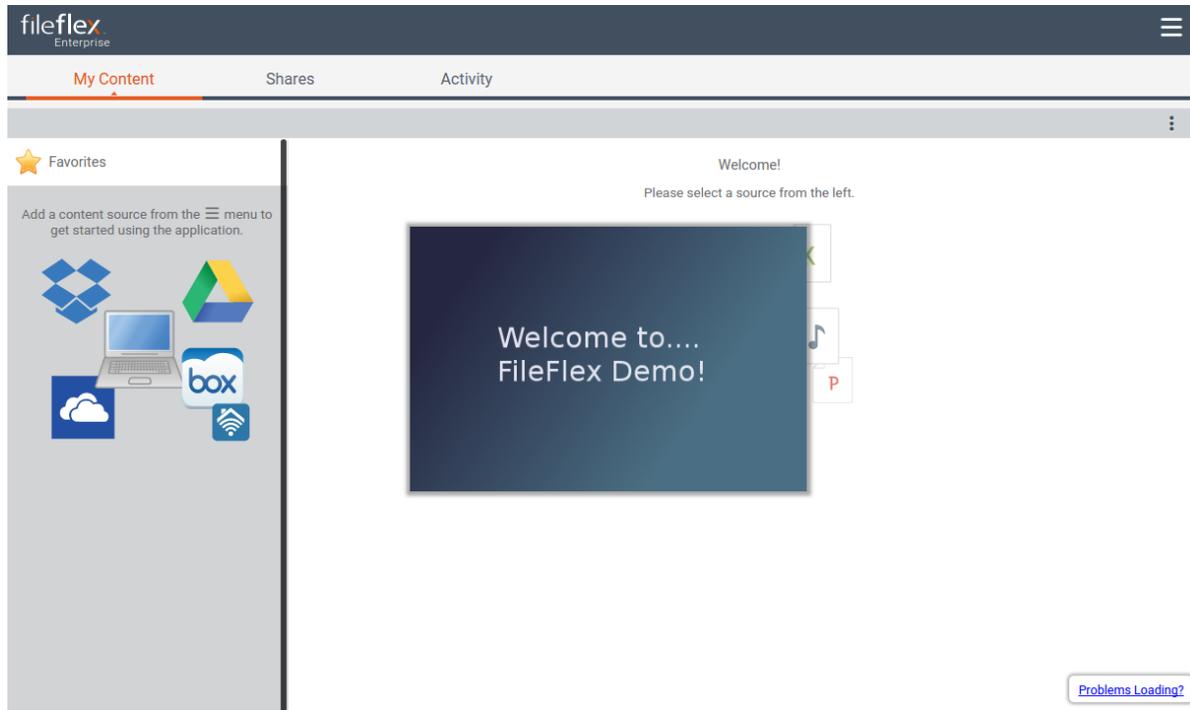
Manage Servers	Overview	The following resources are available for customization. You can revert to the d
Credentials		
Email		
Login Control		
Certificates		
User Administration		
Control Panel	Web Resources	
		privacy.txt
		avatar
		splash

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:

-  Your FileFlex credentials have been verified.
-  Email delivery have been configured.
-  Two factor authentication have been configured.
-  A custom certificate has not been provided.
-  A User Administration account has been created.
-  A customized splash screen has not been provided.

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

This is the server SSH public key which you should use if you add any slave machines. Copy the key and paste it into the dialog when requested during the slave machine setup. You don't need the SSH key for a single machine setup and configuration.

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCoIZRbdgToeGEFigOuWWkvArVnpRQUxk5fA
WCGETuw1q1nLzWinTUGPbkyHC3rbjmnAehT6QS7NTv6jwClSo5XluQm1br9NdTv4MFi
3trKZ7ptJwhsXld+IGGYs1xaBJpNq8qGfyRNUm9aHTX1mfniXmAQHMIRgEUCXJ1GvPa
laSAoa6IRVSJSk3taB7BQchP2c3giz+IvIAtofBU11z1iLx/zKwJWpM/o3I5pGVGA3iU6s4R
0QpAZkNfGRZ/3Z67gTQu3yHNrps5ikyENhDe3sJV4GL/grk6II0bUiGx7YqPkdU4DSnt+P
g45ZP+H8d2XxL5dcAGPYEuCo4nRGm// root@test.fileflexdemo.com
```

Copy

Provider Encryption Policy

None Raw Sgx

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 encryption, 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 encryption (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" encryption from the provider encryption policy checkboxes:

Provider Encryption Policy  None Raw Sgx

Note that an SSL certificate must have been installed before this functionality can be used. Once you have verified that 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:

Server	Process ID	State
Messaging Server	7479	
Web Server	7623	
Administration Server	7927	
Storage Server	7376	
PKI Server	-	

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:

PKI Server	9616	
------------	------	---

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 certificate 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.

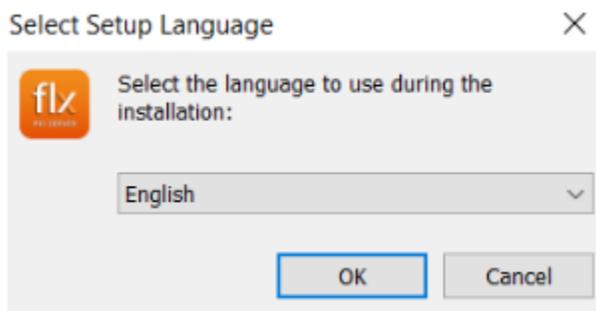
i PKI Server Download

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

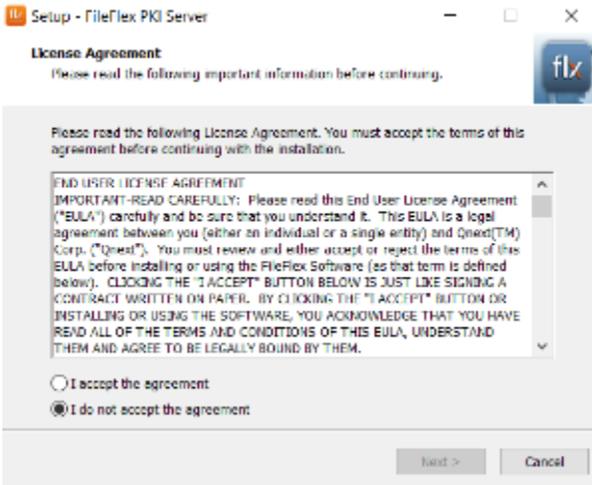
https://res.fileflex.com/packages/installers/pki/PKIServerInstaller_Latest.exe

8.9.4.1. Installing the PKI Server

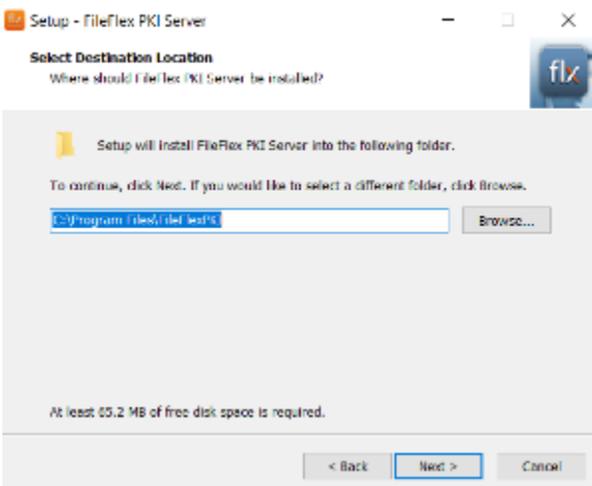
Once you've downloaded the PKI server, and have it available on a compliant machine, it's time to run the installer. Doing so will open the installation, and request your language of choice:



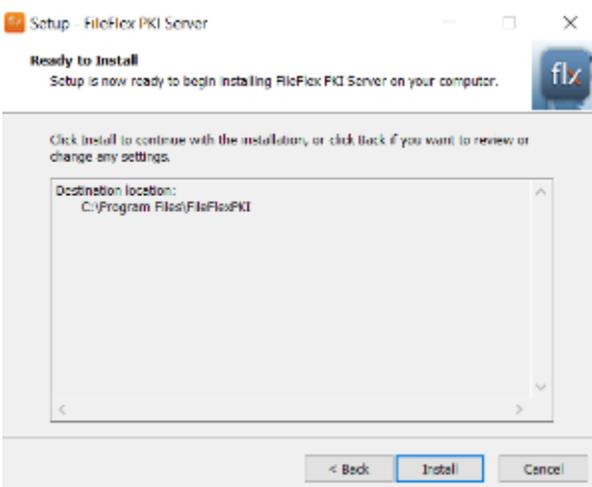
Select the language you prefer, then click OK. You will then be presented with the licensing agreement:



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.



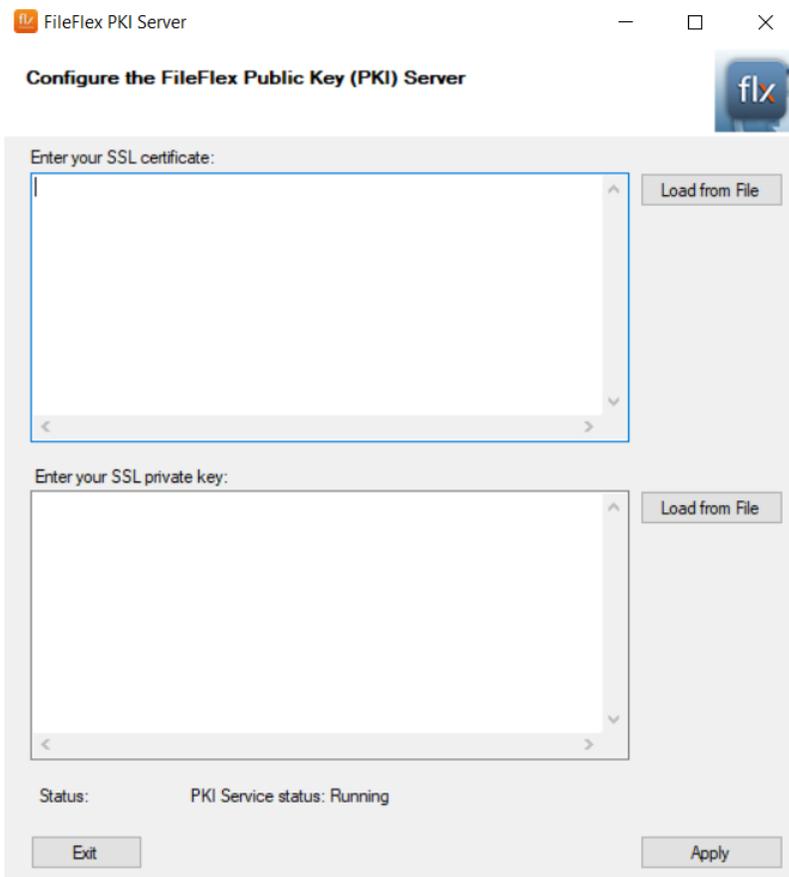
If you're satisfied with your choices, click "Install" to proceed. The files will then be installed, as will Intel's DataGuard runtime which may take some time. When the process completes you will receive a confirmation:



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:

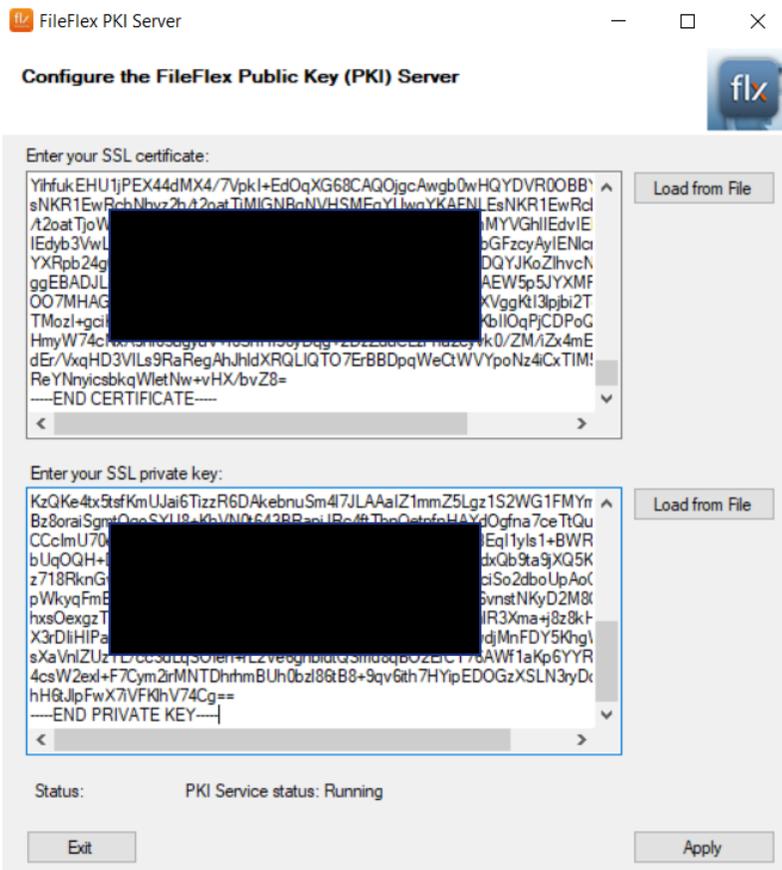
Concatenate Certificate and Bundle

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

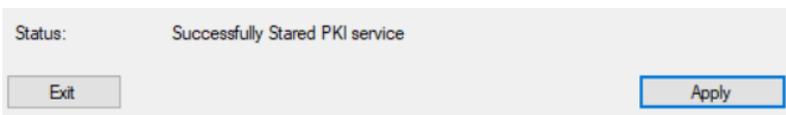
Direct Certificate Entry

It is possible to enter the certificate 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:

Your Server Deployments					
Status	Deployment ID	Deployment Key	Deployment URL	Name	Action
Enabled	5b310[REDACTED]5f642 43[REDACTED]	TG0D[REDACTED]Q6E 59[REDACTED]62C	https://test2.fileflexdemo.com	Test FileFlex Demo	Edit/View

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

Edit Server Deployment

Deployment ID: 5b310[REDACTED]e7

Deployment Key: TG0D[REDACTED]CH9PS0NCGI62C

Deployment URL: <https://test2.fileflexdemo.com>

Deployment Name:

PKI URL:

Email:

Status:

[Delete](#) [Cancel](#) [Update](#)

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.

PKI URL:

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:

User Activity Logging Target: Disabled File Nagios

Use local timezone when generating reports. 

Test log connection

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

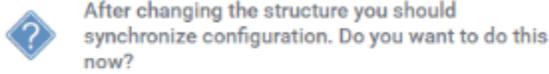
When generating a user activity report from within the user administration module, changing this option will caused the times to be stored with local time, rather than the default UTC+0 timezone. If unsure, leave this unchecked.

8.10.2. Logging Activity to a File

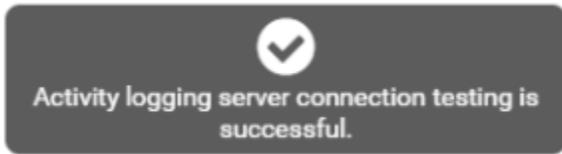
To enable logging user activity to a file, click on the target dropdown and select the "File" option.

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

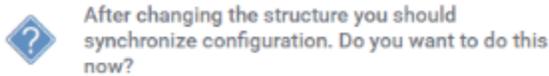
If you previously had a different value set, you may be promoted to synchronize the changes:



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:nnRgNKfQxxxxxxxxyz2X503Yw9MISntnoIM.  
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:

User Activity Logging Target: Disabled
 File
 Nagios

Nagios IP:

Use local timezone when generating reports.

Test log connection

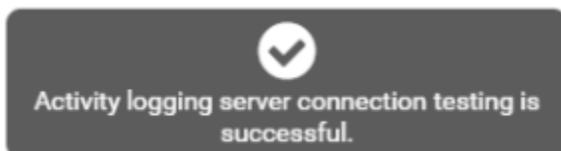
Enter the IP address of a running Nagios server in the "Nagios IP" field.

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:

 After changing the structure you should synchronize configuration. Do you want to do this now?

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:



After changing the structure you should synchronize configuration. Do you want to do this now?

No

Yes

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:

ALL EVENTS
Fields

0 to 5 of 5 available for paging

@timestamp	<host>	<type>	<message>
2017-12-14T15:02:47.406+02:00	192.168.0.182	syslog	<14>1 2017-12-14T13:02:47.412Z lily[...].net fileflex --- 14/12/17 13:02:02 ProviderRemove [prrm] liliab@[...].om (liliab@[...].om) remov...
2017-12-14T15:01:47.419+02:00	192.168.0.182	syslog	14/12/17 13:01:24 ProviderVerify [prvr] liliab@[...].om (liliab@[...].om)'s content source (file) was verified.
2017-12-14T15:01:47.406+02:00	192.168.0.182	syslog	<14>1 2017-12-14T13:01:47.410Z lily[...].net fileflex --- 14/12/17 13:01:23 ProviderCreate [prcr] liliab@[...].om (liliab@[...].om) added...
2017-12-14T14:54:58.625+02:00	192.168.0.182	syslog	<14>1 2017-12-14T12:54:58.626Z lily[...].net fileflex --- 14/12/17 12:54:58 TestCollector [L_test] Testing activity collection/logging
2017-12-14T14:54:47.704+02:00	192.168.0.182	syslog	<14>1 2017-12-14T12:54:47.704Z lily[...].net fileflex --- 14/12/17 12:54:47 TestCollector [L_test] Testing activity collection/logging

0 to 5 of 5 available for paging

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:

14/12/17 13:01:24 ProviderVerify [prvr] liliab@[...].om (liliab@[...].om)'s content source (file) was verified.

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

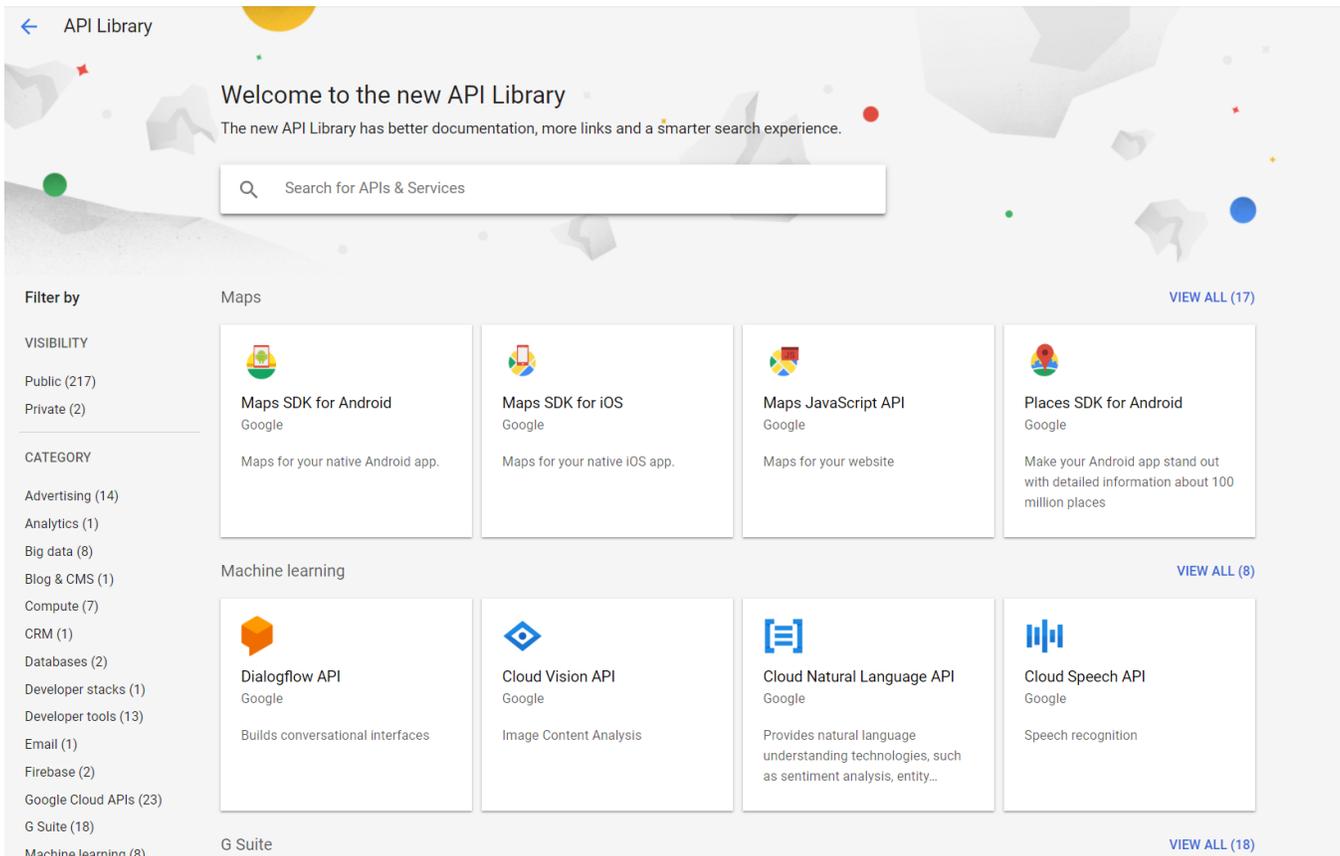


It's important to complete the "Supplying an SSL Certificate" steps prior to configuring Google Drive Access.

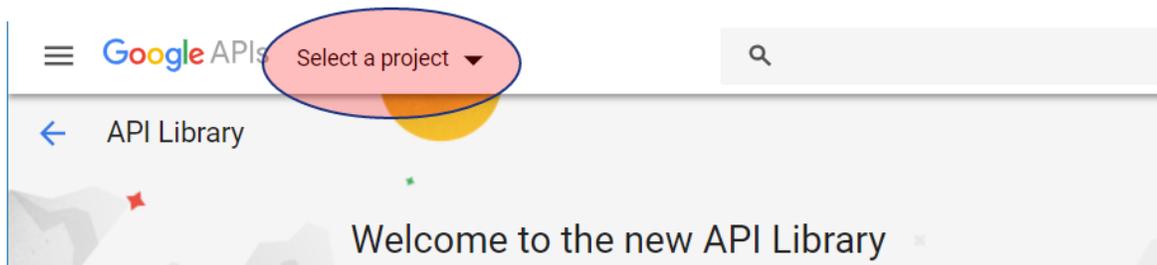
In order to configure Google Drive access from within FileFlex Enterprise, you must obtain a Google API Key and Secret from Google. Sign in to your Google account, and navigate to the following Google URL which is used to configure their APIs:

<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:

Select a project

 NEW PROJECT

Search projects and folders



RECENT

ALL

Name	ID
 No organization	0

CANCEL OPEN

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

New Project



You have 9 projects remaining in your quota. Request an increase or delete projects.

[Learn more](#)

[MANAGE QUOTAS](#)

Project Name *

MyFileFlexProject



Project ID: myfileflexproject-229412. It cannot be changed later. [EDIT](#)

Location *



No organization

[BROWSE](#)

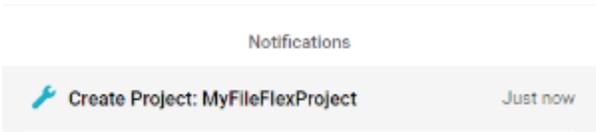
Parent organization or folder

CREATE

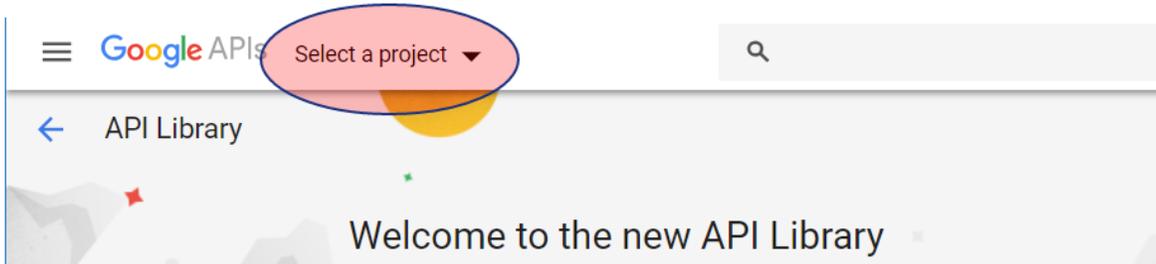
CANCEL

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

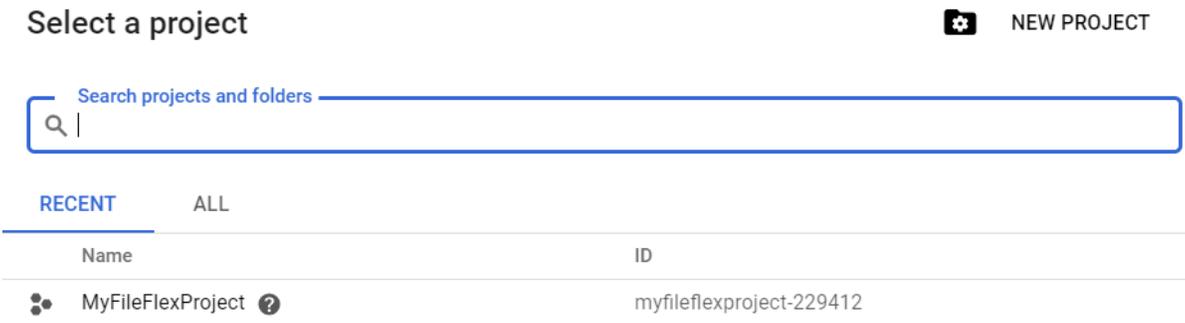
You will see a notification when the project is ready:



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



Select your project from the list:



CANCEL OPEN

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

Google APIs MyFileFlexProject

API Library

Search for APIs & Services

Filter by

VISIBILITY

- Public (217)
- Private (2)

CATEGORY

- Advertising (14)
- Analytics (1)
- Big data (8)
- Blog & CMS (1)
- Compute (7)
- CRM (1)
- Databases (2)
- Developer stacks (1)
- Developer tools (13)
- Email (1)
- Firebase (2)
- Google Cloud APIs (23)
- G Suite (18)
- Machine learning (8)
- Maps (17)
- Mobile (14)
- Monitoring (4)
- Networking (4)
- Security (2)
- Social (4)
- Storage (4)

Maps VIEW

- Maps SDK for Android**
Google
Maps for your native Android app.
- Maps SDK for iOS**
Google
Maps for your native iOS app.
- Maps JavaScript API**
Google
Maps for your website
- Places SDK for Android**
Google
Make your Android app stand c with detailed information about million places

Machine learning VIEW

- Dialogflow API**
Google
Builds conversational interfaces
- Cloud Vision API**
Google
Image Content Analysis
- Cloud Natural Language API**
Google
Provides natural language understanding technologies, such as sentiment analysis, entity...
- Cloud Speech API**
Google
Speech recognition

G Suite VIEW

- Google Drive API**
Google
The Google Drive API allows clients to access resources from Google Drive
- Google Calendar API**
Google
Integrate with Google Calendar using the Calendar API.
- Gmail API**
Google
Flexible, RESTful access to the user's inbox
- Google Sheets API**
Google
The Sheets API gives you full control over the content and appearance of your spreadshe

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

API Library



Google Drive API
Google

The Google Drive API allows clients to access resources from Google Drive

[ENABLE](#) [TRY THIS API ↗](#)

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

Navigation menu APIs
Google Drive API

Overview ■ DISABLE API PROVIDE FEEDBACK

Details

Name
Google Drive API

By
Google

Service name
drive.googleapis.com

Overview
The Google Drive API allows clients to access resources from Google Drive.

Activation status
Enabled

Traffic by response code

Request/sec (2 hr average)

No data is available for the selected time frame.

1.0/s
0.8/s
0.6/s
0.4/s
0.2/s
0

Dec 30 2019 2019 2019

CREATE CREDENTIALS

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

Google APIs fileflexdemo drive app

APIs & Services
Google Drive API

Credentials + CREATE CREDENTIALIAL DELETE

Credentials compatible with this API

To view all credentials or create new credentials visit [Credentials in APIs & Services](#)

Overview
Metrics
Quotas
Credentials
Drive UI Integration

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

API APIs & Services

Credentials

Add credentials to your project

1 Find out what kind of credentials you need

We'll help you set up the correct credentials
If you wish you can skip this step and create an [API key](#), [client ID](#), or [service account](#)

Which API are you using?

Different APIs use different auth platforms and some credentials can be restricted to only call certain APIs.

Choose...

What credentials do I need?

2 Get your credentials

Cancel

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

The dialog box will then change to the following:

Dashboard

Library

Credentials

Add credentials to your project

1 Find out what kind of credentials you need

We'll help you set up the correct credentials

If you wish you can skip this step and create an [API key](#), [client ID](#), or [service account](#)

Which API are you using?

Different APIs use different auth platforms and some credentials can be restricted to only call certain APIs.

Google Drive API

Where will you be calling the API from?

Credentials can be restricted using details of the context from which they're called. Some credentials are unsafe to use in certain contexts.

Choose...

What data will you be accessing?

Different credentials are required to authorize access depending on the type of data that you request.

User data

Access data belonging to a Google user, with their permission

Application data

Access data belonging to your own application

[What credentials do I need?](#)

2 Get your credentials

Cancel

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:

API APIs & Services

Credentials

Dashboard

Library

Credentials

Add credentials to your project

- 1 Find out what kind of credentials you need

We'll help you set up the correct credentials
If you wish you can skip this step and create an [API key](#), [client ID](#), or [service account](#)

Which API are you using?
Different APIs use different auth platforms and some credentials can be restricted to only call certain APIs.

Google Drive API

Where will you be calling the API from?
Credentials can be restricted using details of the context from which they're called. Some credentials are unsafe to use in certain contexts.

Web server (e.g. node.js, Tomcat)

What data will you be accessing?
Different credentials are required to authorize access depending on the type of data that you request.

User data
Access data belonging to a Google user, with their permission

Application data
Access data belonging to your own application

What credentials do I need?
- 2 Get your credentials

Cancel

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

API APIs & Services

Credentials

Dashboard

Library

Credentials

Add credentials to your project

- Find out what kind of credentials you need
Calling Google Drive API from a web server
- Create an OAuth 2.0 client ID
Name 

Restrictions
Enter JavaScript origins, redirect URIs, or both [Learn More](#)
Origins and redirect domains must be added to the list of Authorized Domains in the [OAuth consent settings](#).
Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.
- Set up the OAuth 2.0 consent screen
- Download credentials

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:

API APIs & Services

Credentials

- Dashboard
- Library
- Credentials

Add credentials to your project

- ✔ Find out what kind of credentials you need
Calling Google Drive API from a web server
- ✔ Create an OAuth 2.0 client ID
Created OAuth client 'Web client 1'

3 Set up the OAuth 2.0 consent screen

Email address ?

Product name shown to users ?

[More customization options](#)

[Continue](#)



The consent screen will be shown to users whenever you request access to their private data using your client ID. It will be shown for all applications registered in this project.

You must provide an email address and product name for OAuth to work.

4 Download credentials

[Cancel](#)

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:

API APIs & Services

Credentials

- Dashboard
- Library
- Credentials

Add credentials to your project

- ✔ Find out what kind of credentials you need
Calling Google Drive API from a web server
- ✔ Create an OAuth 2.0 client ID
Created OAuth client 'Web client 1'
- ✔ Set up the OAuth 2.0 consent screen

4 Download credentials

Client ID 1017510489367-4i88fdhgn75jh8s5gbt4gjrlrq6pmqj.apps.googleusercontent.com

Download this credential information in JSON format. This is always available for you on the credentials page.

[Download](#)
[I'll do this later](#)

[Done](#)
[Cancel](#)

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

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

Name	Creation date	Type	Client ID
<input type="checkbox"/> MyFileFlexClientID	Jan 22, 2019	Web application	1017510489367-4i88fdhgn75jh8s5gbt4gjlrq6pmqj.apps.googleusercontent.com

Select your OAuth 2.0 client IDs:

Name	Creation date	Type	Client ID
<input checked="" type="checkbox"/> MyFileFlexClientID	Jan 22, 2019	Web application	1017510489367-4i88fdhgn75jh8s5gbt4gjlrq6pmqj.apps.googleusercontent.com

You will then see your credentials:

Client ID for Web application

DOWNLOAD JSON RESET SECRET DELETE

Client ID	1017510489367-4i88fdhgn75jh8s5gbt4gjlrq6pmqj.apps.googleusercontent.com
Client secret	iy2aR31xCVLeh_NbbD_B5D11
Creation date	Jan 22, 2019, 8:59:17 AM

Name ?

MyFileFlexClientID

Restrictions

Enter JavaScript origins, redirect URIs, or both [Learn More](#)

Origins and redirect domains must be added to the list of Authorized Domains in the [OAuth consent settings](#).

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

https://www.example.com

Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

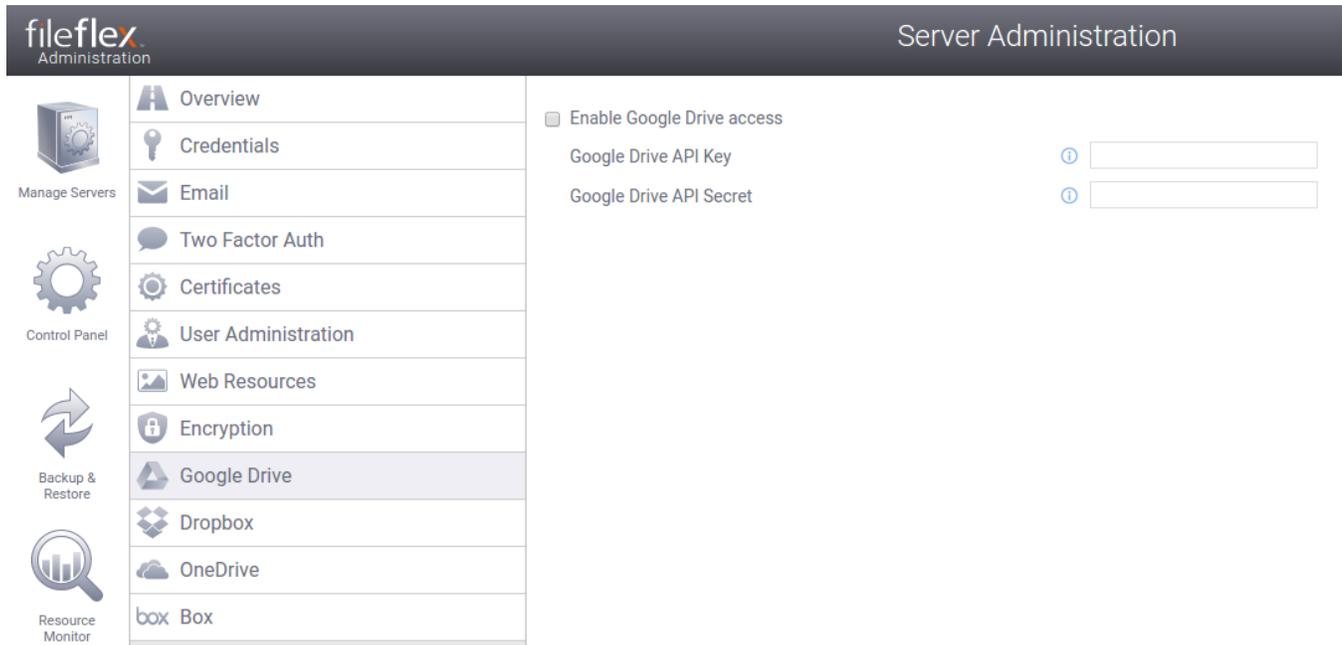
https://test.fileflexdemo.com/fbweb/app/public/view/authorize_partner/google

https://www.example.com

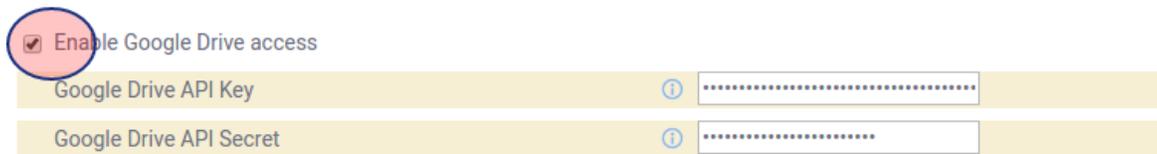
Save Cancel

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:

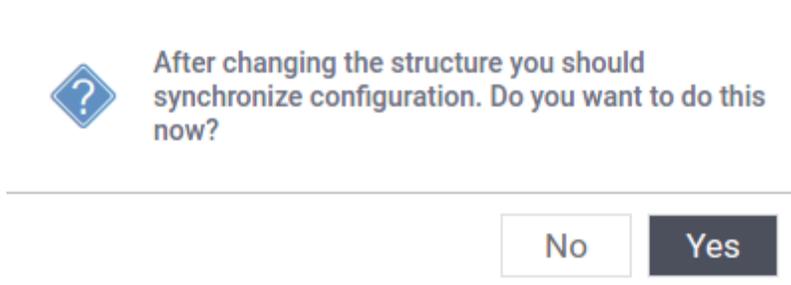


You will then need to enter the API Key (Client ID) and Secret (Client Secret) provided earlier by Google.

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 app isn't verified

This app hasn't been verified by Google yet. Only proceed if you know and trust the developer.

If you're the developer, submit a verification request to remove this screen. [Learn more](#)

[Hide Advanced](#)

BACK TO SAFETY

Google hasn't reviewed this app yet and can't confirm it's authentic. Unverified apps may pose a threat to your personal data. [Learn more](#)

[Go to komero.net \(unsafe\)](#)

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.

Type **Continue** to go to komero.net

Enter text

Continue|

CANCEL NEXT

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:

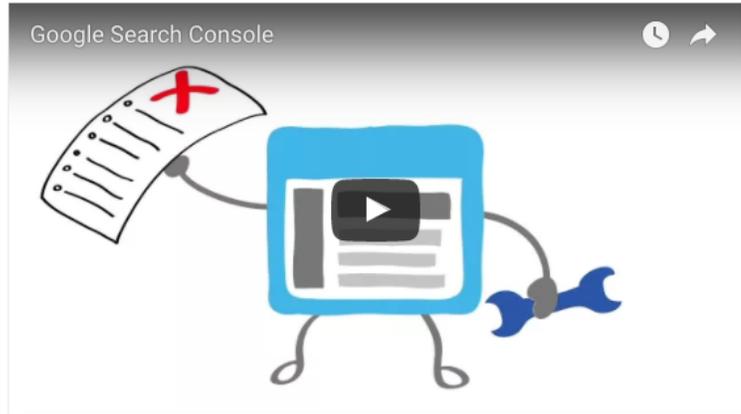
Welcome to Search Console

Get the data, tools, and diagnostics needed to create and maintain Google-friendly websites and mobile apps. To get started, just add your site or app now.

Website

Here are some of the things you can do once you add your property:

- Analyze clicks from Google Search. [Learn more.](#)
- Get alerts for critical errors or issues. [Learn more.](#)
- Test whether Google can successfully understand your content. [Learn more.](#)



- 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:

Search Console

Verify your ownership of <http://fileflexdemo.com/>. [Learn more.](#)

Recommended method

Alternate methods

Recommended: Domain name provider

Sign in to your domain name provider.

Namecheap.com

Follow the steps below to create a DNS (Domain Name System) record that proves to Google that you own the domain.

1. Add the TXT record below to the DNS configuration for **fileflexdemo.com**.

```
google-site-verification=aeCzwcVsZVzVlid9WTrRchHCQD00EZ3
```

2. Click **Verify** below.

When Google finds this DNS record, we'll make you a verified owner of the domain. (Note: DNS changes may immediately, we'll check for it periodically.)

To stay verified, don't remove the DNS record, even after verification succeeds.

Note: adding this record won't affect your mail flow or any other feature in any way.

Having trouble? Contact your domain name provider directly for further assistance.

VERIFY

Not now

- 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:



Congratulations, you have successfully verified your ownership of

[Continue](#)

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 for 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:

API APIs and Services **MyFileFlexProject**

APIs and Services **Credentials**

Dashboard
Library
Credentials

[Credentials](#) [OAuth consent screen](#) [Domain verification](#)

[Create credentials](#) [Delete](#)

Create credentials to access your enabled APIs. [Refer to the API documentation](#) for details.

OAuth 2.0 client IDs

<input type="checkbox"/>	Name	Creation date	Type	Client ID
<input type="checkbox"/>	Web client 1	Jul 26, 2017	Web application	1007999542710-k38reuoo6b5vnt0eqv3u5digo9u1ufne.apps.googleusercontent.com

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

Select

Recent All

Name	ID
<input checked="" type="checkbox"/> MyFileFlexProject	myfileflexproject

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

Product name that will appear on the scope consent screen. *

FileFlexDemo

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

Privacy policy URL

Optional until you deploy your app

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

Have you verified website ownership of your domain with [Search Console](#) ? *

Yes

No

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

<https://www.googleapis.com/auth/drive>

What scopes does your app need to access? *

User data accessed through these apps must be approved. Please include full scope names separated by a comma.

Example: <https://www.googleapis.com/auth/calendar.readonly>

A full list of scopes can be seen here: <https://developers.google.com/identity/protocols/googlescopes> [↗](#)

<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

List the specific ways your app will use **each** of the scopes you're requesting and explain the features in your app that require these scopes. *

Example: my app will use <https://www.googleapis.com/auth/calendar.readonly> [↗](#) to show a user's calendar data on the scheduling screen of my app to help users manage their schedule directly through my app.

The app will use <https://www.googleapis.com/auth/drive> to allow a user to download his files to 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:

Enter the number of accounts you estimate you'll need OAuth tokens for.

*

- <5
- 5-100
- 100-1000
- 1000+

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

Who is this app for?

- Myself
- Anyone on the internet
- Users in my business who have G Suite accounts.

- 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:

SUBMIT

* Required field

- 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

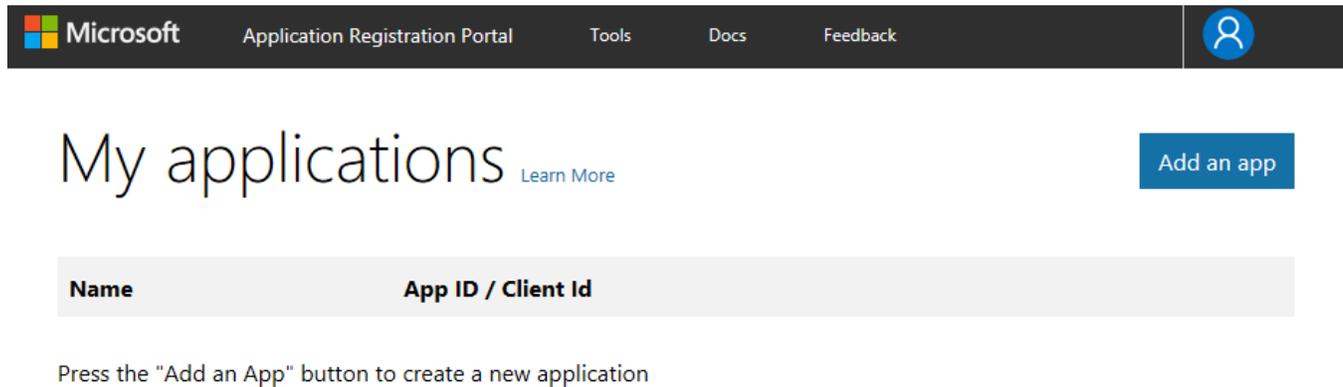
8.12.1. Registering for Microsoft OneDrive API Credentials

 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:

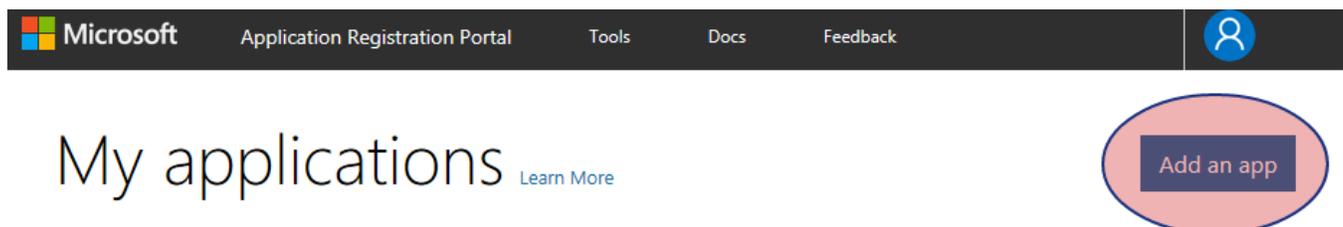
`https://apps.dev.microsoft.com`

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



The screenshot shows the Microsoft Application Registration Portal interface. At the top is a dark navigation bar with the Microsoft logo, 'Application Registration Portal', 'Tools', 'Docs', 'Feedback', and a user profile icon. Below the navigation bar, the main heading is 'My applications' with a 'Learn More' link. To the right of the heading is a blue 'Add an app' button. Below the heading is a table with two columns: 'Name' and 'App ID / Client Id'. Below the table, there is a text instruction: 'Press the "Add an App" button to create a new application'.

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



This screenshot is identical to the previous one, but the 'Add an app' button is highlighted with a red oval to draw attention to it.

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:

Register your application

Application Name

FileFlexDemo

Contact Email

Used for important communications about your application

██████████@gmail.com

Guided Setup

Let us help you get started

By proceeding, you agree to the [Microsoft Platform Policies](#)

Create

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:

FileFlexDemo Registration

[Click here for help integrating your application with Microsoft.](#)

Properties

Name

FileFlexDemo

Application Id

b654fdd[REDACTED]1fe05a92

Application Secrets

[Generate New Password](#)

[Generate New Key Pair](#)

[Upload Public Key](#)

Scroll down and click on "Add Platform":

Application Secrets

[Generate New Password](#)

[Generate New Key Pair](#)

[Upload Public Key](#)

Platforms

[Add Platform](#)

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

Add Platform



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":

Platforms

Add Platform

Web	Delete
<input checked="" type="checkbox"/> Allow Implicit Flow	
Redirect URLs ? Add URL	
<input type="text" value="https://www.fileflexdemo.com/fbweb/partner/skydrive/authorized"/>	
Logout URL ?	
<input type="text" value="e.g. https://myapp.com/end-session"/>	

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

Home page URL

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

Save Discard Changes There are unsaved changes.

You will see a confirmation that your changes were saved:

FileFlexDemo Registration

[Click here for help integrating your application with Microsoft.](#)

Your changes were saved.

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

Application Secrets

Generate New Password Generate New Key Pair Upload Public Key

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:

New password generated

This is the only time when it will be displayed. Please store it securely.

ShFV [REDACTED] FfdaV



Click the OK button to close the dialog.

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

Application Id

b654 added -a659-4d93-803d-05ce1fe05a92

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



Manage Servers

Control Panel

Backup & Restore

Resource Monitor

Manage Users

Help

Overview

Email

Two Factor Auth

Certificates

User Administration

Web Resources

Encryption

ActivityLogging

Google Drive

Dropbox

OneDrive

Box

Enable OneDrive access

OneDrive Key ⓘ

OneDrive Secret ⓘ

Synchronize
Reset
Apply

Enable the checkbox to enable OneDrive access:

Enable OneDrive access

OneDrive Key ⓘ

OneDrive Secret ⓘ

- 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:

Synchronize
Reset
Apply

You will be presented with a confirmation to restart:



After changing the structure you should synchronize configuration. Do you want to do this now?

No

Yes

Select "yes". Congratulations - 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

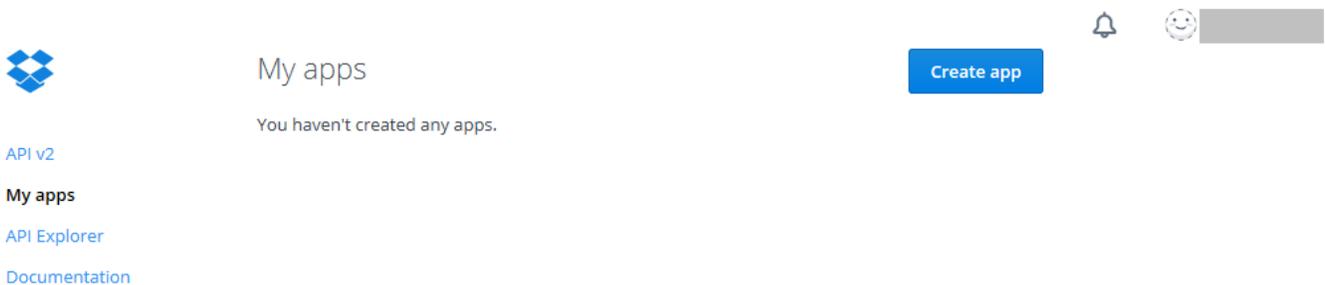


It's important to complete the "Supplying an SSL Certificate" steps prior to configuring DropBox Drive Access.

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.

Create a new app on the Dropbox Platform

1. Choose an API

<input checked="" type="radio"/> Dropbox API For apps that need to access files in Dropbox. Learn more		<input type="radio"/> Dropbox Business API For apps that need access to Dropbox Business team info. Learn more	
--	---	--	---

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

2. Choose the type of access you need

[Learn more about access types](#)

<input type="radio"/> App folder – Access to a single folder created specifically for your app.
<input checked="" type="radio"/> Full Dropbox – Access to all files and folders in a user's Dropbox.

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

3. Name your app

 Agree to Dropbox API Terms and Conditions

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:

FileFlexDemo

Settings	Branding	Analytics
Status	Development	Apply for production
Development users	0 / 500	Unlink all users
Permission type	Full Dropbox <i>i</i>	

⚠ Development or Production?

DropBox allows up to 500 users to be registered within a single API application before requiring the operator to apply for "production" and submit to a review process. This document assumes that requesting production access is required. While this process is ongoing, you may still start using the integration up to the 500 user limit.

Following this section are your application credentials:

App key **t1b2h7a5yoatifv**

App secret **Show**

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

App key **t1b2h7a5yoatifv**

App secret **om [REDACTED] 10**

Write down both values temporarily for later entry into FileFlex.

Scroll down to the "OAuth 2" section:

OAuth 2

Redirect URIs

Add

Allow implicit grant *i*

Generated access token *i*

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:

OAuth 2 **Redirect URIs**

https://fileflexdemo.com/fbweb/partner/dropbox/authorized ✕

https:// (http allowed for localhost) Add

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

Development users Only you Enable additional users

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

Limit raised to 500 users

Your app can now be linked with up to 500 users. If you'd like to link more than 500 users, please **apply for production** status. [Learn more about production status requirements.](#)

Okay

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

Development users 0 / 500 Unlink all users

Click on the "branding" tab at the top:

FileFlexDemo

Settings

Branding

Analytics

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

App name

FileFlexDemo

Publisher

FileFlexDemo Co

Description

File access and sharing

App website

https://fileflexdemo.com

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:



64x64



Choose from Dropbox



256x256



Choose from Dropbox

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:



64x64



Choose from Dropbox



256x256



Choose from Dropbox

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

Save changes

Cancel

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:

Overview
Credentials
Email
Login Control
Certificates
User Administration
Web Resources
Encryption
User Activity Logging
Google Drive
Dropbox
OneDrive
Box
Additional

Enable Dropbox access

DropBox API Key

DropBox API Secret

Click to enable Dropbox access:

8.13.1.1.

Enable Dropbox access

DropBox API Key	<input type="text"/>
DropBox API Secret	<input type="text"/>

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:

After changing the structure you should synchronize configuration. Do you want to do this now?

No Yes

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.

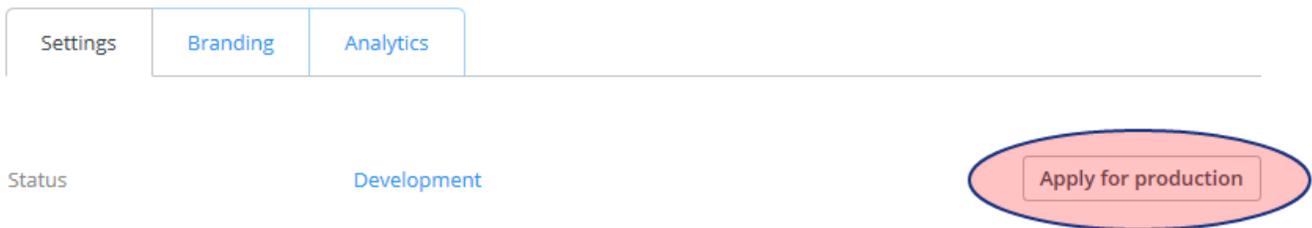
Before proceeding with these steps, you must have created a user with which the DropBox team will conduct it's testing of the solution. That user must have "Manage Content Source" privileges, so that they can add their own Dropbox content source!

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:

Please test this app

There are no users linked to this app. Please test this app's API integration with your liam.g.wade@gmail.com account before applying for production status.

Okay

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

Request production status

Production status removes the limits on the number of Dropbox users your app can link.

You may apply for production status at anytime, but your application **will not be reviewed** until your app has at least **50 Dropbox users** (Business API apps are not subject to this requirement). While your app has development status, it can link up to **500 Dropbox users**, so in most cases, it's safe to release your app to the world before it's been granted production status.

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

Confirmation

Does your app need production status?

The only difference between production status and development status is that production status sets no limit on the number of Dropbox users that can link with your app.

Apps that do not need to link with more than 50 Dropbox users **should not apply for production status.**



My app will need to link with more than 50 Dropbox users

Scroll down to "Dropbox integration":

Dropbox integration

How does your app use the Dropbox API?

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

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":

Platform(s)

Android

iOS

OS X

Web

Windows

Other

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

Under "Testing instructions", enter the following instructions:

i 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:

Test account credentials

What's a test account we can use to test your app?

some_user@example.com

some_password

My app doesn't require the user to login to connect with Dropbox

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:

Testing conditions

Please ensure at least ONE of the following conditions is true: i

My app can be downloaded and tested **free of charge** by an **external party**

I have provided either **test account** login info or a link to a **test build** or a link to **screenshots** or a **screencast** detailing my app's integration with Dropbox

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):

i 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:

Submit app

You will then be prompted to confirm your application submission:

Confirm your application submission

Please confirm your application submission. Note: your application will **not** be reviewed until your app links with at least **50 Dropbox users** (unless it is a Dropbox Business API app, in which case it will be reviewed immediately). If you feel there is a compelling reason why your application should be reviewed earlier, please explain in the **Request early review** field of the application form.

For more information, visit the [Dropbox Platform developer guide](#).

Cancel

Confirm

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.

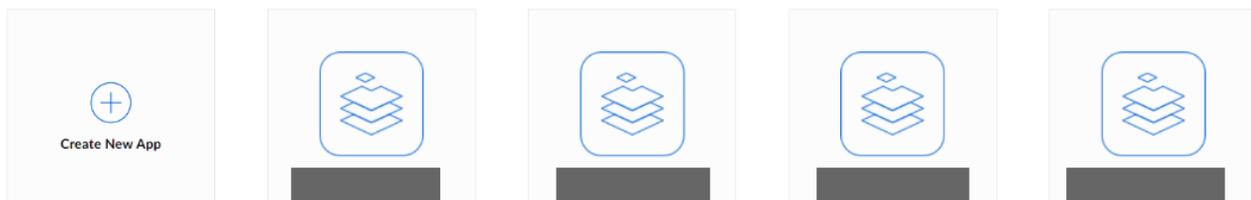
In order to configure [Box.net](#) from within FileFlex Enterprise, you must obtain a Client ID and Secret from [Box.net](#). Sign in to your [Box.net](#) account, and navigate to the following URL which is used to configure their APIs:

```
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](#):

My Apps

Create New App



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



Custom App

Build a standalone app with Box's content services, such as managing and rendering files and enabling end-user collaboration.

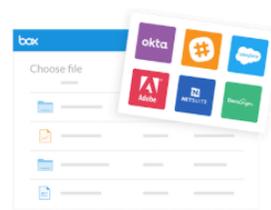
For developers using Box's content services without requiring Box user accounts.



Enterprise Integration

Extend your Box instance with programmatic processes and backend integrations, such as user, group, and event management.

For Box admins and developers building an integration for their existing Box users.



Partner Integration

Allow users to access, edit, and save their Box content within your third-party app, such as an e-signature or project management service.

For developers building an integration for existing Box users.

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

What would you like to name your app?

Don't worry—you can change this later.

By clicking 'Create App', you agree to the terms of the [Box Developer Agreement](#) and the [Box Privacy Policy](#).

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

Woot! Your app has been created.

Make your first API call and retrieve a list of folders from your personal Box account using a developer token. This token will expire after 60 minutes.

```
curl https://api.box.com/2.0/folders/0 -H \
  "Authorization: Bearer eRnN5TeLdbwFYfZq5TUAeVsz9Q2E9uk2"
```

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.

OAuth 2.0 Credentials

Credentials for using OAuth 2.0 as your Authentication type.

Client ID

tzb3tecx [REDACTED] 0hjviyt2 [COPY](#)

Client Secret

..... [COPY](#)

[Reset](#)

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:

OAuth 2.0 Redirect URI

The redirect URI is the URL within your application that will receive OAuth 2.0 credentials

Redirect URI

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:

OAuth 2.0 Redirect URI

The redirect URI is the URL within your application that will receive OAuth 2.0 credentials

Redirect URI

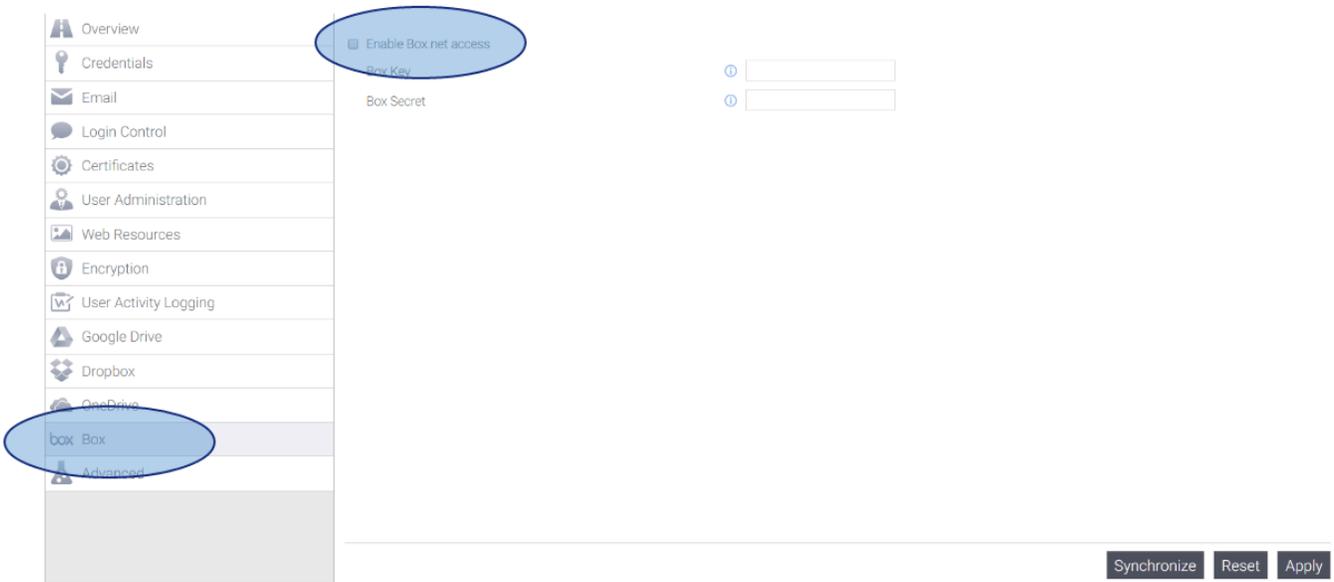
Click the "Save Changes" at the top right:

[Save Changes](#)

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:

Enable Box.net access

Box Key	
Box Secret	

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:

After changing the structure you should synchronize configuration. Do you want to do this now?

No	Yes
----	-----

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



Changes will be seen after you restart all servers.
Do you want to do it now?

No

Yes

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:

 BoxNet access has been configured.

Congratulations - you are now ready to start using [Box.net](#) from within FileFlex Enterprise!

8.15. Configuring Amazon S3 Access

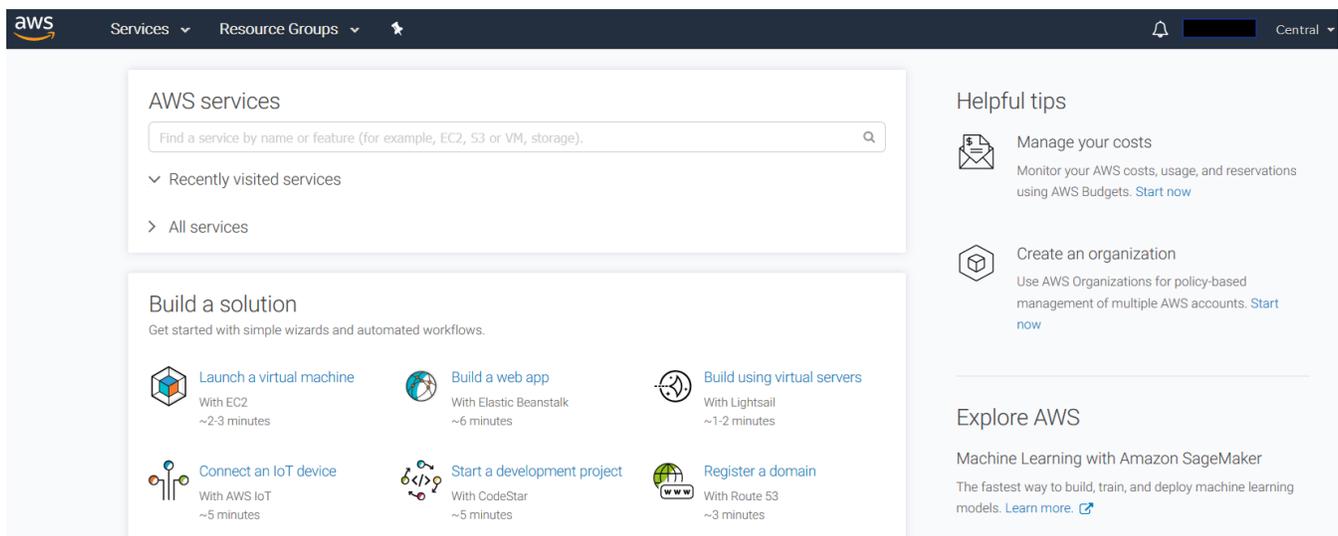
In order to configure Amazon S3 for access from within FileFlex Enterprise, you must first have an S3 bucket to which FileFlex can be connected. This guide is in three parts - creating an S3 bucket, enabling S3 access, following by adding an S3 content source.

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:



The screenshot shows the AWS Management Console interface. At the top, there is a navigation bar with the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, a search icon, a notification bell, and a user profile icon labeled 'Central'. Below the navigation bar, the main content area is divided into several sections. On the left, there is a search bar for 'AWS services' with the placeholder text 'Find a service by name or feature (for example, EC2, S3 or VM, storage)'. Below the search bar, there are links for 'Recently visited services' and 'All services'. In the center, there is a 'Build a solution' section with the subtitle 'Get started with simple wizards and automated workflows.' This section contains six cards, each with an icon, a title, and a description: 'Launch a virtual machine' (With EC2, ~2-3 minutes), 'Build a web app' (With Elastic Beanstalk, ~6 minutes), 'Build using virtual servers' (With Lightsail, ~1-2 minutes), 'Connect an IoT device' (With AWS IoT, ~5 minutes), 'Start a development project' (With CodeStar, ~5 minutes), and 'Register a domain' (With Route 53, ~3 minutes). On the right side, there is a 'Helpful tips' section with two cards: 'Manage your costs' (Monitor your AWS costs, usage, and reservations using AWS Budgets. Start now) and 'Create an organization' (Use AWS Organizations for policy-based management of multiple AWS accounts. Start now). At the bottom right, there is an 'Explore AWS' section with a card for 'Machine Learning with Amazon SageMaker' (The fastest way to build, train, and deploy machine learning models. Learn more.).

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

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Compute

- EC2
- Lightsail [↗](#)
- Elastic Container Service
- EKS
- Lambda
- Batch
- Elastic Beanstalk

Developer Tools

- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- Cloud9
- X-Ray

Analytics

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- QuickSight [↗](#)
- Data Pipeline
- AWS Glue

Storage

- S3
- EFS
- Glacier
- Storage Gateway

Management Tools

- CloudWatch
- AWS Auto Scaling
- CloudFormation
- CloudTrail

Security, Identity & Compliance

- IAM
- Cognito
- Secrets Manager

Click on the "Create bucket" button:



Amazon S3

[+ Create bucket](#)

[Delete bucket](#)

[Empty bucket](#)

Enter a bucket name, and click next:

Create bucket ✕

1 Name and region 2 Configure options 3 Set permissions 4 Review

Name and region

Bucket name ⓘ

Region

Copy settings from an existing bucket

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.

Create bucket

1 Name and region 2 **Configure options** 3 Set permissions 4 Review

Properties

Versioning
 Keep all versions of an object in the same bucket. [Learn more](#)

Server access logging
 Log requests for access to your bucket. [Learn more](#)

Tags
You can use tags to track project costs. [Learn more](#)

Key	Value
-----	-------

[+ Add another](#)

Object-level logging
 Record object-level API activity using AWS CloudTrail for an additional cost. See [CloudTrail pricing](#) or [learn more](#)

Default encryption
 Automatically encrypt objects when they are stored in S3. [Learn more](#)

[Previous](#) [Next](#)

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

Create bucket ✕

1 Name and region ✓ 2 Configure options ✓ 3 Set permissions 3 4 Review 4

Manage users

User ID ⓘ	Objects ⓘ	Object permissions ⓘ
██████████ (Owner)	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write ✕

Access for other AWS account + Add account

Account ⓘ	Objects ⓘ	Object permissions ⓘ
-----------	-----------	----------------------

Manage public permissions

Do not grant public read access to this bucket (Recommended) ▼

Manage system permissions

Do not grant Amazon S3 Log Delivery group write access to this bucket ▼

Previous Next

Change permissions if needed, but otherwise click next.

Create bucket

Progress: Name and region ✓, Configure options ✓, Set permissions ✓, 4 Review

Name and region [Edit](#)

Bucket name: 75testbucket15 Region: Canada (Central)

Options [Edit](#)

Versioning	Disabled
Server access logging	Disabled
Tagging	0 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled

Permissions [Edit](#)

Users	1
Public permissions	Disabled
System permissions	Disabled

[Previous](#) [Create bucket](#)

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



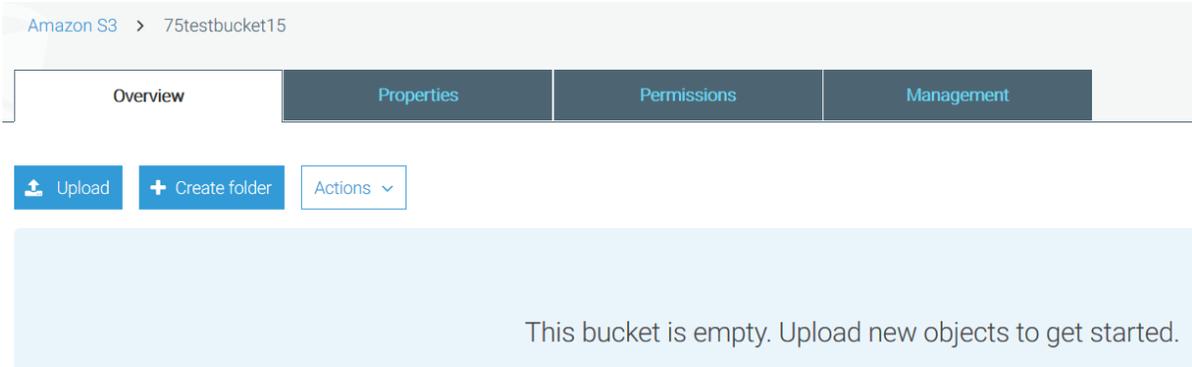
Amazon S3

Search for buckets

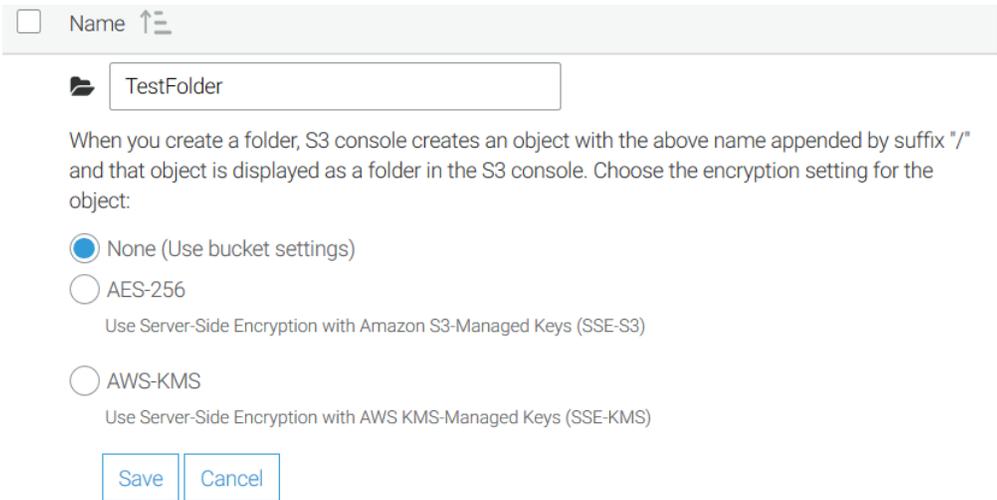
[+ Create bucket](#) [Delete bucket](#) [Empty bucket](#)

Bucket name	Access
75testbucket15	Not public *

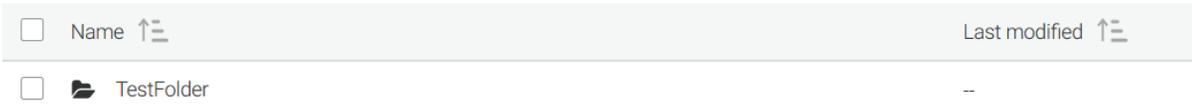
Let's create a bit of content so we can access it from FileFlex. Click on the bucket in the list and you will see an empty bucket screen:



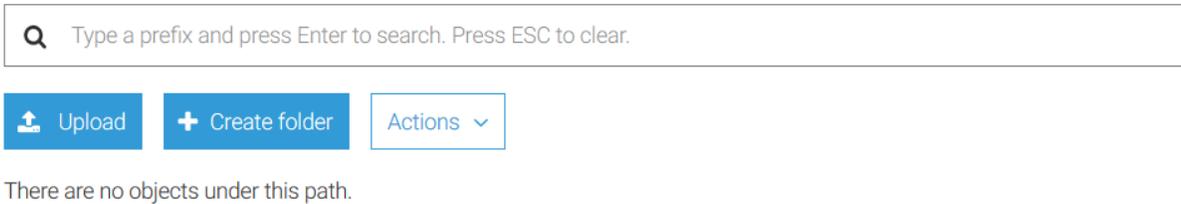
Click on "Create folder" to create a new folder:



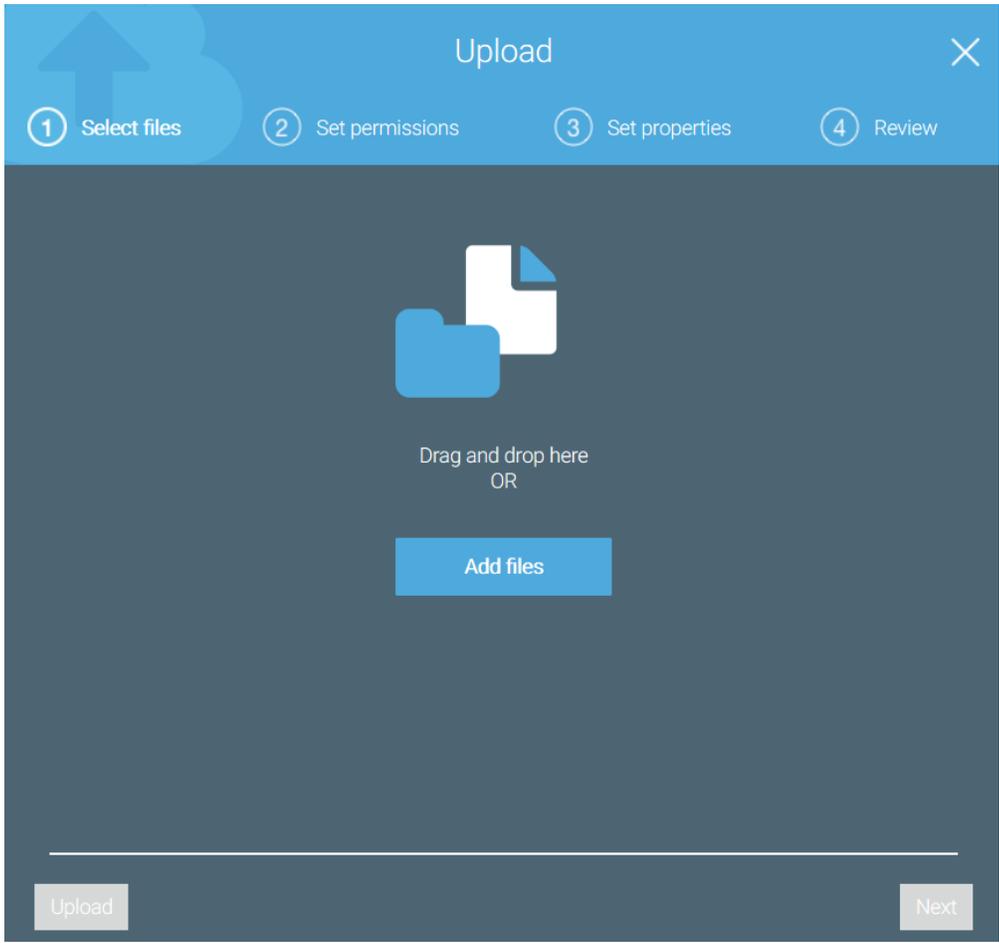
Enter a folder name ('TestFolder' in this case), then click save. You will then see it listed:



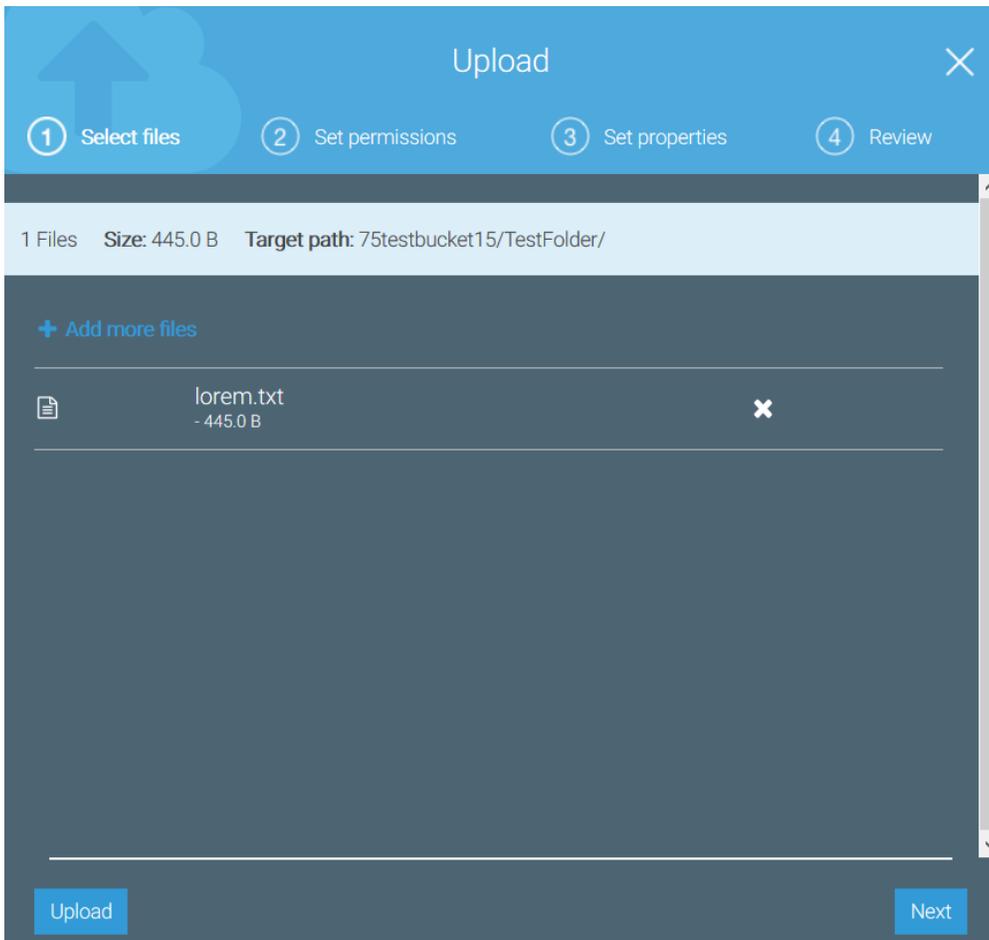
Click the folder to enter it. Click the upload button:



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:

Upload

1 Select files 2 Set permissions 3 Set properties 4 Review

1 Files Size: 445.0 B Target path: 75testbucket15/TestFolder/

Manage users

User ID	Objects	Object permissions
[Redacted] (Owner)	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write

Access for other AWS account [+ Add account](#)

Account	Objects	Object permissions
---------	---------	--------------------

Manage public permissions

Do not grant public read access to this object(s) (Recommended)

Upload Previous Next

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

Upload

1 Files Size: 445.0 B Target path: 75testbucket15/TestFolder/

1 Select files 2 Set permissions **3 Set properties** 4 Review

Storage class

Choose one storage class depending on your use case scenario and access requirements.

[Learn more](#)

Standard Standard-IA One Zone-IA Reduced redundancy

Encryption

Protect data at rest by using Amazon S3 master-key or by using AWS KMS master-key.

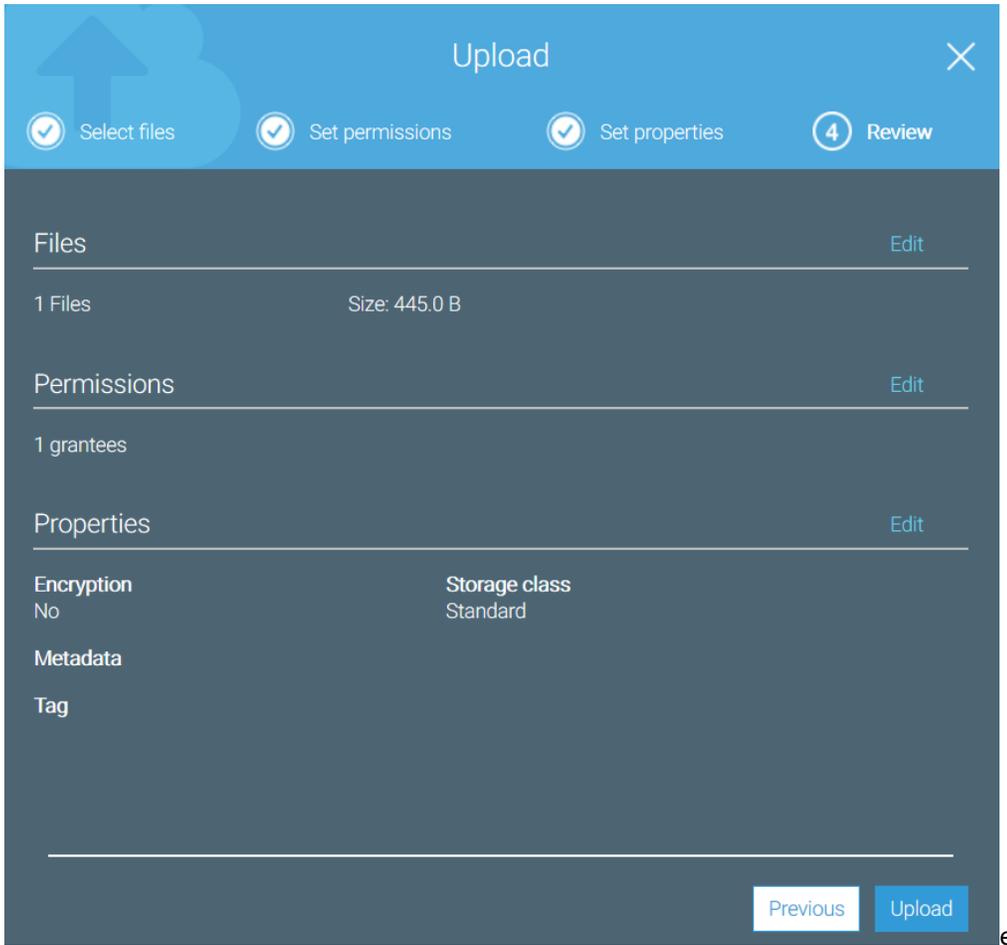
None ⓘ Amazon S3 master-key AWS KMS master-key

Metadata

Metadata is a set of name-value pairs. You cannot modify object metadata after it is uploaded.

Header	Value
<input type="text" value="Select a key"/>	<input type="text"/>

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



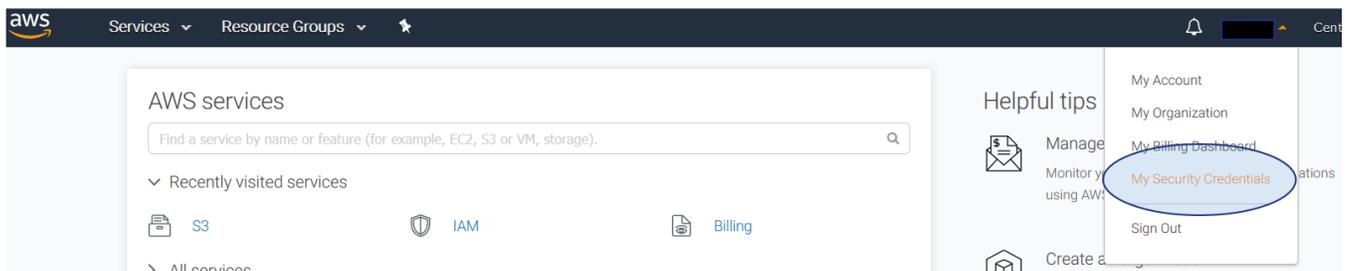
To complete the process, click upload. You will see the file listed:

<input type="checkbox"/>	Name ↑	Last modified ↑
<input type="checkbox"/>	lorem.txt	Sep 11, 2018 10:51:06 AM GMT-0400

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 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".

You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.

To help secure your account, follow an [AWS best practice](#) by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

[Continue to Security Credentials](#)

[Get Started with IAM Users](#)

Don't show me this message again

i 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:

Search IAM

Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).
To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- +
- +
- Access keys (access key ID and secret access key)

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the [signing documentation](#). For your protection, store securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.
Note: You can have a maximum of two access keys (active or inactive) at a time.

Created	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status
---------	---------	---------------	-----------	------------------	-------------------	--------

[Create New Access Key](#)

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

Create Access Key

✔ Your access key (access key ID and secret access key) has been created successfully.
Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.
To help protect your security, store your secret access key securely and do not share it.

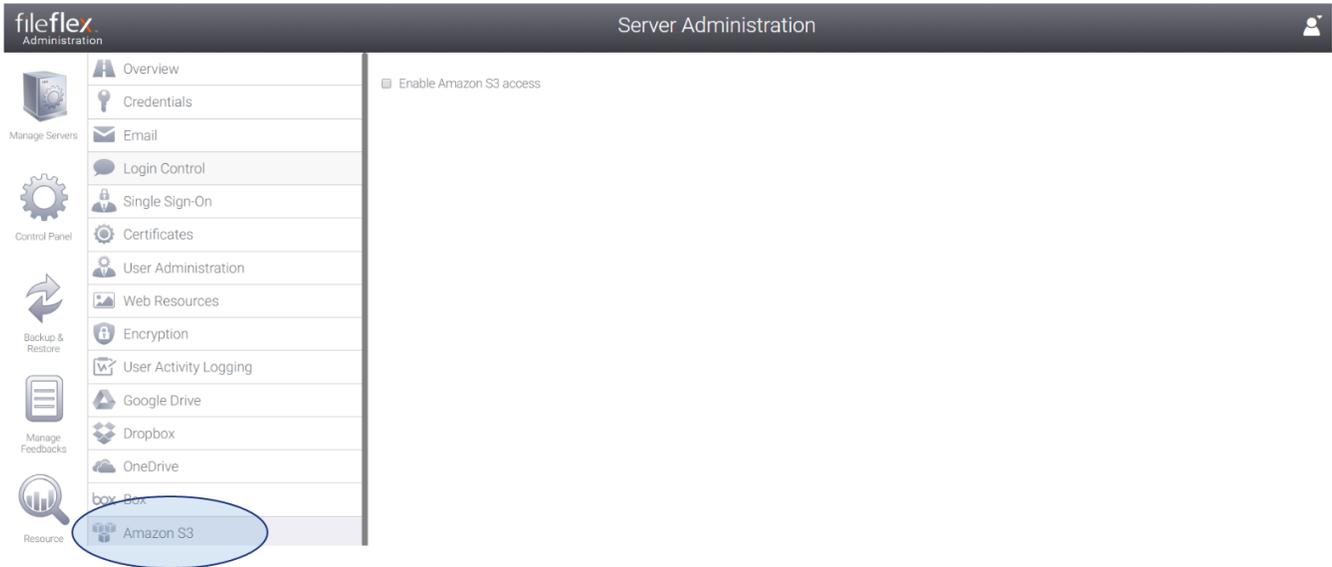
[Show Access Key](#)

[Download Key File](#) [Close](#)

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

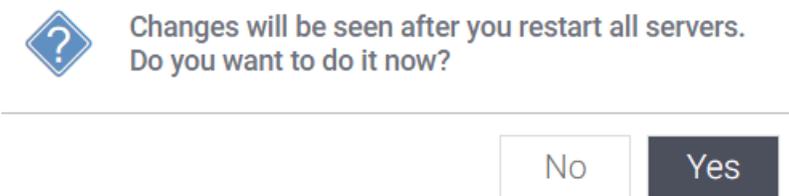
Open FileFlex Server Administration, and open the control panel tab. From there, open the "Amazon S3" panel:



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.

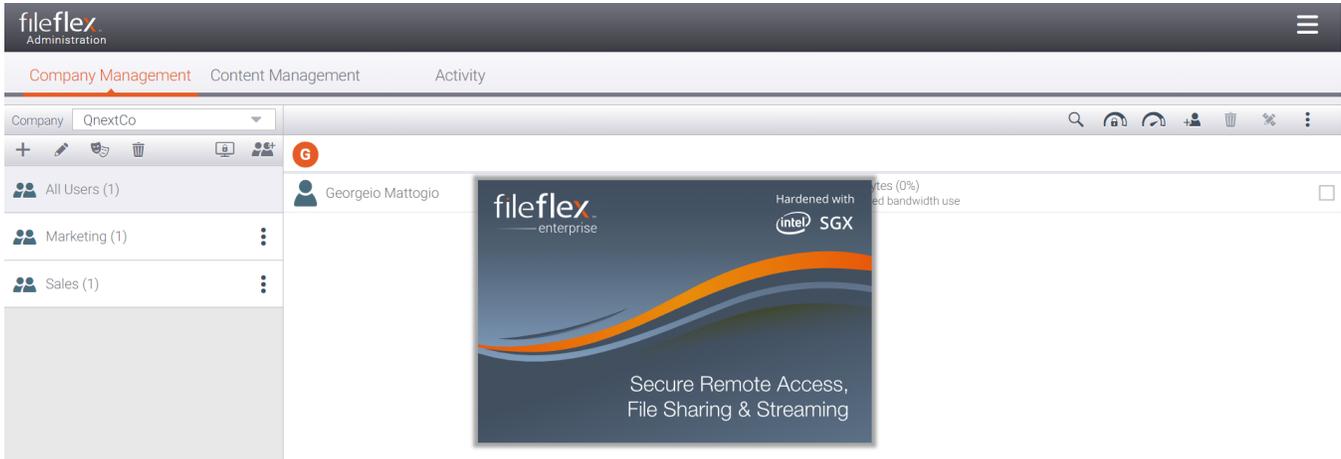
From Server Administration, click on the "Manage Users" tab from the left hand side. This will open User Administration in a new browser tab:

Login to FileFlex Enterprise Secure File Access

admin@fileflexdemo.com

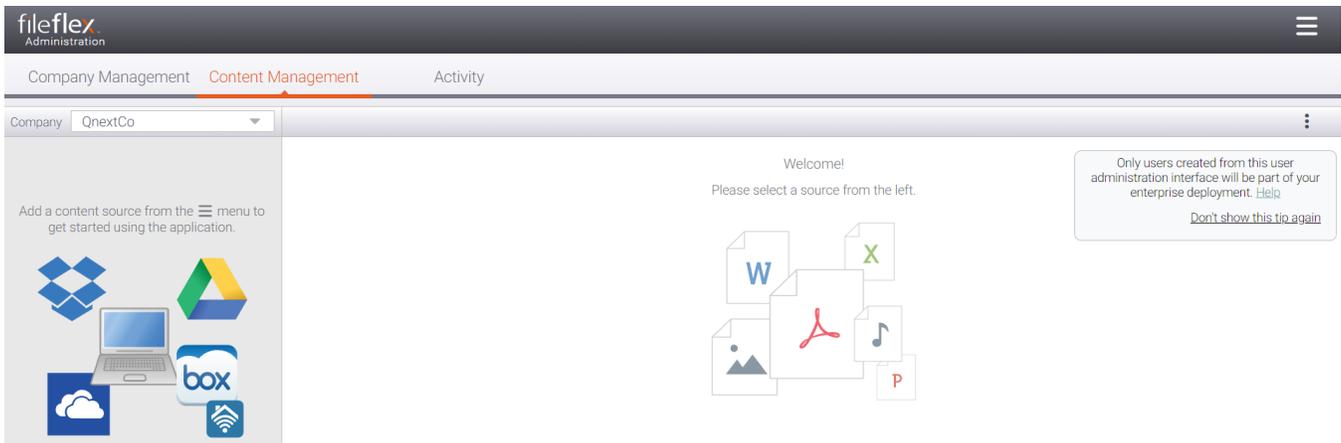
Next

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:



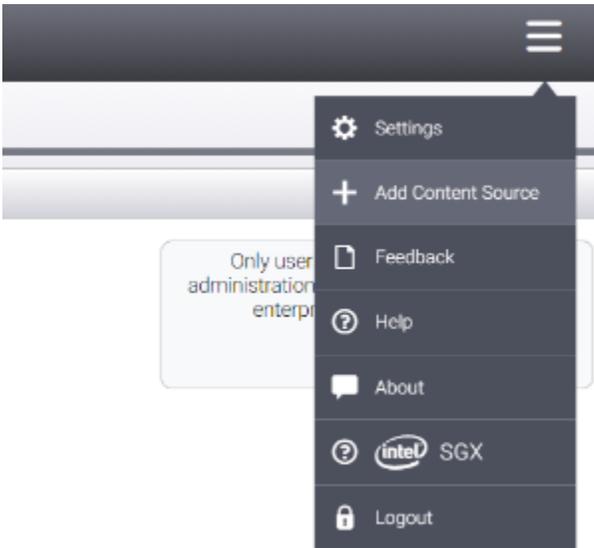
The screenshot shows the FileFlex Enterprise Administration interface. The top navigation bar includes "Company Management", "Content Management", and "Activity". The "Company" dropdown is set to "QnextCo". The left sidebar lists user groups: "All Users (1)", "Marketing (1)", and "Sales (1)". The main content area displays a user profile for "Georgeio Mattogio" with a profile picture and a red "G" icon. A large banner for "fileflex enterprise" is visible, featuring the text "Hardened with intel SGX" and "Secure Remote Access, File Sharing & Streaming".

Click the "Content Management" tab:

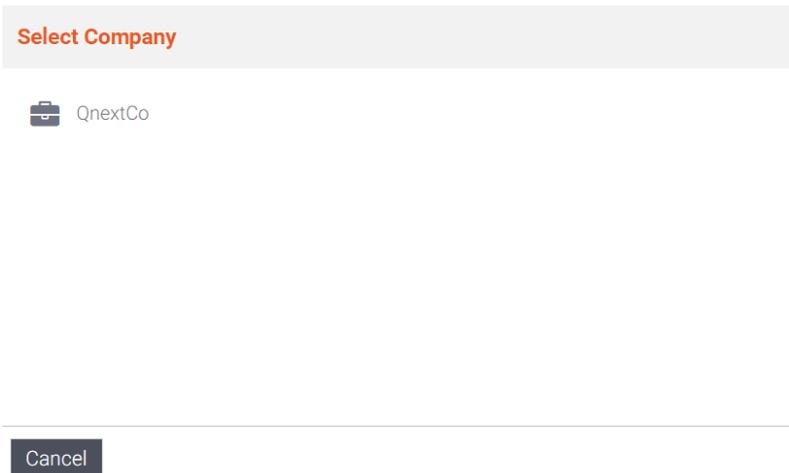


The screenshot shows the FileFlex Enterprise Administration interface with the "Content Management" tab selected. The top navigation bar includes "Company Management", "Content Management", and "Activity". The "Company" dropdown is set to "QnextCo". The left sidebar contains a message: "Add a content source from the ☰ menu to get started using the application." Below this message are icons for various content sources: OneDrive, Google Drive, Box, and a laptop icon. The main content area displays a "Welcome!" message with the text "Please select a source from the left." and a collection of file icons (Word, Excel, PDF, Music, PowerPoint). A tip box on the right states: "Only users created from this user administration interface will be part of your enterprise deployment. [Help](#) [Don't show this tip again](#)".

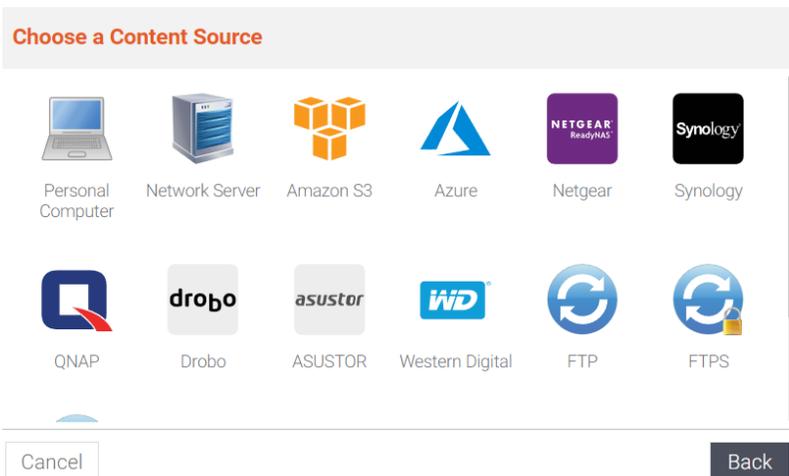
From the right hand menu, select "Add Content Source":



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":

Amazon S3 Setup

Amazon S3 is a file storage and synchronization service. It provides cloud storage for users and enables file management and sharing.

Enter the device name to display on the dashboard (optional):
(You can always change this later)

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:

Configure Amazon S3 Source

You will need to generate an access key pair from your Amazon AWS account in order to access Amazon S3 from your FileFlex Enterprise application.

Access Key ID *

Secret Access Key *

AWS Region *

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

Content Source Verify



Amazon S3 Storage added.

Do you have other content sources?

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

8.16. Configuring Microsoft Azure Access

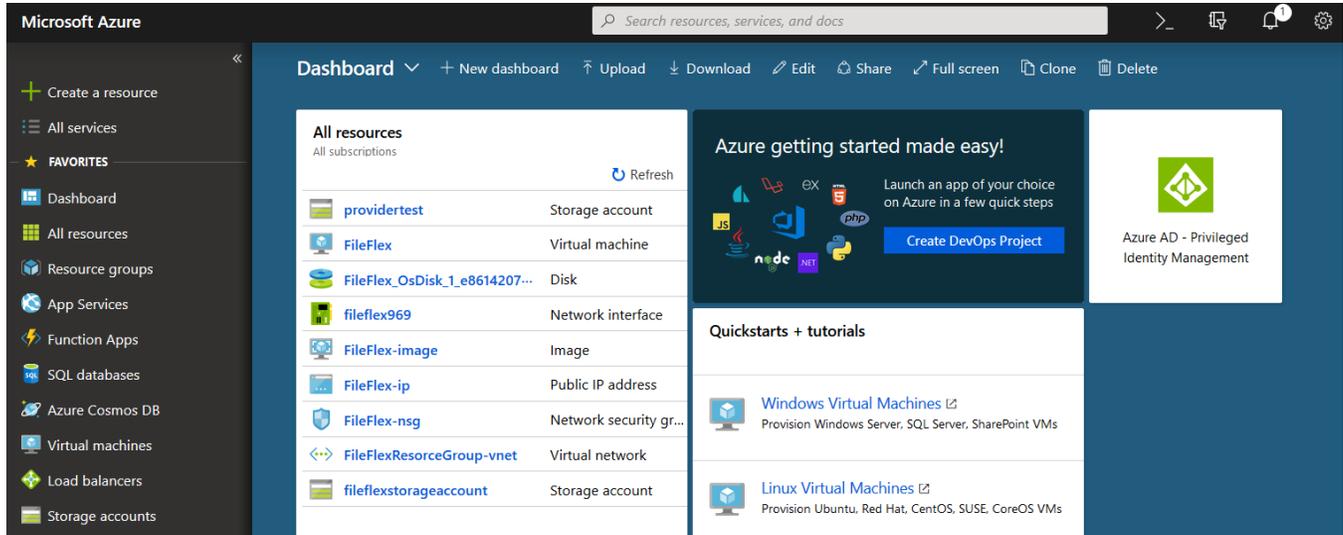
In order to configure Microsoft Azure for access from within FileFlex Enterprise, you must first have an Azure storage bucket to which FileFlex can be connected. This guide is in three parts - creating an Azure storage account, then enabling Azure access, followed by adding an Azure content source.

8.16.1. Creating an Azure Storage Account

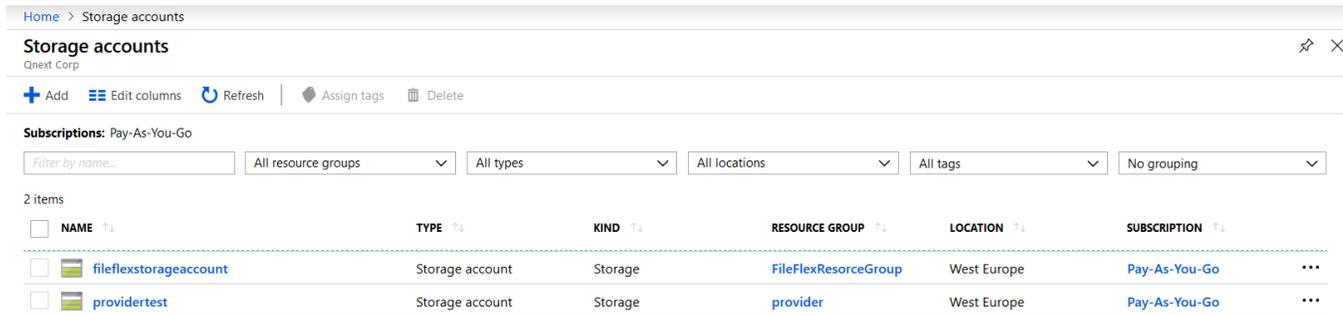
Log in to the Microsoft Azure portal:

`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:



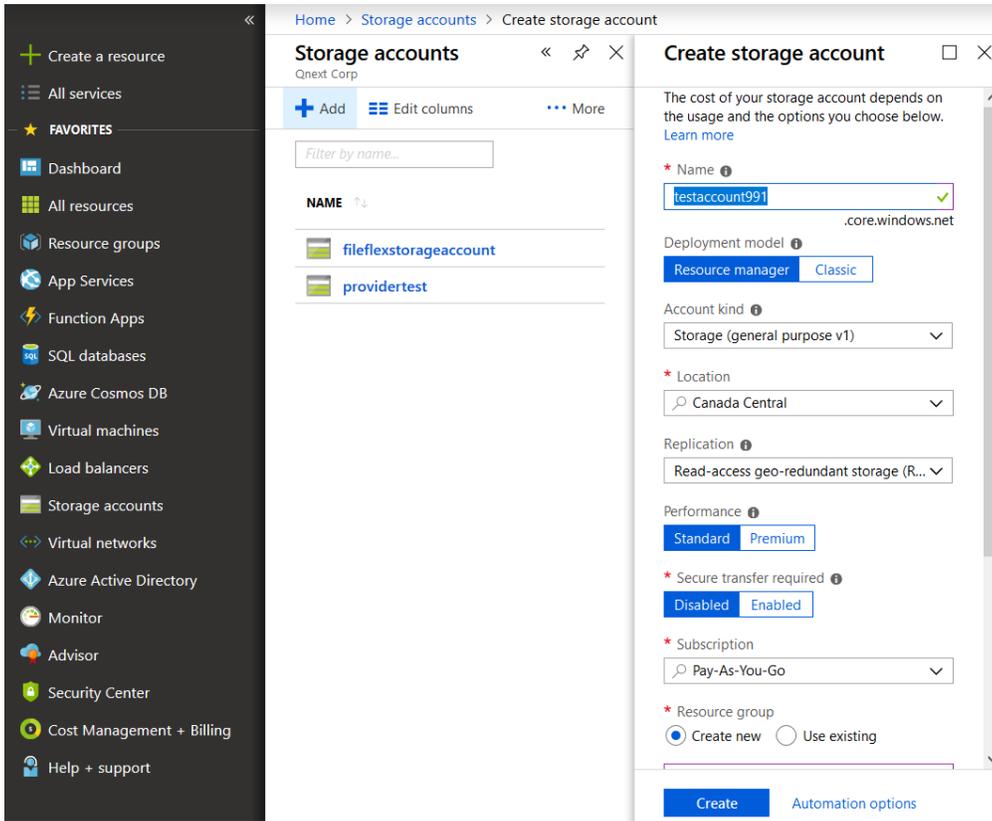
Click the "Add" button:



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).

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

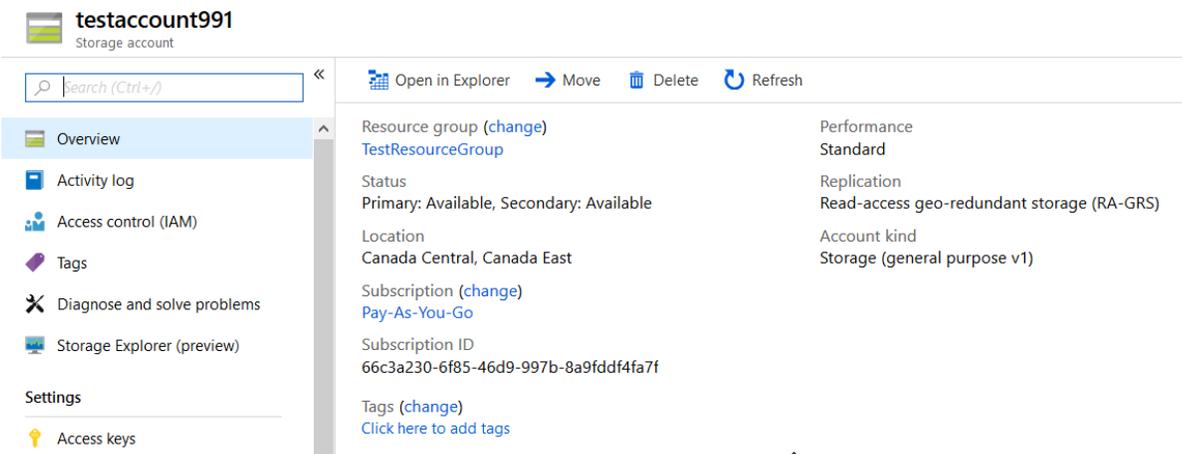
For example:



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:

NAME	TYPE	KIND	RESOURCE GROUP	LOCATION	SUBSCRIPTION
fileflexstorageaccount	Storage account	Storage	FileFlexResourceGroup	West Europe	Pay-As-You-Go
providertest	Storage account	Storage	provider	West Europe	Pay-As-You-Go
testaccount991	Storage account	Storage	TestResourceGroup	Canada Central	Pay-As-You-Go

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:

Blobs
REST-based object storage for unstructured data
[Learn more](#)

Files
File shares that use the standard SMB 3.0 protocol
[Learn more](#)

Tables
Tabular data storage
[Learn more](#)

Queues
Effectively scale apps according to traffic
[Learn more](#)

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

+ File share
Refresh

Storage account: testaccount991

NAME	MODIFIED	QUOTA
You don't have any file shares yet. Click '+ File share' to get started.		

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

File share

✕

*** Name**

✓

Quota ⓘ

GB

Create
Discard

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

Storage account: testaccount991

NAME	MODIFIED	QUOTA
test-file-share	9/11/2018, 5:17:43 PM	5 TiB

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

Home > testaccount991 - Files > test-file-share

test-file-share

File share

Search (Ctrl+/)

Connect Upload Add directory Refresh Delete share Quota View snapshots Create Snapshot

Backup (Preview) is not enabled for this file share. Click here to enable backup.

Location: test-file-share

Search files by prefix

NAME	TYPE	SIZE
No files found.		

Overview

Settings

- Access policy
- Properties

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

New directory

* Name

Test Folder 

OK

Cancel

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

Search files by prefix

NAME	TYPE	SIZE
 Test Folder	Directory	

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:

Upload files

test-file-share/Test Folder

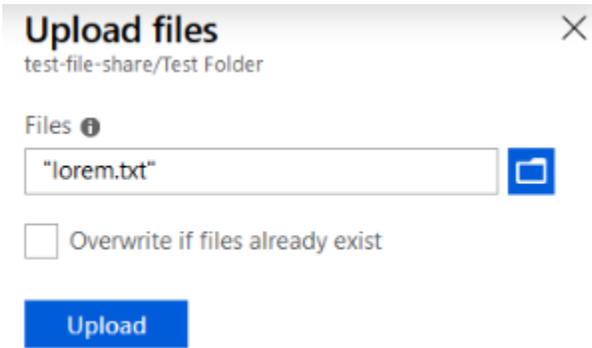
Files 

Select a file 

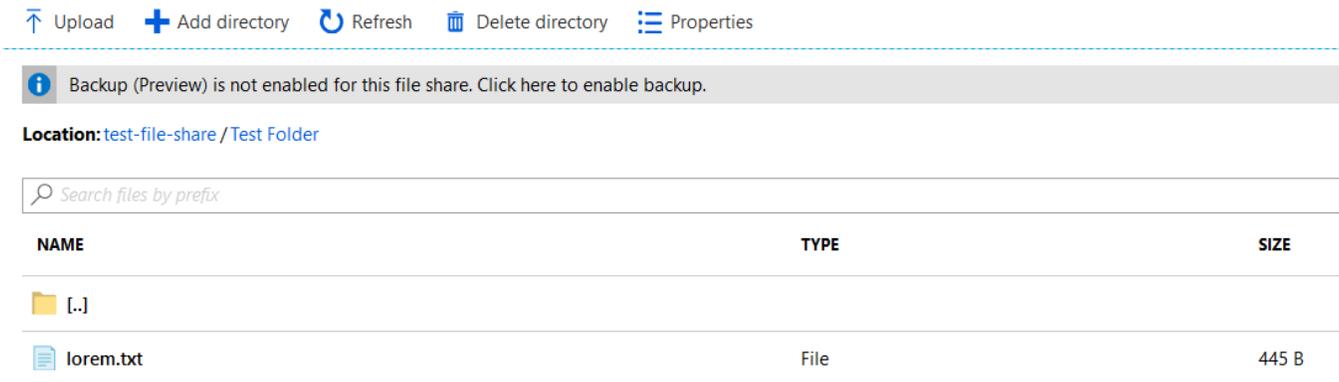
Overwrite if files already exist

Upload

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

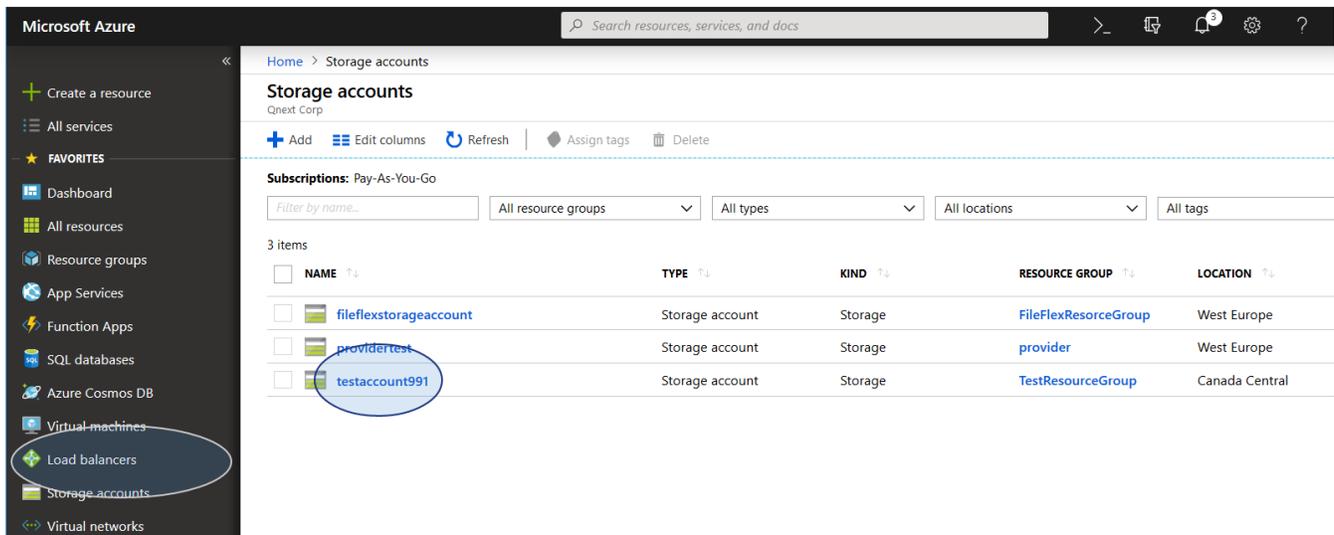


Click upload to proceed. Your file will now be listed:



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.

testaccount991
Storage account

Search (Ctrl+/)

Open in Explorer Move Delete Refresh

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Storage Explorer (preview)
- Settings
 - Access keys
 - CORS

Resource group (change)
TestResourceGroup

Performance
Standard

Status
Primary: Available, Secondary: Available

Replication
Read-access geo-redundant storage (RA-GRS)

Location
Canada Central, Canada East

Account kind
Storage (general purpose v1)

Subscription (change)
Pay-As-You-Go

Subscription ID
66c3a230-6f85-46d9-997b-8a9fddf4fa7f

Tags (change)
Click here to add tags

From there, select "Access keys":

Storage account name

testaccount991

key1

Key

P4ZIkH4Hb [REDACTED] QhA/Afew12+xcAy0t5er+g/QjHUoGtWzHDgQ==

Connection string

DefaultEndpointsProtocol=https;AccountName=[REDACTED]

key2

Key

T2ZMOzF [REDACTED] mfaryyVtu0x3MGU4LPIVQ==

Connection string

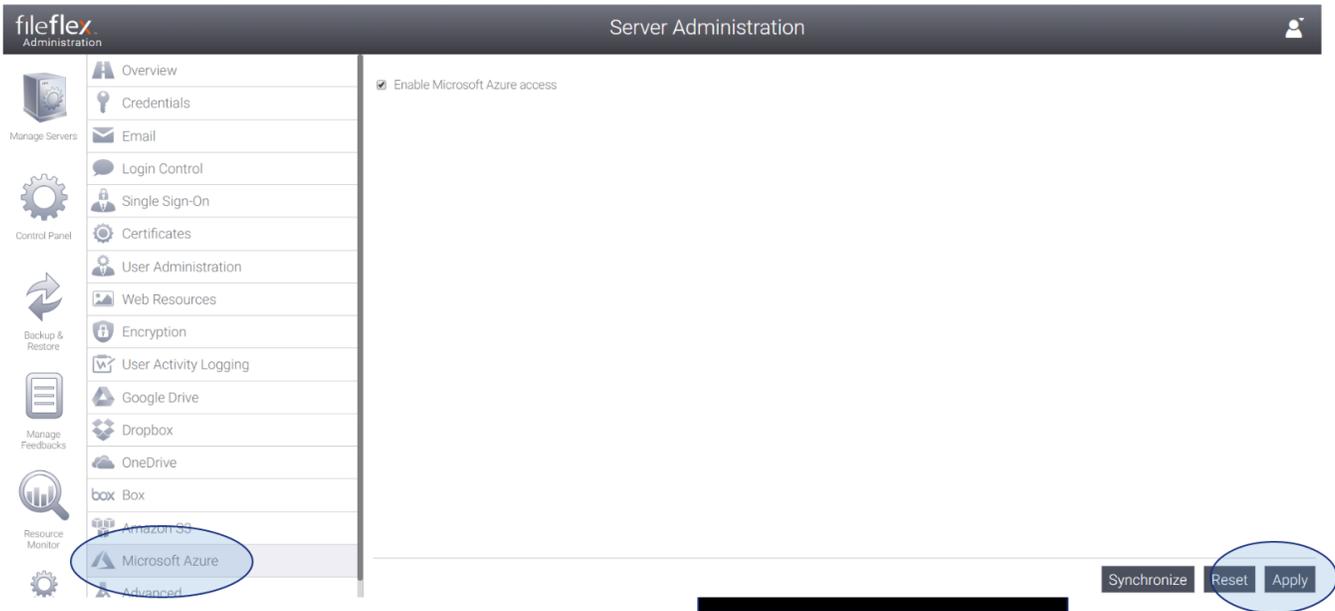
DefaultEndpointsProtocol=https;AccountName=te [REDACTED]

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.

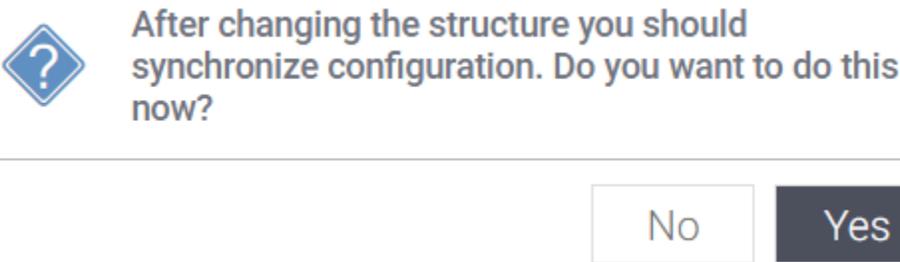
i Hint: Use the blue copy-to-clipboard icons on the right hand side to make this easier.

8.16.3. Enabling Azure Access

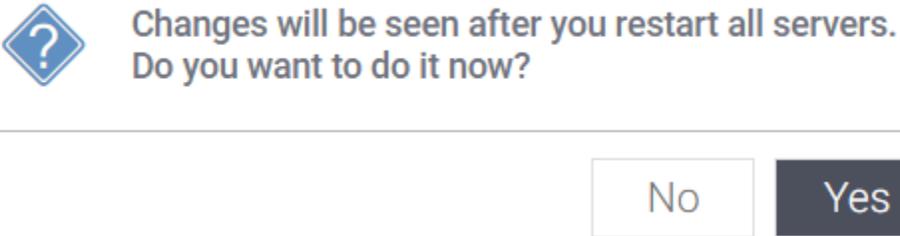
Open FileFlex Server Administration, and open the control panel tab. From there, open the "Microsoft Azure" panel:



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.

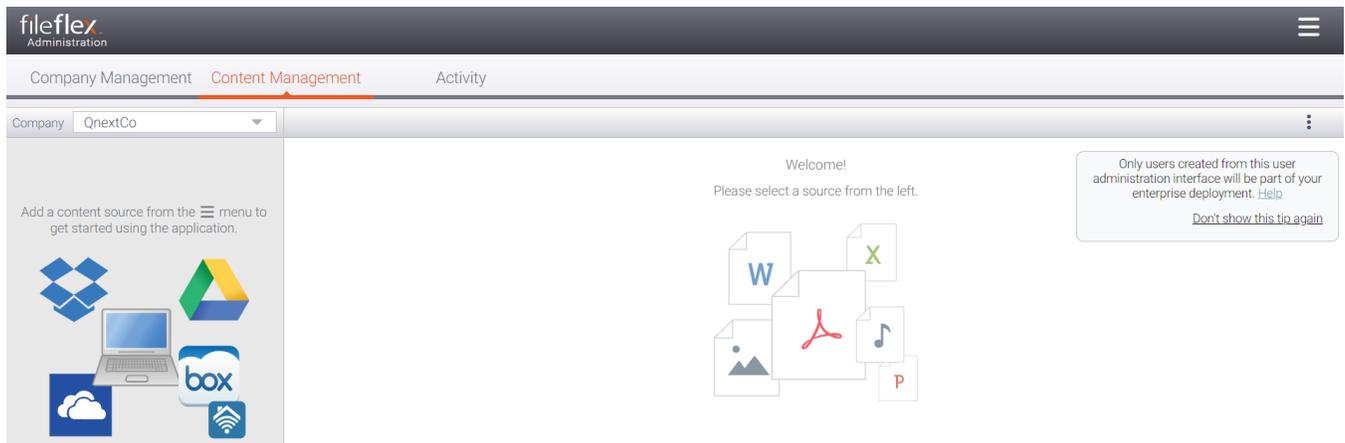
From Server Administration, click on the "Manage Users" tab from the left hand side. This will open User Administration in a new browser tab:



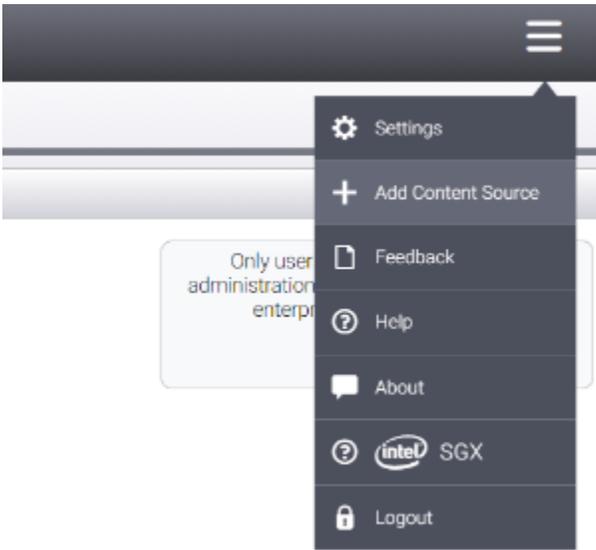
Enter your user administrator email address, followed by clicking on the Next button. Enter the password, followed by clicking on "Login" to complete the login. Once in, you will see the user administration application:



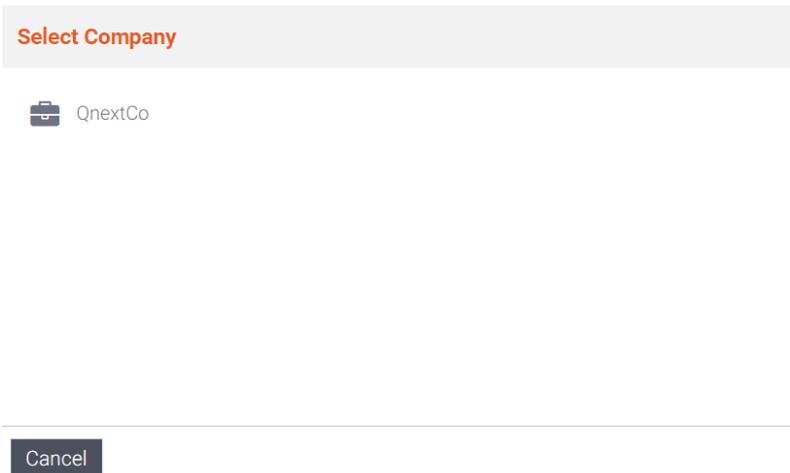
Click the "Content Management" tab:



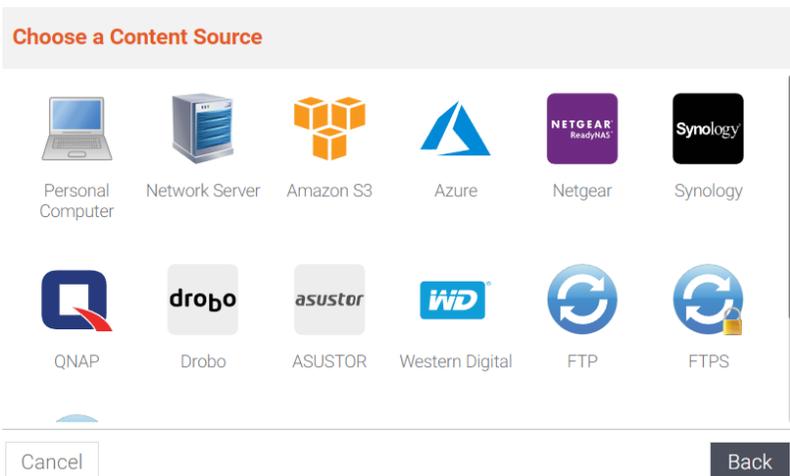
From the right hand menu, select "Add Content Source":



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":

Azure Setup

Azure is a file storage and synchronization service created and managed by Microsoft. It enables user cloud storage, file sharing and collaborative editing.

Enter the device name to display on the dashboard (optional):
(You can always change this later)

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).

Configure Azure Source

You will need to connect your Azure account to your FileFlex Enterprise account in order to access your Azure storage before you can access and use those files from your FileFlex Enterprise application.

Enter your Azure access keys:

Access Key ID *

Secret Access Key *

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

Content Source Verify

✔ Microsoft Azure Storage added.

Do you have other content sources?

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.

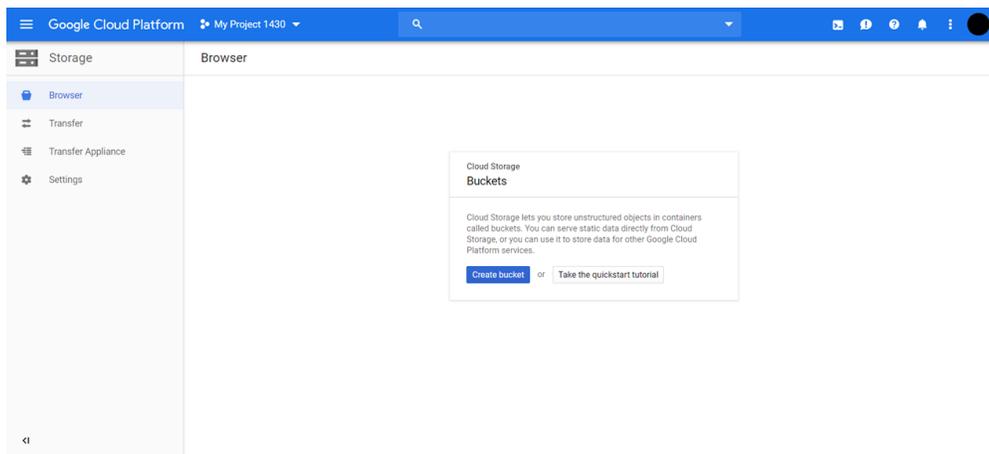
8.17.1. Creating a GCP bucket in a project

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.

← Create a Bucket

1 Name your bucket
Pick a globally unique, permanent name. [Naming guidelines](#)

fileflex-test-prem

Tip: Don't include any sensitive information

CONTINUE

- Choose a default storage class
- Choose how to control access to objects
- Advanced settings (optional)

CREATE CANCEL

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

← Create a Bucket

2 Name your bucket

- **Choose a default storage class**
Objects added to the bucket are assigned the selected storage class by default.
Choose based on where and how often your objects will be accessed. [Learn more](#)

Multi-Regional
Best for data accessed frequently in multiple regions

Regional
Best for data accessed frequently in a single region

Nearline
Best for backups and data accessed once a month or less

Coldline
Best for disaster recovery and data accessed once a year or less

Location

us (multiple regions in United States)

CONTINUE

- **Choose how to control access to objects**

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

← Create a Bucket

- ✓ Name your bucket
- ✓ Choose a default storage class
- Choose how to control access to objects
 - Access control model
 - Set permissions uniformly at bucket-level (Bucket Policy Only)
Enforces the bucket's IAM policy without object ACLs. May help prevent unintended access. If selected, this option becomes permanent after 90 days. [Learn more](#)
 - Set object-level and bucket-level permissions
Enforces the IAM policy and object ACLs for more granular control of object access.

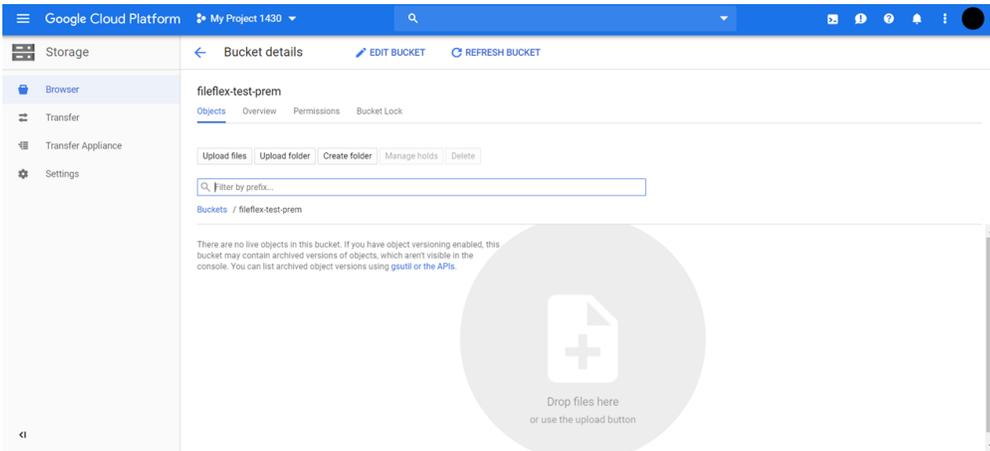
- Advanced settings (optional)

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

← Create a Bucket

- ✓ Choose how to control access to objects
- Advanced settings (optional)
 - Encryption
 - Google-managed key
No configuration required
 - Customer-managed key
Manage via Google Cloud Key Management Service
 - Retention policy
 - Set a retention policy to specify the minimum duration that this bucket's objects must be protected from deletion or modification after they're uploaded. You might set a policy to address industry-specific retention challenges. [Learn more](#)
 - Set a retention policy
 - Labels
 - Labels are key/value pairs that allow you to group related buckets together or with other Cloud Platform resources. [Learn more](#)
 -

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

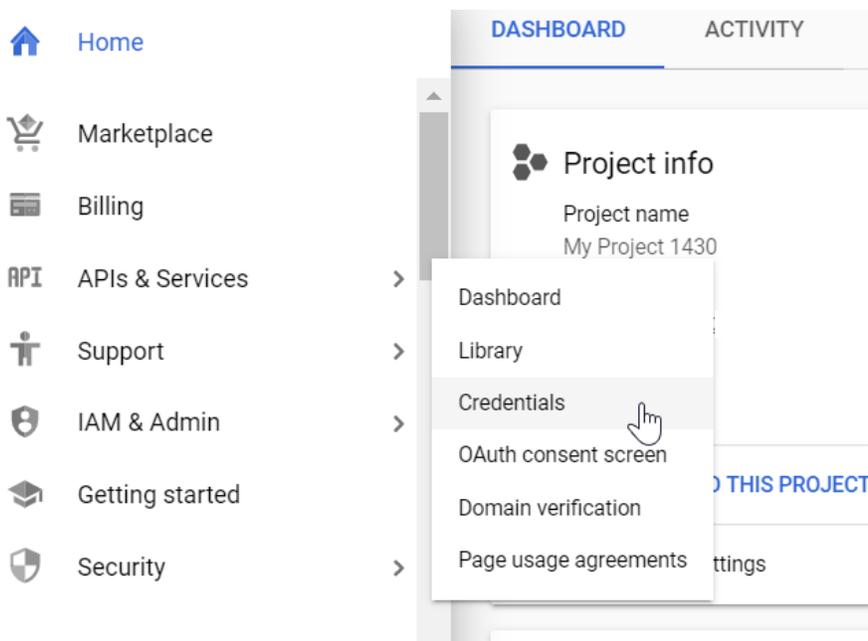


8.17.2. Creating OAuth-Credentials

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"

API APIs & Services

Credentials **+ CREATE CREDENTIALS** DELETE

Dashboard

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

Create credentials to access your enabled APIs. [Learn more](#)

Select "OAuth client ID"

API key
Identifies your project using a simple API key to check quota and access.

OAuth client ID
Requests user consent so that your app can access the user's data.

Service account
Enables server-to-server, app-level authentication using robot accounts

Help me choose
Asks a few questions to help you decide which type of credential to use

Select "Web application"

← Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See [Setting up OAuth 2.0](#) for more information.

Application type

- Web application
- Android [Learn more](#)
- Chrome App [Learn more](#)
- iOS [Learn more](#)
- Other

Create Cancel

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

← Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See [Setting up OAuth 2.0](#) for more information.

Application type

- Web application
- Android [Learn more](#)
- Chrome App [Learn more](#)
- iOS [Learn more](#)
- Other

Name 

Web client 2

Restrictions

Enter JavaScript origins, redirect URIs or both [Learn more](#)

Origins and redirect domains must be added to the list of authorised domains in the [OAuth consent settings](#).

Authorised JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It cannot contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a non-standard port, you must include it in the origin URI.

 https://mspdev.cnexus.com 

https://www.example.com

Type in the domain and press Enter to add it

Authorised redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorisation code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

 https://mspdev.cnexus.com/fbweb/app/public/view/authorize_partner/googlestorage 

https://www.example.com

Type in the domain and press Enter to add it

Click Create.

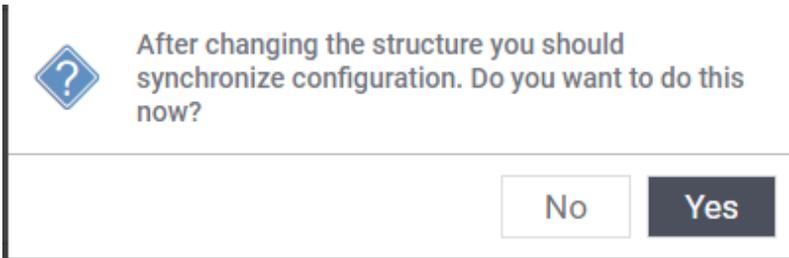
8.17.3. Enabling Google Cloud Access

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

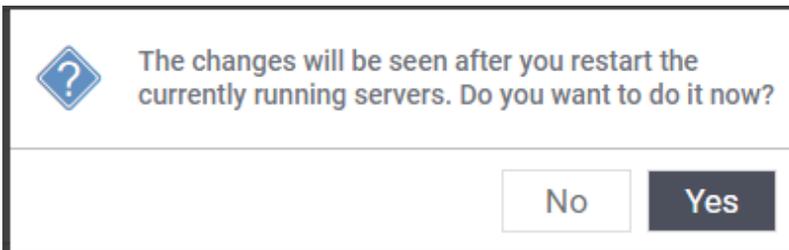
Select the checkbox to enable Google Cloud access.



You will see the following dialog:



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

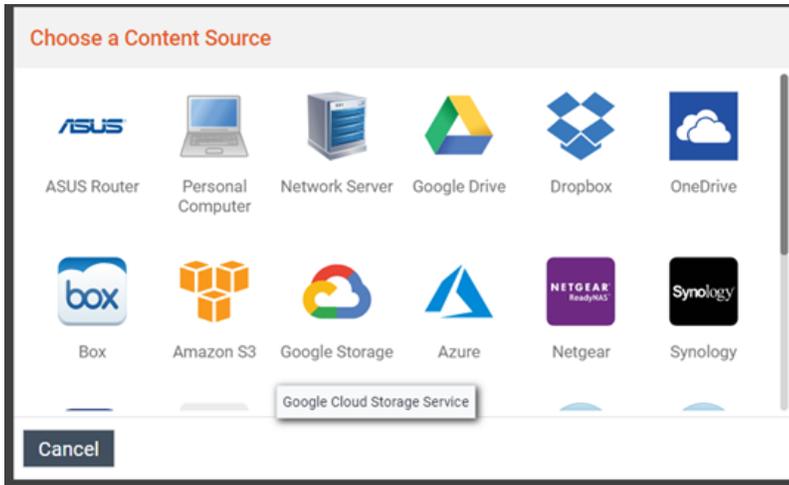


Click "Yes" to restart the servers. After a few minutes, the server list will appear indicating that your servers are running normally. Click the control panel tab to verify that Google Cloud has been configured.

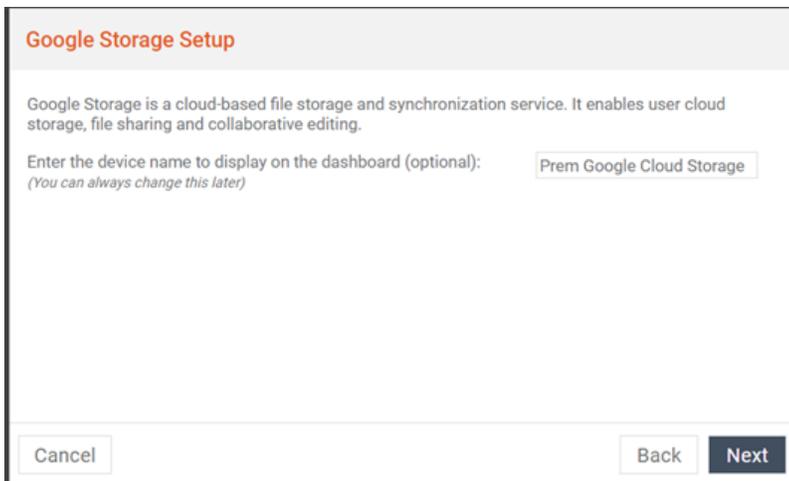
8.17.4. Configuring FileFlex

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 FileFlex 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.

Configure Google Storage Source [X]

You will need to connect your Google Cloud Storage account to your FileFlex Enterprise account in order to access your content on Google Cloud. You need to provide details of your Google Cloud Storage account.

Client ID *

Client secret *

Project ID *

Prompt users to provide their credentials

Cancel Next

"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.

Content Source Verify

✓ Google Storage added.
Do you have other content sources?

Cancel Add more Done

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:

<input checked="" type="checkbox"/> Enable antivirus scan	i
<input type="checkbox"/> Enable lenient virus scanning (allowing large file uploads with reduced threat detection)	i
Maximum concurrent view-only conversions:	i <input type="text" value="2"/>
Health monitoring access code	i <input type="text"/>
Trusted external IPs	i <input type="text"/>

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.

[i](#) 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.

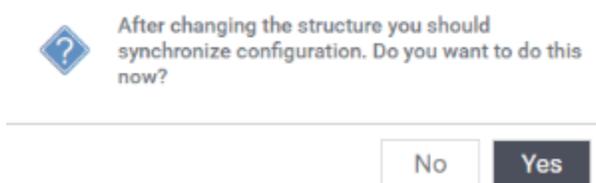
The number of conversions that can happen at the same time is directly connected to the amount of CPU and RAM allocated to the server. Each "concurrent view-only conversion" requires 1 dedicated CPU core, and 1gb of RAM.

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):

Maximum concurrent view-only conversions:

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 monitoring 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:

Health monitoring access code

 Please select a more rigorous access code for your real FileFlex deployments!

 Without a health check access code, access to the health check URL is not possible.

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:

Trusted external IPs

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 were 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:

Health monitoring access code	<input type="text" value="....."/>
Trusted external IPs	<input type="text" value="192.168.2.*"/>

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:

Nagios®

General
Home
Documentation

Current Status
Tactical Overview
Map (Legacy)
Hosts
Services
Host Groups
 Summary
 Grid
Service Groups
 Summary
 Grid
Problems
 Services (Unhandled)
 Hosts (Unhandled)
 Network Outages

Quick Search:

Reports
Availability
Trends (Legacy)

Nagios® Core™

✓ Process running with PID 3300

Nagios® Core™
Version 4.3.4
August 24, 2017
[Check for updates](#)

A new version of Nagios Core is available!
Visit nagios.org to download Nagios 4.4.0.



Click "services" from the left hand menu. After a few minutes you should see the following:

fileflexdemo	HTTPS Health Check	OK	06-22-2018 14:56:49	0d 0h 48m 28s
--------------	--------------------	----	---------------------	---------------

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 screenshot shows the Backup & Restore panel. On the left is a sidebar with "Manage Servers" and "Control Panel" options. The main area has a toolbar with icons for adding, deleting, and refreshing. Below the toolbar is a list of backup tasks: "Manual" (Manually created) and "Uploaded" (Uploaded by user). To the right, under "Backups info:", it shows "Last backup: n/a". Below this is a table with columns for Date, Size, Version, and Action.

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:



 **Daily Backups**
Everyday at 19:38

 **Manual**
Manually created

 **Uploaded**
Uploaded by user

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:

Backups info:
Last backup: 28/03/17, 15:59:54

Date	Size	Version	Action
28/03/17, 15:59:54	91.17 KB	0.0.155 / 7	
28/03/17, 15:43:37	91.18 KB	0.0.155 / 7	
28/03/17, 15:43:24	91.18 KB	0.0.155 / 7	

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

Manual
Manually created

Click on the backup now icon to initiate an immediate backup. After a moment you will see it listed on the right hand side:

22/03/17, 19:02:19 | 92.19 KB | 0.0.153 / 7 |

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:

What would you like to download?

Configuration

Data

Configuration and 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

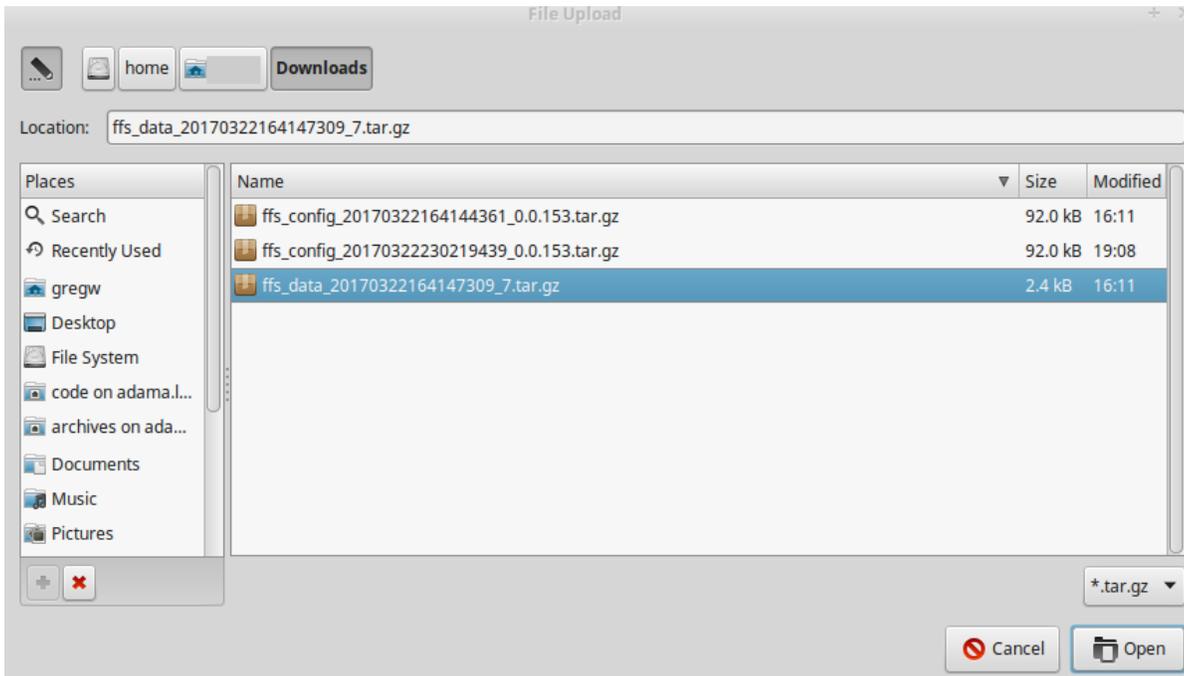
Once you have a backup you must be able to restore it. If the data is already contained in your VM as a backup set, you can restore it directly from there without uploading it in to your VM. If however you backed up your data somewhere manually (as suggested above), you'll need to upload your archives 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:

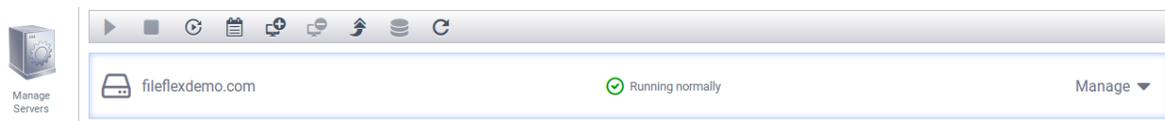
22/03/17, 12:41:47 | 2.34 KB | 7 | ⏸ ⏪ ⏩ 🗑

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:

fileflexdemo.com Running normally Manage ▲

Server IP: 192.168.2.33 | Zone: Default ✎ >

Server	Process ID	State	Info
Messaging Server	1405	✔	Started at: 03-22 15:17
Web Server	1493	✔	Started at: 03-22 15:17
Storage Server	1330	✔	Started at: 03-22 15:17
Administration Server	1275	✔	Started at: 03-22 15:17

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:

fileflexdemo.com Some processes are stopped Manage ▼

Return to the backup and restore tab and select the "uploaded" backup task filter. Locate the backup set you wish to restore.

22/03/17, 12:41:47 | 2.34 KB | 7 | 

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):

What would you like to restore?

Configuration

Data

Configuration and Data

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:

Schedule **Upload**

Name:

Time: GMT 

Period:

Summary: Backup executes daily, at 23:49 GMT.

Copies: 5 

Cancel OK

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:

Name:

Select a backup start time (defined in Greenwich Mean Time - GMT) for the backup set. For example, we will select midnight GMT:

Time: 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:

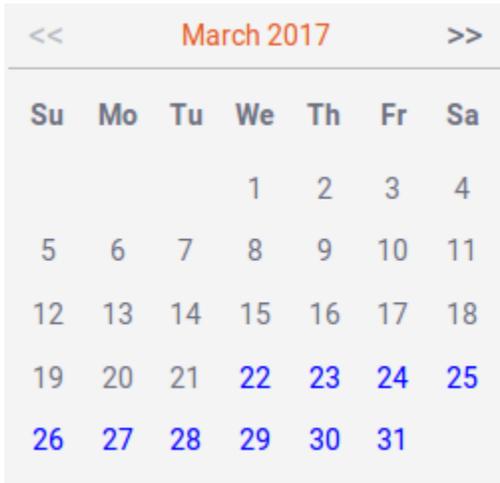
Period:

A summary will be shown along with an empty date field.

Summary: Select concrete date and time for task to be executed.

Date:

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:

Period:

Summary: Backup executes daily, at 23:49 GMT.

9.1.5.1.3. Weekly Backups

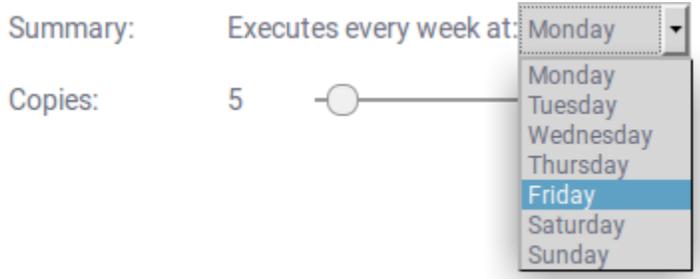
Weekly backups allow you to backup once a week on a selected day of the week at the specified time.

Select "Weekly" from the period dropdown:

Period:

Summary: Executes every week at:

Select the day of the week you'd like to have the backups performed:



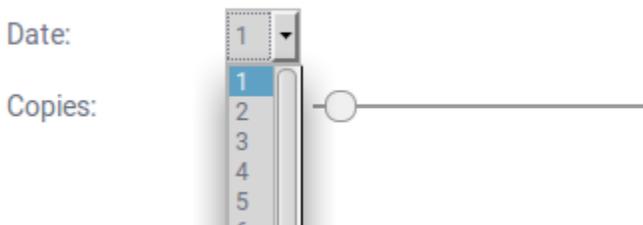
9.1.5.1.4. Monthly Backups

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

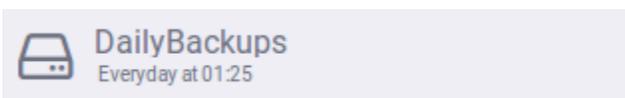
Since backups consume space within the virtual machine, it's important to limit the number of copies to retain for any backup task.



Drag the slider left or right to adjust the number copies. Values from 1 to 100 may be selected.

i 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.

i 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:

Schedule **Upload**

Offsite Backup:

Protocol: SFTP

Host:

Login Type: SSH Key

User:

Public Key: **Generate** [View](#)

Destination Path:

You will then have to click the "Offsite Backup" check box to enable automated uploads of your backups:

Offsite Backup:

From the "Protocol" dropdown, select the "SFTP" option:

Protocol: SFTP

i 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:

Protocol:

Destination Path:

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:

Host:

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.

Login Type:

! 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:

User:

Next, you will need to generate a public/private keypair. Click the "generate" button to do so:

Public Key: [View](#)

Click the "view" link to show the public key contents:

Public Key

```
ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQDTBYyE59Y5xhi  
Mx4sJE1kKLWbWw+OhD5h0yzftkTkW0Rdt7ZYSgy90leKf  
wCp14rGmQyggclcoeC0MV5WfUqnJPQXicWmPDILQvi07
```

Copy

Close

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:

Destination Path:

Click the test button to ensure everything is working. You should see a success message:



Successful connection

OK

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 feedbacks 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:

Send user feedback to Fileflex support

Please take the time to send us your feedback via our online form. If our service has not met your expectations or if it has we'd like to know.

Email address:

Message:

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:

```

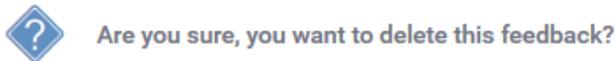
Feedback received on: 2017.12.12 02:03:08:785 GMT
Date Sent: 2017.12.11 21:03:09:467
Received on: 10091@fileflexdemo.com
UID: QNadmin@fileflexdemo.com
Email: guy@notmyemail.com
Reference Number: node0c1leqtgkppod43qmdherp2ti0
Address: 192.168.2.80
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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

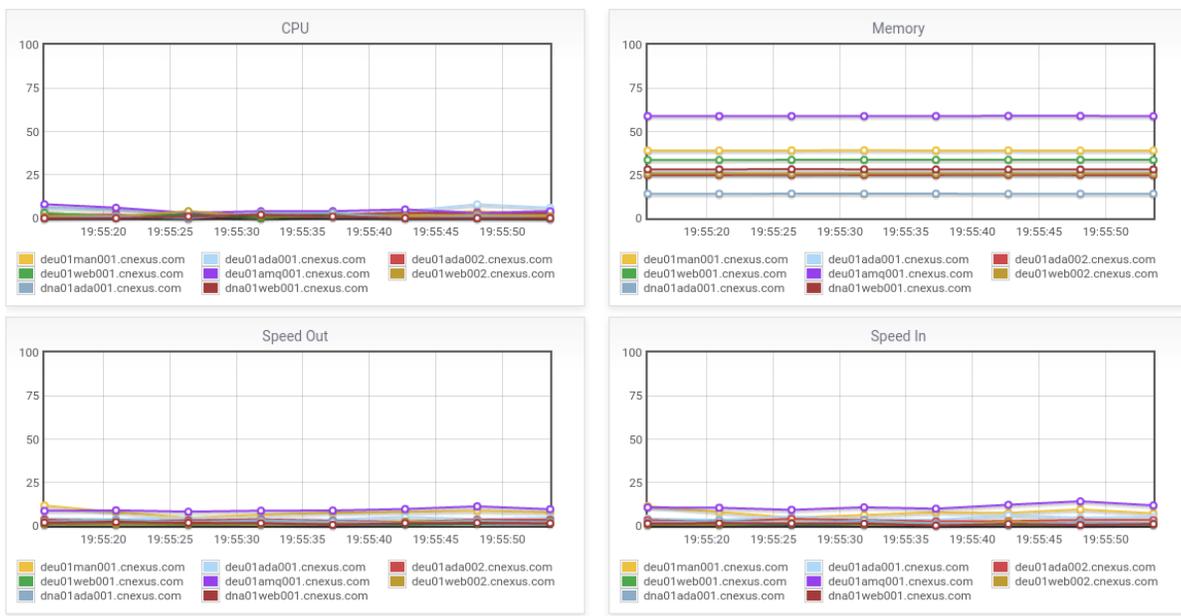
Over time you may accumulate many feedbacks from your users, and you can save space and clutter by periodically deleting items that are no longer of user. Clicking the "delete" icon will provide you with a prompt:



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:

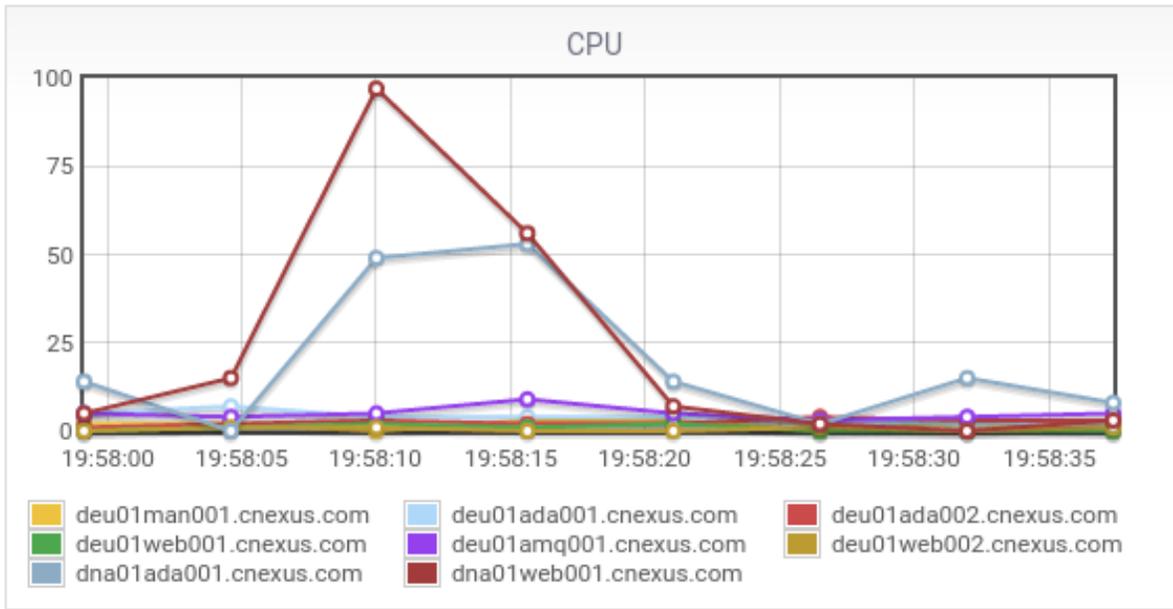


Each graph represents a different performance metric, while each colour of line represents a different machine within the clustered deployment.

⚠ Single machine deployments will only have single lines as shown in the image below.

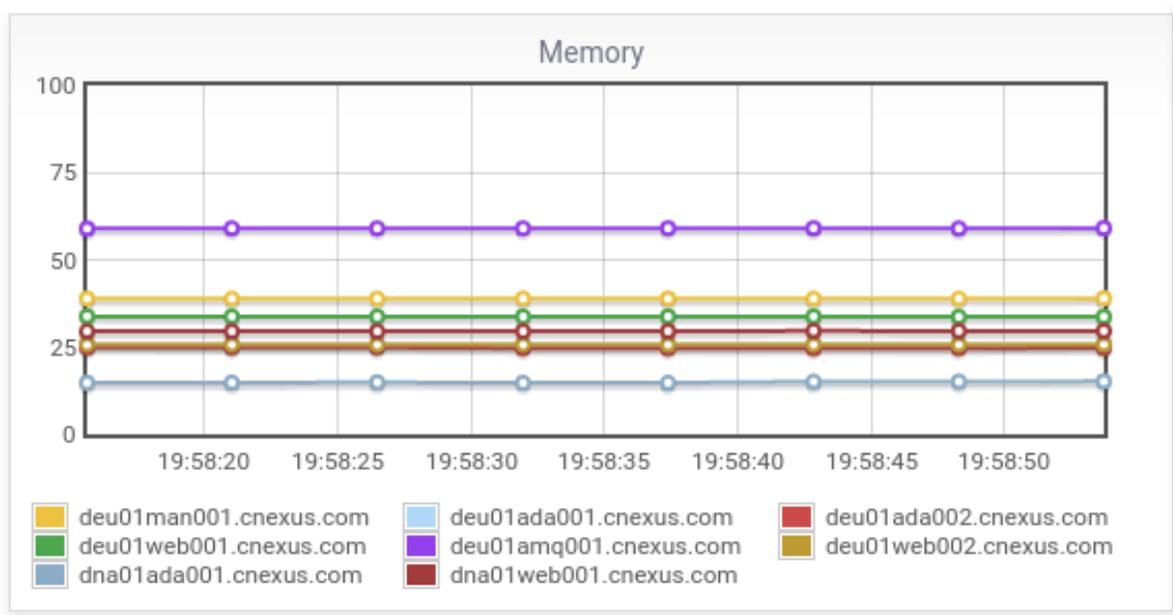
11.1. CPU Utilization

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.



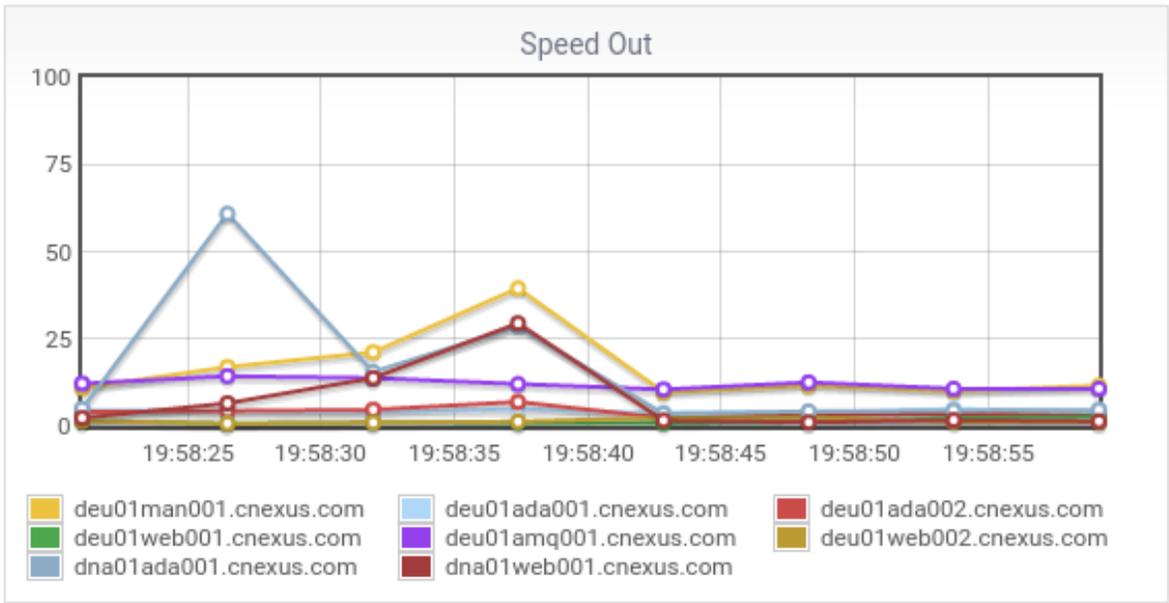
11.2. Memory Utilization

The memory utilization represents the total amount of memory in use on the system relative to the total amount available at a given time.



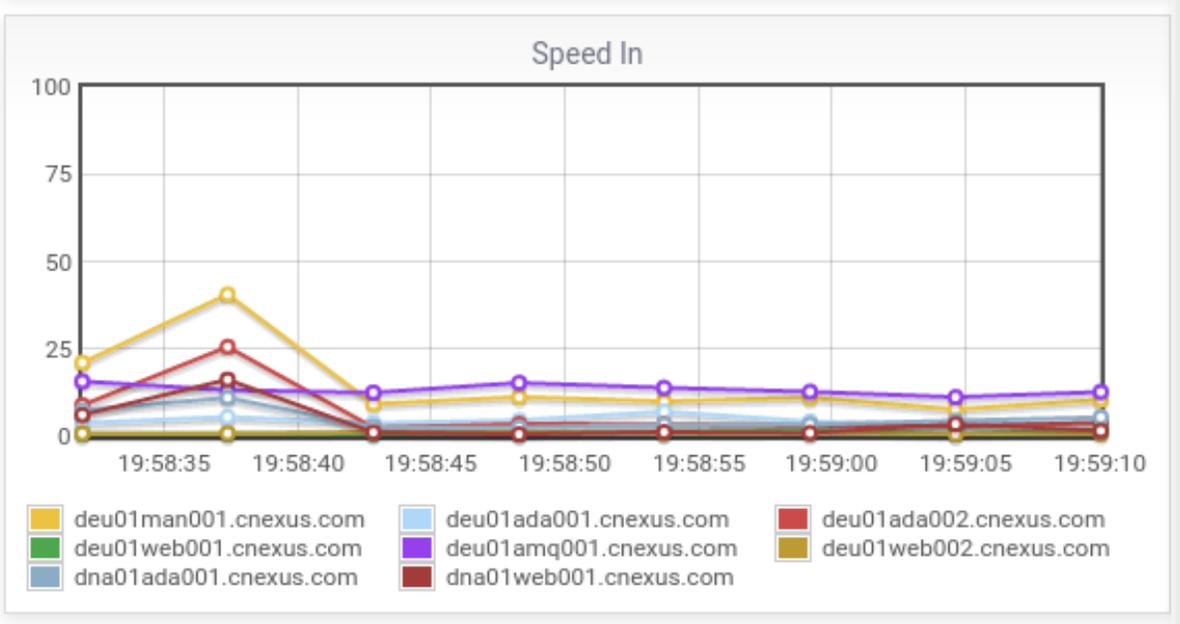
11.3. Speed Out

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

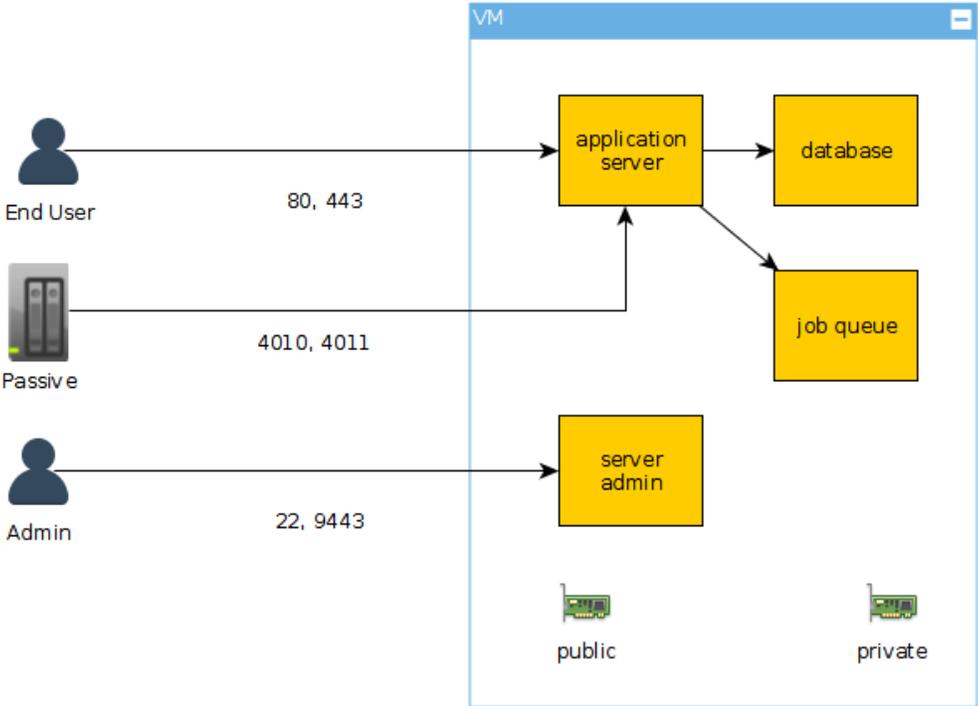
The speed in represents the proportional traffic ingress relative to the maximum burst used on any machine in the cluster within the visualized time range.



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 certified under the FIPS 140-1 and 140-2 NIST /U.S government cryptographic standards, and brings additional security features including improved cryptographic 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://comodossllstore.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 certificate 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 ownership 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.