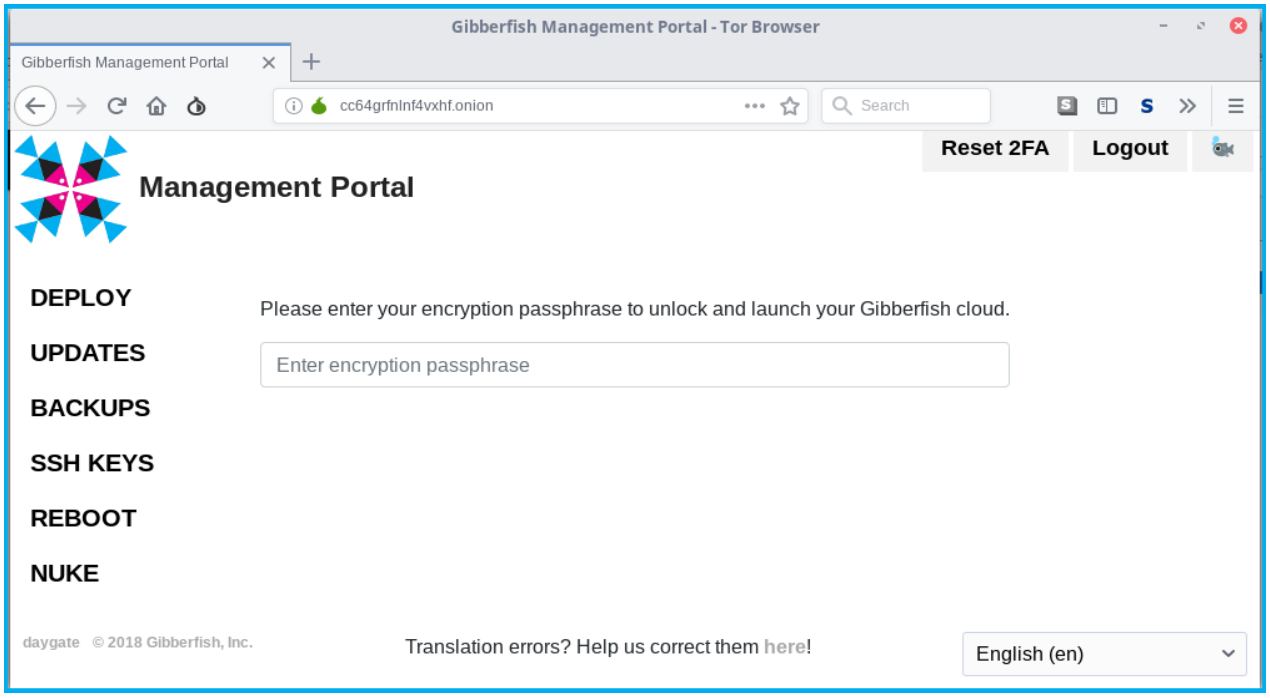
Gibberfish Management Portal User Guide



Introduction

Welcome. The “Gibberfish Management Portal” is a web application that’s designed to make it as simple as possible to deploy and manage your Gibberfish cloud server. It runs as a special kind of web site known as an “onion site”, which is only available via the Tor anonymity network using a special browser called the Tor Browser (Orfox on mobile devices). The reasons we have done it this way are threefold:

- It allows you to access the site with a high degree of anonymity, making surveillance virtually impossible, even from inside your local network.
- It can bypass most firewalls.
- It provides strong encryption right out of the box, avoiding the need for 3rd party certificates.

Additionally, the Management Portal send all *outgoing* connections to Gibberfish sites and resources through the Tor network, so that anyone spying on *us*, cannot follow the trail back to *you*.

You can read more about Tor, and onion sites at the Tor Project website.

The Management Portal will be your first stop in setting up your Gibberfish Cloud server. Once you have logged in, you will be able to deploy the server, configure backups, access your VPN keys, and more. Please read this document thoroughly before proceeding to become familiar with all of the features, advice, and caveats.

If you have questions or feature requests, please email them to info@gibberfish.org, or contact us via our encrypted web form at https://gibberfish.org/contact-us.

General Settings

Passphrases

Your **portal_admin** account allows you to manage many aspects of your Gibberfish server, so it is important that you protect it with a strong passphrase. The *only* password scheme we recommend is the Diceware method, which generates easily memorized passphrases using real words (and no clunky symbols, e.g. '!' or '%') which are phenomenally strong. Please take the time to select a secure passphrase *before* you log in.

For more information on Diceware, look here: https://www.eff.org/dice

Admin Email

The first time you log in to the Management Portal, after setting a new password, you will be prompted to enter an email address. This address will be used as your contact address when the system requests an encryption certificate from LetsEncrypt.org. It may also be used by the server occasionally to alert you about problems. It is important to set this to a real email account that you check on a regular basis. You will have the opportunity to change it later from the **Settings** menu.

Two-Factor Authentication

Most cyber-security experts now recognize that traditional username and password combinations are inherently vulnerable to attack, and insufficient for protecting sensitive data. Accordingly, the most powerful features of our Management Portal are disabled unless you set up two-factor authentication (2FA) on your **portal_admin** account.

To do so, you must install a TOTP-compatible app such as FreeOTP on your mobile device, click on the **Configure 2FA** link, then follow the on-screen instructions. Once configured, you will need to get a code from your device in order to log in. Because phones can be lost, stolen, or damaged, you should also click the **Get backup tokens** link to pre-generate a list of codes that you can write down somewhere safe in case of emergency.

Timezone

Your Gibberfish server will run various maintenance tasks on a set schedule to do things such as checking for updates and running backups. These tasks are scheduled to run in the early morning hours when they are less likely to impact users. Selecting your local timezone from the Settings menu will ensure that these jobs run at the appropriate time. If unset, the default is UTC.

Features

Many of the features listed below will not be available in the Management Portal unless you have set up two-factor authentication (see the previous section). This is because these features require an extra layer of security for your protection. The sections requiring 2FA have been marked with an asterisk(*).

Deploy

The Deploy process is the core feature of the Management Portal. It allows an administrator to unlock the encrypted storage and launch their Gibberfish cloud server. The first time a passphrase is entered, the server encrypts the storage volume using the passphrase provided, and then downloads and runs all of the necessary software. Henceforth, any time the server is rebooted the admin must return to this page and enter the original passphrase to unlock the storage and start the cloud server.

The passphrase entered here is kept temporarily in encrypted memory and then erased as soon as the storage is unlocked. It is never written to disk, in any form.

DNS †

If you are running your Gibberfish cloud from a residental internet connection, your internet address may change at your ISP's whim, making your site inaccessible. To counter this, you can use a dynamic DNS service, which will automatically update your DNS records with your new IP address whenever it changes.

Confgure this feature using settings from your dynamic DNS provider. Once you have dynamic DNS configured, you will need to modify the DNS records for your Gibberfish server to be aliases (CNAMEs) of your dynamic DNS subdomain.

The DNS feature currently supports the dyndns2 protocol, which is compatible with free services such as https://www.nsupdate.info. We plan to add more protocols in the near future.

(† This feature is hidden for hosted clients, as we manage the DNS for you.)

Updates

Gibberfish has desgined our software to update itself automatically. Every update is verified using a cryptographic signature to ensure that it is genuine and un-altered before it is applied. However, we don't want to push new code to your server without your permission, so you must opt in on this tab for updates to work. You can choose to permit automatic updates for the Management Portal, the Cloud platform, or both.

We strongly recommend enabling updates, to ensure your server has the latest features and security enhancements. You can undo this change at any time.

Backups *

Hardware fails. It's a fact of life. Therefore, it's important to make sure your most important data is saved in more than one place.

The Management Portal supports two ways to back up your data to an external server:

- Secure shell ('SSH', used mainly by linux servers)
- Windows/Samba (used by Windows and linux)

When configured, the server will take a nightly "snapshot" of your data, and synchronize any changes to the location you specify. We use two layers of encryption underneath your files. Our backup process snapshots the lower layer, which allows it to track changes to individual files while still keeping them encrypted. The files sent to your backup server will be encrypted (using your encryption passphrase) with encrypted filenames, so they should be *reasonably* safe, even on systems you don't control.

These backups are intended for *disaster recovery* only, meaning they are intended to be used to recover from a complete hard disk failure, not for retreiving individual files. Each night, the files on the backup server are synchronized with your cloud server. This means that if you accidentally delete a file on your server, it will be deleted from the backup as well.

SSH

To configure backups over SSH, you must enter a connection string which includes the username, hostname, and file path of the backup server.

Example:

someusername@example.com:/path/to/files

The Management Server automatically generates a keypair for authentication and will display the public key, which you must copy to the "authorized_keys" file on the backup host.

Windows/Samba

The configure backups to a Windows or Samba server, you will need to specify a connection string, username, password, and Windows domain.

Example:

target:	//**example.com/path/to/files**
username:	**someusername**
password:	**really really really secure password**
domain:	**EXAMPLE**

Please be aware that the Management Portal will store your Windows password in clear text (not encrypted) in its database, where it could *conceivably* be stolen. For this reason, ***never*** use an account with elevated privileges on the backup server. It is best practice to create an account specifically for this purpose with minimal privileges.

SSH Keys *

This feature is intended for advanced users only. If you are comfortable using the linux command line interface, you may upload your public ssh key, which will be added to the authorized_keys file for the **root** user account. You may then log in via ssh to root@example.org to perform server maintenance and repair.

Please note that it is very easy to accidentally damage the software and operating system on your server and/or destroy data. A user with shell access can also read, alter, delete, and/or download your data in unencrypted form, so **please use extreme caution** and **do not install keys for third parties**.

Reboot *

When in the Course of human events it becomes necessary to reboot one's server, we have created a button for it.

This will trigger a reboot of your server within 1 minute of clicking the button. While your server is rebooting it will be inaccessible (including the Management Portal) for several minutes. Once it comes back online, you will need to re-enter the encryption passphrase on the **Deploy** tab to re-launch the cloud services.

VPN Client *

In order to set up their Gibberfish VPN connections, all users must install the VPN client bundle, which can be downloaded from this screen. It is up to individual administrators how best to distribute this file in a secure fashion. Please see our VPN Guide for more information.

Self-destruct *

We have built our cloud platform with security and privacy in mind, so that you can feel safe storing your sensitive private data on it. If you no longer need your Gibberfish cloud server, or for any reason feel that it may have been compromised, this feature gives you the option to *completely and irrevocably* eradicate all of your data.

In order to make sure this “nuclear option” is not triggered accidentally, you must manually type in a randomly generated code phrase, check a confirmation checkbox, and click the submit button. Once this is done, the following events will occur in order:

1. Your cloud services will be shut down
2. All of your files will be deleted
3. Your hard drives will be overwritten three times with random noise, to prevent forensic file recovery.

While steps one and two should complete in less than a minute, the final step may take up to several hours to complete, depending on the size and speed of your hard drive(s).

The partition that your Management Portal is installed on will be left intact, so you may re-deploy your cloud from scratch using a new encryption passphrase if you wish.