



# Securing Your Lamplight

## Using Features in Lamplight to improve the security of your system

Lamplight includes several features that will reduce the risk of compromise of the confidentiality of your data and help you to enforce your internal policies. This guide explains how to use: 2-factor authentication; password policies; and login policies.

### Two factor authentication

#### What is two factor authentication?

Two factor authentication adds a layer of protection to the login process. At the moment, you need something you know – your password. Two-factor authentication also requires something you have – your mobile phone. When set up, an app on your phone generates a 6-digit code every 30 seconds, which is only valid for 30 seconds. (This is a bit like the little widgets some banks give you to do online banking). You have to enter your username/password, and then this 6-digit code, to log in. This improves the security of your account because to log in with your details, an attacker would need both your password and your mobile phone.

Each operator logging in will have their own secret code (and not everyone has to use it, if it's impractical for some). We strongly recommend enabling two-factor authentication if at all possible. While it adds an extra step to the login process, the security benefits are so significant it's worth doing.

#### Adding 2FA to your account

1. **First** install an app on your phone (see links to app store versions of the Authenticator app below).

Google Play:

[https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en\\_GB](https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_GB)

Windows Marketplace

<https://www.microsoft.com/en-gb/store/p/authenticator/9wzdncrfj3rj?rtc=1>

Apple App Store

<https://itunes.apple.com/gb/app/google-authenticator/id388497605?mt=8>

2. Go into system admin and in the 'Manage database operators'

section, click on 'Enable two-factor authentication'.

3. Lamplight will generate a **secret** code that you need to enter into the app on your phone, like this one (this is just a sample code):

**Shared secret:**

Enter this into your Authenticator app on your phone

IVG5PY36WGEA4M42

4. You'll only need to enter the code you are given into your phone once. When this is done, your phone and Lamplight can both generate the 6-digit code you need to log in.

## Removing 2FA from your account

If your phone is lost or stolen, you should ask your system administrator to reset two-factor authentication for your login as soon as possible.

1. Go to system admin > Add, edit and remove database operators.
2. From the table of operators, find your name and click this or the menu button to the left of the row.
3. Click on 'remove two-factor authentication' in the menu.

Manage database operators

**Operators currently registered on the system:**

menu	ID	Name	First name	Surname	Email	Role	Two factor authentication enabled	Locked out
	586		M		@lamplightdb.co.uk	projectadmin	Yes	No
	592		m		s@lamplightdb.co.uk	staff	No	No
	594		m		s2@lamplightdb.co.uk	staff	Yes	No

Download | Print | split

**Add a new operator**

To create a new operator

- View full details
- Edit
- Delete
- Communicate
- Add new
- Reset password
- Force password change
- Remove two-factor authentication**
- Lock operator login

You can then set up two factor authentication again, which will generate a new shared secret.

Please note that Lamplight is unable to remove two-factor authentication on any account. If you are the system administrator, and you only have one system administrator account on the system, we would recommend adding a second that can be used in emergencies.

## Checking 2FA

Some organisations may take a risk-based approach to decide whether to require certain operators to use 2FA. For example, you may decide that only system administrators need to use it, or that operators with access to particularly sensitive data should, or perhaps everyone has to.

Once you have decided, System Administrators can verify which operators have 2FA enabled by going to **admin > system administration > Add, edit and remove database operators** and checking the operator table as shown in the screenshot above.

## More Details about 2FA

Two factor authentication significantly increases the security of your system, and is strongly recommended by security experts for use with all online services that support it. This pdf from SANS (a well-respected IT security organisation) explains why in a bit more detail. The National Cyber Security Centre and CyberAware both recommend use of 2FA.

Lamplight implements the Time-based One-time Password Algorithm (TOTP) defined in RFC 6238. As well as phone apps you can look for hardware tokens that also implement this algorithm if you are not able to use phones.

## Password Policies

Password policies enforce certain requirements of operator passwords. For example, your internal policy may require passwords to be at least 10 characters long with a mixture of characters. You can then set this up in Lamplight to ensure that everyone has a long enough password.

There's some good guidance on passwords and related matters on the NCSC website, at <https://www.ncsc.gov.uk/blog/identity-and-passwords>. Advice for system owners responsible for determining password policy can be found here: <https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach>

To set up your password policy in Lamplight (which will apply to all operators):

1. Go to admin > system administration > Set up or edit your password policy

## Password policy

Minimum password length	<input type="text" value="20"/>
Passwords must include at least one lower case letter	<input type="checkbox"/>
Passwords must include at least one UPPER case letter	<input type="checkbox"/>
Passwords must include at least one number	<input type="checkbox"/>
Passwords must include at least one punctuation character	<input checked="" type="checkbox"/>
Passwords must not be any of the 500 most common passwords	<input type="checkbox"/>
Passwords must not contain any of the 500 most common passwords	<input checked="" type="checkbox"/>
Number of days until password has to be changed	<input type="text" value="0"/>

Set to 0 to never have to change it

2. The selections shown in the screenshot above will be a reasonable way to implement the NCSC guidance by requiring long passwords (say 20 characters) as this will more or less force operators to use a password manager.
3. Tick the ones that you want to apply, then click 'save' when you are done.

Whatever you choose, when operators next change their passwords, their new passwords will have to comply with this policy.

### Forcing a password change

To force operators to change their passwords:

1. Go to admin > system administration > Add, edit and remove database operators.
2. From the table of operators, click on the menu button next to the relevant operator and select 'Force password change'.

## Manage database operators

### Operators currently registered on the system:

menu	ID	Name	First name	Surname	Email	Role	Two factor authentication enabled	Locked out
	586		Mc		@lamplightdb.co.uk	projectadmin	No	No
	592		mu		s@lamplightdb.co.uk	staff	No	No
	594		mu		s2@lamplightdb.co.uk	staff	Yes	No

Download | Print | split

**Add a new operator**

To create a new operator (

- View full details
- Edit
- Delete
- Communicate
- Add new
- Reset password
- Force password change**
- Remove two-factor authentication
- Lock operator login

3. At their next login operators will have to change their password (and it will have to comply with any password policy).

## Password Managers

Lamplight supports the use of password managers – you can paste your password into the password box on the login page.

### More information on passwords

Passwords are not stored in plain text format. Passwords are ‘salted’ with a random, unique salt, and hashed using the bcrypt algorithm.

If someone tries to login ten times without success, their account will be locked. A system administrator will have to unlock it. This is to prevent brute force guessing of passwords.

When Lamplight generates a new password, it always requires the operator to change it as soon as they log in.

## Login Security Policies

Login policies limit when and from where operators may log in. For example, you might have one that says ‘may only login weekday mornings’, or another that says ‘may only login from the office network Monday – Friday’. Different operators can have different policies applied to them. So your part-time staff might have the first policy, while your office-based system administrator has the second.

## Creating a login policy

1. Go to admin > system administration > Manage database operators > Set up login security policies.
2. You will see a screen like the one below, listing any existing policies and allowing you to create new ones:

### Login policies

Login policies let you control when, and from where, different operators may log in from. You need to set up the policies you need here, and then select the relevant policy for each member of staff in the manage operators section.

**Tuesday only**

**IP Addresses:** Allowed from any IP address

**Days and times:**  
Tuesday: 00:00 - 23:59

**Add new**

3. Click 'add new' and you will see the screen to enter the details of the policy:

### Create a new login policy

[Return to list of policies](#)

*Policy name*

*IP addresses to allow access from*

Enter IP addresses, one on each line. This is only going to work out if you have a fixed IP address - please check with your internet supplier if you are not sure. Leave this blank to allow access from any IP address.

### Monday

*Allow access on Mondays?*

*Allow access after*

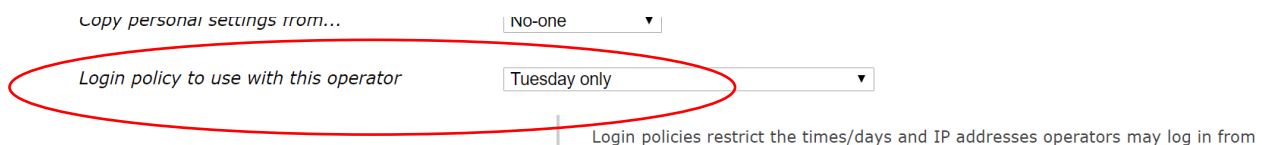
 

*Allow access until*

4. Give the policy a name.
5. If you have static IP addresses and want to restrict access to Lamplight to the ones you specify, you can enter multiple addresses here.
6. You can also set the days and times for the policy, if relevant. Note that times used are UK GMT/BST.

## Applying the policy

1. Go to admin > system administration > Manage database operators > Add, edit and remove database operators.
2. Go to the menu button next to the operator you wish to apply the policy to and choose 'edit'. At the bottom of the form you can select the login policy to use.



Copy personal settings from...

Login policy to use with this operator

Login policies restrict the times/days and IP addresses operators may log in from

3. An operator trying to login at a time or from an IP address that is not allowed will see a message saying that they cannot login at present.

## What is an IP address?

It's the address of a computer on a network. IPv4 addresses consist of four sets of up-to three-digit numbers, separate by a dot, like this: 123.45.6.789

Your computer will have an IP address on your local network (these often start 192.168 or 10.0). Your broadband router will have an internet IP address – this is the one you need to enter into the login policy. To find out your IP address if you don't know it, you can google 'what's my IP address' and it'll tell you. Using this means that only people connecting from that IP address – i.e. through your router – will be able to access Lamplight.

One problem with this is that your IP address may change over time – this is up to your ISP (Internet Service Provider). If this is the case, then you may suddenly find yourself locked out of Lamplight completely when the IP address changes. You can get, and will need, internet connections with static IP addresses, so that you are guaranteed that it won't change.