

FEPS

**SSH Access
with
Two-Factor Authentication

Two-Factor Token**

access.eps.surrey.ac.uk



**UNIVERSITY OF
SURREY**

Contents:

Introduction	-	3
Two-Factor Tokens	-	3
Step 1 – Download an Authenticator App	-	4
Step 2 – Prepare to generate your Token	-	5
Step 3 – Generating your Token	-	6
Step 4 – Register your Token on your Smart Phone	-	7
Step 5 – Complete your Token Setup	-	8
Step 6 – Testing your Two-Factor Token	-	9
FAQ	-	10

Server Details:

Server Address:	access.eps.surrey.ac.uk
IP Address:	131.227.81.254
Operating System:	Ubuntu Linux 16.04

Help and Assistance:

For Help and Support for SSH Two-Factor Authentication, please contact:

Web:	https://www.surrey.ac.uk/fepsit/contact
Email:	itservicedesk@surrey.ac.uk
Tel (external):	01483 68 9826
Tel (internal):	9826

Introduction

To improve account security at the University of Surrey, two-factor authentication is becoming a requirement for all users who wish to access services from off-campus locations.

Two-Factor Authentication is an extra step used to verify your identity when you log in. Traditional authentication is based on your **Username** (*something you are*) and **Password** (*something you know*). Two-Factor authentication uses both of these two methods but adds as third method, the **Token** (*something you have*).

FEPS IT has launched a new SSH service, **access.eps.surrey.ac.uk**. All users who access SSH Services from computers external to the University will be required to switch to using **access.eps.surrey.ac.uk**.

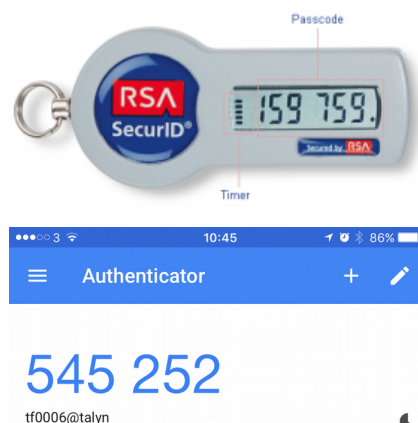
Two-Factor Tokens

Two-Factor Tokens work on the basis that a username or password can be stolen (without your knowledge), but a Token is something you carry with you. The token is unique to you, and is paired with your account. Once you log in using your username and password, you will then be prompted for a Verification Key. This is generated by the token and usually consists of a string of numbers that is regenerated every 30-seconds. These strings of numbers have a limited validity and are only valid at time of request – if you try to use a code generated an hour ago to log in, you will be rejected.

Two-Factor tokens come in two forms:

Hard Tokens and Soft Tokens. Hard Tokens are a unique physical device that display their number string on a LCD Display, or inputted directly into the computer.

Soft Tokens are stored in an App on your smart phone (see next page), but work in exactly the same way by displaying a string of numbers unique to the account it is paired with.



For access to the FEPS SSH Service, we will be using a Soft Token as it allows for the greatest flexibility. This will require an Authenticator App for your smart phone.








Access through the SSH gateway 'access.eps.surrey.ac.uk' from outside the campus network will **require** a two-factor authentication method. Internal access through this server **will not require** two-factor authentication.

Step 1 – Download an Authenticator App

First you will need to install an Authenticator App for your smartphone. It is recommended you use the Google Authenticator app or the Microsoft Authenticator app

This document uses screenshots from the Microsoft Authenticator app for its examples, however the procedure for Google Authenticator will be almost identical. If you already use Google Authenticator for accessing the University of Surrey VPN (other two-factor enabled services), you can continue to use that, however your Authentication Token will be unique to each service.

Authenticator Apps

		
Google Authenticator 	Download Google Authenticator for Android (free)	Download Google Authenticator for iPhone/iPad (free)
Microsoft Authenticator 	Download Microsoft Authenticator for Android (free)	Download Microsoft Authenticator for iPhone/iPad (free)
Authy 	Download Authy for Android (free)	Download Authy for iPhone/iPad (free)
LastPass Authenticator 	Download LastPass Authenticator for Android (free*)	Download LastPass Authenticator for iPhone/iPad (free*)
1Password 	Download 1Password for Android (subscription**)	Download 1Password for iPhone/iPad (subscription**)

* = LastPass offers a free and subscription tier of their LastPass service – more information at <https://www.lastpass.com>

** = 1Password is only available as a paid subscription service. More information is available at <https://agilebits.com>

If you use a Windows Phone, please look for the [Microsoft Authenticator](#) app or [LastPass Authenticator](#) app.

If you do not use a smartphone, you will be required to use an RSA Key-pair in order to authenticate ([guide](#)).

WARNING: Authenticator apps do not allow for backup / transfer of two-factor tokens. This means when you replace/restore your phone, your token will need to be regenerated. The exceptions to this are **Authy** and **1Password**.

Step 2 – Prepare to generate your Token

You will need to be on campus at the University of Surrey and logged onto a FEPS Linux machine running Ubuntu 16.04 (Xenial) or CentOS 7.3.

FEPS Linux Machine → Start here:

- I Open a new Terminal Window. You are able to run the commands from your local machine.
- II. Now continue to the ‘**Step 3 – Generating your Token**’ section on

University of Surrey Windows Machine → Start here:

- I. In a web browser, go to Surrey Software (<https://surreysoftware.surrey.ac.uk>) and sign in with your University of Surrey credentials. Choose PuTTY from the software list.
 - II. Once PuTTY is installed, run the ‘PuTTY’ application from the Start Menu.
 - III. Under ‘Host Name’ enter ‘*access.eps.surrey.ac.uk*’ and make sure the port is ‘22’. Now click open. Log in with your *Username* and *Password*
 - III. Now continue to the ‘**Step 3 – Generating your Token**’ section
- IMPORTANT NOTE:** Before continuing, please resize your PuTTY Terminal window to correctly display the QR Code. See *FAQ* page for details

Non-University of Surrey machines, or laptops on Wireless

You will be unable to set up your two-factor authentication by connecting to access.eps.surrey.ac.uk from a computer which is not on University of Surrey wired network, as doing so will require two-factor authentication.

In order to set up your two-factor authentication you will need to use a University of Surrey managed desktop machine (see above) or establish a VPN connection using <https://remote.surrey.ac.uk> (Staff only).

Step 3 – Generating your Token

1. From the command line or terminal, run the following command and press Enter:

google-authenticator

You will now be guided through the security settings for your Google Authenticator Two-Factor authentication. For all responses, enter y or n to signify Yes or No, then press 'Enter'.

- Do you want authentication tokens to be time-based (y/n)

Choose: ‘Yes’

This will now begin the token generation process

2. Your token will now be generated and displayed in the terminal. It will show the following:

Your QR Code



you will need to scan this using your Authenticator App.

Your Secret Key

you can manually enter this code if
you cannot scan the QR Code

Your Verification Code

This will be the first code generated by the device. This won't match if 30 seconds have passed between generation and scanning

Your emergency scratch codes

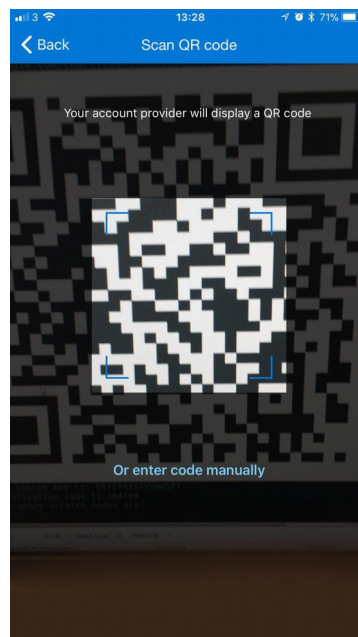
Make a note of these and store them somewhere safe. These are single use codes that let you gain emergency access to your account in the event of the Two-Factor key not working or not being available.

your Smart phone and authenticator app.

You can now scan the QR Code using

Step 4 – Register the Token on your smart phone:

- Open your Authenticator App.
- If this is your first time using the App then you will be prompted to add a new account. If you already have other accounts added to the App then touch the + symbol on the top right corner to add a new account.
- Choose 'Other (Google, Facebook, etc.)'.
- This will now activate the camera and ask you to scan the QR Code. Point the camera at the QR Code displayed and it will add an entry to the Authenticator App.
(If you cannot use your camera to scan the QR Code, you can choose to Enter the Code manually)



- Your new Two-Factor Token should now be displayed in the App.

Now return to the terminal window on your computer to continue the process.



Step 5 – Complete your Token Setup

You will now be asked a series of questions. Please enter the responses as documented under each question. You can enter **y** for yes and **n** for no, confirming each entry with the Return/Enter key.

- Do you want me to update your `"/user/<path_to_home>/<username>/.google_authenticator"` file (y/n)

If you are replacing / updating your token, this will replace / invalidate / void your previous Two-Factor Authentication token!

Choose: 'Yes' (choosing 'no' will not apply any changes)

- Do you want to disallow multiple uses of the same authentication token? This restricts you to one login about every 30s, but it increases your chances to notice or even prevent man-in-the-middle attacks (y/n)

Choose: 'Yes'

- By default, tokens are good for 30 seconds and in order to compensate for possible time-skew between the client and the server, we allow an extra token before and after the current time. If you experience problems with poor time synchronization, you can increase the window from its default size of 1:30min to about 4min. Do you want to do so (y/n)

Choose: 'No'

- If the computer that you are logging into isn't hardened against brute-force login attempts, you can enable rate-limiting for the authentication module. By default, this limits attackers to no more than 3 login attempts every 30s. Do you want to enable rate-limiting (y/n)

Choose: 'Yes'

You have now successfully generated your two-factor authentication token. This token is not required for use when logging into your local machine.

It will be required when connecting via SSH to the External SSH gateway – **access.eps.surrey.ac.uk**

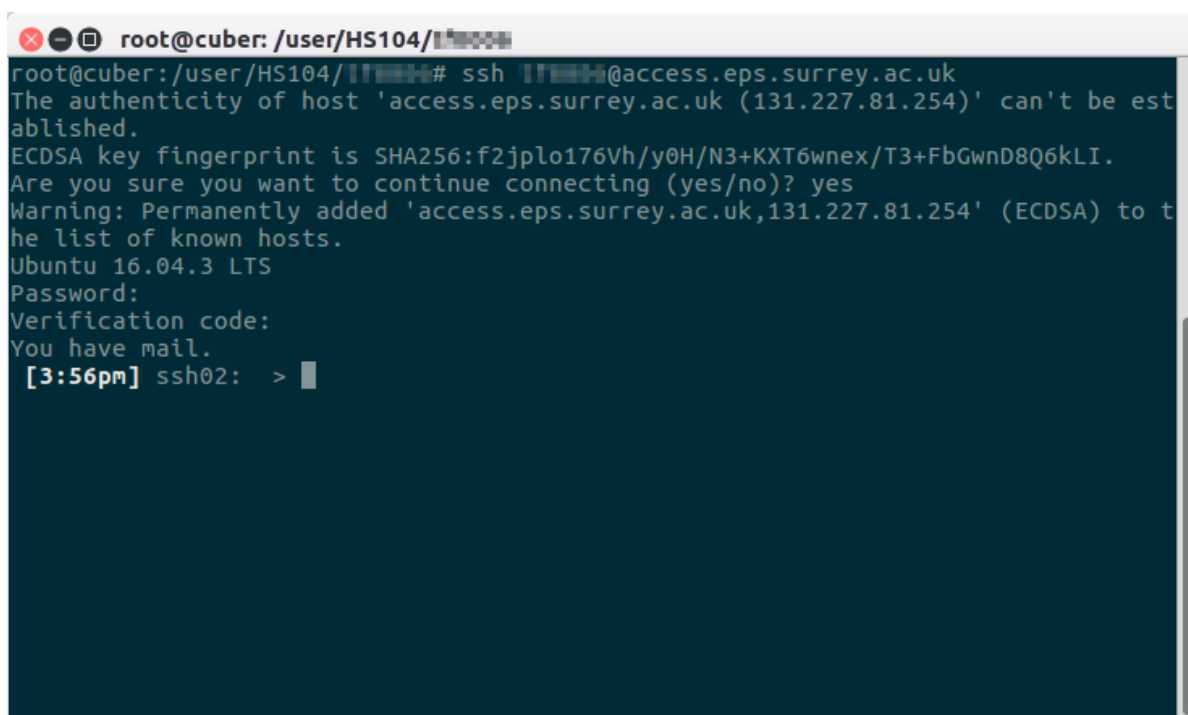
Step 6 - Testing your Two-Factor token

You can test if your token is working by establishing an SSH connection to **access.eps.surrey.ac.uk** from a computer external to the university, or a laptop connected to Eduroam.

Connecting to access.eps.surrey.ac.uk from an internal University of Surrey machine will not require two-factor authentication.

During login, you should be prompted for:

- Username
- Password
- Verification Code



```
root@cuber: /user/HS104/ [REDACTED]
root@cuber: /user/HS104/ [REDACTED]# ssh [REDACTED]@access.eps.surrey.ac.uk
The authenticity of host 'access.eps.surrey.ac.uk (131.227.81.254)' can't be est
ablished.
ECDSA key fingerprint is SHA256:f2jplo176Vh/y0H/N3+KXT6wnex/T3+FbGwnD8Q6kLI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'access.eps.surrey.ac.uk,131.227.81.254' (ECDSA) to t
he list of known hosts.
Ubuntu 16.04.3 LTS
Password:
Verification code:
You have mail.
[3:56pm] ssh02: > █
```

NOTE: The Google Two-Factor authentication will be bypassed if a matching SSH keypair is present! In this instance you will just be prompted to enter the password for your keypair, and the two-factor challenge/response prompt will not be presented.

FAQ

Q: I already have a Two-Factor token for the University of Surrey VPN Service (Pulse Secure). Can I just use that?

A: Unfortunately the VPN Service and SSH Service require unique tokens. At this time there is no way to integrate the two services to use a common token.

Q: Can I bypass the Two-Factor requirement for SSH if I use the University VPN Service (Pulse Secure)?

A: Yes. Once you have established a VPN Connection to the University and authenticated, SSH'ing to access.eps.surrey.ac.uk will only prompt you for a Username and Password

Q: I do not own a smartphone and therefore cannot create a Two-Factor Token. Is there an alternative?

A: Yes. You are able to generate an RSA key-pair. Please follow the '[SSH Access with Two-Factor Authentication: RSA Key-Pairs](#)' guide. At this time the only way to use the Two-Factor Token method is with a smartphone.

Q: I have lost / replaced / reinstalled my phone or two-factor token and can no longer authenticate.

A: While on campus, please log in to a FEPS IT Linux machine or create an SSH connection to access.eps.surrey.ac.uk . Now follow the instructions from Step 3 to replace your token. You will need to scan your new token with your smart phone.

If you are off-campus for an extended period of time and require this to be reset remotely, please check the FEPS IT website for the procedure.

Q: An application I use that connects over SSH does not support the Challenge / Response part of using the two-factor authentication token. Can I authenticate using a different method?

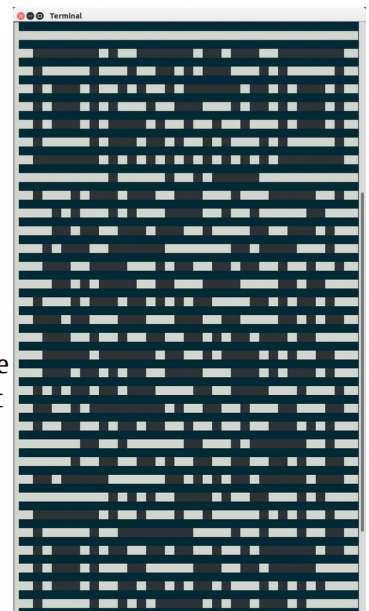
A: Yes. You are able to generate an RSA key-pair, installing the Public key into your ~/.ssh/ folder and using the private key on your local computer. Please follow the '[SSH Access with Two-Factor Authentication: RSA Key-Pairs](#)' guide.

Q: When I generate the Token in my terminal window, the output looks corrupted (see right), or unlike the QR code that is displayed in the above documentation

A: This has happened because the size of your terminal window is too small. This will happen before the creation / replacement of your Google Authenticator token.

For some terminals (like the ones in Linux) you will be able to resize the terminal window and continue on with Step 3.

For other terminals (like ones generated in PuTTY) you will need to choose 'No' as an option (so the token is not saved), resize your window, then start again by returning to Step 2 and (re)running the 'google-authenticator' command.



Q: Occasionally I get disconnected when using SSH, resulting in the program I am running to stop working. Is there a way around this?

A: Yes. Using the command 'screen' followed by the command you wish to run will detach the command from your active session. This means that if your connection is lost, the screen / session containing your application is able to be restored. For a quick guide to using screen, visit here: <https://www.mattcutts.com/blog/a-quick-tutorial-on-screen/>

Q: Which SSH commands work with Two-Factor Tokens?

A: So far, the following SSH commands have been tested:

- ssh
- scp
- sshfs
- rsync

Q: Can I log into access.eps.surrey.ac.uk and use it to run application X, Y, or Z?

A: FEPS IT have built the new SSH service with the most commonly used apps. The exceptions to this are CPU/Memory Intensive packages such as Matlab, Mathematica, etc. The SSH servers should not be used for anything computational.

- Mathematica
- Matlab
- Eclipse
- Maple
- R

If you wish to run computational applications, please establish your connection to access.eps.surrey.ac.uk before then creating another SSH connection from there to the machine you wish to run the application on (i.e. your own desktop or dedicated application or departmental server).

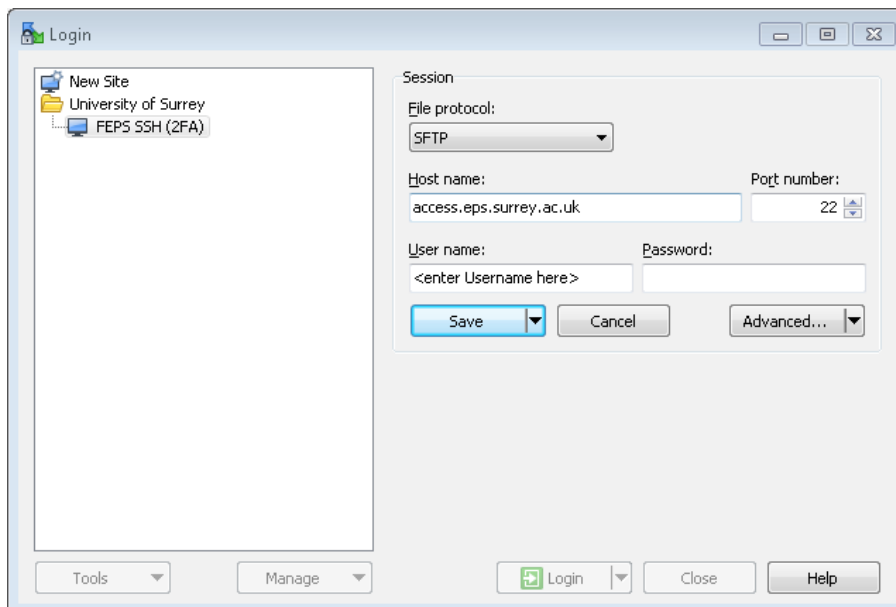
Please remember that the SSH servers are a shared resource open to every member of the FEPS faculty.

Q: Does the two-factor authentication work with *WinSCP* or *FileZilla* under Windows?

A: Yes. Please follow the instructions below for each application

WinSCP

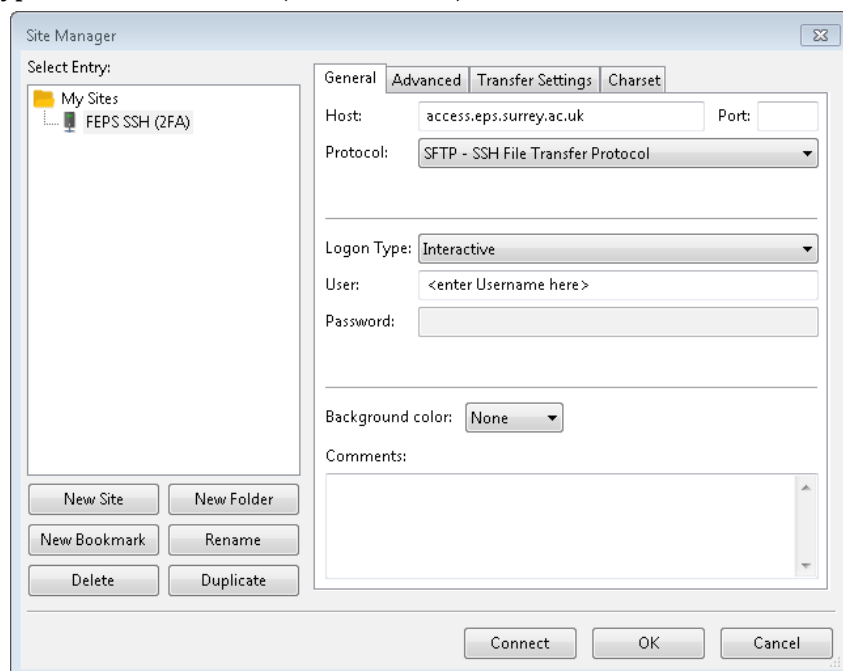
WinSCP works as normal. Please create a 'Session' in the Session manager, specifying your Username and Password as normal.



When you open the profile, you will be prompted for your Two-Factor code.

FileZilla

You cannot use FileZilla with the 'quickconnect' option. You will need to create an entry under 'Site Manager' with the 'Logon Type' set to 'Interactive' (see screenshot).



Alternatively, both applications will function with RSA keypairs

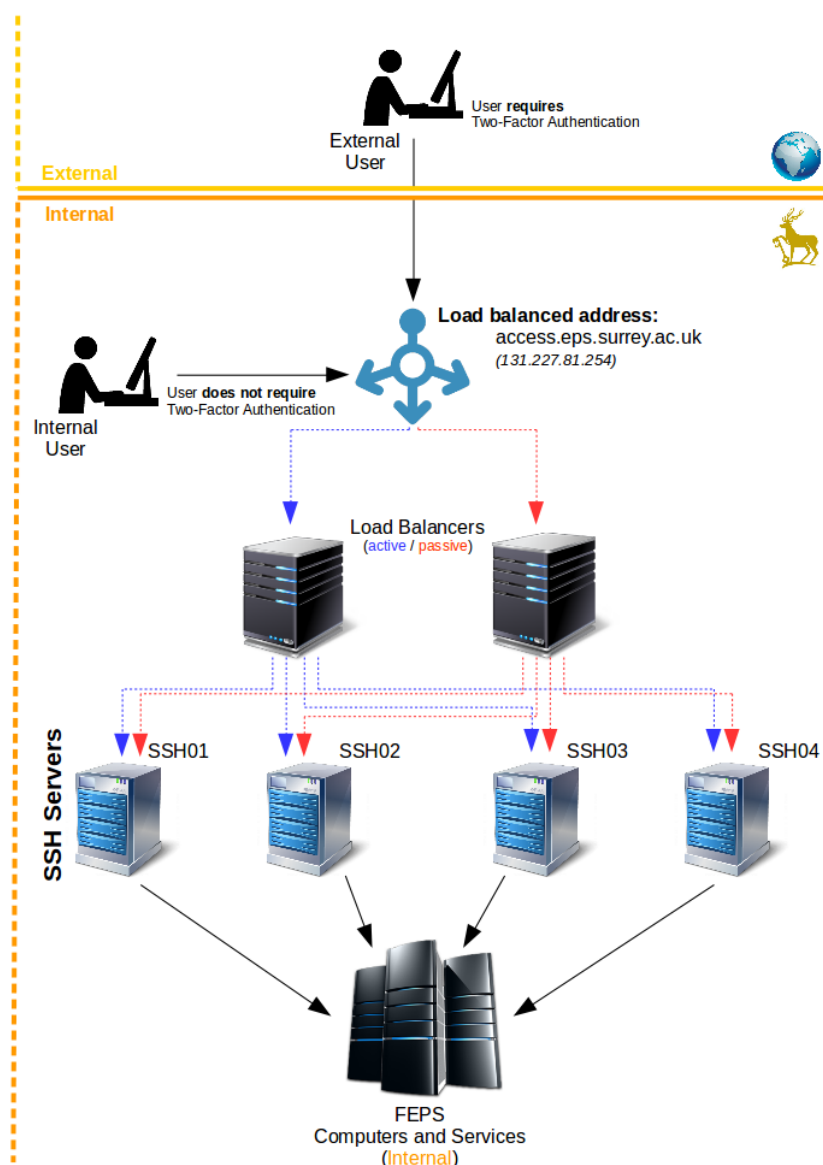
Q: Sometimes when I log in I get a different machine name. Is this normal behaviour?

A: In order to improve the reliability of our services, FEPS IT has implemented a small cluster of SSH servers. This allows us to share the load between servers and minimise any downtime caused by a single machine failing.

There are currently four SSH Servers running the access.eps.surrey.ac.uk service:

- SSH01
- SSH02
- SSH03
- SSH04

These servers sit behind a load-balancer which routes traffic accordingly, and also monitors the state of the servers, not routing traffic to any server which is offline.



If you are accessing from an external machine, you will be directed to **SSH01** or **SSH02**.
If you are accessing from an internal machine, you will be directed to **SSH03** or **SSH04**.

FEPS IT can add more SSH Servers in the future without any disruption to the service.

