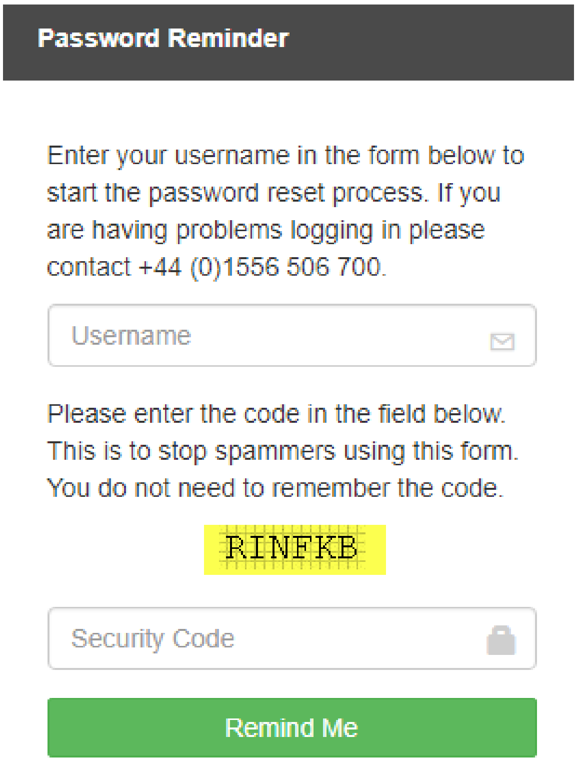
Password and Login issues

I can’t log in, how do I reset my password?

1. Go to https://secure.supercontrol.co.uk and click on “Forgotten your password?”

2. Enter your user name and type in the security code as it is displayed.



Password Reminder

Enter your username in the form below to start the password reset process. If you are having problems logging in please contact +44 (0)1556 506 700.

Username

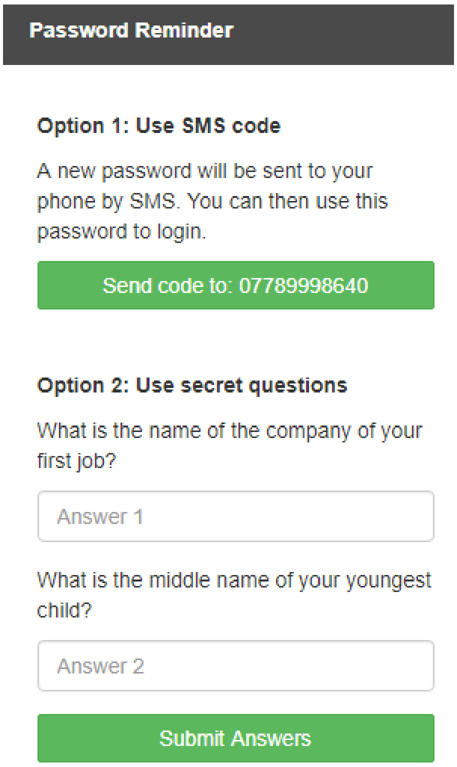
Please enter the code in the field below. This is to stop spammers using this form. You do not need to remember the code.

RINFKB

Security Code

3. Click “Remind me”.

4. The next page will either ask, if you want your password sent to your mobile number (only if you have your mobile number added in SuperControl) or it will prompt you to answer your security questions.
Enter your answers and click “Submit answers”.
Click the link, if you don't know the answers to your security questions any longer. Please use this link



Password Reminder

Option 1: Use SMS code

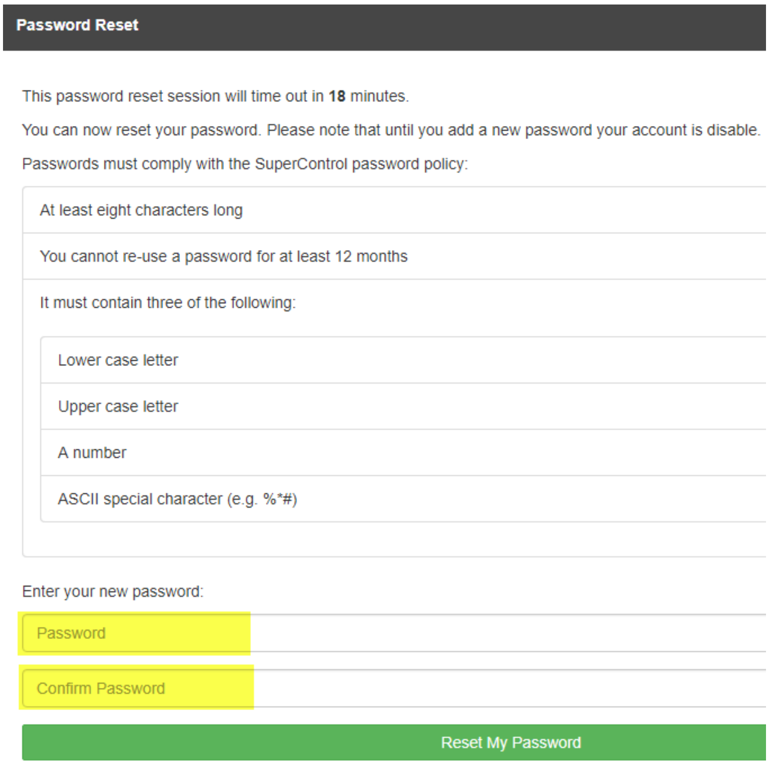
A new password will be sent to your phone by SMS. You can then use this password to login.

Option 2: Use secret questions

What is the name of the company of your first job?

What is the middle name of your youngest child?

5. If you have answered your security questions, the next page will ask you to create a new password. Then click "Reset My Password".



Password Reset

This password reset session will time out in **18** minutes.

You can now reset your password. Please note that until you add a new password your account is disable.

Passwords must comply with the SuperControl password policy:

At least eight characters long

You cannot re-use a password for at least 12 months

It must contain three of the following:

Lower case letter

Upper case letter

A number

ASCII special character (e.g. %*#)

Enter your new password:

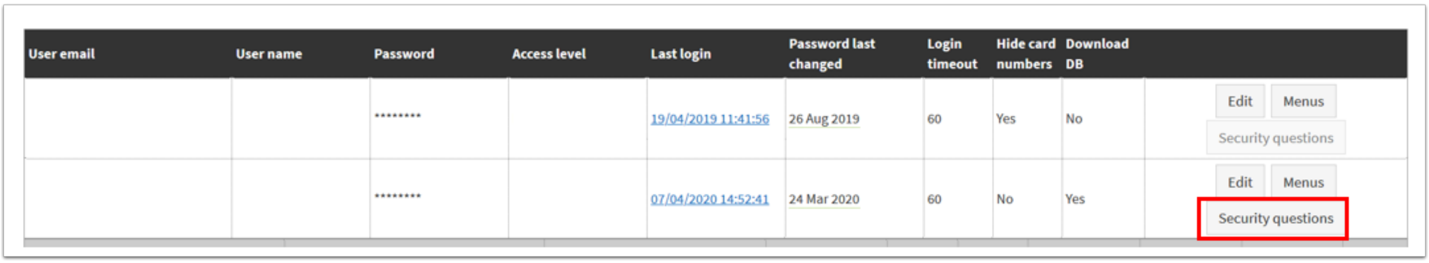
6. If you have triggered a new password to be sent to your mobile, you can use this new password to log in as normal.

Note: Having a new password sent to your mobile is the most efficient method. This option will only be available if you enter your mobile number within *Admin > Login users > Security questions (on the right hand side of your login details).* Remember to do this when you log in the next time.

I don’t know the answers to my security questions to log in?

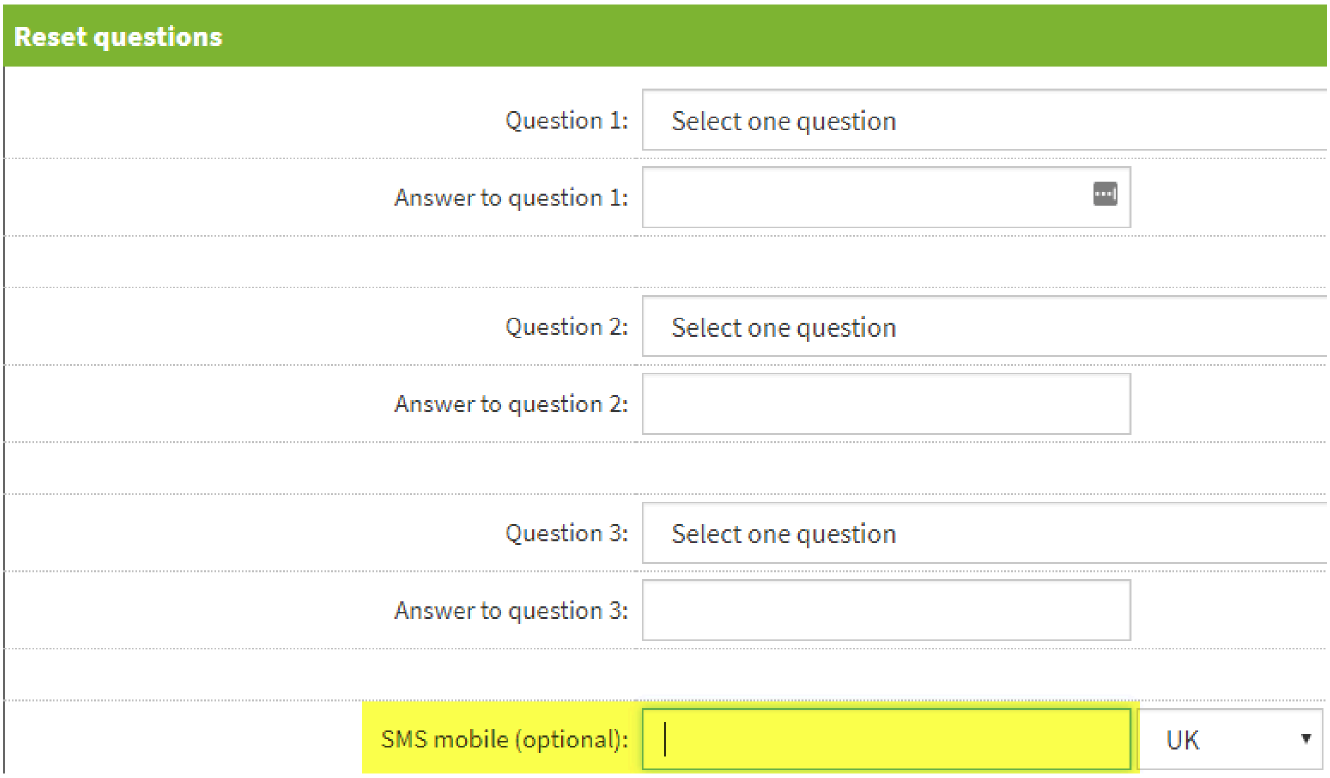
1. In this instance you will need to contact support@supercontrol.co.uk in order for us to reset your password and provide a new one.

2. Once you’re logged in go to *Admin > Login users* and click “Security questions” against your user name.



User email	User name	Password	Access level	Last login	Password last changed	Login timeout	Hide card numbers	Download DB	
		********		19/04/2019 11:41:56	26 Aug 2019	60	Yes	No	Edit Menus Security questions
		********		07/04/2020 14:52:41	24 Mar 2020	60	No	Yes	Edit Menus Security questions

3. You must select three questions, enter the answers and click Save. Also enter your mobile number, this means we can easily send you a new password by SMS if you forget your password in future.



Reset questions

Question 1:	Select one question
Answer to question 1:	
Question 2:	Select one question
Answer to question 2:	
Question 3:	Select one question
Answer to question 3:	
SMS mobile (optional):	UK ▾

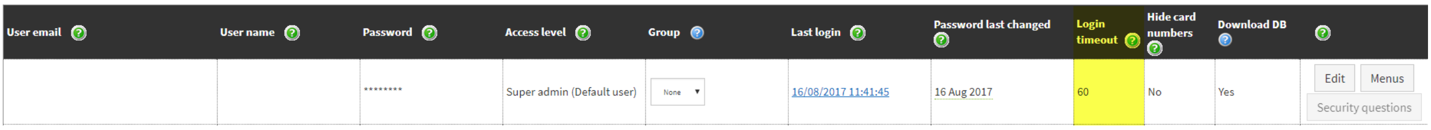
Note: Having a new password sent to your mobile is the most efficient method.

This option will only be available if you enter your mobile number within *Admin > Login users > Security questions (on the right hand side of your login details).*

Remember to do this when you log in the next time.

Why do I keep getting logged out?

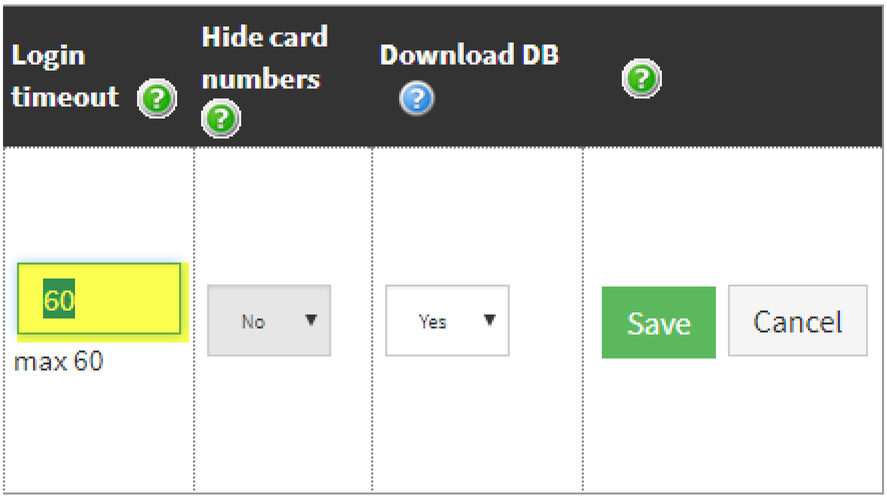
1. Firstly check that you have not adjusted your log out session time to below 60 minutes. To do this go to *Admin > Login users*



User email ?	User name ?	Password ?	Access level ?	Group ?	Last login ?	Password last changed ?	Login timeout ?	Hide card numbers ?	Download DB ?	?
		********	Super admin (Default user)	None ▾	16/08/2017 11:41:45	16 Aug 2017	60	No	Yes	Edit Menus Security questions

2. Your login time out should be set at 60. This means that if you are inactive in SuperControl for 60 minutes then you will be automatically logged out.

If you need to change this back to 60, click Edit, update the number and click Save.



Login timeout	Hide card numbers	Download DB	
60 max 60	No	Yes	

3. Another reason for your account being logged out frequently can be caused by browser settings or anti-virus software timing out your sessions.

In this scenario, we advise that you try logging in using a different browser. Also check your browser settings for any plug-ins or extensions and disable them. This resolves most login issues.

If you still experience issues please contact our support team.

Browsers available are Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge and Safari.

Note: Always check your computer clock is set to the correct time. If this is not set correctly it means your login sessions will not be timed correctly causing frequent logouts.

Why do I have to update my password every 90 days?

According to PCI DSS "Requirements and Security Assessment Procedures" Version 3.2.1, Chapter "Detailed PCI DSS Requirements and Security Assessment Procedures", section 8.2.4 requires to change user passwords/passphrases at least once every 90 days.

Passwords that are valid for a long time without changing gives an attacker more time to guess or break them (e.g. by using dictionary attack, by using advanced decryption algorithms, by eavesdropping etc.) Attackers who have more time to break the password can prepare a more advanced attack. There are also other important factors and risks e.g. in case of data leak, leaked passwords or their hashes can be present in databases that are shared over internet. So, thousands of attackers can try to break such passwords. The longer a password is valid, the more chance the attacker will find the password using slow dictionary attack or find the proper dictionary of leaked passwords from one of services that are used by user (note that a lot of people still use the same password across different systems). Attackers will also have more time to perform brute force attacks. If passwords are changed every 90 days or less, the leaked passwords will be useless for the attackers if the leaked dictionary is more than 90 days old. If periodical password changes are not forced, then the same password can be used in few systems for years. So, if there is a security breach to one of these systems or a data leak, the leaked passwords will became available, and attacker can use dictionaries based on these leaked passwords to break other systems. It is also important to realize, that some people unknowingly (e.g. by distraction) can use a password defined for system A to log in to system B. Some malicious administrators of system B can log every invalid login attempt and create dictionaries that consist of wrong passwords, then such dictionaries can be shared via the internet and used to get access into other systems. So, if you use the same password for a long time, there are various security risks that can apply to you.

However by forcing a change in passwords frequently, it might result in people creating simple passwords based on the month, year or a number that is increased on every change. So frequent password changes can lead to creating weak passwords. That is true if we assume that users are unaware of basic security concepts and don't care about security. This is why we encourage you to use a free password manager (eg LastPass) which makes life so much easier as you only have to remember your password for LastPass and then you can easily access all of your accounts securely (even from your phone), or other generator tools (eg Dinopass or Norton) to creates strong and unique password. By using such tools you reduce the risk of creating weak passwords and make it harder for attackers to break your passwords.

But what about the National Institute of Standards and Technology (NIST) guidelines?

According the NIST Special Publication 800-63B "Digital Identity Guidelines" section 5.1.1.2: "Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically)."

So yes, NIST has published guidelines, *however we still need to be compliant with PCI DSS*.

The PCI DSS "Requirements and Security Assessment Procedures" Version 3.2.1, Chapter "Detailed PCI DSS Requirements and Security Assessment Procedures", section 8.2.3, mentions industry standards (e.g., the current version of NIST SP 800-63.). However, this applies only to the requirement PCI DSS 8.2.3, which refers to password complexity and strength, but not to password change interval.

Password change interval is defined in the PCI DSS 8.2.4 requirement. It requires password/passphrase is changed at least once every 90 day. It is worth noting that PCI DSS guidance for 8.2.4 makes no reference to NIST SP 800-63.

Without a clear reference to NIST SP 800-63 in PCI DSS 8.2.4 requirement, there is no justification to use new NIST guidance for this requirement. So, the current 8.2.4 requirement is still in force.

Until the Council makes a change to the PCI DSS, we must comply with current requirements regardless of what other standards setting bodies state.

In summary:

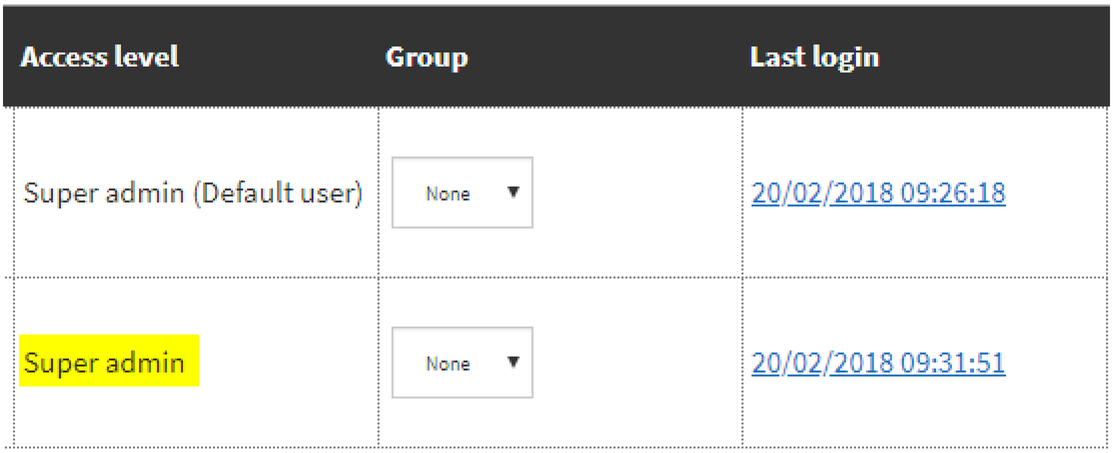
1. Passwords still need to be changed periodically, because NIST guidelines only apply to the PCI DSS 8.2.3 requirement which describes the password strength and complexity.
2. NIST guidelines don't apply to the PCI DSS 8.2.4 requirement which describes the periodical password changes, because there is no reference to NIST SP 800-63 in the PCI DSS 8.2.4 requirement.
3. We are obligated to comply with PCI DSS. Until the Council makes a change to the PCI DSS we must comply with the current requirements regardless of what other standards setting bodies state. Therefore we still have to comply with the PCI DSS 8.2.4 requirement and force periodical password changes.

Further info about NIST Password Guidance

Why can't I download the database?

When you want to download the database, but find that you don't have the option to do so, you can enable it in the settings for your login (user).

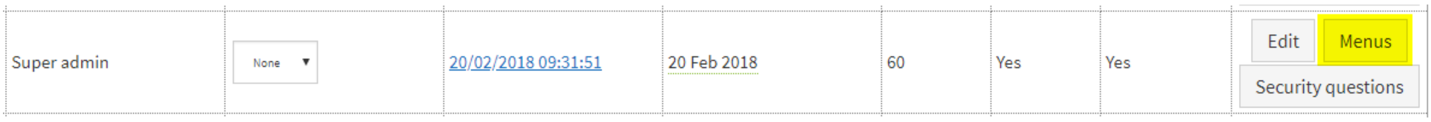
⚠ To do this, ensure your login access level is set to "Super admin" in *Admin > Login users.* If you're not set to this access level please ask your "Default user" to change this setting for you.



Access level	Group	Last login
Super admin (Default user)	None ▼	20/02/2018 09:26:18
Super admin	None ▼	20/02/2018 09:31:51

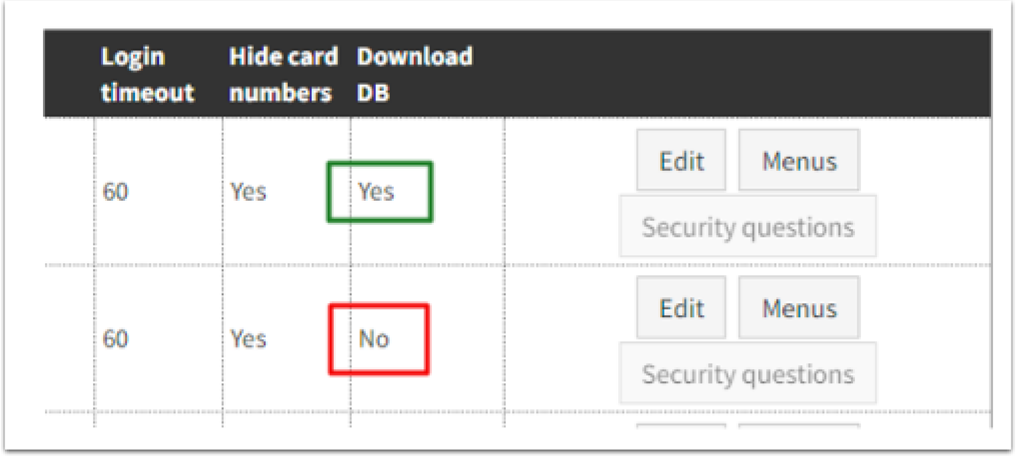
1. Go to *Admin* > *Login users.*

2. Click on "Edit" to the right of the login username you wish to enable the database download for.



Super admin	None ▼	20/02/2018 09:31:51	20 Feb 2018	60	Yes	Yes	Edit Menus Security questions

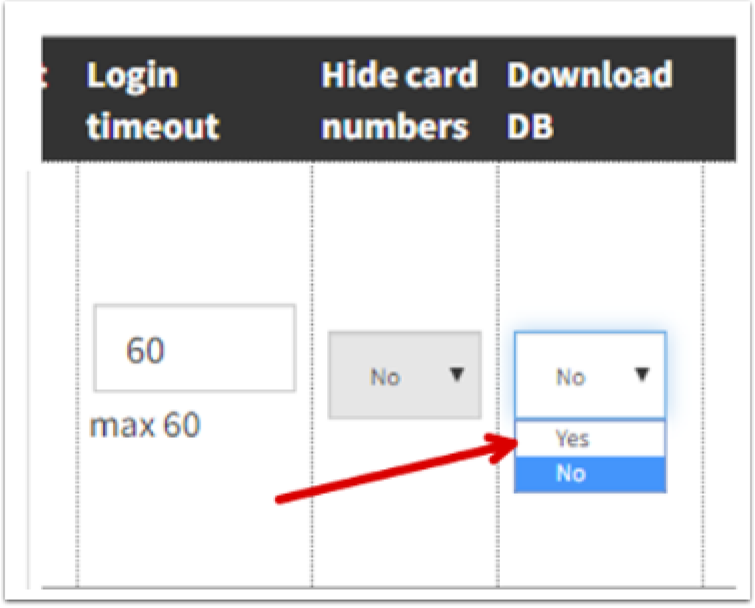
On the right hand side in the column **Download DB** should be showing **Yes**. If it is showing **No**, the setting needs to be changed.



Login timeout	Hide card numbers	Download DB
60	Yes	Yes
60	Yes	No

3. Click **Edit.**

4. In the column Download DB change the setting from **No** to **Yes**.



Login timeout	Hide card numbers	Download DB
60 max 60	No	No

5. Click **Save**.

When you now go to Database > Filter you can download the guest data as required.