SmartSurvey

Securing Your Account

What features can you implement to keep your account secure?

Keeping data safe is more important than ever

Being in a position of responsibility for personal data can be nerve-wracking at times as your clients or survey respondents have placed trust in you to keep their data safe and secure.

One of the most important things you can do to maintain this trust is to keep your account and those of any team members secure. In this eBook, we're going to be exploring the tools SmartSurvey puts at your disposal to make sure that it's only ever you that logs in to your account and keeps your, as well as your respondents' data safe and secure.

Two-Factor Authentication

Two-factor authentication (or 2FA for short) adds an additional layer of security to an account by requiring the user to enter a unique one time pass code, typically sent to their mobile device.

Make your accounts more secure with 2FA

What makes 2FA particularly strong from a security perspective is the second password isn't stored in the database and is usually a time-limited uniquely generated code or number.

The most common implementation is that the user is sent, or must retrieve, an activation code to enter after they've entered their password. This means that the account is still secure if the user's password itself has been compromised, because the attacker won't have (or even know how to get) the activation code required to complete the login.

SmartSurvey's Two-Factor Authentication Options

If you have any paid SmartSurvey account, you can use 2FA to secure it. This is done by installing an app on a smart phone, and then authenticating the app and device by scanning a QR code inside SmartSurvey (you only have to do this once). The user then enters a unique passcode generated via the app each time they login.

Users on an Enterprise plus plan have the option of using SMS messaging as the second factor. The user simply enters their mobile phone number and then every time they go to log in to their account, they're sent an SMS message with an activation code.

IP Restriction

IP restriction applies a rule to an account that means it can only be accessed from a defined point (or points) on the internet. The IP address is like the internet equivalent to a street address, and all devices that access the internet will have one.

Reducing the surface area for attack

Restricting Access by IP is a simple and effective way of ensuring that your account is not accessed from any point that's not authorised. Attempts to log in to your account from addresses that aren't on the authorised list will be rejected, regardless of the username and password that are entered. Using IP restriction reduces the visibility of applications in turn reducing the surface area for attack minimising vulnerabilities.

SmartSurvey's IP Restriction options

Enterprise Team or Enterprise Plus master accounts can specify one or more IP addresses from which all accounts, master or sub, can be accessed. Any log in attempts from outside these addresses won't be accepted.

Password Policies

Password policies enable you to apply a custom set of rules to passwords created, enabling organisations to ensure that passwords used to access a company account are of a high level of complexity in order to defeat brute-force attacks.

Complex passwords are harder to crack

The passwords users are most likely to use, if left to their own devices are all-lowercase dictionary words or relatively common names which means that they can be easy for attackers to discover via the application of a lot of computer power, known as a "brute-force" attack. For this reason, lots of organisations insist on rules for the passwords that are created, such as the inclusion of a digit, text in more than one case, and a special character. This added randomness can make the password much harder to crack.

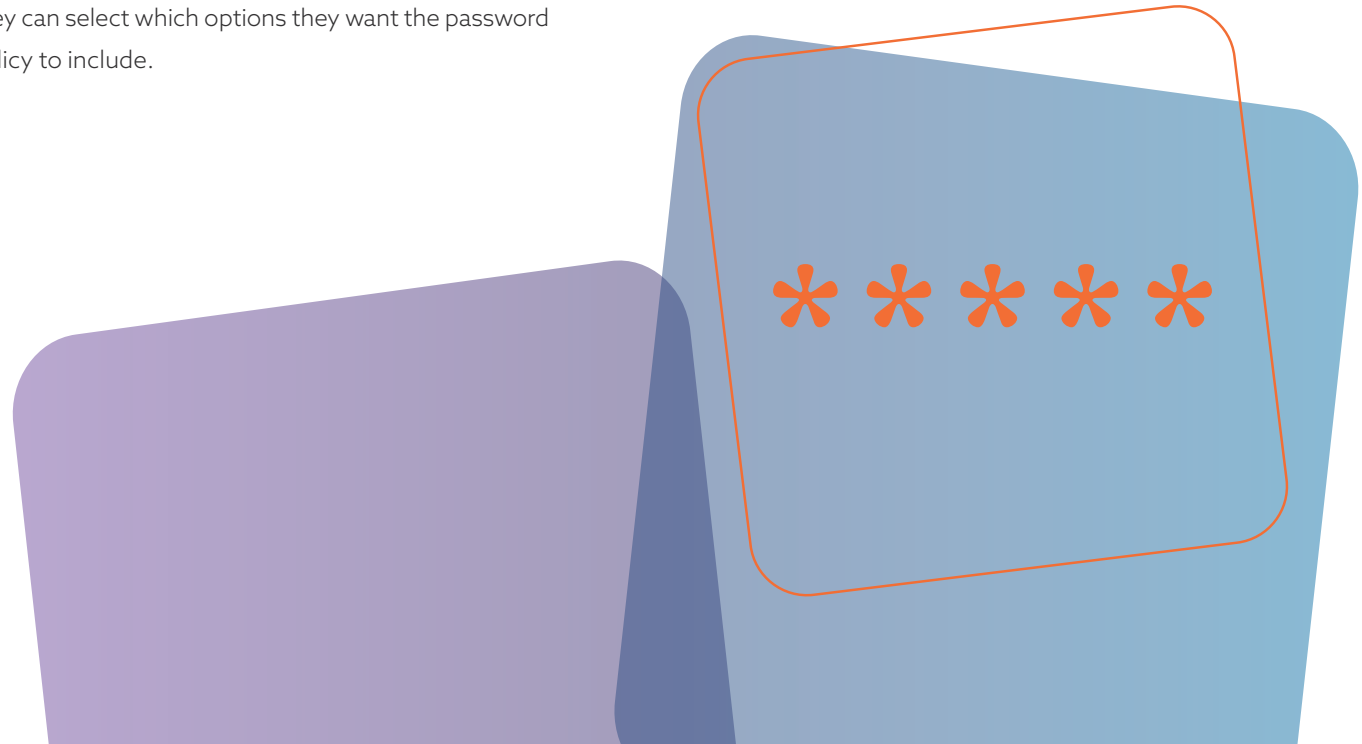
Another policy is the enforced expiry of passwords, where a password must be replaced with a new one after a set period of time. This is often 30 days but can be shorter or longer.

SmartSurvey's Password Policy Options

Enterprise Plus Master Users can set password policies for their account via a simple user interface, where they can select which options they want the password policy to include.

Advanced users can also use RegEx code to form the definition for the ultimate in control and allow any possible existing policy to be replicated.

An expiry window can also be set, ensuring all users change their passwords on a regular basis inline with your IT policies..



Single Sign On (SSO)

Single Sign On increases account security by removing the separate SmartSurvey Authentication from a group of users. On the face of it, this sounds counterintuitive, so a little more explanation of what this means seems like a good idea.

Under normal circumstances, someone who works at a large organisation who uses SmartSurvey needs at least two logins. They will have a login that allows them access to their work computer, and then when they access SmartSurvey, they enter a separate username and password to access the application.

Applying Single Sign On means that a connection is put in place between SmartSurvey and the corporate network, SmartSurvey allows access (or not) based on whether the user has authenticated with that network.

Streamline user management with SSO

There are several benefits to this approach. The first is for the user – they don't have to remember an extra username and password. This means fewer failed logins and locked accounts.

This is a minor benefit compared to the main security benefits. The fact that access is based on the corporate login means, depending on how the organisation has set up their security, they can ensure that organisational SmartSurvey accounts cannot be accessed from unauthorised devices or locations. It also means that if an employee leaves or changes role, their rights to access the SmartSurvey account can be rescinded instantly from the organisation, rather than having to get the master user to log in to SmartSurvey and remove them. Finally, the more passwords that a user has to deal with, and the increasing complexity required of those passwords, increases the likelihood of a user repeating a password or writing it down.

SmartSurvey's Single Sign On Options.

Enterprise Plus account holders can opt to implement Single Sign On as an extra for their account. Any SAML or Active Directory system is supported, and the user-facing element of the system is that users are directed to a specific landing page that handles the authentication automatically.

SmartSurvey

Want to add additional security to your account?
Speak to a member of our team

www.smartsurvey.co.uk

SmartSurvey Ltd. Basepoint Business Centre, Oakfield Close, Tewkesbury, Glos. GL20 8SD, United Kingdom

0800 0937 822 sales@smartsurvey.co.uk www.smartsurvey.co.uk