SDI Service Desk Institute

Password Management On The Service Desk

Prepared by Ollie O'Donoghue, SDI Industry Analyst

September 2016

In partnership with FastPassCorp Password security made easy

Declaration

While every care has been taken to ensure the accuracy of this report, the results, estimates and opinions stated are based on sources which, while we believe them to be reliable, are not guaranteed. No liability can be accepted by SDI, its Directors or Employees for any loss to any person acting or failing to act as a result of anything contained in or omitted from this report, or conclusions stated.

Prepared by SDI

About SDI

The SDI company mission is to inspire service desks to be brilliant. To achieve this mission SDI has developed a set of goals by which it aims to inspire service desks to:

Embrace: To raise the quality of service delivery by valuing best practice

Engage: To create an inspiring and engaging customer experience

Invest: To empower their teams to be inspired, take action and be better

Shine: To demonstrate and deliver exceptional business value

SDI sets the globally recognised best practice service desk standards that provide clear and measurable benchmarks for service desk operations and professionals. The standards are designed to encourage service desks to embrace and value best practice in order to raise the quality of service delivery.

For more information about SDI please visit www.servicedeskinstitute.com

Contact SDI

Service Desk Institute
21 High Street
Green Street Green
Orpington
Kent
BR6 6BG
☎
✉ +44 (0)1689 889100
🐦 hello@sdi-e.com
🖥 @sdi_institute
servicedeskinstitute.com

Contents

Introduction

For the service and support industry users with password problems are a considerable burden and one that takes up substantial resources. For those experiencing password issues, the urgency can be significant, particularly if it concerns a core application or device. Coupled with the high volume of password calls service desks receive, this combination can make password management the most resource intensive service provided.

To meet this challenge, software vendors have developed innovative management tools with increasingly powerful capabilities, smoother user interfaces, and stronger security pedigrees. As these technologies develop and become more widespread, it is vital to understand what impact password management is having on the valuable resources of the service desk and what results organisations who have gone on to implement the solutions have recognised.

This report will shine a spotlight on one of the industry's most common resource drains[1] and in the process investigate the true impact password management has, what organisations are currently doing and what return those that have implemented self-service solutions are enjoying.

1.1. In a recent SDI research report, Anatomy of the Service Desk, password resets were noted by 4% of service desk professionals as their biggest time drain in 2015. Although a considerable decrease from 6% in 2012, it is still a notable inclusion to a list of time drains that included people management and creating a service desk strategy.

Key Findings

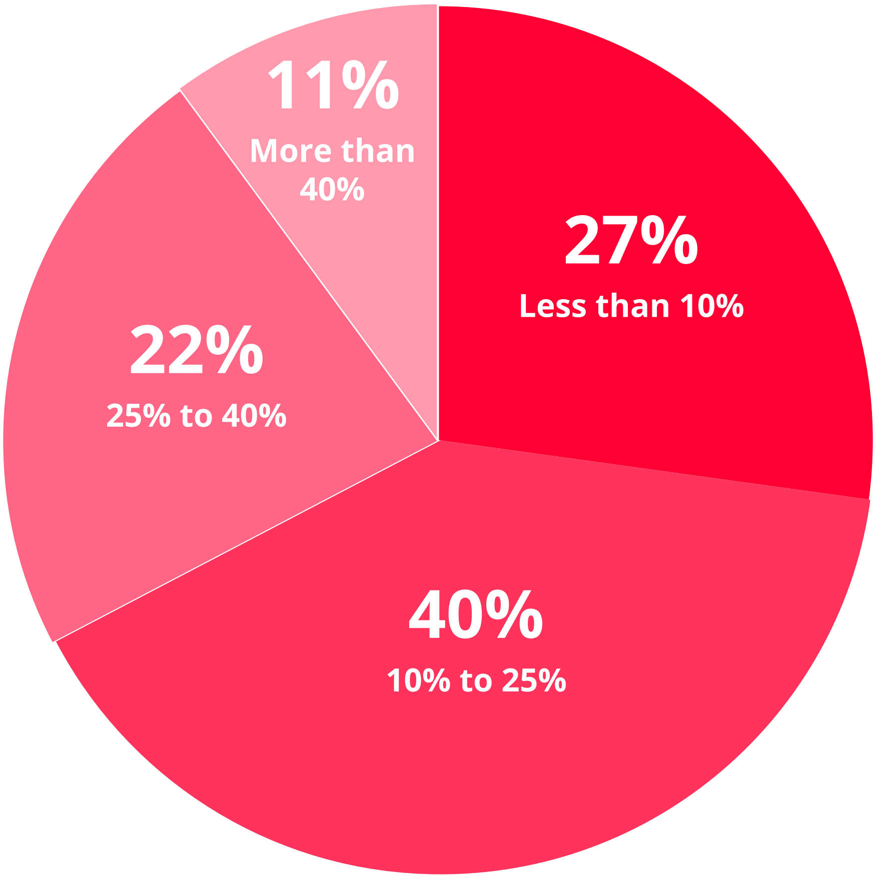
- Almost a third of organisations expect password related issues to take up more than 25% of their calls.
- Password self-service solutions have been implemented by the majority of organisations, with signs that even more will be implementing solutions over the next year.
- The majority of self-service implementations are unsuccessful with only 18% recognising more than 70% return on investment.
- Only 9% of organisations with a self-service solution convert more than 60% of password issues to self-service, the considerable majority, 86% convert less than 40%.
- Service desk professionals have identified three key inhibitors to the success of password self-service in their organisations:
    - User enrolment
    - Issues with the authentication process
    - Users preferring to contact the service desk directly
- Service desks without a self-service solution face considerable security and authentication challenges, with 35% having no clear authentication process at all.
- Current password self-service solutions rely heavily on traditional forms of authentication, particularly security questions, with only 7% of implemented solutions offering more innovative authentication methods.

Password Management And The Service Desk Industry

Frequently the impact of password management on the service desk is estimated to take up between 20% and 35% of a service desks total calls. The data gathered for this report confirms this with the majority of organisations expecting password related calls to take up between 10% and 25% of the total. Significantly, one-third of service desks expects password related issues to take up more than 25% of their total calls, emphasising the considerable burden password management has on their organisation.

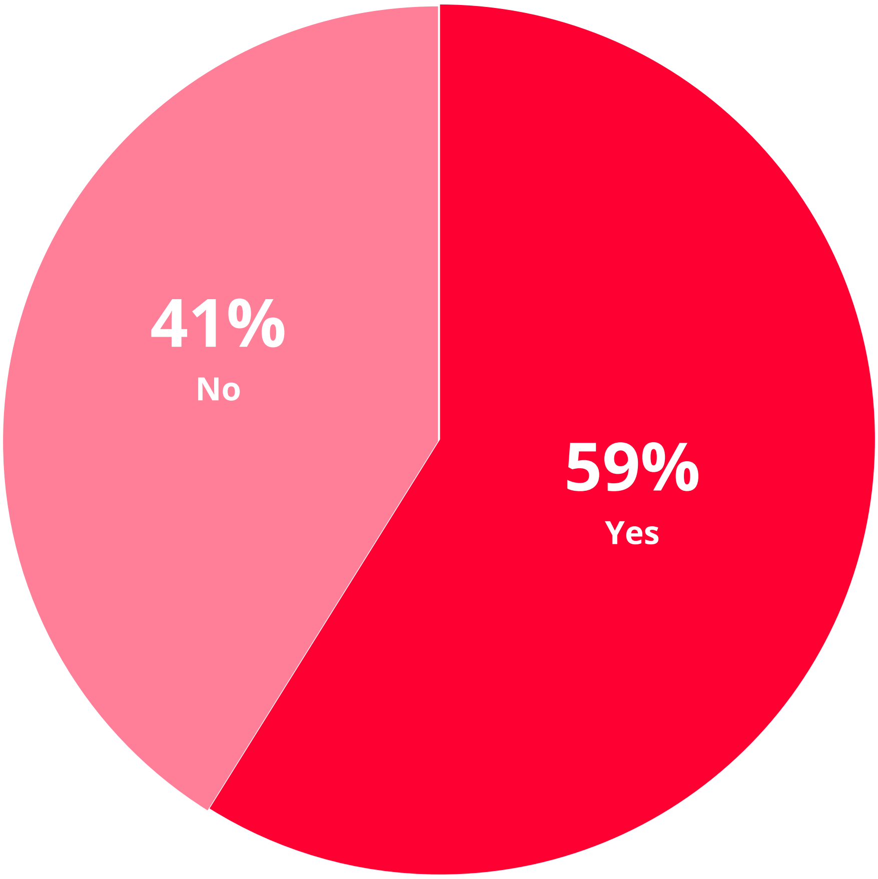
The impact is even greater still when considering factors such as lost employee productivity, making password related issues an area of IT support that carries a considerable business cost.

What Percentage of total calls to the desk are password related?



To get a better understanding of how password related issues impact the service desk industry, this report has been broken into two specific streams dependent on whether an organisation has a self-service password management tool. Those that do not will be covered in the first half of the report, with analysis of how these organisations currently manage passwords, what impact this has and how likely they are to implement a self-service tool in the future. The second half focuses on organisations that currently have a password management tool. This section of the report will cover aspects such as methods of authentication in the tool, the successes and challenges of the solution and a review of the recognised return on investment.

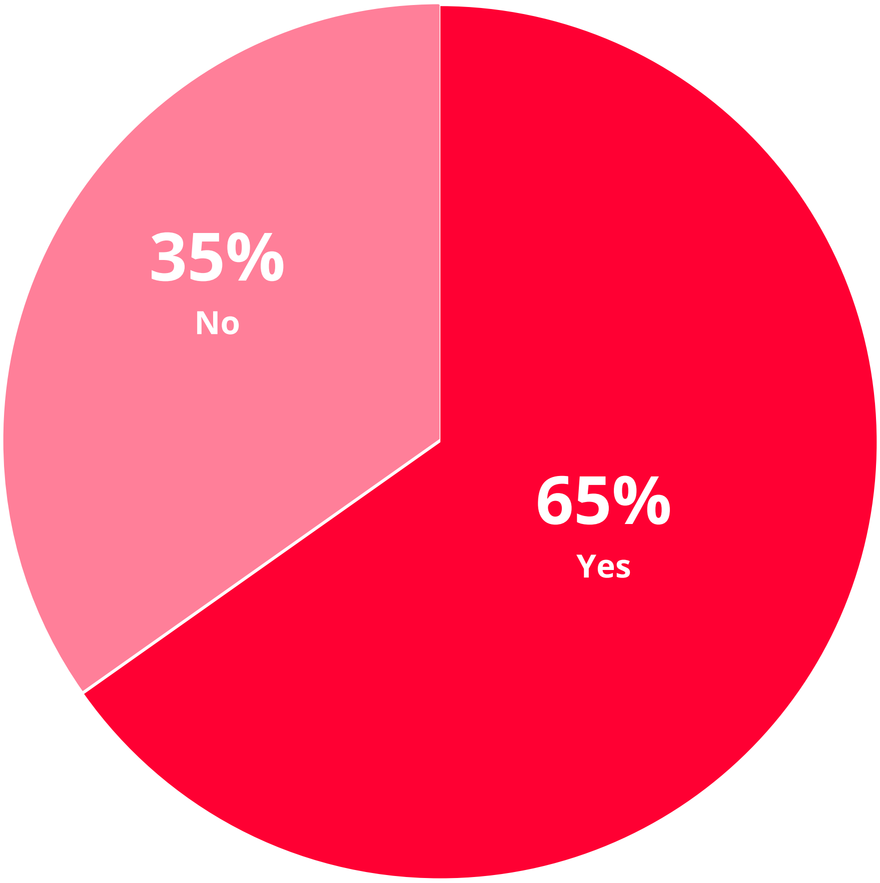
Do you have a password reset tool?



Significantly, 59% of service and support organisations currently have a self-service password tool in place, a reflection of the technologies perceived value in the industry. With only 41% of service desk professionals advising they do not have a solution, it is clear that the industry has recognised the challenges that password management presents and are seeking innovative solutions that will reduce the resources currently required to manage them.

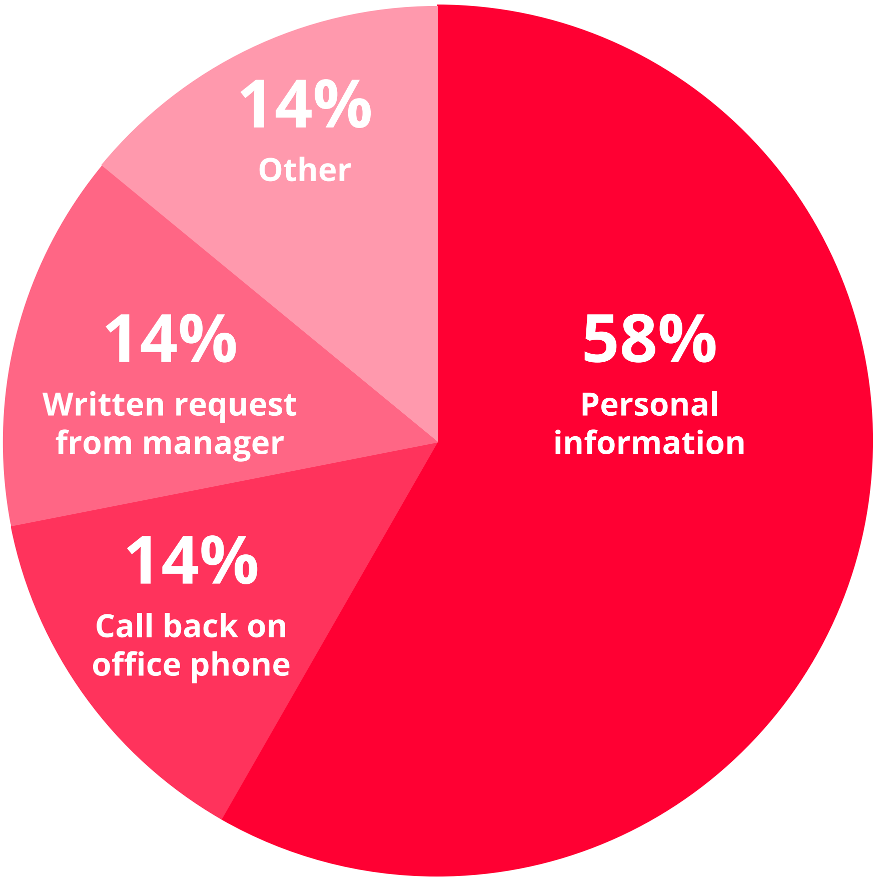
Service Desks Without A Password Management Tool

Do you have a clear process of user authentication when users call for a password reset?



Of the 41% of service desk professionals who advised they do not have a password management tool, only 65% have a clear process of user authentication when users call for a password reset. For the 35% who do not, they are not only open to security risks as they dispense credentials without clear and consistent authentication processes, but are also at risk of exacerbating password management challenges by encouraging potentially damaging end-user behaviours.

What authentication method is the process based on?

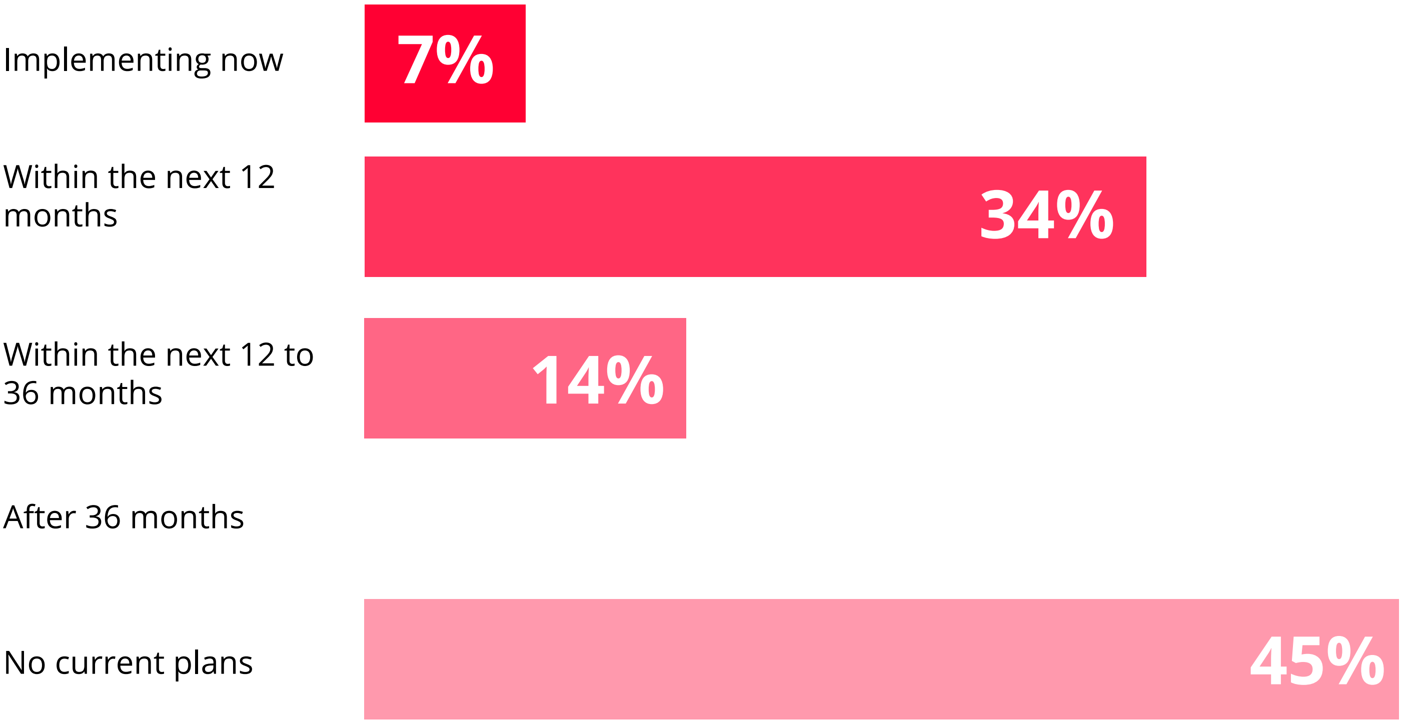


Subsequently, we asked the respondents who had a clear authentication process what method this was based on. The majority, 58%, use a system of authentication based on personal information provided by the end-user and validated by a service desk professional. Written requests from line managers and a call back on a pre-determined office phone are less common authentication methods at 14% each. The verbatim responses captured in the other category were largely representative of organisations that employ all, or a mixture of the options available, for example initially authenticating with personal information and then a written request from a manager if the information is incorrect.

Notably, the use of personal information as an authentication method can present significant challenges. For example, authenticating users based on commonly used personal information such as username, full name or asset ID's may be easy to recall for end-users but in a similar vein, can also be utilised by third parties. Conversely, requesting personal information that is harder to come across or guess may make for tougher security, but will undoubtedly cause problems should end-users struggle to recall the information or refuse to divulge it in the first place.

Furthermore, all of these methods have the potential to be significantly time-consuming for all parties, with some of the options presenting an undeniable inconvenience to end users and their managers.

Do you have plans to introduce self-service for password management?



A considerable amount of organisations are planning to introduce a self-service tool for password management. A total of 55% of organisations are at various stages of implementing self-service password management, of which 7% are currently implementing the solution. 41% of organisations will have implemented a self-service password management solution within the next 12 months bringing the total number of organisations with the solution up to approximately three-quarters of the service desk industry.

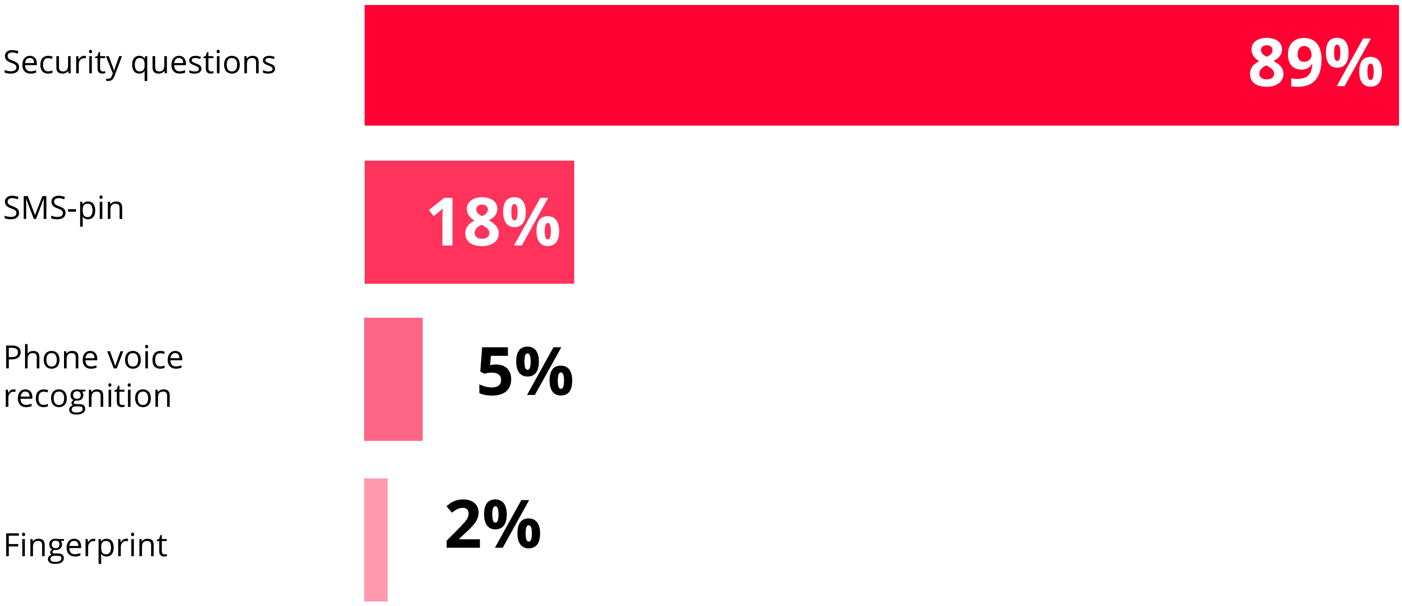
Given the impact password management is having on service and support organisations, it seems entirely reasonable that those that have not automated the process as part of a self-service portal are increasingly turned on to the benefits that this could bring. To get a better understanding of these benefits, this report will now move on to investigate how self-service password management is viewed by organisations who already have it implemented.

Service Desks With A Self-Service Password Management Tool

Method of authentication

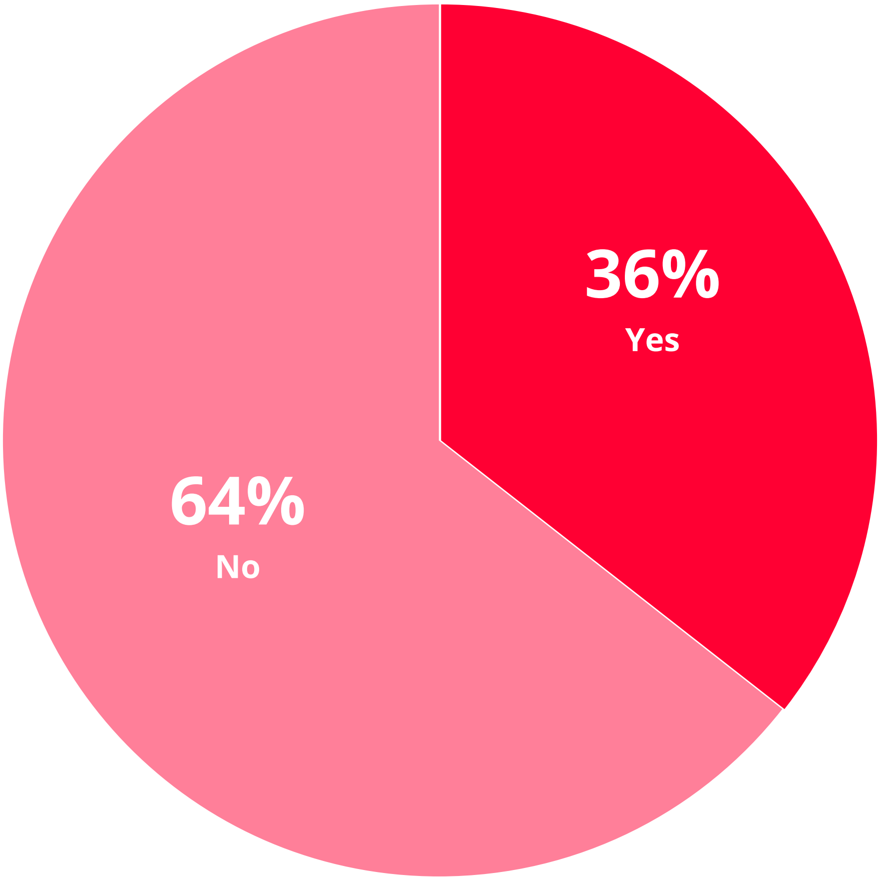
The challenges organisations experience when attempting to authenticate users, and the myriad security concerns that can accompany organisations without complex processes or no process at all, can be rectified through self-service password management tools. Authentication methods in tools can be much more complex or employ new innovative techniques to both ensure security compliance and provide a smoother customer experience.

What method is used for user authentication?



Of the respondents who advised they have a self-service password management tool, 89% use security questions as the method of authentication – a method that is also popular in the consumer space. Other more innovative approaches are increasing in popularity with SMS PIN verification used by 18% of the industry. Voice and fingerprint recognition are also emerging into the enterprise password management space with 5% and 2% of the industry utilising these methods. Furthermore, a considerable amount of organisations use two-factor authentication with the most popular combination being security questions supported by SMS PIN.

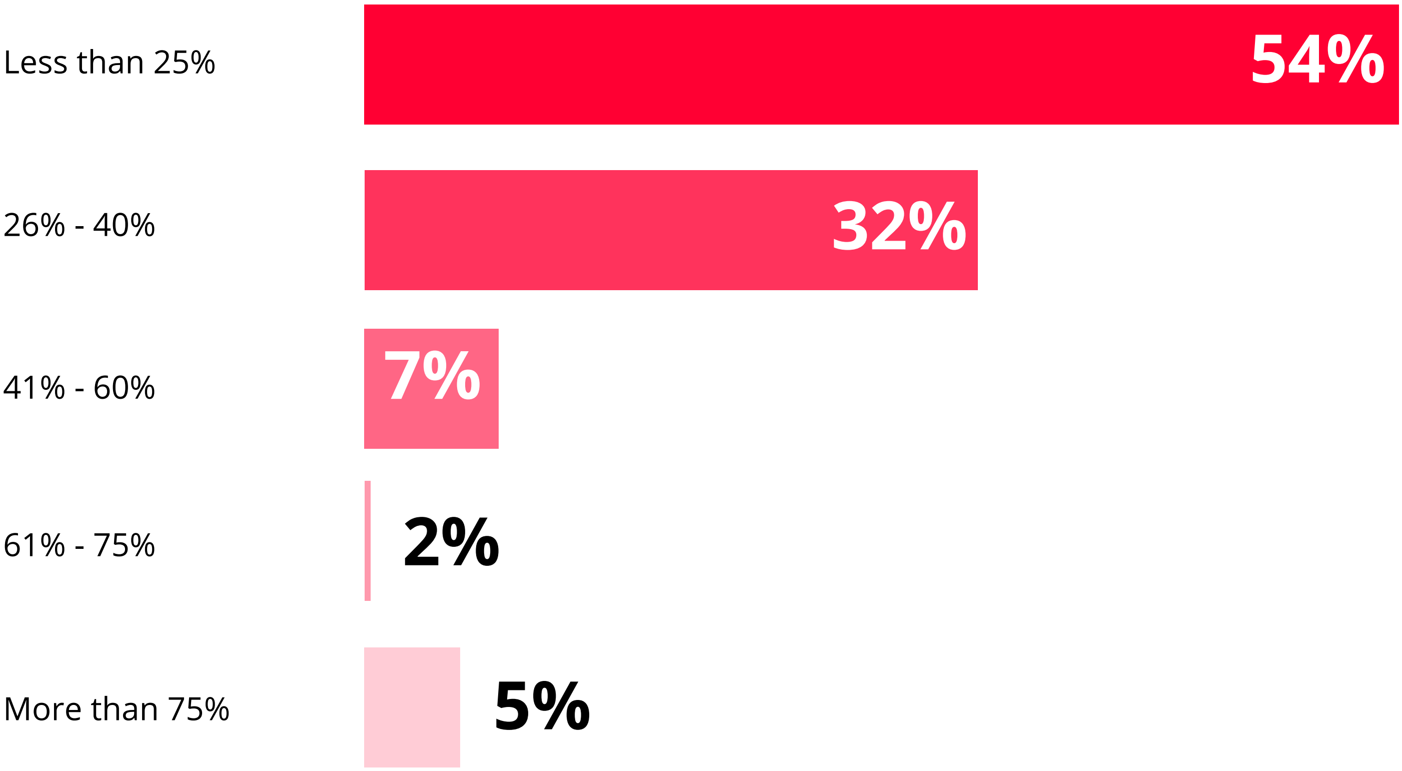
Do you have two factor authentication?



The majority of organisations, comprising 64%, do not use two-factor authentication in their password self-service solution. Two-factor authentication not only offers increased security but can also enable organisations to provide a smoother self-service experience. Foremost, two-factor authentication can provide end-users with greater flexibility in how they and where they reset their passwords. For example, single authentication may only comply with security guidelines if managed in a certain way – in an office building or on a business computer.

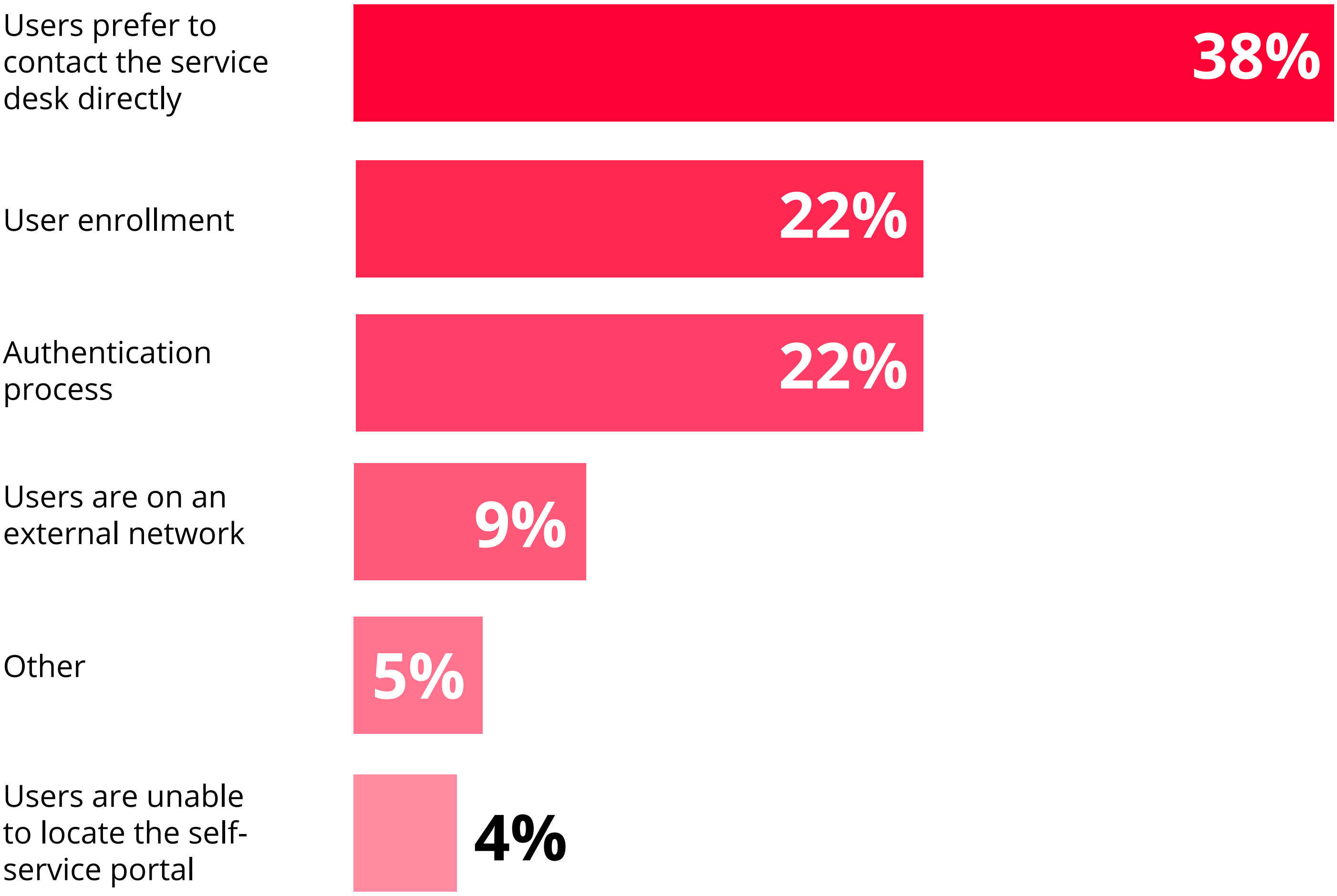
As self-service solutions develop more innovative methods of authentication, such as voice recognition, the percentage of organisations that use two-factor authentication is likely to increase as a need for more robust security drives businesses to find more secure technologies that do not reduce the overall user experience.

As a percentage, how many password calls have been managed through self-service in the last three months?



Significantly, a large section of service desks only manage a small amount of their passwords through self-service with the majority reporting the management of less than 25% of total password related issues through self-service. At the other end of the spectrum, only 5% of organisations have more than 75% of their password related issues managed through the self-service tool. Undoubtedly a disappointing result for the many organisations who will have invested in a solution to remove the burden of password related issues on their service desk, only to shave off a small portion of the calls.

What is the greatest inhibitor to the success of your self-service password management solution?



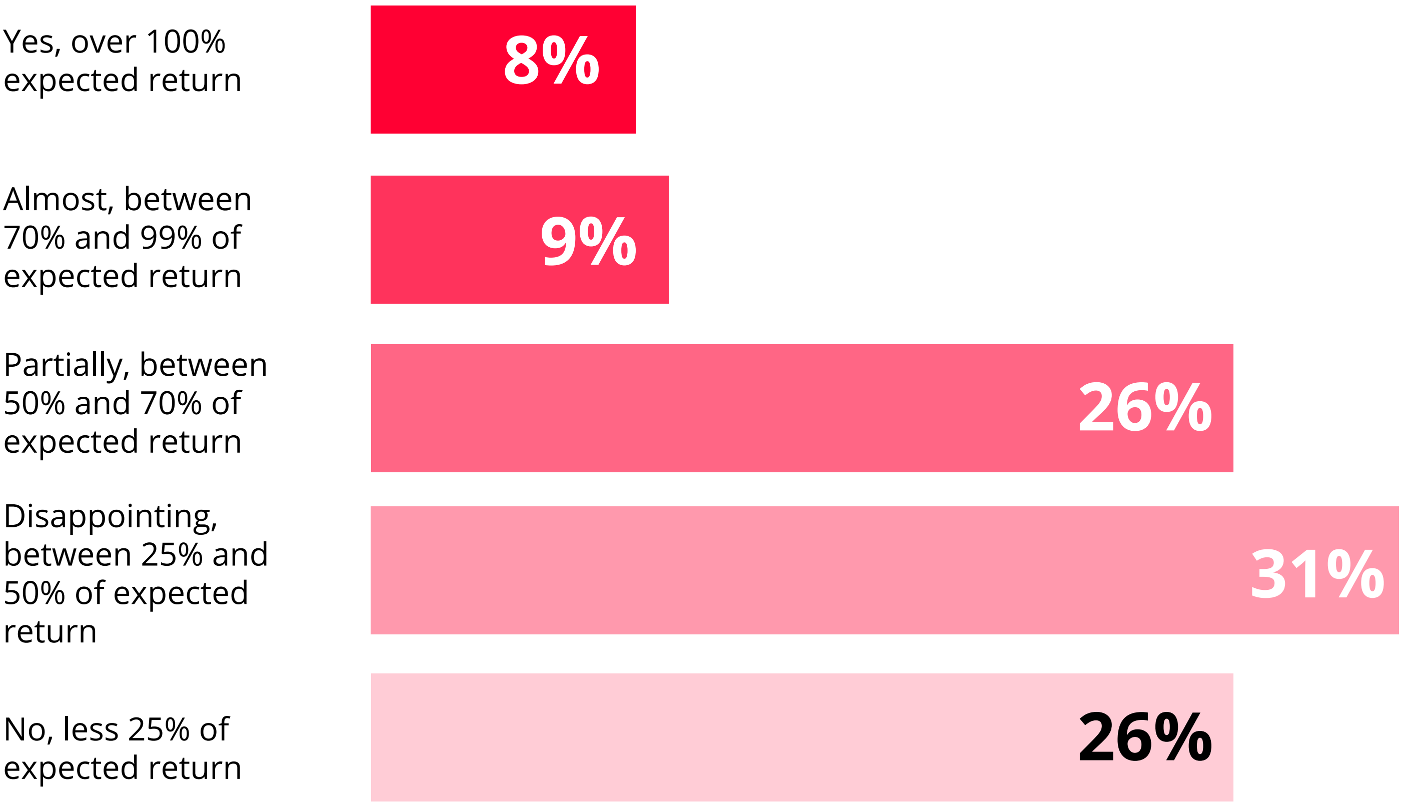
Understanding why self-service password management solutions are not delivering the results service desk professionals are expecting is vital. When asked what the greatest inhibitor to success was, the most popular response was that users simply prefer to contact the service desk. Further challenges with user enrollment further emphasise the theme of user preferences as an inhibitor to the success of self-service password management. The particular challenge with user enrollment is potentially due to the need for customers to register with the solution and provide security questions and their answers in advance, signalling potential process challenges.

There are several likely reasons for users avoiding the solution. Primarily the solution may not be user-friendly, not be easily found and delivering a poor experience, or one that cannot rival that of the service desk. The speed of resolution may also be an issue if the system is overly complex and similarly cannot rival the speed of the service desk. Finally, there may be challenges with the culture of the organisation, in which it expects the service desk to handle all IT issues, regardless of whether there is a self-service option.

Service desks may be able to mitigate these problems by designing a solution from a customer's perspective to ensure the experience is conducive to repeated use. Also, they should market the tool to ensure all users are aware of its existence and benefits. Careful marketing may also help tackle one of the other issues raised - users being unable to locate the self-service tool.

A considerable 22% of respondents advised that the authentication process itself is an inhibitor to success. It is clear that for some of these organisations there are challenges with users struggling to recall the answers to security questions. Innovations in authentication methods in self-service tools can rectify this issue by offering users the opportunity to use another authentication method to manage their passwords.

Has your solution provided expected return on investment?



When considering the challenges service desks are having when attempting to build reasonable self-service utilisation rates, it is somewhat unsurprising albeit disappointing to see such a small amount of organisations recognising a reasonable amount of return on the investment in the tool. Only 8% of organisations have recognised a return of over 100% while more than 80% achieved less than 70% return of which 26% achieved less than 25%.

The clear challenges organisations are having with self-service password management clearly leads to the poor returns the majority are reporting. With over three-quarters of service desks advising that their tool returned less than half of that expected in the initial business case, there are clear concerns for the industry. Moreover, as more organisations focus on security in the future, a solution that has historically offered negligible returns is unlikely to be considered. Service desk professionals and password management software vendors alike must work together to build a solution that tackles the challenges experienced in the industry with the desirable outcome of a solution that not only delivers expected return but overachieves it.

Conclusion

There are many competitors for the title of the greatest challenge for the service and support industry. However, password management will undoubtedly feature on the shortlist. For this reason, organisations have worked to provide a solution to the challenge, or at least mitigate its impact. Self-service password solutions offer organisations the opportunity to shift this section of support to the customer and in the process offer a more flexible and faster service with a reduced resource overhead for the service desk to handle.

The value of reducing the impact on the service desk is considerable alone. Key findings in this report, supported by other SDI research reveals the true scale password related issues have on a service desk, in some instances becoming accountable for over half of all tickets logged. For many organisations, implementing a solution that offers to remove even a fraction of this burden would be a tempting proposition.

Despite the considerable value that these solutions can bring to an organisation, there is a clear cautionary tale to be taken from this research. The majority of organisations have enjoyed a negligible return on investment, with considerable percentages of password related issues still passing straight through to the service desk. The challenges organisations are facing are clear, however, which can serve as valuable insight for others seeking to implement a solution. For example, a strategy to encourage user adoption underpinned by clear processes owned by the service desk will tackle some of the most common inhibitors to success detailed in this report.

Furthermore, the majority of implemented solutions are based on traditional forms of authentication which offer little likelihood of a smoother user experience. The reliance on security questions, albeit a method widely used in the consumer space, is unlikely to provide a smoother or faster experience for end-users should the service desk solicit similar information. Similarly, the majority of current implementations rely on a single authentication method, presenting potential security issues for organisations and potentially reducing the convenience of the tool if end-users are unable to manage their password outside of certain parameters.

It is evident, then, that for self-service password solutions to be a success, organisations need to implement a tool that has been designed with convenience, and an improved user experience, in mind. A tool that offers users the opportunity to manage their password swiftly and easily is likely to see a much higher adoption rate than many of the organisations that took part in this research. When supported by a well thought out adoption strategy, internal processes and marketing plan, the amount of organisations recognising return on investment should be far more encouraging.

Furthermore, service desks need to lead the charge by pushing the self-service password management tool when talking to customers. Every password related call is an opportunity for analysts to convert users over to the system.

Finally, self-service password management solutions need to be planned out across the entire IT estate to ensure as many systems as possible can be managed through them. If only particular passwords can be managed through the systems, end-users are unlikely to make the solution their first point of call. Only when all of these factors are taken into consideration can service desks start enjoying the returns of a successful self-service password management solution.

FastPassCorp
Password security made easy

About FastPass

FastPass is the leading European solution for corporate self-service of passwords. Combined with “FastPass Best practices” customers achieve high adoption rates of 75-90%. The solution is available on-premise and cloud for AD/Windows password and other corporate passwords. Strong integration to most ITMS systems. FastPassCorp is listed on Nasdaq/Copenhagen/FirstNorth