



Self-Service Password Reset (SSPR)



Contents

3	Summary
5	Definition
8	Benefits of Using SSPR
14	How it Works
16	Customer Success Stories
18	What to Look for in a Solution
20	Conclusion

Are you looking to:



Reduce not only help desk costs, but the associated costs from the loss in productivity for your users.



Set stronger password policies that work with users to improve password management and avoid bad habits.



Eliminate the need for a help desk ticket or a phone call to the service desk to reduce the wait time for users.



Estimated reading time: **10 minutes**

Summary

Today, passwords are a struggle for everyone who uses and supports them. Users have too many **passwords** to manage, and security best practices require them to have complex passwords and change them frequently. All of this causes passwords to be forgotten leading to a call to the help desk and a disruption for the IT team.

Password resets can be a significant drain on **resources**.



To solve these issues and alleviate the stress on your help desk, you should look to Self-Service Password Reset (SSPR). Having an SSPR solution can improve security and productivity for your users while reducing costs for your IT teams, freeing them up to focus on more strategic initiatives.



Definition

Self-Service Password Reset

Self-Service Password Reset (SSPR) is the process that allows users to reset their forgotten password after proving their identity through other means.

Users can utilize multiple authentication methods, including challenge answers, OTPs, or biometrics to identify who they are in order to use the SSPR solution to reset their forgotten password. Many solutions also give users options to recover a password without resetting it and unlock their account.



This decreases frustrations for both employees and the help desk while also improving security measures by decreasing the risk from users sharing passwords, writing them down and re-using the same one for multiple applications. SSPR allows IT directors to enforce stronger password policies including higher character requirements and password expiration knowing their users have a way to quickly reset or recover a password if they forget it.



Without Self-Service Password Reset

Without a Self-Service Password Reset solution, organizations can be inundated with help desk calls and stretched to their limit trying to handle all the password-related requests. The call volume and wait times put a huge strain on both the end-users and the IT support team. Meanwhile, their end-users will continue to struggle with their complex passwords, leading to bad password management as users begin sharing their passwords, writing them down, or re-using the same password across their accounts.





With Self-Service Password Reset

With a Self-Service Password Reset solution, IT administrators can enforce stronger password policies like password expiration and minimum password length while reducing the number of password-related help desk calls. Users can manage their own passwords, so they can continue with their day-to-day activities without calling the help desk.

Benefits of Using SSPR

Organizations use an SSPR solution for many reasons.



Help desk call volumes are reduced.

Password reset tickets drop rapidly, saving the IT department time and money by averting unnecessary time from other projects. There is also a massive decrease in the overall disruption a forgotten password can cause, improving productivity throughout the organization.



Users can manage their passwords without involving IT.

SSPR allows users to reset and manage their own passwords without interrupting their day.





Increased Security by Eliminating Bad Password Habits

IT administrators can enforce stricter password policies, while users are more likely to have better "password hygiene" since they can quickly reset or recover a forgotten password on their own.

Additionally, SSPR can be combined with Multi-factor Authentication (MFA) to make the reset/recovery process more secure by requiring additional credentials for a user to verify they are who they say they are.





Security

Most studies show that the cost of a **password reset** can range from **\$25 to \$75** per incident and account for around **30%** or more of help desk calls.

[Forrester Research](#)

SSPR can reduce costs.

A major benefit with implementing SSPR is that it reduces the costs from help desk calls. Help Desk calls cost a lot of money with the average cost of \$25 to \$30 per call. Other research shows help desk calls cost an organization \$70 from the hourly rate of the help desk and staffing costs.

For IT Administrators, most help desk calls are password-related, ranging from account lockouts, account reactivation, and forgotten passwords. Deploying a self-service password reset solution can curb Help Desk costs, reduce help desk calls,

[Forrester Research](#)





enable end-users to perform better security practices, and save the IT department money. An SSPR solution can cost a mere fraction of what is currently being spent on the password-related help desk calls offering tremendous ROI for organizations who implement it.

How it works: PortalGuard SSPR

BIO-key PortalGuard leverages challenge questions and answers and/or multi-factor authentication to authenticate the user before completing a password reset, recovery, or other self-service actions. Challenge answers are cryptographically hashed and stored on a central server to support roaming users and prevent the need to re-enroll on multiple machines. The following actions can also be performed from mobile devices such as iPads and smartphones. PortalGuard integrates seamlessly with Microsoft Active Directory, Novell eDirectory, any LDAP-compliant directories and custom SQL user repositories.



STEP 1

A user goes to login and forgets their password.

STEP 2

They click the 'Forgot Password' link to start a password reset.

STEP 3

They are prompted by PortalGuard to authenticate using Multi-factor Authentication and answer 2 of 3 previously enrolled challenge questions.

STEP 4

The user is then brought to the password reset screen where they create a new password following the complexity rules IT has configured including length and complexity.





STEP 5

The user completes the password reset and can continue to login with their newly created password.


The Trouble with Help Desk Password Resets

20-50%
of all help desk calls are for password resets


\$25-70
Avg. cost per password reset done by help desk

-  Tedious to navigate to a help desk by telephone or email
-  Most help desk password resets involve a second person
-  Help desk staff could be over-worked or under pressure
-  An unauthorized caller may be impersonating a valid user

Most SSPR solutions provide users with access to a wide range of self-service functionality including:

-  Password Reset
- Password Recovery
- Account Unlock
- Account Info Update
- User Registration

Self-Service Password Reset



Empower end-users with SSPR

Forgot password?

Email

Reset Password

Password reset through IT help desk:

20 mins

Password reset using SSPR solution:




< 1 min

IT admins can also utilize:

- Multi-Factor Authentication
- Single Sign-On

with SSPR to provide a secure and user-friendly experience

Benefits of SSPR

-  Bring Down the Costs
 - help desk costs
 - costs from lost productivity
-  Everyone Saves Time
 - no need to seek help desk for password resets
 - reduce help desk wait times
-  Increased security
 - no SSPR can expose the password to anyone other than the authorized user



Customer Success Stories

NORTHEAST IOWA COMMUNITY COLLEGE

The Northeast Iowa Community College (NICC) was faced with delivering an optimized digital experience while still improving cybersecurity throughout the campus. They were able to secure new services like GSuite for students without adding extra friction around logging in.

CITY OF SACRAMENTO

With a population of 500,000 citizens, the City of Sacramento needed a SSPR solution that would enhance security and relieve pressure on their help desk. Because of SSPR, they were able to significantly reduce help desk calls related to account lockout and password resets.

Did you know:

90%

Northeast Iowa Community College experienced a 90% decrease in password reset calls.


[Northeast Iowa Community College](#)

Did you know:

95%

The City of Sacramento experienced a 95% decrease in password reset calls.

[City of Sacramento](#)

A person is seen from behind, wearing large headphones and working at a desk. They are looking at a computer monitor which displays a web application with various data fields and buttons. The person is positioned in front of a large window that offers a view of a sunset or sunrise, with the sun low on the horizon and the sky filled with soft, orange and yellow clouds. The room is dimly lit, with the primary light source being the natural light from the window. On the desk, there are some items including a water bottle and a bag with the text 'ART NEW YORK' visible.

What to look for in an SSPR Solution

What to Look for

When searching for an **SSPR solution**, knowing what to expect and what to consider is vital to getting a solution that helps both your users and your IT team.

EASY INTEGRATION

One of the main reasons you are looking to deploy SSPR is to streamline access. This should start from the beginning with installing the solution in your environment. Your ideal Self Service Password



Reset solution should be a plug and play set up, integrating seamlessly with whatever your identity repository may be: Active Directory, general LDAP, or even custom SQL tables.



CONSISTENT USER INTERFACE

Keeping a consistent UI is important to reduce user training and increase adoption of SSPR. Furthermore, it is important that the UI is cross functional and will appear the same no matter if the user is operating on a Mac, PC, tablet, or mobile phone. Additional features should also be considered in your evaluation including visual indicators of password complexity rules when a user creates their new password.

GREAT TECHNICAL SUPPORT

Choosing a company that backs their product with excellent technical support is a must. This means finding a vendor that does **NOT** farm out their solution to a third-party service, that has no real experience with the product, or is only reading from scripts. Great technical support teams will partner with your IT team and focus on making sure your users maintain their productivity.

Conclusion

Reducing password-related help desk calls not only benefits end-users, but also the IT support team. SSPR will empower your users to manage their own passwords and practice better, more secure password management. Users are satisfied with having a way to manage their passwords, whether they are in office, on the go, or during off hours, without having to contact the help desk.

For IT, an SSPR solution will reduce costs, avoid team burnout, and free them up to focus on more strategic projects.



Try SSPR Today!

BIO-key's [PortalGuard](#) solution enables users to complete multiple self-service actions including:

- Password resets
- Password recoveries
- Offline password recoveries
- And account unlocks

Beyond Self-Service Password Reset, PortalGuard is an award-winning Identity-as-a-Service (IDaaS) platform with multiple layers of functionality to help you achieve your security goals, including multi-factor authentication, contextual authentication, single sign-on, and industry-leading identity-bound biometric authentication.

[Sign-up for a Free Trial of PortalGuard](#)

Try [PortalGuard IDaaS](#) and its flexible options for meeting your security goals and delivering an optimized user experience.

WHAT'S INCLUDED:

- [Multi-factor Authentication](#)
- [Single Sign-on](#)
- [Self-Service Password Reset](#)
- [BIO-key MobileAuth](#)

More information available at:

<https://www.bio-key.com/self-service-password-reset/>

If you have any questions, feel free to contact us:

<https://www.bio-key.com/contact-us/>

About BIO-key International

BIO-key International is a trusted provider of Identity Access Management and Identity-Bound Biometric solutions that enables convenient and secure access to devices, information, applications, and high-value transactions.

BIO-key offers the simplicity and flexibility required to secure the modern digital experience for on-prem and remote users, while easing the burden on IT teams. Backed by decades of expertise, BIO-key has a proven track record of successful IAM project delivery, strong partner relationships, and low TCO.

