A BIO-key® Solution.

Tech Brief

Centralized Self-Service Password Reset

Table of Contents

Table of Contents

Summary

Supporting an entire user base can be taxing for IT departments of all sizes – especially on the administrative side of things. Most studies show that the cost of password resets can range from $25 to $75 per incident and account for around 30 percent or more of help desk calls. This provides ample reason and demand for password reset and recovery tools which empower the end-user with self-service.

Unfortunately, shopping for a self-service tool isn't always easy. To simplify matters, the first step is to understand the scope of your requirements by documenting your user access scenarios. For example, how will roaming users change their passwords remotely, or how will a forgotten password be recovered on a laptop with an encrypted hard drive? Along with these requirements, determining your budget and current help desk costs without a solution in place will allow you to forecast your Return on Investment (ROI) and further narrow down the vendor selection.

Another point to consider is the evolution of self-service password reset and whether or not the vendors that you are evaluating are keeping pace. You'll find that, on their own, many tools are not fully compliant with the security standards of most companies.

The problem of forgotten passwords has been around since passwords were first used, but expanding access scenarios and advanced attacks are requiring the adoption of more advanced solutions.

For example: Simply providing basic password reset is no longer enough in the current digital climate. An entry point solution is now expected to provide options for additional scenarios, such as

- Offline or disconnected users who need to reset or recover a password
- Advanced auditing and reporting functionality
- Ability to leverage personal devices (such as mobile phones)

True success of a Self-Service Password Management solution is measured by user satisfaction and return on investment through reduced password-related helpdesk calls.

"By allowing users to self-service their own account and password management needs, organizations can effectively offer 24/7 access and maintain productivity. "

The Basics

What Is Self-Service Password Reset?

Self-service Password Reset (SSPR) is the process by which a user is able to reset a forgotten password through his or her own efforts, without the need to involve a third party (such as the local help desk).

NOTE: Self-Service Password Recovery is similar, but the goal is to obtain the current password without changing it.

In order to achieve either of the above noted functionalities, the user can be authenticated using various methods.

Most tools use challenge questions and answers as an acceptable means of authentication. While still a valid choice today, associated security threats - including easily guessed answers or information that is readily available on social media - raise valid concerns. A secure solution puts additional precautions in place.

Some precautions that should be in place to help mitigate any risk inherent in password reset and recovery include:

- Requiring different answers for each question.
- Requiring a Minimum Password Length
- Requiring a larger number of answered questions (e.g. three out of six total)

PortalGuard Centralized SSPR

The PortalGuard Self-Service Password Reset solution is a complete, flexible option that provides users with access to a wide range of self-service functionality. PortalGuard is continually evolving to meet industry demands, and provides the same interface and functionality across Windows and Mac desktops, as well as in a web-based portal - minimizing the initial learning curve and promoting user adoption.

The three major components of PortalGuard Self-Service are:

- Password Reset
- Password Recovery
- Account Unlock

For increased usability and ease of access, each of these features can be accessed on various mobile devices, including tablets (both Android and Apple-based) and smartphones. There is even a mobile application for end-users to download (See **SSPR Mobile App** section below for more details).

Additional Information

Administrative

- Help Desk Console - provide interface for Help Desk staff to easily perform account actions
- Verbal Authentication - allows help desk to authenticate a user calling in
- Administrator Auditing Dashboard - logging and reporting of user access activity

General Features

- Forced user enrollment (optional)
- Offline/Disconnected user support
- Encrypted hard drive support - perform a password recovery through PortalGuard on an alternate or mobile device (e.g. Symantec Endpoint Encryption)
- Multiple Authentication method support (e.g. challenge questions/answers, Two-Factor Authentication, etc.)
- Email notifications for password resets to the user and/or admin
- Configurable Lock-out thresholds for incorrect responses to authentication attempts
- Support for various mobile browsers

Challenge Questions & Answers

- Centralized - challenge information stored on server
- Configurable number of mandatory/optional questions
- Allows import/pre-population of challenge answers
- Prevent repeat answers for multiple challenge questions
- Prevent answers from containing words from the question text
- Answers can be case sensitive
- Configurable minimum length for challenge answers

Integration Methods

Direct Web Access

For customers without a central portal already in place, PortalGuard provides a direct web access portal for Password Reset and associated password management functionality. Through this web portal, users can change or enroll phone numbers for Two-Factor Authentication, update/change challenge questions/answers, etc.

Sidecar Mode

PortalGuard can enhance the login process for remote HTTP servers on which PortalGuard is not directly installed. This is referred to as "Sidecar" mode.

A small JavaScript library is added to the login form for the target HTTP server. This new code temporarily suppresses the login to the target server and calls out to the PortalGuard server instead. PortalGuard validates the user's credentials and verifies that the user does not need to take any specific PortalGuard actions (e.g. setting challenge answers).

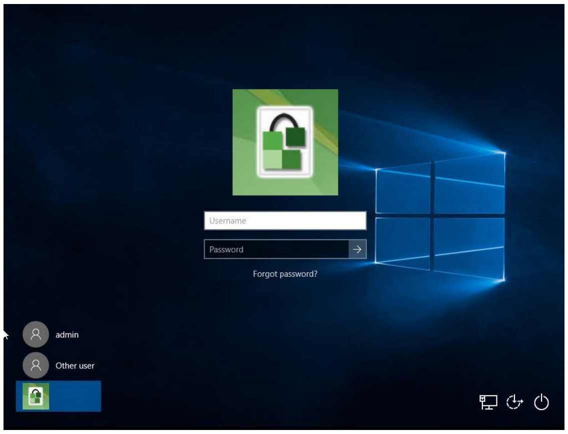
If PortalGuard requires the user to take action, a floating frame appears over the top of the target server's HTML login form. The user uses this frame to perform the requested action directly against the PortalGuard server. Once no further action is required, the floating frame is closed and the original login attempt to the target server proceeds as normal. If no PortalGuard action is required of the user, then the floating frame never appears and the login attempt passes directly to the target server.

Sidecar mode achieves a high level of integration to existing login forms without requiring any changes to the target server's back-end or authentication configuration. This allows for simple addition of "Forgot password?" links directly to normal login forms, allowing the PortalGuard "Reset Password" wizard to appear on demand. By leaving preexisting login forms intact, end-user training, development changes and administrative overhead are almost completely eliminated.

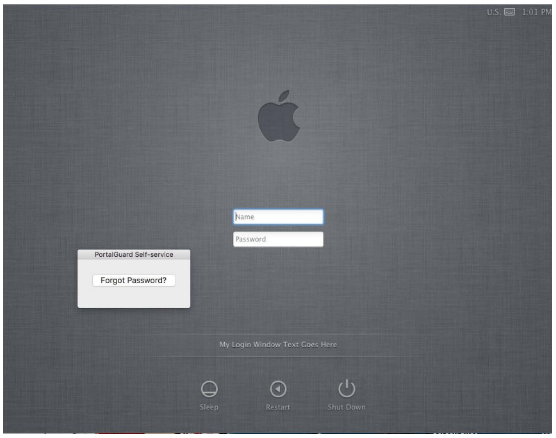
Desktop Password Reset

Support Multiple Windows-based Operating Systems

- Windows 8.1
- Windows 10
- Microsoft Terminal Services
- Remote Desktop Services



While using a PortalGuard SSPR on a Windows Operating System, users can have access to Self -Service directly from the login screen, or by using the Ctrl+Alt+Del shortcut when already logged in. This functionality removes the need to access an alternate machine/kiosk or login with a guest account in order to reset or change a password.



Supports MAC OS Versions 10.13 and later, including:

- Catalina
- Mojave
- High Sierra

On a Mac, users can reset or change their domain password directly from the login screen. PortalGuard also allows for the recovery of the Mac OS X Keychain Password in the event that a user forgets it, and still needs access to the passwords stored on the machine.

Mobile Password Reset App

For environments where convenience and security must go hand in hand, PortalGuard has an answer: the Mobile Password Reset App. In an age where the mobile phone has taken over virtually every vertical – from educational environments to financial institutions – PortalGuard turns a common personal device into a useful tool for both managing passwords and adding a second factor, all in one application.

The three major features of the Mobile Password Reset App are:

- One-touch Password Reset
- Familiar Password Generator
- Mobile Time-based One-Time Password (TOTP) generator

One-Touch Password Reset

Not only does our mobile app provide a simple method for resetting a password, the changes take effect immediately. There is no waiting for updated credentials to synchronize with the local server, and users can get back to doing the work that matters. Just type in a new password and tap 'Reset Password'. It's that simple.

Familiar Password Generator

Creating a memorable password that is also complex and secure enough to last is often a difficult process. Users are more likely to choose weak passwords than to put in the effort this process entails. The mobile app offers a solution for these issues in the familiar password generator.

The steps are simple:

- Answer a few personal questions that only the user would know
- Tap 'Personalized Password'
- Set the new, uniquely familiar password as described above

Time-based OTP

The mobile app also removes the need to download a separate application, or deal with extra hard tokens for Two-Factor Authentication. By providing a continuously cycling One-Time Password, users have simple access to a ready-to-go TOTP through a familiar interface.

How the TOTP Works:

- User Enrolls the phone with PortalGuard by scanning a QR Code
- The OTP Seed is synchronized alongside the QR Code during enrollment
- The phone becomes a shared secret between the user and PortalGuard
- Added visual timer to illustrate OTP generation and expiration

The PortalGuard Mobile Password Reset App integrates easily with any environment, without requiring additional effort on the part of administrators or users. Simply by using an interface and familiar operating systems, end-users have the power of secure password management in the palm of their hands.

Our app is available on both major mobiles operating systems; Get it on iTunes or Google Play today!

Identity Federation

PortalGuard SSPR can also be integrated with Identity Federation while providing Single Sign-On capabilities. Through Identity Federation, PortalGuard provides users with the ability to manage and reset a single password that is usable, strong, and secure, and use that password to gain access to various applications.

For more information, download our **Single Sign-On Tech Brief**

The Benefits of Self-Service Password Reset

- Increased Usability - users have the ability to enact all password management functions via Self-Service, without involving a third-party (e.g. help desk support).

- Increased Security - Works alongside Knowledge-Based and Two-Factor Authentication.

- Centralized Solution - Same user interface for the Web and Mac/Windows Desktop.

- No Kiosks - perform all self-service actions directly on the user's machine.

- Reduced Costs - alleviate password-related help desk calls and demands on IT staff.

- Configurable - Administrators can specify configuration at the user, group or application levels.

- Seamless Integration - Works alongside existing application portals via 'Sidecar Mode', as well as on Mac, Windows and Mobile devices.

How It Works

The following steps illustrate the processes of user enrollment and resetting a password using the PortalGuard self-service functionality. The screenshots provided show the process being completed from a web browser, but the user can also complete each process from either the Windows or Mac desktop, using the same steps and an identical interface.

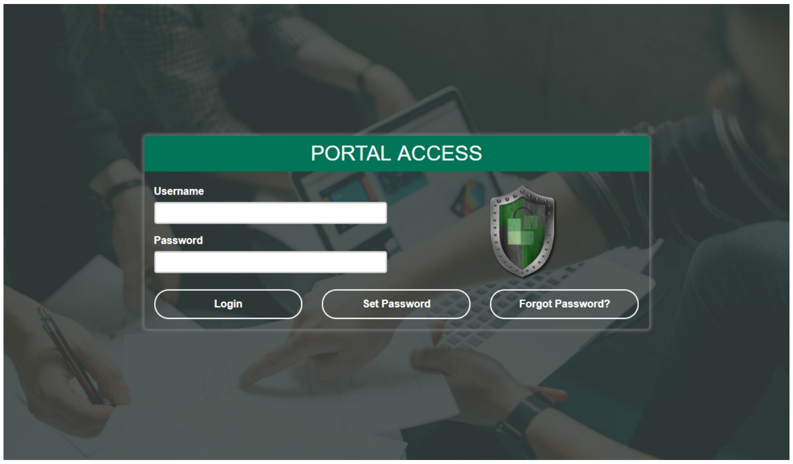
Enrollment

When the user attempts to access the password reset functionality for the first time, he or she will be guided through a series of enrollment steps. Depending on the authentication methods configured by the admin for that particular user, multiple authentication types may need to be enrolled (e.g. challenge questions, mobile authenticator, hard-token two-factor, etc.).

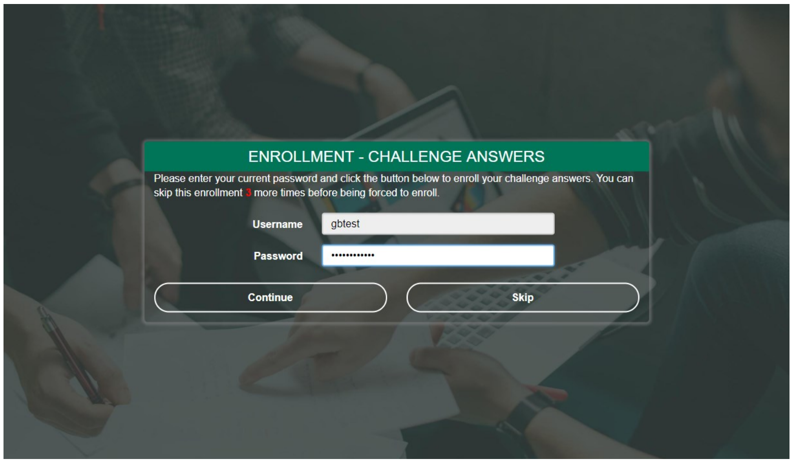
In order to promote convenience, PortalGuard provides flexibility by allowing the configuration of enrollment for each authentication type to either be forced immediately, or able to be postponed “x” number of times. This increases the usability for users, simplifying a task that may otherwise be found to be obstructive.

Enrollment Process

Step 1: The user attempts to login the new PortalGuard-associated portal.



Step 2: If the user has not yet enrolled, PortalGuard automatically displays the enrollment screen. In this example, the user account has Challenge Questions configured to complete a successful password reset.



ENROLLMENT - CHALLENGE ANSWERS

Please enter your current password and click the button below to enroll your challenge answers. You can skip this enrollment 3 more times before being forced to enroll.

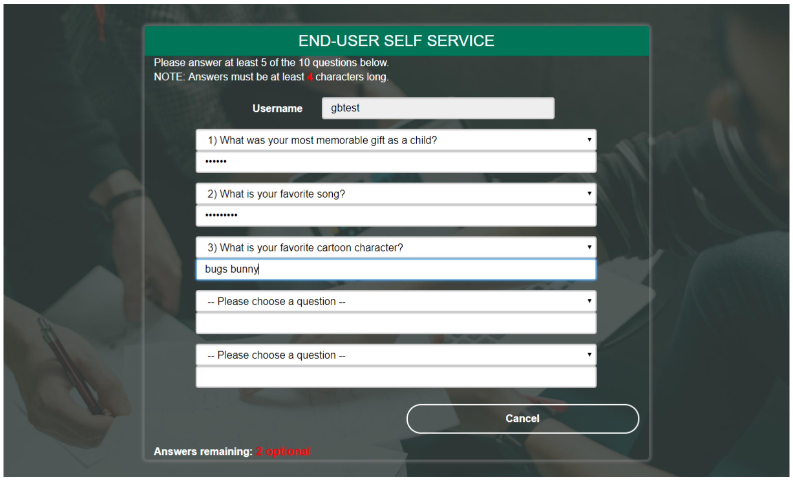
Username: gbtest

Password: ••••••••••••

Step 3: The user is prompted to provide answers to a certain number of challenge questions. The number of both mandatory and optional questions that the user is required to answer is configurable. PortalGuard also increases security by helping the user stick to best practices for challenge answers, such as:

- no repeat answers
- avoiding the use of words which are included in the question text.
- noting that answers are case-sensitive

Throughout the enrollment process, the user is also provided with helpful warning notices - such as the number of answers remaining - in order to ease the frustrations that some may feel during this process.



END-USER SELF SERVICE

Please answer at least 5 of the 10 questions below.
NOTE: Answers must be at least 4 characters long.

Username: gbtest

1) What was your most memorable gift as a child? ▾
••••••

2) What is your favorite song? ▾
•••••••••

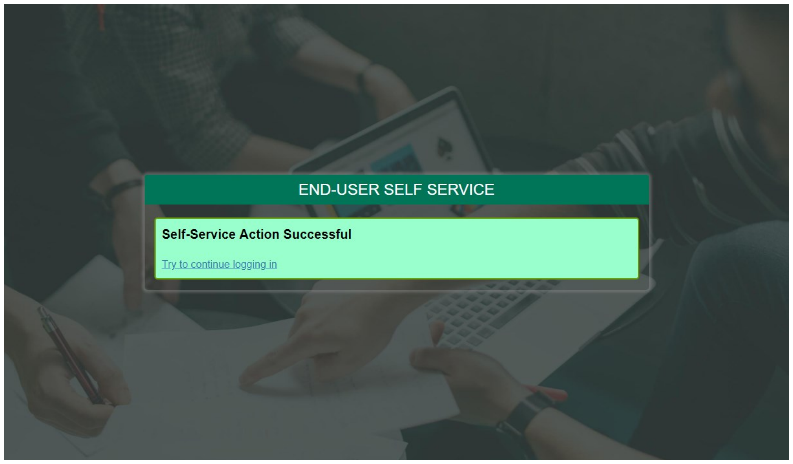
3) What is your favorite cartoon character? ▾
bugs bunny

-- Please choose a question -- ▾

-- Please choose a question -- ▾

Answers remaining: 2 optional

Step 4: Once the user answers the required number of questions, the process is complete and the user is enrolled. Clicking the provided link will close the PortalGuard dialog and continue the original login process.



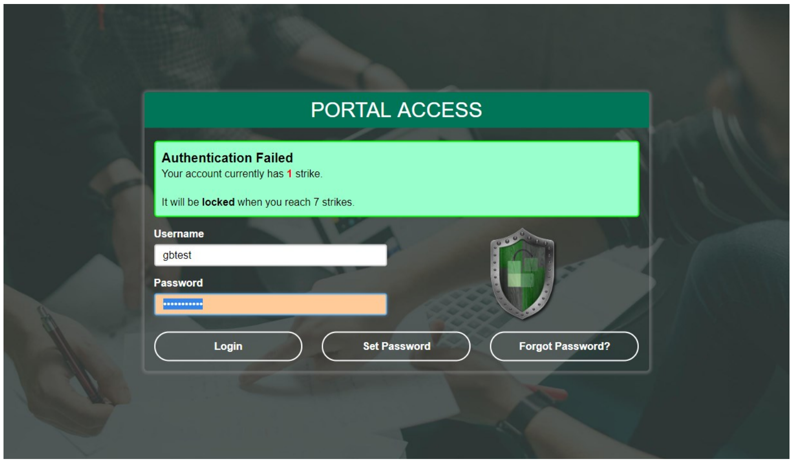
END-USER SELF SERVICE

Self-Service Action Successful

Try to continue logging in

Self-Service Password Reset Process

Step 1: The user attempts to login to the existing company portal, but has forgotten his or her password. The user then clicks the “Forgot your password?” link.



PORTAL ACCESS

Authentication Failed
Your account currently has 1 strike.

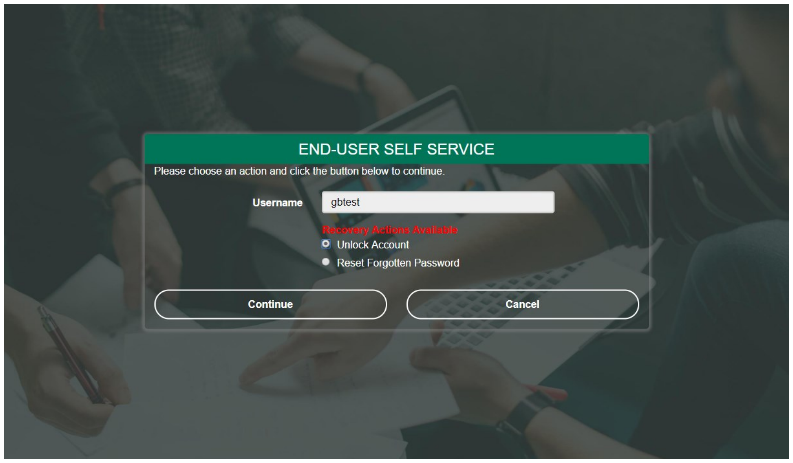
It will be **locked** when you reach 7 strikes.

Username: gbtest

Password: ••••••••••••

Step 2: From the “Recovery Actions Available” section, the user chooses which self service action should be performed. To reset a password, the user chooses the “Reset Forgotten Password” radio button and clicks “Continue”.

NOTE: The dialog shows the most common actions, an account unlock and password reset, but password recovery is also available.



END-USER SELF SERVICE

Please choose an action and click the button below to continue.

Username: gbtest

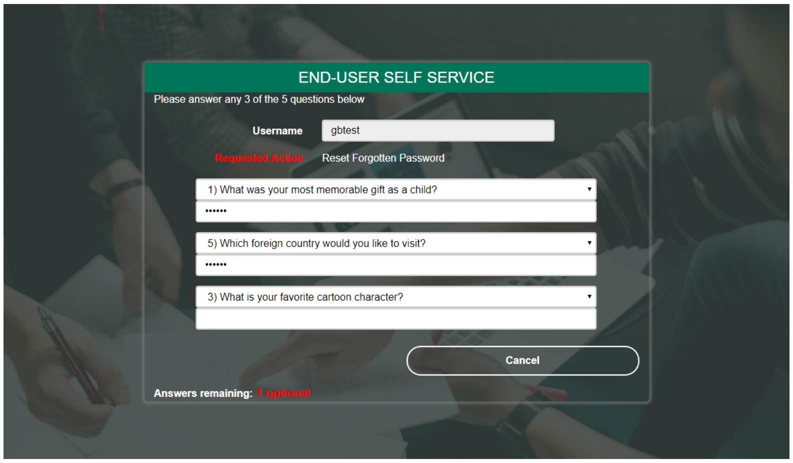
Recovery Actions Available

● Unlock Account

○ Reset Forgotten Password

Step 3: The user is then prompted to choose a method to authenticate before being able to reset the password. For this example, the user is ask to provide the correct answers to the previously enrolled challenge questions. PortalGuard provides helpful warning messages throughout this process.

Once the user has supplied the required number of answers, the ‘Continue’ button will be available to click.



END-USER SELF SERVICE

Please answer any 3 of the 5 questions below

Username: gbtest

Requested Action: Reset Forgotten Password

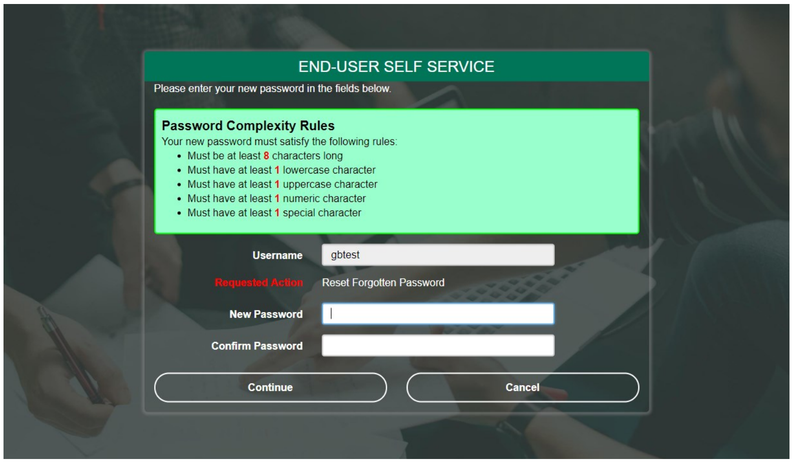
1) What was your most memorable gift as a child?
••••••

5) Which foreign country would you like to visit?
••••••

3) What is your favorite cartoon character?

Answers remaining: 1 optional

Step 4: The identity of the user is then verified, and the user is able to set a new password. For added usability the required complexity rules are shown and give visual indication when they're met as the user enters their new password.



END-USER SELF SERVICE

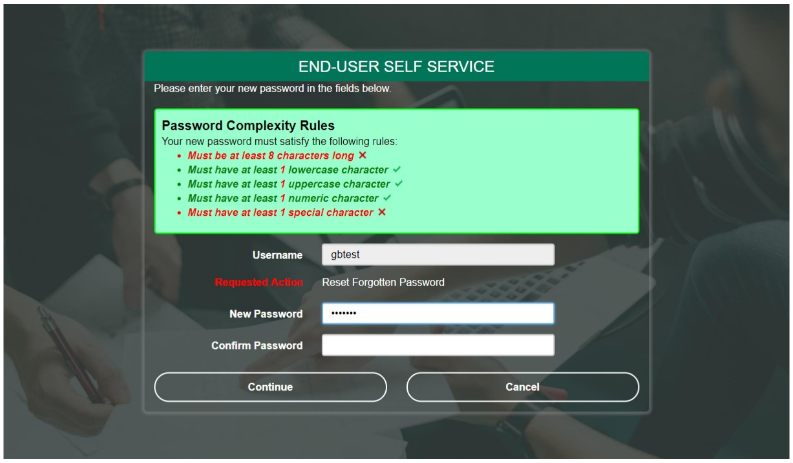
Please enter your new password in the fields below.

Password Complexity Rules

Your new password must satisfy the following rules:

- Must be at least 8 characters long
- Must have at least 1 lowercase character
- Must have at least 1 uppercase character
- Must have at least 1 numeric character
- Must have at least 1 special character

Username	gbtest
Requested Action	Reset Forgotten Password
New Password	|
Confirm Password	



END-USER SELF SERVICE

Please enter your new password in the fields below.

Password Complexity Rules

Your new password must satisfy the following rules:

- *Must be at least 8 characters long* ✗
- *Must have at least 1 lowercase character* ✓
- *Must have at least 1 uppercase character* ✓
- *Must have at least 1 numeric character* ✓
- *Must have at least 1 special character* ✗

Username	gbtest
Requested Action	Reset Forgotten Password
New Password	•••••••
Confirm Password	

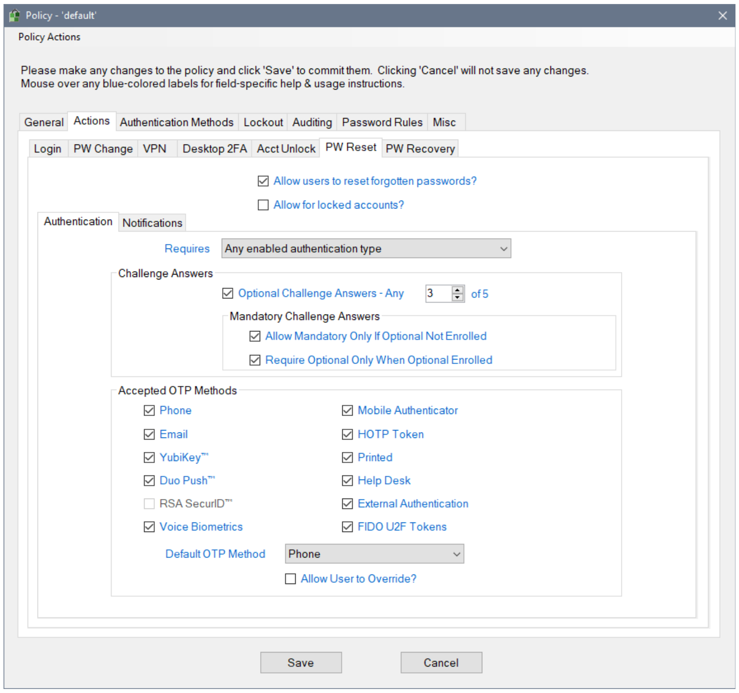
Configuration

NOTE: All the following settings are policy specific; different values can be set for each user, group, or hierarchy as necessary.

Configurable through the PortalGuard Configuration Utility

Main

- Self-Service options available to users
- Authentication types available for each Self-Service action


Policy - 'default'
Policy Actions

Please make any changes to the policy and click 'Save' to commit them. Clicking 'Cancel' will not save any changes.
Mouse over any blue-colored labels for field-specific help & usage instructions.

General | Actions | Authentication Methods | Lockout | Auditing | Password Rules | Misc
Login | PW Change | VPN | Desktop 2FA | Acct Unlock | PW Reset | PW Recovery

☑ Allow users to reset forgotten passwords?

☐ Allow for locked accounts?

Authentication | Notifications

Requires: Any enabled authentication type

Challenge Answers

☑ Optional Challenge Answers - Any 3 of 5

Mandatory Challenge Answers

☑ Allow Mandatory Only If Optional Not Enrolled

☑ Require Optional Only When Optional Enrolled

Accepted OTP Methods

☑ Phone

☑ Email

☑ YubiKey™

☑ Duo Push™

☐ RSA SecurID™

☑ Voice Biometrics

☑ Mobile Authenticator

☑ HOTP Token

☑ Printed

☑ Help Desk

☑ External Authentication

☑ FIDO U2F Tokens

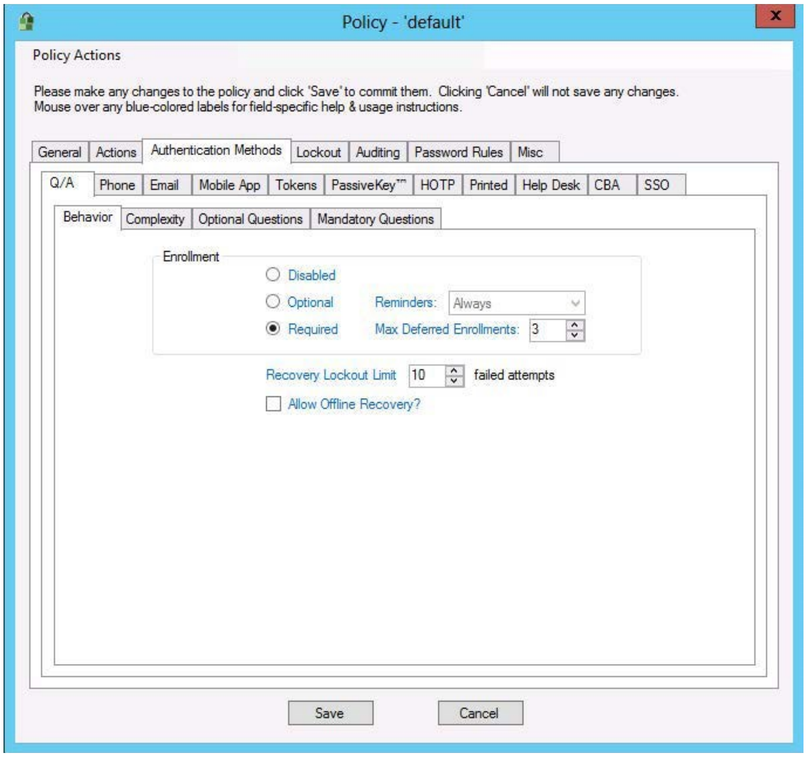
Default OTP Method: Phone

☐ Allow User to Override?

Authentication Types

- Challenge Questions and Answers
  - Enrollment - optional, required, disabled
  - Recovery lockout limit
  - Answer complexity including minimum length, case sensitivity, prevent answer repetition and prevent question words as answers
  - Number of optional questions
  - Number of mandatory questions

- Mobile Phone
  - Enrollment - optional, required, disabled
  - Phone number format
  - Delivery format
- Email
  - Enrollment - optional, required, disabled
  - Domain blacklist
  - Email display
  - Email format including From, Subject and Body fields
- Notifications
  - Type of Self-Service including Account Unlock, Password Reset and Recovery



Policy - 'default'

Policy Actions

Please make any changes to the policy and click 'Save' to commit them. Clicking 'Cancel' will not save any changes.
Mouse over any blue-colored labels for field-specific help & usage instructions.

Enrollment

○ Disabled

○ Optional — Reminders: Always

● Required — Max Deferred Enrollments: 3

Recovery Lockout Limit 10 failed attempts

□ Allow Offline Recovery?

Installation

Implementation of the PortalGuard platform is seamless and requires no changes to existing Active Directory/LDAP schema. For an on-premises solution, a server-side software installation is required on at least one IIS server. However, PortalGuard Self-Service Password Reset is also available through our cloud-hosted Nebula platform.

In order to perform Self-Service from the Login screen via Desktop Password Reset, an additional client-side software installation is required.

IIS Installation

An MSI is used to install PortalGuard on IIS 10. If installing PortalGuard on IIS 8.5/ Windows Server 2012 R2, make sure to have installed the following feature roles prior to launching the MSI:

1. All the Web Server Management Tools role services
2. All the Application Development role services
3. All IIS 8.5 Management Compatibility role services

The MSI is a wizard-based install which will quickly guide you through the installation.

System Requirements

PortalGuard supports both direct access and authentication to cloud/web-based applications. PortalGuard has the following requirements:

Server Requirements

PortalGuard is fully supported for installation on physical and virtual machines. PortalGuard supports running on the following platforms:

- Microsoft Windows Server 2012 / R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019