

A BIO-key® Solution.

Tech Brief

# **Configurable Password Management: *Balancing Usability and Compliance***

# Table of Contents

<b>Summary</b>	<b>3</b>
<b>The Basics</b>	<b>4</b>
<b>PortalGuard Password Management</b>	<b>5</b>
<b>Features</b>	<b>6</b>
<b>Benefits</b>	<b>7</b>
<b>How It Works</b>	<b>8</b>
Password Policies	8
Policy Search Order and Precedence	9
User Profiles	9
Step-by-Step Process	10
<b>Configuration</b>	<b>13</b>
<b>Deployment</b>	<b>18</b>
<b>IIS Install</b>	<b>18</b>
<b>System Requirements</b>	<b>18</b>
<b>Schedule a Demo</b>	<b>19</b>
<b>Platform Layers</b>	<b>20</b>

# Summary

---

Implementing strong authentication security for web-based applications before deployment to your production environment is the ideal approach however, many projects take longer than expected so some applications are deployed without security policies in place, such as password quality, password expiration and strike counts.

Password management is usually added later when a security audit uncovers an application as being non-compliant. To make a web-based application compliant, you need to decide whether to build or buy a complete authentication security solution. Buying an off-the-shelf solution, such as PortalGuard, offers the much needed enterprise-ready security functionality that easily integrates into your existing web-based and SQL applications.

Sometimes developers may not consider the organization's data accessed by the web-based application to be sensitive and therefore, increasing security becomes a secondary consideration during deployment. A low risk application may require either no authentication or the use of just a username and password, though this approach should not be used in applications with medium or high risk. Please review other PortalGuard tech briefs on increasing web-based authentication security with approaches such as Contextual and Two –Factor Authentication. These tech briefs provide more information on the security risks of using just passwords as a single barrier to blocking unauthorized access to your organization's data.

# The Basics

---

Passwords remain an important aspect of authentication security. A poorly chosen password may result in unauthorized access and/or exploitation of an organization's resources and critical data. The purpose of password management policies is to establish and enforce the security standard for the creation of strong passwords, the protection of those passwords, and the frequency of which to change them.

However, one of the first steps to password management is educating your users on password best practices via a security awareness program with information such as:

- Never share your account
- Never use the same password for multiple systems
- Never tell a password to anyone, including those claiming to be from security or customer service within your organization
- Never write down a password
- Never provide a password over the phone, e-mail or instant messaging
- Make sure to log off or lock your workstation before leaving a computer unattended
- Change your password whenever you suspect it may have been compromised
- Passwords should be alpha-numeric at a minimum

General password management best practices provide the foundation for strong organizational security policies, including:

- How complex a password needs to be should be based on risk
- The frequency to which you change your passwords should be based on risk
- At all points, passwords should be protected from being exposed

# PortalGuard Password Management

---

PortalGuard's password management goes beyond the foundational principles and provides enhanced functionality which improves the security of passwords while improving usability for users. This is done with features such as strong password policy enforcement, password synchronization, and Self-Service Password Reset. By creating this balance between security and usability PortalGuard can significantly reduce Help Desk calls and increase user adoption

To provide you with flexibility, PortalGuard's password management policies can be configured down to the individual user, group or domain hierarchy, enforcing the appropriate level of security for each.

# Features

---

- Password Complexity - customizable rules for minimum and maximum length, and uppercase, lowercase and special characters. Complexity checks can also be performed during each login to assure compliance.
- Password History - prevent users from reusing their last "n" passwords
- Password Expiration - set expiration and grace periods
- Strikeout/Lockout Limits - enforce a configurable number of strikes before an account lockout and optionally specify a minimum "lockout time" the user must wait before the account is automatically unlocked and they can again attempt to login
- Prevent Users from Sharing Credentials - limit multiple concurrent logon sessions
- Lockout Inactive User After "n" Days - identify and stop access from dormant user accounts
- Help Desk/Verbal Authentication - prove user's identity when calling into the Help Desk by answering a series of challenge questions
- Email Calendar Reminders - set reminders in user's email client calendar of upcoming password expirations
- Password Meter - provide users with visual clue of the strength of the password when resetting or creating one
- Auditing/Logging - record user login activity including invalid usernames, last login, last password change, etc.
- Administrative Dashboard - provides administrators with a snapshot of recent user login activity
- Tailored Authentication - extend the PortalGuard framework to include specific functionality which provides an exact fit with your requirements

# Benefits

---

- Configurable - to the individual user, group or domain hierarchy
- Increased usability – maintains user productivity and satisfaction with functionality such as the password strength meter, email calendar reminders, and Self-Service Password Reset
- Increased security – prevents both common password and code injection attacks by enforcing strong password management best practices
- Balances security and usability – with functionality to support both compliance and user demands
- Implement password best practices – including account lockout limit, unlock threshold, and password history
- Compliance – web-based and SQL applications now meet required industry and regulatory standards
- Cost effective – reduce password related Help Desk calls

# How It Works

---

## Password Policies

PortalGuard uses the concept of policy-based security settings to enforce password management rules for users. You can have multiple sets of rules defined within PortalGuard. Each set of rules is referred to as a policy. You can then assign users to a policy on an individual basis or by a group or domain hierarchy. If a policy is not applied to anyone, then its rules will never be enforced. Policies can be enabled or disabled. Only policies which are both enabled and have users assigned to them are enforced by PortalGuard.

There are key aspects to each password policy including password length, formation, duration and practice. With those in mind you can define password policies so that all user accounts are protected with strong passwords. Below are examples of policies you can enforce:

- Define password history policy setting so that several previous passwords are remembered. With this policy setting, users cannot reuse old passwords when their password expires.
- Define the maximum password age policy setting so that passwords expire as often as necessary for your environment, typically, every 30 to 90 days. With this policy setting, if an attacker cracks a password, the attacker only has access to the network until the password expires.
- Define the minimum password age policy setting so that passwords cannot be changed until they are more than a certain number of days old. This policy setting works in combination with the password history policy setting. If a minimum password age is defined, users cannot repeatedly change their passwords to get around the password history policy setting and then use their original password. Users must wait the specified number of days to change their passwords.
- Define a minimum password length policy setting so that passwords must consist of at least a specified number of characters. Long passwords--seven or more characters--are usually stronger than short ones. With this policy setting, users cannot use blank passwords, and they have to create passwords that are a certain number of characters long.

## Policy Search Order and Precedence

With policies capable of being applied to individual users, groups and domain hierarchies, it is a common occurrence for a user to have multiple policies applied to them. At run-time however, only a single policy will be enforced for the user. This disparity is resolved by searching for applicable policies in the following manner with each subsequent search becoming a less explicit match:

1. Policies applied directly to a user
2. Policies applied to a group
3. Policies applied to a domain or OU
4. The default policy

## User Profiles

User profiles are where PortalGuard's user-specific information is stored. Some examples of the data include, but are not limited to:

- Strike count
- Last login time
- Password expiration date
- Hashed answers to challenge question
- Last password change time
- Accepted Terms of Use time

A profile is created for each user automatically as they log in through PortalGuard so it is not necessary to preload any user accounts. These user profiles can be stored as flat files on the PortalGuard server or in a SQL database for accessibility in clustered configurations.

## Step-by-Step Process

**Step 1:** The user's password is expired, but within the grace period. PortalGuard notifies the user, but provides the option of temporarily skipping the password change and going directly into the application because they are still in the grace period. The user defers the password change by clicking the link shown and is allowed to login.



**Step 2:** A few days later, the user attempts to log in and the password is now expired. PortalGuard enforces this by requiring the user to change their password before being allowed into the application.



- a. If PortalGuard is configured to use a password meter, it is automatically updated as the user types their new password. Only when the new password is sufficiently complex will the user be allowed to submit the password change.

**Set Password**  
Please provide your username, current password and new password in the fields below

Username  
stewie

Password  
..... Show password(s) ☐

New Password  
..... Strong

Confirm New Password  
.....

Set Password Cancel

b. If PortalGuard is configured to use standard password quality rules, the user is notified which rules have been satisfied by the new password and which must still be addressed.

**Set Password**  
Please provide your username, current password and new password in the fields below

**New Password Insufficiently Complex**  
Your new password must satisfy the following rules:

- Must be at least 6 characters long **(Failed)**
- Must have at least 1 lowercase character **(OK)**
- Must have at least 1 uppercase character **(OK)**
- Must have at least 1 numeric character **(Failed)**

Username  
stewie

Password  
..... Show password(s) ☐

New Password  
.....

Confirm New Password  
.....

Set Password Cancel

**Step 3:** When password history is enabled, a password that satisfies the complexity rules may still be rejected by the PortalGuard server for being previously used by the user.



**Set Password**  
Please provide your username, current password and new password in the fields below

**Password Cannot Be Reused**  
Your new password cannot match previously used passwords

Username: stewie

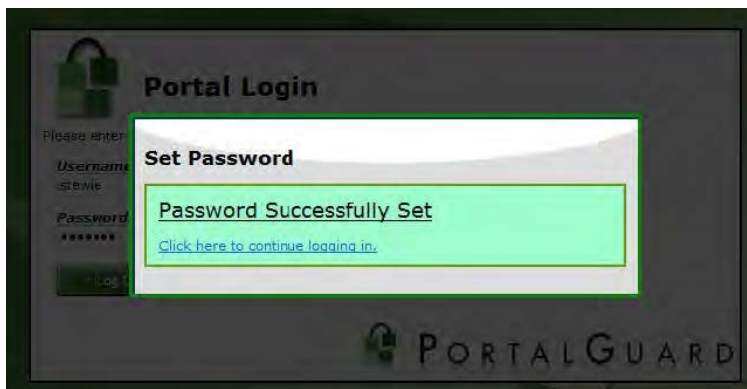
Password: [masked] Show password(s) ☐

New Password: [masked]

Confirm New Password: [masked]

Set Password Cancel

**Step 4:** Once the new password is acceptable, PortalGuard changes it in the target user repository (e.g. Active Directory, LDAP or a custom SQL table) in real-time and notifies the user of the success.



**Portal Login**

**Set Password**

**Password Successfully Set**

[Click here to continue logging in.](#)

PORTALGUARD

**Step 5:** If a password minimum age is enabled and the user attempts to manually change their password again, PortalGuard will prevent it.



**Set Password**  
Please provide your username, current password and new password in the fields below

**Password Cannot Be Changed**  
Your password cannot be changed because it is not old enough  
You must wait another 60 minutes

Username: stewie

Password: [masked] Show password(s) ☐

New Password: [masked]

Confirm New Password: [masked]

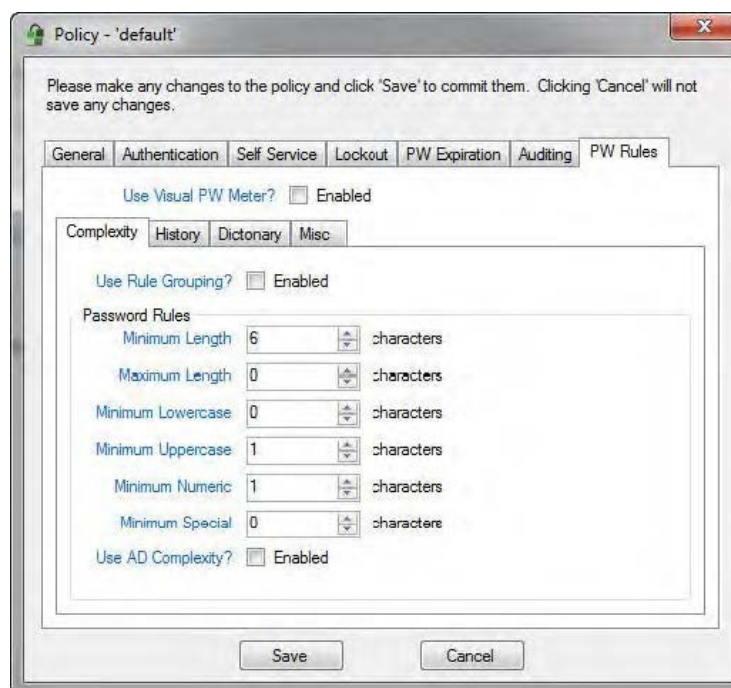
Set Password Cancel

# Configuration

**NOTE:** All the following settings are policy specific, so you can have different values for different users/group/hierarchies.

## Configurable through the PortalGuard Configuration Utility:

- Password Rules (Policies):
  - Minimum length
  - Maximum length
  - Minimum lowercase
  - Minimum uppercase
  - Minimum numeric
  - Minimum special
  - Active Directory Complexity



- Rule Grouping - for combining standard password rules into pools where only a subset must be met

Policy - 'default'

Please make any changes to the policy and click 'Save' to commit them. Clicking 'Cancel' will not save any changes.

General Authentication Self Service Lockout PW Expiration Auditing **PW Rules**

Use Visual PW Meter? ☐ Enabled

Complexity History Dictionary Misc

Use Rule Grouping? ☒ Enabled **Any 1 of 2** Grouped?

Password Rules

Minimum Length	6	characters	<input type="checkbox"/>
Maximum Length	0	characters	<input type="checkbox"/>
Minimum Lowercase	0	characters	<input type="checkbox"/>
Minimum Uppercase	1	characters	<input checked="" type="checkbox"/>
Minimum Numeric	1	characters	<input checked="" type="checkbox"/>
Minimum Special	0	characters	<input type="checkbox"/>

Use AD Complexity? ☐ Enabled

Save Cancel

- Enable/Disable Password Meter - minimum required "score" when enabled

Policy - 'default'

Please make any changes to the policy and click 'Save' to commit them. Clicking 'Cancel' will not save any changes.

General Authentication Self Service Lockout PW Expiration Auditing **PW Rules**

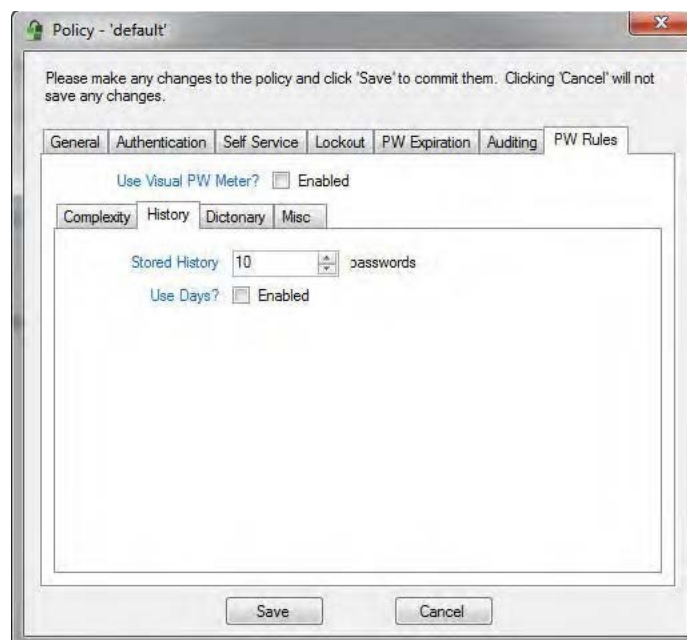
Use Visual PW Meter? ☒ Enabled

Complexity History Dictionary Misc

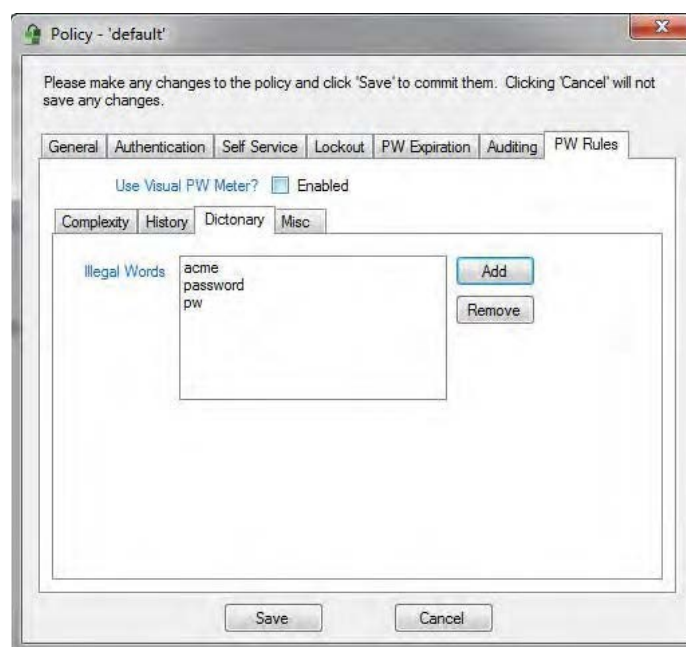
Minimum Score 70

Save Cancel

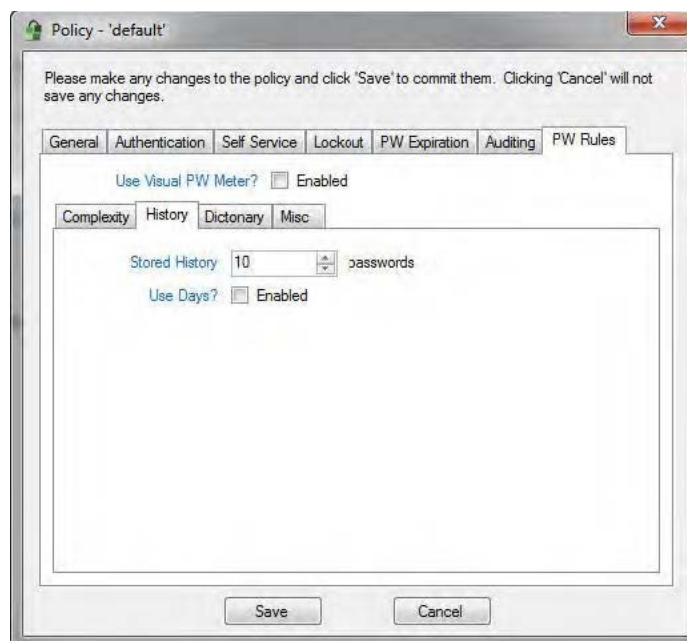
- Password History - by number of entries or time



- Password Dictionary - standard words that passwords cannot contain



- Enforce Complexity Rules During Login - any policy changes can be enforced immediately instead of waiting until the next time the user's password expires
- Regular Expression checking - for rules that cannot be enforced using the out-of-the-box rules in PortalGuard



- Password Expiration:
  - Expiration period - number of days between required password changes
  - Grace period - number of days before the expiration date when the user will receive notification of the impending expiration
  - Expire first use - expire the password the first time the user authenticates through PortalGuard
  - Minimum Age - number of minutes until a password can be changed again
  - Calendar reminders - optional sending of reminders for the day the user's password will expire next

- Lockout:
  - Strike limit - number of consecutive failed authentication attempts until the user's account is locked in PortalGuard
  - Lock expiration - optional number of seconds until a lockout automatically is cleared
  - Strike messages - controls the level of information when a strike or lockout occurs, from the most generic ("bad username or password") to the most helpful ("bad password - you have 1 strike and your account will be locked when 3 strikes are reached")
  - Inactivity - the number of days of PortalGuard inactivity until an account is considered "dormant" in PortalGuard. The PortalGuard server will then prevent login through its interface using these accounts
  - Session concurrency - prevent multiple simultaneous login sessions through the PortalGuard interface using the same credentials
  - Help Desk/Verbal Authentication - enables the optional functionality that allows Help Desk staff to verbally identify users over the phone by asking a configurable set of questions
- Auditing:
  - Log last login - track last login date/time for users
  - Log last password change - track last password change date/time for users
  - Log last password recovery - track last password reset/recovery date/time for users
  - Require acceptance - optional setting for requiring users to accept a Terms of Use agreement before allowing a login to complete
  - URL for rejection - the URL where users should be redirected if they decline the Terms of Use

## Deployment

Implementation of the PortalGuard platform is seamless and requires no changes to Active Directory/LDAP schema. A server-side software installation is required on at least one Microsoft IIS server on the network.

## IIS Installation

A MSI is used to install PortalGuard on Microsoft IIS 6 or 7.x. If installing PortalGuard on Microsoft IIS 7.x/Windows Server 2008, 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 Microsoft IIS 6 Management Compatibility role services

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

## System Requirements

This version of PortalGuard supports direct access and authentication to cloud/web-based applications, only.

PortalGuard can be installed directly on the following web servers:

- IBM WebSphere/WebSphere Portal v5.1 or higher
- Microsoft IIS 6.0 or higher
- Microsoft Windows SharePoint Services 3.0 or higher
- Microsoft Office SharePoint Server 2007 or later

The PortalGuard Web server also has the following requirements on Windows operating systems:

- .NET 2.0 framework or later must be installed
- (64-bit OS only) Microsoft Visual C++ 2005 SP1 Redistributable Package (x64)

PortalGuard is fully supported for installation on virtual machines. Furthermore, PortalGuard can currently be installed on the following platforms:

- Microsoft Windows Server 2000
- Microsoft Windows Server 2003 (32 or 64-bit)
- Microsoft Windows Server 2008 (32 or 64-bit)
- Microsoft Windows Server 2008 R2

**NOTE:** When run in "Sidecar" mode, PortalGuard can provide its functionality on any web server that uses a HTML login page.

If you have a platform not listed here, please contact us at [sales@portalguard.com](mailto:sales@portalguard.com) to see if we have recently added support for your platform.

## Schedule a Demo

---

Interested in seeing a demo of PortalGuard's password management offerings?

[Schedule a Demo](#) today!

## Platform Layers

Beyond password management, PortalGuard is a flexible authentication platform with multiple layers of available functionality to help you achieve your authentication goals:

- Contextual Authentication
- Tokenless Two-Factor Authentication
- Real-time Reports / Alerts
- Knowledge-Based
- Self-Service Password Reset
- Single Sign-On

