A BIO-key® Solution.

Tech Brief

# Server-based Password Synchronization: Managing Multiple Passwords

# Table of Contents

# Summary

A common concern across organizations is that users have too many passwords to manage, each with a separate management interface to become familiar with. This creates user frustration and increased costs around Help Desk and IT support. Enterprise Single Sign-On (SSO) is looked at as a solution but for many organizations it proves too costly and many encounter internal resistance due to security concerns.

Password synchronization is a possible midpoint that can ease user frustrations by enabling access to different systems using the same password and a single interface. This proves easier to implement than SSO and most solutions can force enrollment and do not require client-side software.

However, organizations have struggled with forgotten passwords as a sticking point with password synchronization as each system must be reset independently.

PortalGuard addresses these challenges by providing a cost-effective, flexible approach to server-based password synchronization plus Self-Service Password Reset allowing users to easily manage passwords for multiple systems from a single, consistent interface.

# The Basics

The process of password synchronization correlates the passwords for multiple user accounts, enabling users to authenticate to all systems leveraging a single password. Since only one password needs to be remembered, overall system security can now be increased by enforcing stronger password policies such as more frequent expiration.

# Password Complexity Challenges

Password complexity rules often differ from system to system. These differences are a common hurdle when implementing password synchronization since a password that is acceptable on one system may be rejected by another thus preventing password synchronization altogether. This can be a difficult problem to troubleshoot as it may only occur for a small subset of user-chosen passwords. Identifying password complexity rules for all systems that will be included in the synchronization process is a critical first step to mitigating this challenge.

After identification, a typical response to this issue may be to change the password rules on one or more systems to reach a common set that can be enforced for each. This approach can often be impeded by potential compliance issues or trepidation that the change may cause other unforeseen maintenance issues (e.g. legacy service or embedded accounts). Alignment of password policies across systems may not even be technically feasible if the systems do not support a common set of enforceable password rules. As an example, Microsoft Active Directory cannot natively enforce a maximum password length or prevent new passwords from containing specific characters. IBM System i servers typically have a maximum password length of 10 and can only accept letters, numbers and the ‘$’, ‘@’, ‘#’ and ‘_’ characters in new passwords. AD and System i server password policies cannot be aligned natively because they only support incompatible proprietary password complexity rules.

PortalGuard helps reconcile these problems by enforcing a consistent set of password rules that are always enforced when a password is changed or reset through it. By configuring the PortalGuard policies such that they will only allow new passwords that comply with all included systems, password synchronization will not be prevented due to password policy rules.

# PortalGuard Server-based Password Synchronization

PortalGuard offers a comprehensive password synchronization solution which supports Microsoft Active Directory, Novell eDirectory, IBM System i, any LDAP v3-compliant directory and custom SQL user tables. Beyond being easy to implement and forcing user enrollment, PortalGuard enables Self-Service Password Reset, recovery and account unlock to manage forgotten passwords.

Users can now be allowed to reset forgotten passwords from one place, including the Windows logon screen, corporate web portal login or a stand-alone website. When performing resets across all systems, PortalGuard passes the password change down to all linked accounts in real-time.

PortalGuard also has an optional component for further Active Directory integration. This Active Directory Password Filter can prevent users from setting domain passwords natively through the Ctrl-Alt-Del Windows Password Change process that do not comply with custom rules that AD itself cannot enforce. This ensures that what may be the most common interface for changing user passwords will comply with the necessary rules for password synchronization to occur seamlessly

# Features

- Ability to link a user’s primary account (e.g. Active Directory) to accounts on multiple systems/directories
- All password changes, resets and account unlocks through PortalGuard flow to all linked systems in real-time
- Align password complexity rules to reduce barriers to password propagation across systems
- The requirement to link to accounts is policy driven which can be specific to the user, group or password repository
- Account linking can be enforced or made optional - enforcement points include website login and Windows desktop login
- Supported user account repositories include:
    - Microsoft Active Directory
    - Novell eDirectory
    - And LDAP v3-compliant directory
    - IBM System i
    - Custom SQL user tables

# Benefits

- Password Synchronization - eliminates the need for users to remember different passwords for each system/directory
- Ease of Use - the user can manage passwords for multiple systems from a single, consistent interface
- Self-Service - accounts can be unlocked and passwords can be reset from one place, including the Windows login screen, a corporate web portal login or a stand-alone website
- Seamless Integration with existing website logon pages using PortalGuard in "Sidecar" mode
- Lower Costs - reduces password-related Help Desk calls and required IT support
- Increased Productivity and user adoption for new services/websites

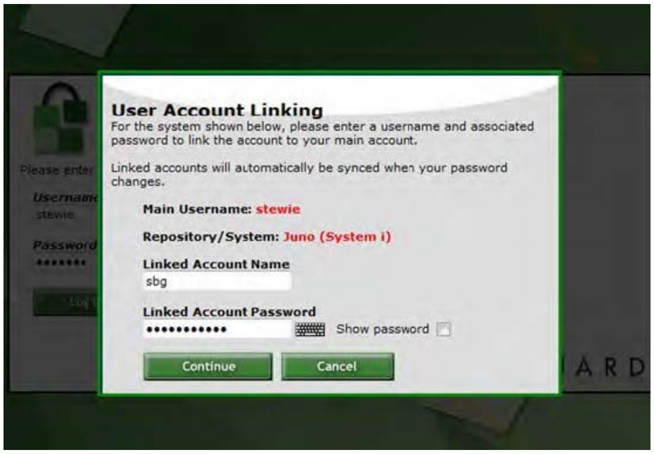
# How It Works

## Account Linking

**Step 1**: The user logs into a Windows workstation or an existing internal website. PortalGuard is notified of the logon and checks its policies to see if the user:

- Is required to link to an account in another directory, and
- If they have yet to do so

If both conditions are true, PortalGuard will prompt the user to enter a username in the secondary directory and the current password for that account. The user must know the account's current password to link it to their primary account.



User Account Linking

For the system shown below, please enter a username and associated password to link the account to your main account.

Linked accounts will automatically be synced when your password changes.

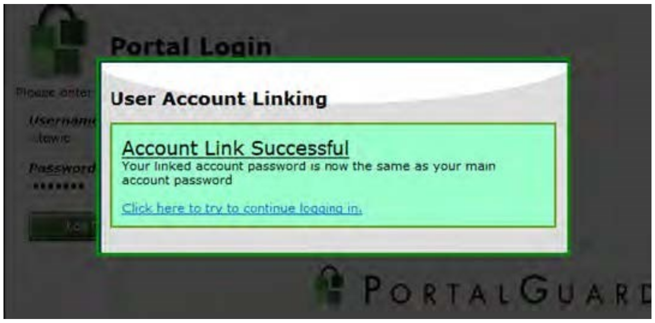
Main Username: stewie

Repository/System: Juno (System i)

Linked Account Name: sbg

Linked Account Password: ••••••••••• Show password □

**Step 2**: Once the user provides the correct password, the secondary account password will be immediately synchronized with the primary if necessary.



Portal Login

User Account Linking

Account Link Successful

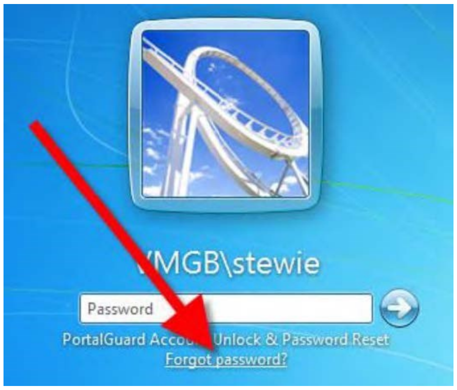
Your linked account password is now the same as your main account password

Click here to try to continue logging in.

# Self-Service Password Reset Process

**Step 1**: The user has forgotten their password and clicks "Forgot Password?" link on the Windows logon screen or website logon page.

Windows 7 Desktop Support



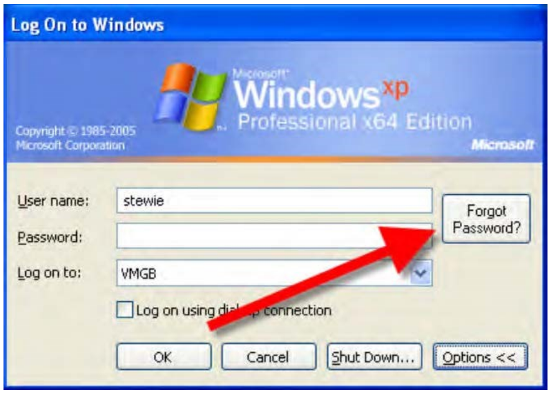
\MGB\stewie

Password

PortalGuard Accou Unlock & Password Reset

Forgot password?

Windows XP Desktop Support



User name: stewie

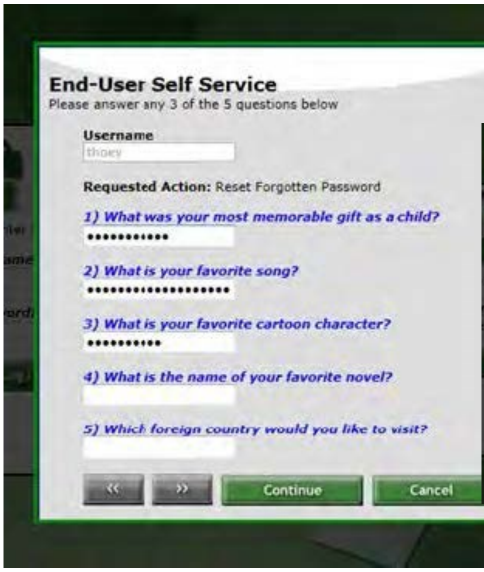
Password:

Log on to: VMGB

□ Log on using dial-up connection

**Step 2**: The user chooses to reset their forgotten password and proves their identity by correctly answering a series of challenge questions and/or entering a One-Time Password (OTP) sent to their mobile phone or email.

Challenge Questions and Answers



End-User Self Service

Please answer any 3 of the 5 questions below

Username: thoey

Requested Action: Reset Forgotten Password

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

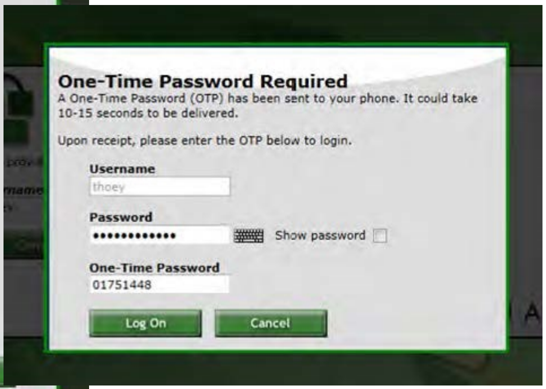
2) What is your favorite song?
●●●●●●●●●●●●●●●●●●●

3) What is your favorite cartoon character?
●●●●●●●●●●

4) What is the name of your favorite novel?

5) Which foreign country would you like to visit?

One-Time Password (OTP)



One-Time Password Required

A One-Time Password (OTP) has been sent to your phone. It could take 10-15 seconds to be delivered.

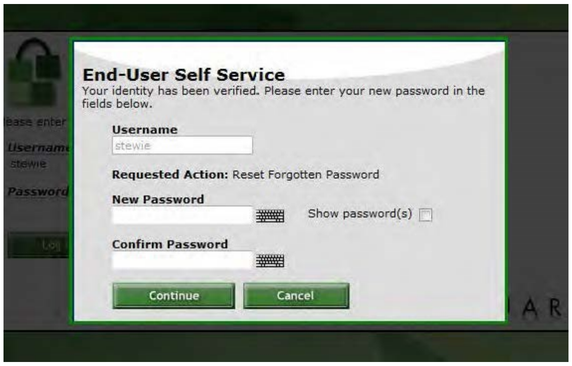
Upon receipt, please enter the OTP below to login.

Username: thoey

Password: ●●●●●●●●●●●●● Show password □

One-Time Password: 01751448

**Step 3**: The user enters a new password that satisfies all linked account systems. The PortalGuard server resets all linked accounts to use this password and unlocks the account as well.



End-User Self Service

Your identity has been verified. Please enter your new password in the fields below.

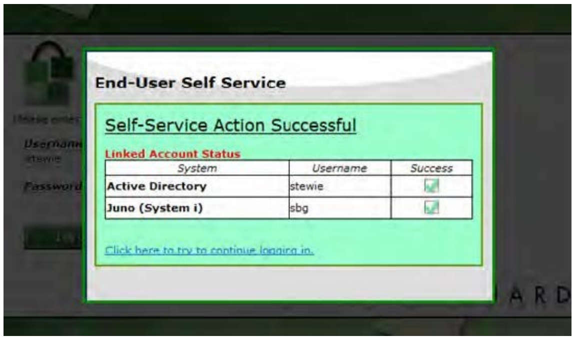
Username
stewie

**Requested Action:** Reset Forgotten Password

New Password

Confirm Password

**Step 4**: Immediate feedback is given to the user that the password reset was successful on all linked accounts. The user is now able to login to all linked systems with the new password.



End-User Self Service

Self-Service Action Successful

Linked Account Status

| System | Username | Success |
|---|---|---|
| Active Directory | stewie | ✓ |
| Juno (System i) | sbg | ✓ |

Click here to try to continue logging in.

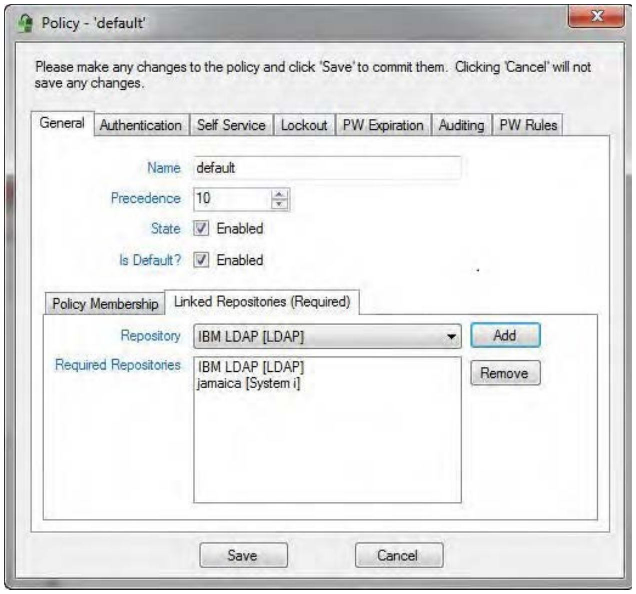
# Configuration

*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 Synchronization**

- Linked Repositories



Policy - 'default'

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

Name: default

Precedence: 10

State: ☑ Enabled

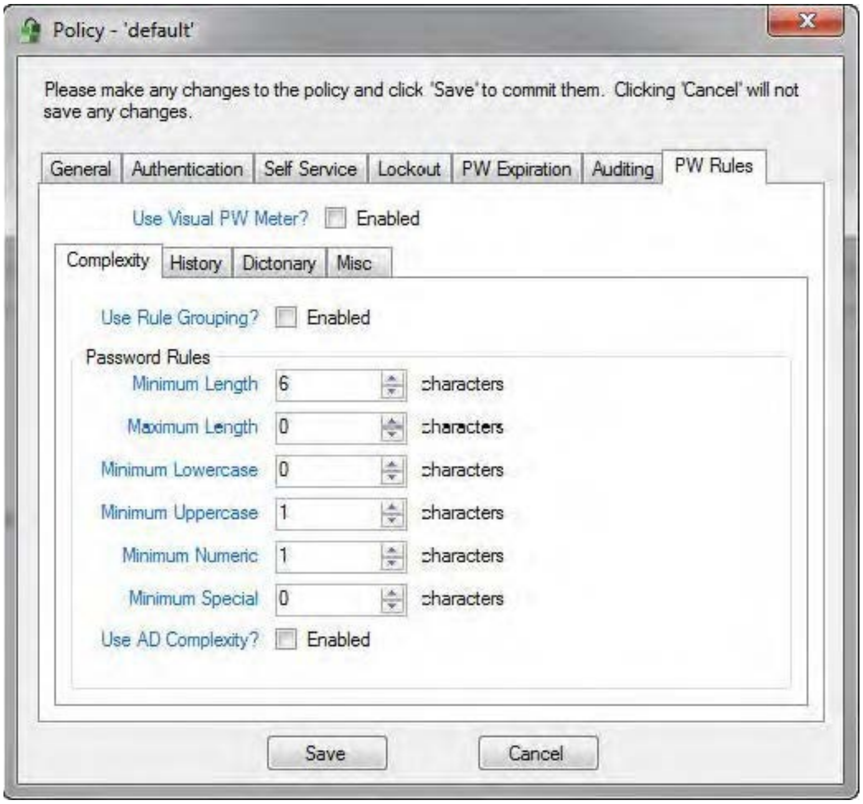
Is Default?: ☑ Enabled

Repository: IBM LDAP [LDAP]

Required Repositories: IBM LDAP [LDAP]<br>jamaica [System i]

**Password Synchronization**

- Minimum length
- Maximum length
- Minimum lowercase characters
- Minimum uppercase characters
- Minimum numeric characters
- Minimum non-alphanumeric characters
- Enforce Active Directory complexity (3 out of 4 character classes)
- Password rule grouping (subsets)
- Use of a visual password strength meter
- Password history
- Prevention of passwords containing dictionary words
- Use of regular expression for custom rules



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

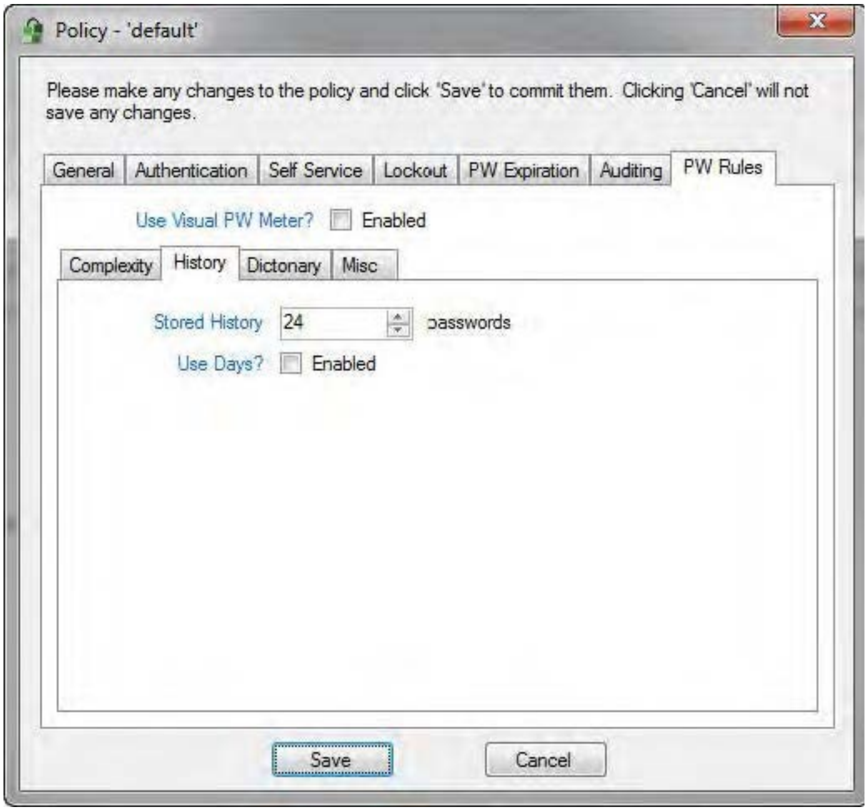
Use Visual PW Meter? □ Enabled

Use Rule Grouping? □ Enabled

Password Rules

| | | |
|---|---|---|
| Minimum Length | 6 | characters |
| Maximum Length | 0 | characters |
| Minimum Lowercase | 0 | characters |
| Minimum Uppercase | 1 | characters |
| Minimum Numeric | 1 | characters |
| Minimum Special | 0 | characters |

Use AD Complexity? □ Enabled

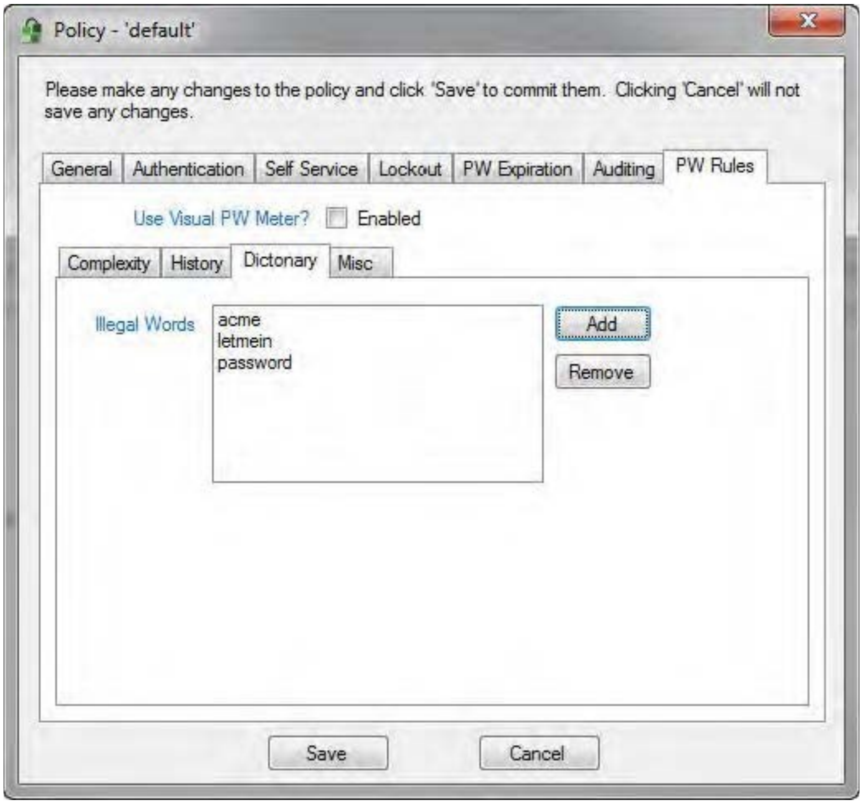


Please make any changes to the policy and click 'Save' to commit them. Clicking 'Cancel' will not save any changes.

Use Visual PW Meter? □ Enabled

Stored History 24 passwords

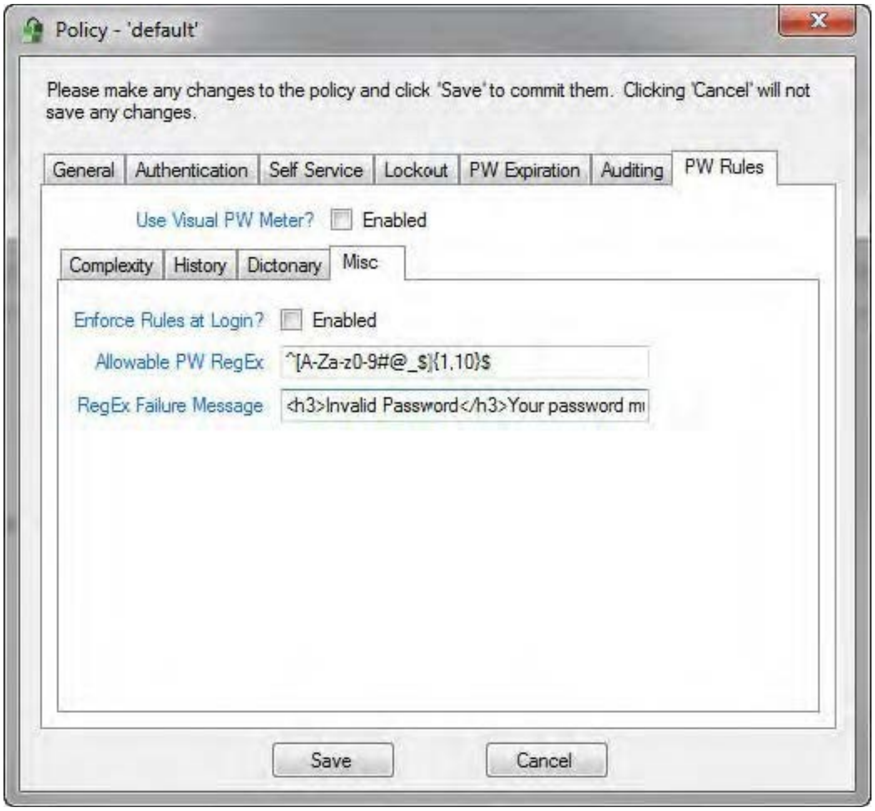
Use Days? □ Enabled



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

Use Visual PW Meter? □ Enabled

Illegal Words: acme, letmein, password



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

Use Visual PW Meter? □ Enabled

Enforce Rules at Login? □ Enabled

Allowable PW RegEx: ^[A-Za-z0-9#@_$]{1,10}$

RegEx Failure Message: <h3>Invalid Password</h3>Your password mı

# 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 IIS server on the network.

To enforce account linking on Windows workstations, the PortalGuard Desktop must be deployed. This is done using a standard MSI which can be pushed out silently. To enforce account linking on an existing website login, PortalGuard Sidecar mode must be integrated.

To enforce custom password complexity rules for native Ctrl+Alt+Del Windows password changes, the Active Directory Password Filter must be installed on all Active Directory domain controllers. This is also packaged as a MSI for easier deployment. This component is compatible with all versions of Windows Server and has separate MSIs for either 32-bit or 64-bit architectures.

# IIS Installation

A MSI is used to install PortalGuard on IIS 6 or 7.x. If installing PortalGuard on 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 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/browser-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

PortalGuard works with Windows Terminal Services on Win2003 servers and Remote Desktop Services on Win2008 servers.

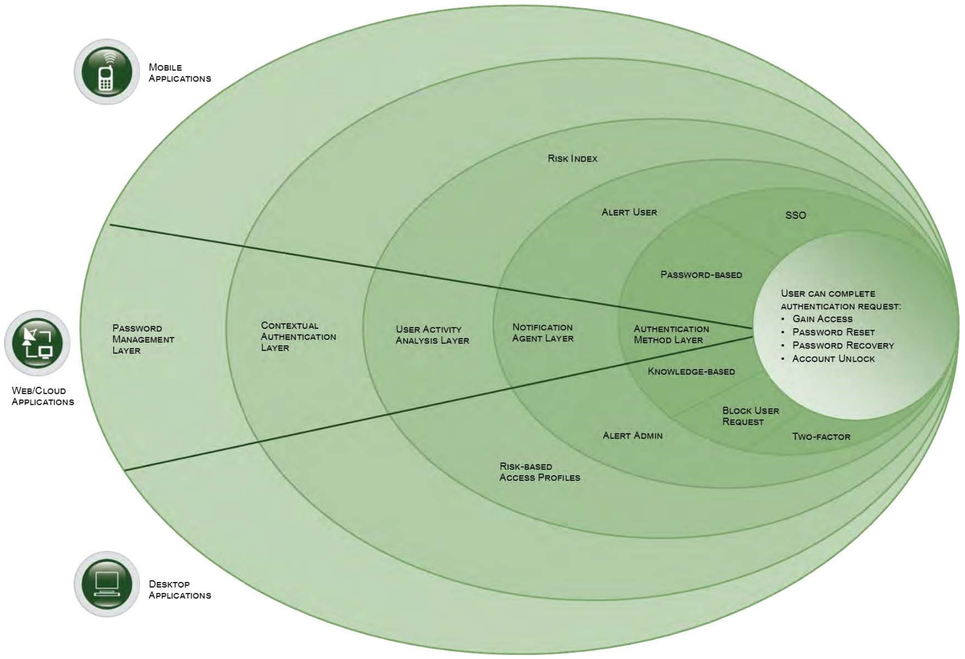
If you have a platform not listed here, please contact us at sales@portalguard.com to see if we have recently added support for your platform.

# Platform Layers

Beyond password synchronization, PortalGuard is a flexible authentication platform with multiple layers of available functionality to help you achieve your authentication goals (*visual on pg.17*):

- Contextual Authentication
- Tokenless Two-factor Authentication
- Real-time Reports / Alerts
- Knowledge-based
- Password Management
- Self-Service Password Reset
- Single Sign-On

PortalGuard: A Contextual Authentication Platform


Mobile Applications
Web/Cloud Applications
Desktop Applications
Password Management Layer
Contextual Authentication Layer
User Activity Analysis Layer
Notification Agent Layer
Authentication Method Layer
Risk Index
Alert User
SSO
Password-based
User can complete authentication request:
• Gain Access
• Password Reset
• Password Recovery
• Account Unlock
Knowledge-based
Block User Request
Alert Admin
Two-factor
Risk-based Access Profiles