



Multi-Factor Authentication with PowerSC

Overview

PowerSC Multi-Factor Authentication (PMFA) is an IBM offering designed to greatly reduce the risk of data breach caused by compromised credentials by providing numerous flexible options for implementing Multi-Factor Authentication on Power. PMFA is implemented with a Pluggable Authentication Module (PAM), and can be used on AIX, VIOS, RHEL, SLES, IBM i, HMC, and PowerSC Graphical User Interface.

In this proof-of-concept service, clients receive a guided introduction to the installation and configuration of PMFA by an experienced IBM security consultant.

Authentication Methods Supported

- TOTP (for example, IBM TouchToken for iOS)
- Generic TOTP (for example, IBM Verify, Google Authenticator, Duo Mobile)
- SafeNet RADIUS
- RSA SecurID
- RSA SecurID RADIUS
- Gemalto SafeNet RADIUS
- Generic RADIUS
- YubiKey
- PIV/CAC or X.509 Certificate
- IBM Security Verify Access
- LDAP Simple Bind
- Local Password

Minimum Software Level Requirements (PMFA Client)

- AIX 6.1.9.8
- AIX 7.1.5.2
- AIX 7.2.1.1
- VIOS 2.2.5.20
- RHEL 8 (Power, LE)
- SLES 15 (Power, LE)
- IBM i 7.2
- HMC V9R1.921
- Virtual HMC V9.1.940
- PowerSC Graphical User Interface Server – 1.2.0.2



The screenshot shows the IBM PowerSC MFA configuration interface. The top navigation bar includes 'User Provisioning', 'Policy Definitions', 'Authentication Methods' (selected), and 'IBM | Servers'. The 'Authentication Methods' section lists various methods, with 'LDAP Simple Bind' selected. The 'Method Details' section for 'LDAP Simple Bind' includes fields for 'Trace Level' (0), 'LDAP Primary Server' (129.40.40.66), 'LDAP Primary Server Port' (389), 'LDAP Secondary Server', 'LDAP Secondary Server Port' (0), 'LDAP Tertiary Server', 'LDAP Tertiary Server Port' (0), 'Receive Timeout' (3), and 'Trusted CAs Path'.

Common Use Cases

- Organizations needing to comply with regulatory or industry-specific requirements, such as PCI DSS
- Organizations wanting to eliminate weak authentication methods, such as using passwords only
- Organizations wanting to better protect sensitive data by ensuring only authorized personnel can access their systems
- Organizations wanting to implement stronger authentication for remote and all administrative access
- Organizations seeking to reduce the security risk of one of the top causes of a data breach: compromised login credentials

Engagement Process

- Consultant arranges prep call to discuss requirements, scheduling, and agenda
- Consultant works with client to install and configure PowerSC MFA in client environment
- Consultant provides advice on best practice implementation
- Consultant works with client to verify the PMFA functions most important to the client
- Consultant provides presentations to facilitate knowledge transfer concerning the numerous capabilities of PowerSC MFA

Deliverables

1. Presentation Slides – an electronic copy of all presentation slides
2. Configuration documents – an electronic copy of configuration documents