**DATASHEET** *(Cybersecurity)*

# Powertech Multi-Factor Authentication

Multi-factor authentication (MFA) software is a simple and effective way to ensure the users accessing your systems are who they say they are.

MFA is also essential for compliance with the Payment Card Industry's Data Security Standard (PCI DSS). Once MFA was only required for remote access to the cardholder data environment. Now PCI DSS requires MFA for any kind of non-console administrative access to the cardholder data environment, including access from within the network or from the cardholder data environment itself.

Powertech Multi-Factor Authentication is a robust MFA solution for IBM i (AS/400, iSeries)—a platform that was often outside the scope of PCI's previous MFA requirement. With Powertech MFA, it's easy to enforce risk-driven security policies and require users to provide two or three forms of authentication before logging in to a green screen session or connecting to IBM i through an exit point, such as FTP or Telnet.

## PRODUCT SUMMARY

### KEY FEATURES

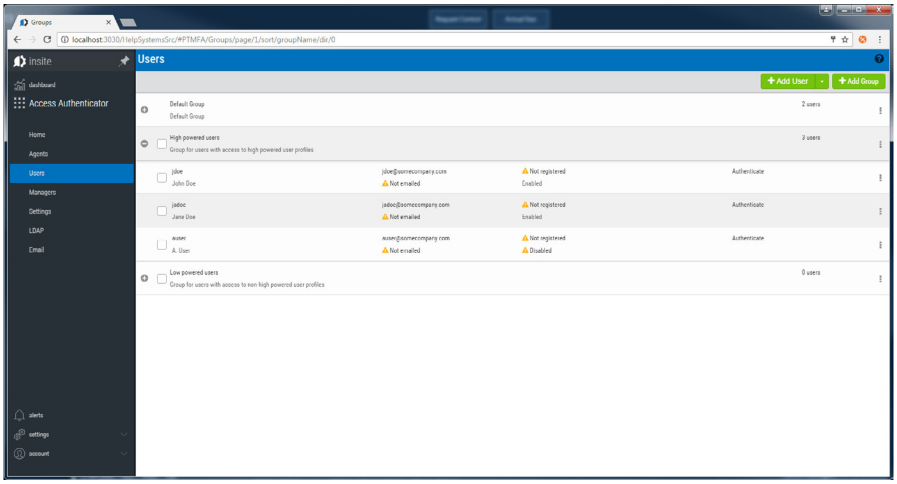
- Comprehensive Authentication Manager
- Intuitive User Portal
- Multiple Authentication Methods
- Complete Audit Trail
- Mobile App for iOS and Android
- Centralized Administration
- No Custom Coding Required
- High Availability
- API Integration
- RADIUS Integration

## A Robust Authentication Manager Centralizes Administration

Powertech MFA is administered from the HelpSystems Insite web interface—a mobile-friendly single pane of glass that displays key metrics on drag-and-drop dashboards. These metrics can include enabled and disabled users, the percentage of authentication failures, and users who have been inactive for a set number of days.

From the authentication manager, user profiles can be imported quickly from the active directory via LDAP. The authentication manager database is also synchronized with the active directory, so that new user profiles are added automatically, while profiles that exist in the authentication manager database but not active directory are highlighted as candidates for removal.

The authentication manager simplifies user administration.



Default Group
Default Group — 2 users

High powered users
Group for users with access to high powered user profiles — 3 users

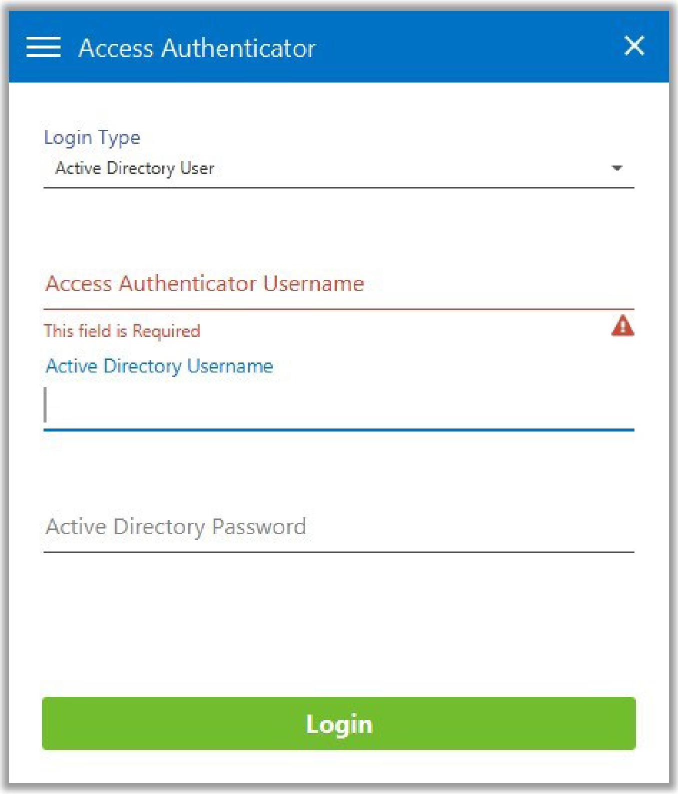
| | | | |
|---|---|---|---|
| jdoe<br>John Doe | jdoe@somecompany.com<br>⚠ Not emailed | ⚠ Not registered<br>Enabled | Authenticate |
| jadoe<br>Jane Doe | jadoe@somecompany.com<br>⚠ Not emailed | ⚠ Not registered<br>Enabled | Authenticate |
| auser<br>A. User | auser@somecompany.com<br>⚠ Not emailed | ⚠ Not registered<br>⚠ Disabled | Authenticate |

Low powered users
Group for users with access to non high powered user profiles — 0 users

Once users have been added, Powertech MFA can send them an email with a link to the self-service portal, where they can complete the registration process and maintain their own account details.

Administrators can also use the authentication manager to:

- Enable and disable authentication methods
- Enable and disable users without removing them from the database altogether
- Set whether multi-factor authentication is switched on for users as soon as they are added to the database or only once they've completed registration in the self-service portal
- Configure Powertech MFA to meet their security requirements, such as activating or deactivating authentication for users or groups and setting values for automatic user lockout
- Maintain the IP addresses of the main and backup authentication managers
- Configure Powertech MFA to disable users who have been inactive for a defined number of days (PCI DSS requires user accounts that have been inactive for 90 days to be removed or disabled)



Access Authenticator

Login Type: Active Directory User

Access Authenticator Username

This field is Required

Active Directory Username

Active Directory Password

Users provide their active directory user name and password to access the self-service portal.

## Complete Audit Trail

With audit and reporting functionality, Powertech MFA makes it easy to meet stringent compliance requirements. Administrators can report on authentication attempts, user maintenance activity (user registrations, mobile app registrations, one-time password updates), and user information (disabled users, users who haven't completed registration). Administrators can enable or disable all types of auditing and determine how long to retain data.

## Intuitive User Portal

Powertech MFA's self-service portal allows users to complete the registration process after their accounts are added to the authentication manager database. The portal is the interface where users maintain their authentication credentials.

From the portal, users can activate the Powertech MFA mobile app. The self-service portal generates a QR code, which transfers settings to a user's mobile device.

The portal is also where users can update the seed used for one-time password generation in the event they suspect the existing seed has been compromised. The self-service portal generates a new random seed and the user transfers it to the mobile app via QR code.

Users can manage the devices registered to them and maintain their preferences from the user portal. The portal also enables users to generate a list of one-time passwords that they can print and use when offline. This feature can be turned off by the administrator.

## Multiple Authentication Methods

Powertech MFA provides several different methods of authentication for your users' convenience and to meet your organization's security requirements. Administrators determine which methods are available from the authentication manager.

- **YubiKey** is a FIDO-certified U2F USB authentication device. When a user is prompted to authenticate, she selects the YubiKey authentication option and inserts the YubiKey into a USB port.
- **One-time password generation** relies on source algorithms to deliver a single, unique password via the mobile app via the mobile app or desktop agent.
- **Push notifications** are sent to users' mobile devices via the app. A notification displays the user profile that's attempting to sign in, information about the system that's being signed into, and a prompt to confirm or deny whether the sign-in attempt is legitimate. If the user confirms the attempt is a legitimate, a message is returned to the authentication manager and the user is allowed to sign in.
- **Biometric** scanning is available for mobile devices with a fingerprint scanner. Similar to a push notification, a notification is sent to the user's mobile device prompting him to authenticate using the fingerprint scanner.

## No Custom Coding Required

Powertech MFA includes an IBM i agent that resides on the IBM i server, and a desktop agent than can be deployed on Windows desktops, allowing users to authenticate from their work stations when the green screen agent isn't available.

The IBM i agent can be tied into the initial program, prompting for MFA at sign-on. It can also be tied to an exit program, where it prompts when a user attempts an FTP request, for example.

## RADIUS Integration

Powertech MFA supports the RADIUS protocol, which allows you to leverage your enterprise multi-factor authentication solution for IBM i.

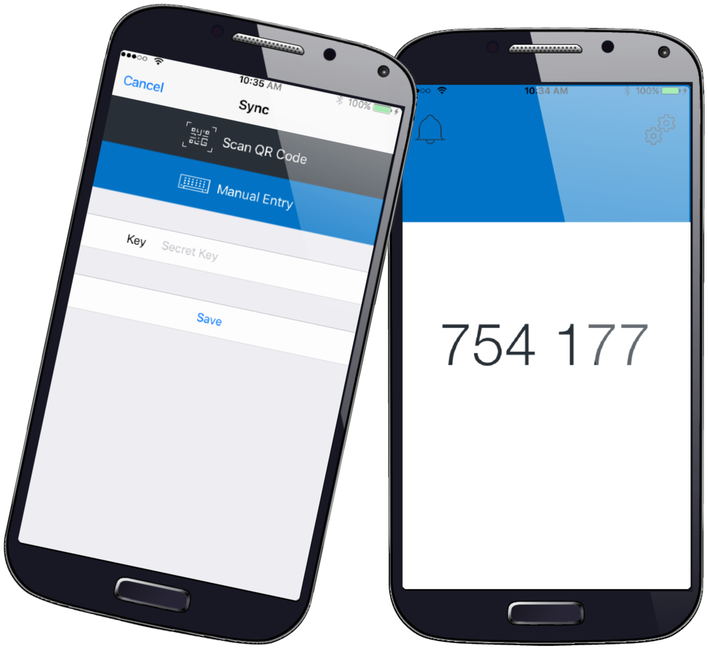
When MFA RADIUS processing is activated, the authentication manager forwards credentials entered by the user to your RADIUS server. The credentials are validated, and returned to Powertech MFA's IBM i agent via RADIUS.

## High Availability

Users have the ability to authenticate 24/7. If the authentication manager is unavailable for some reason, such as schedule maintenance or a hardware fault, an alternative authentication manager will be available to process users' authentication attempts.

## Let's Get Started

To find out how easy multi-factor authentication is with Powertech MFA, request your demo today.



With the mobile app, users can authenticate their identities away from the office.