



User Guide
Powertech Multi-Factor
Authentication
1.5



Copyright Terms and Conditions

Copyright © HelpSystems, LLC.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from HelpSystems is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to HelpSystems with appropriate and specific direction to the original content. HelpSystems and its trademarks are properties of the HelpSystems group of companies. All other marks are property of their respective owners.

202104070142

Welcome to Powertech Multi-Factor Authentication	1
Installing Powertech Multi-Factor Authentication	2
System Requirements	2
Installation Overview	4
Upgrading Powertech Multi-Factor Authentication	16
Upgrade Procedure Overview	16
Implementing Powertech Multi-Factor Authentication	20
Administrator Setup Procedure	20
User Setup Procedure	27
User Authentication	33
Reference	35
Agents screen	36
Audit Log screen	37
Authentication Log screen	38
Copy/Move Configuration screen	38
Powertech Multi-Factor Authentication Desktop Agent	39
Edit Default System	41
Email Settings	43
Powertech Multi-Factor Authentication Home	44
Import Users	45
LDAP Settings screen	47
Managers	48
New/Edit Group	49
New/Edit Managers	50
New/Edit System	51
New/Edit User	54
Reports screen	55
Select a Group	57
Select IBM i Profiles	57
Select Systems	58
Server Health and Failover screen	58
Settings screen	60

System Event Log screen	65
Troubleshooting Authentication with your Mobile Device	65
Users screen	68
IBM i Agent Reference	70
Appendix	79

Welcome to Powertech Multi-Factor Authentication

NOTE: Prior to version 1.4, Powertech Multi-Factor Authentication was named *Access Authenticator*.

Powertech Multi-Factor Authentication allows administrators to ensure only authorized users are granted access to their IBM i systems by requiring two pieces of evidence in order to validate each user's identity, a method of access control known as *multi-factor authentication*. Powertech Multi-Factor Authentication allows network users to easily register a mobile device or YubiKey to act as the second authentication factor, in addition to their IBM i or Active Directory credentials.

Powertech Multi-Factor Authentication is designed to challenge users as they access the IBM i. It can be used to sign on to interactive sessions or when FTP is used to connect to the system.

The installation components required to administer the authentication process include:

- **Version 1.15 or higher of Insite Server.** HelpSystems Insite is the web browser interface used to manage Powertech Multi-Factor Authentication.
- **The *Authentication Manager Server*.** The Authentication Manager is Powertech Multi-Factor Authentication's central processing component.
- **The *Data Services Server*.** The Data Services includes Powertech Multi-Factor Authentication's database and backup, recovery, and HA services.

These components can be installed together on one server, or divided on two or more servers. For example, in one possible configuration, the Insite server can be installed where users can connect, and the Authentication Manager Server and Data Services can be installed together on a different server. (These systems can be Windows servers, or Linux or Unix systems.)

See [Administrator Setup Procedure](#) for details on configuring and administering Powertech Multi-Factor Authentication.

The installation components for user authentication include:

- **The *Android app*.** This app, available from Google Play, can be used to authenticate using Android.
- **The *iOS app*.** This app, available from Apple, can be used to authenticate using an iPhone.
- **The *Desktop Agent*.** This desktop application can be used to authenticate connections made through methods outside of traditional log on screens (like FTP).

The administration and configuration of Powertech Multi-Factor Authentication is done from a connection with the Insite server. Network users can register their devices using a URL provided via an email they receive after enrolling with Powertech Multi-Factor Authentication.

See [User Setup Procedure](#) for details on setting up Powertech Multi-Factor Authentication for authentication.

See [User Authentication](#) for details on how to authenticate using Powertech Multi-Factor Authentication as an end user.

Installing Powertech Multi-Factor Authentication

These instructions guide you through the process of installing Powertech Multi-Factor Authentication.

System Requirements

The following requirements are necessary in order to install and run Powertech Multi-Factor Authentication.

Compatibility with HelpSystems Insite

Powertech Multi-Factor Authentication 1.5 requires Insite 3.5.

To use HelpSystems Insite to access your products through a web browser, you must meet the following browser and/or operating system requirements.

Hardware Type	Minimum Browser and/or OS Requirements
Desktop/Laptop	Firefox 11 or higher Chrome 21 or higher Internet Explorer 11 Safari 6.1 or higher Microsoft Edge
Mobile Device	iOS: Browsers on iOS 8 or higher Android: OS 6.0 Marshmallow or higher Windows: OS 10 using Edge
IBM i	V7R2 or higher operating system

For more details, see [Insite System Requirements](#).

Authentication Manager System Requirements

- Supported Linux OS Versions:
 - RedHat Enterprise/Centos 7 & 8
 - X86_64
 - PPC64
 - PPC64LE
 - Suse Enterprise Linux 12 & 15
 - X86_64
 - PPC64LE
 - Ubuntu Linux 19 & 20
 - X86_64
 - PPC64LE
- Supported Windows OS Versions:
 - Windows Server 2016
 - Windows Server 2019
- For Linux, the /opt drive must have at least 20 GB of disk space.
- Version R01M06 of the Powertech Multi-Factor Authentication IBM i Agent (shipped with Powertech Multi-Factor Authentication 1.4).
- Version 3.5 of HelpSystems Insite.
- Version 1.5 of the Multi-Factor Authentication Desktop Agent (if authenticating on a PC).

The remaining system requirements for the Authentication Manager are the same as HelpSystems Insite. See [Insite System Requirements](#).

IBM i Agent System Requirements

Powertech Multi-Factor Authentication requires IBM i 7.2 or higher.

The minimum supported IBM i agent for Powertech Multi-Factor Authentication 1.5 is R01M06.

NOTE: During installation an FTP connection is initiated. The FTP server responds with messages that prompt for FTP login credentials. The standard port reserved to establish an FTP connection to the IBM i is port 21. Consequently, it is required that this port is open and 'listening' on the server in order to establish a connection with the Installation Wizard and facilitate a successful installation. Any firewall or exit program technology on the PC or the IBM i system could potentially block the FTP file upload and remote commands running the installation. Ensure any such firewall or program is configured to permit an FTP connection on port 21. If standard FTP is not permitted, contact Technical Support for instructions on how to manually install the product without the installation wizard.

System Values

It is HelpSystems's goal not to change system values on customer systems because we recognize that security-conscious organizations have rigorous change control processes in place for even small changes to system values. Therefore, we ask you to make any system value changes that are needed. However, the Powertech Multi-Factor Authentication IBM agent installation process could change a system value to allow the install to proceed if a system value is not set as specified below. If the Installation Wizard changes a system value during install, it changes it back to its original value when the install completes.

To install the Powertech Multi-Factor Authentication IBM i agent on your system, the following system values that control object restores must be configured as shown.

- Set QALWOBJRST to *ALWPGMADP (at a minimum) to allow the system to restore programs that adopt authority. Many Powertech programs adopt the authority of the product owner, rather than forcing you to give authority directly to administrators and end users. (Note: For some system configurations, *ALL is required temporarily.)
- QALWUSRDMN controls which libraries on the system can contain certain types of user domain objects. You should set the system value to *ALL or include the name of the Powertech Multi-Factor Authentication install library (PTMALIB) for the product to function properly.
- Set QVFYOBJRST to 1, 2, or 3. This allows Powertech Multi-Factor Authentication to restore all objects regardless of their signature. (Note: If you normally check signatures, remember to check this system value after the Powertech Multi-Factor Authentication install process completes.)
- Set QFRCCVNRST (Force conversion on restore) to 0, Do not convert anything.

Desktop Agent System Requirements

- Windows 10 64-bit, Windows 7 64-bit
- 2 GB RAM

NOTE: A new error handling and messaging mechanism was added to the Desktop Agent that enables important messages about upgrades to be displayed. HelpSystems recommends all Powertech Multi-Factor Authentication users upgrade to the latest Desktop Agent as soon as possible. See [User Setup Procedure](#).

Installation Overview

Powertech Multi-Factor Authentication installation on your network is a multi-step process that requires several installation procedures. The following entities should be installed in the order listed here:

- **HelpSystems Insite.** This is required for administrator setup and the User Portal. See [HelpSystems Insite Documentation List](#) for instructions that describe how to install and use HelpSystems Insite.

NOTE: You must create an Insite user profile before creating the Insite Product Connection to Powertech Multi-Factor Authentication. See [Profiles](#) in the HelpSystems Insite User Guide.

WARNING: Credential validation requests are made using the Insite connection profile. If the TCP Signon Server is active and the Insite connection profile has been configured to be prompted to authenticate, the authentication process will interfere with the user credential validation process. We therefore recommend that the Insite connection profile is not set up to be authenticated using Powertech Multi-Factor Authentication.

- **Powertech Multi-Factor Authentication Authentication Manager and Data Services.** The Authentication Manager is Powertech Multi-Factor Authentication's central processing component. Data Services include database and high-availability services used by the Authentication Manager. See [Installing the Authentication Manager and Data Services](#).
- **Powertech Multi-Factor Authentication IBM i agent.** The IBM i agent software must be installed on all systems to be secured by Powertech Multi-Factor Authentication. See [Installing the IBM i Agent](#).

After Powertech Multi-Factor Authentication has been installed and started, network users need to install up to two applications, depending on the method of authentication being used (see [User Setup](#) for details):

- **Powertech Multi-Factor Authentication Mobile app.** The mobile app is required in order to authenticate with a mobile device. (This installation is not necessary if a YubiKey is being used for the second authentication factor.)
- **Powertech Multi-Factor Authentication Desktop agent.** The Desktop Agent allows users to authenticate using a desktop computer as an alternative to the IBM i green screen agent for Exit Point sign on.

Installing the Authentication Manager and Data Services with Failover Support

While Powertech MFA can be operated with a single Authentication Manager instance, in order to provide redundancy in the case of server failure, HelpSystems provides a multi-server deployment that allows for two, three, or more Authentication Manager instances.

Before installing the Powertech Multi-Factor Authentication Authentication Manager, identify the systems that will be used for failover support. These must be configured as part of the installation process. One-, two-, and three-system deployments are possible. A three-system deployment is recommended. Additional systems can be added, further enhancing the integrity of the implementation. At this time, failover is not supported on heterogeneous environments—all systems must have like operating systems (all Windows or all Linux).

If this is an upgrade, a previous two-system deployment already includes a Primary and Secondary server. If this is a new installation, commission the available servers that will be used for your Powertech Multi-Factor Authentication implementation.

NOTE: While Powertech MFA does not require the configuration to use more than one system, failover processes run in the background in all installations.

Application Layer

The application layer in the context of Powertech MFA failover is the mechanism that controls the location of the PostgreSQL master, and the list of the standby systems.

Two-system vs three-system deployment

A three-system deployment is the ideal configuration for Powertech Multi-Factor Authentication failover because, in this environment, replication is always running. In the standard two-system deployment, it is possible for processes to lose the provided High Availability. For example, if an implementation includes only two systems, and maintenance is required on one of those systems, failover processes start when the first system is taken down for maintenance. At that point, there is no replication running for the second system as it is promoted to a master server. While no implementation is guaranteed, a three-system deployment provides continuous replication and HA capabilities.

Primary and Secondary definitions

In previous Powertech MFA versions, a server was designated as either Primary or Secondary. These terms are still used, but they have a slightly different meaning as of Powertech MFA 1.5. "Primary" was previously a static definition, such as 'System1 is the primary server and System2 is the secondary.' Failing over to the Secondary did not make it the new "Primary." Instead, the Secondary had its database promoted to be the master. When the "Primary" system was restored to service, the process would "Failback," promoting System1's database back to master.

As of Powertech MFA 1.5, the process is more dynamic. The Primary server is the node in which the database is assigned to master. When failover is initiated, whatever node has its database promoted becomes the Primary server. There is no longer a "Failback" procedure. Instead, the status of the server configuration can be updated manually.

Port Assignment

During the installation process, you will be asked to designate the ports that are required for Powertech MFA's services. While the default ports can be changed as might be required by, for example, institutional policies, the port numbers for each service should be the same in each installation. As such, prior to installation, designate a port number for each service that is available on each server you intend to use in your Powertech MFA deployment. Firewall setting must allow for communication over these ports.

The default port numbers are:

- Shutdown Port: 3039
- Connector Port: 3040
- Messenger SSL Port: 4707
- Messenger TCP Port: 61616
- Database Port (PostgreSQL): 6432

See [Port Descriptions](#) for additional details.

Transport Layer

ActiveMQ natively supports HA. As indicated in the following installation procedure, the IP address for each node must be entered for each server installation in a deployment. However, once complete, HA is available across all nodes for ActiveMQ. Active MQ is a critical support function for the application layer.

Since the application is using the native HA capability with ActiveMQ, the master database (application layer controlled) can exist on a different node than the transport layer.

EXAMPLE: In a three-system layout (sys1, sys2, sys3), consider the broker fails on sys1. Powertech MFA automatically switches to the next node in the list, which is generated at startup time for the ActiveMQ address list. Failover is *not* random. It proceeds through each node in the given list. In this example, sys2 would be the next available node. However, once the broker has been restored on sys1, HA moves the connections back to that node since it is the first node in the list, and is considered the Primary node.

Failover Notifications

Powertech MFA can be configured to send notifications anytime failover is triggered automatically due to a system outage. Configure failover notifications in the Failover Notification section of the [Settings screen](#).

NOTE: When failover is triggered, Powertech MFA's authentication service will be interrupted for several seconds, up to a minute. This delay is the amount of time required for the services to restart on the new Primary server.

Installing the Authentication Manager and Data Services with Failover Support on Linux

1. Login as root on the server you want to use as your Primary installation. The installer must be run as root or with sudo.
2. Download the Powertech Multi-Factor Authentication for Linux file (installPowertechMFA.tgz) to a temporary directory on the system from the [Powertech Multi-Factor Authentication download page](#). (The "Trial" download is the full product, which can be unlocked with a valid License Key.) If you intend to deploy failover with two or more servers, the installer must be downloaded (or otherwise transferred) to each server being used. The installation procedure must be run on each server being included in the Powertech MFA deployment.

3. Use the following command to extract the contents of the file:

```
tar xvzf installPowertechMFA.tgz
```

Files are extracted to the directory installPowertechMFA.

4. Use the following commands to start the installer:

```
cd installPowertechMFA
./serverInstall
```

WARNING: If you need to terminate the installation process before finishing, delete the `/opt/helpsystems/PowertechMFA` directory and start the installer again.


- When prompted to choose whether you want to use the default ports, either indicate **y** accept and proceed, or **n** to change the ports used.

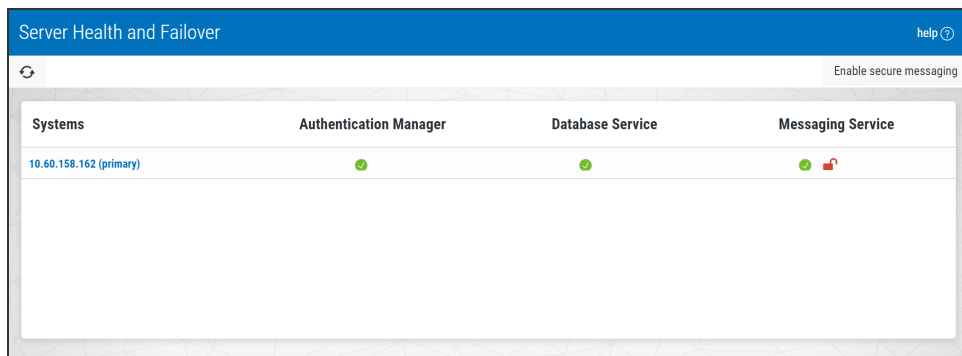
NOTE: In order to use Powertech MFA, your firewall must allow communication over the ports configured here.




- When prompted to provide the ActiveMQ IP address list, enter the IP addresses of the servers being used for this implementation, separated by semicolons (;). The order of the IP addresses entered here must be the same for each Powertech MFA Authentication Manager installation included in this deployment.

EXAMPLE:

```
Configuring ActiveMQ addresses:
  ActiveMQ IP address list - the list should be delimited by a semi-colon
(;)
  and should be entered in the same order on all systems:
  10.60.158.85;10.60.158.148;10.60.158.162
```

- When prompted to verify the server IP, confirm it is correct. Or, if it is not correct, enter **n**, then enter the correct IP.
- Powertech Multi-Factor Authentication creates the Primary database and starts the product. It installs to `/opt/helpsystems/PowertechMFA`.
- Open HelpSystems Insite and open the Powertech MFA module.
- In the Navigation Pane, click **Managers**.
- Click **Add**. The [New Manager screen](#) appears. Enter the IP Address of the first server in this deployment, enter the license key, and click **Save**. Repeat this step for the additional servers in this deployment.
- In the Navigation pane, choose **Server Health and Failover**. All servers configured should appear in this table. The Primary server's name is listed in blue. For a full description, see [Server Health and Failover screen](#). A  in the Authentication Manager and Database Service columns indicate the services are active and ready for you to proceed with the remaining secondary installations.



Systems	Authentication Manager	Database Service	Messaging Service
10.60.158.162 (primary)			

As mentioned previously, the application layer handles governance of the leader. The terms *leader* and *master* are basically synonymous. Leader pertains to the application layer, which determines the database master. The leader and master are synchronized with one another.

If the leader changes, as does the master database, and vice versa. In our recommended three-system deployment, when system 1 fails for any reason, system 2 becomes the leader, and the database is promoted to the master. All other instances are designated secondary and stream from the new master (system 2). To initiate failover manually, see [Manual Failover](#).

13. After you have confirmed the Primary server's Authentication Manager and Database Service are active, repeat steps 2-8 for all additional servers included in this deployment. Be sure the ports and Server List entry is identical for each installation.

To secure the messaging service, see [Enabling Secure Messaging](#).

Installing the Authentication Manager and Data Services with Failover Support on Windows


1. Download the Powertech Multi-Factor Authentication installer ([setupPowertechMFA.exe](#)) from the [Powertech Multi-Factor Authentication download page](#). (The "Trial" download is the full product, which can be unlocked with a valid License Key.) If you intend to deploy failover with two or more servers, the installer must be downloaded (or otherwise transferred) to each server being used. The installation procedure must be run on each server being included in the Powertech MFA deployment.
2. Double-click the installer file to begin the installation process.

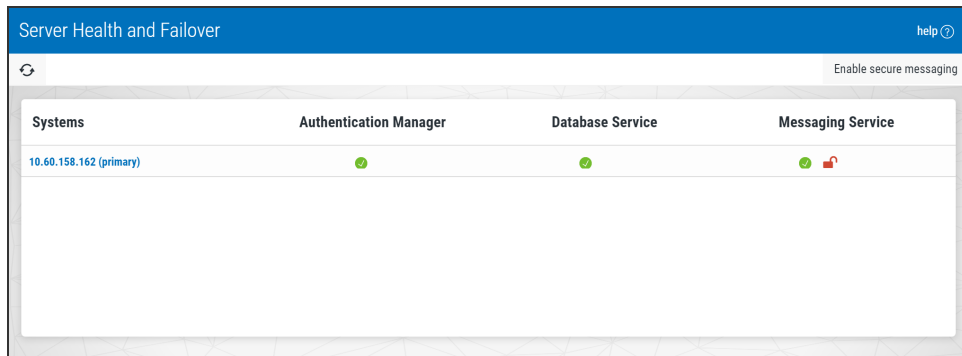
WARNING: If you need to terminate the installation process before finishing, delete the C:\Program Files\Help Systems\Powertech MFA folder and start the installer again.




3. Follow the instructions to continue the installation.
4. When the HelpSystems Access Manager and Data Services Configuration Manager appears, configure ports for the manager and services.

NOTE: In order to use Powertech MFA, your firewall must allow communication over the ports configured here.

The installer informs you if the default ports are available. If a port is not available, enter a new port number and click **Test** to see if it is available.

5. For Server List, enter the IP addresses of the servers being used for this implementation, separated by semicolons (;). The order of the IP addresses entered here must be the same for each Powertech MFA Authentication Manager installation included in this deployment.
6. Click **OK** to save the ports and continue installation. See also [Port Descriptions](#).
7. Click **Finish** to complete installation on the Primary server.
8. Open HelpSystems Insite and open the Powertech MFA module.
9. In the Navigation Pane, click **Managers**.
10. Click **Add**. The [New Manager screen](#) appears. Enter the IP Address of the first server in this deployment, enter the license key, and click **Save**. Repeat this step for the additional servers in this deployment.
11. In the Navigation pane, choose **Server Health and Failover**. The server you have just configured should appear in this table, and be marked "primary." For a full description, see [Server Health and Failover screen](#). A  in the Authentication Manager and Database Service columns indicate the services are active and ready for you to proceed with the remaining secondary installations.



Systems	Authentication Manager	Database Service	Messaging Service
10.60.158.162 (primary)			

As mentioned previously, the application layer handles governance of the leader. The terms *leader* and *master* are basically synonymous. Leader pertains to the application layer, which determines the database master. The leader and master are synchronized with one another. If the leader changes, as does the master database, and vice versa. In our recommended three-system deployment, when system 1 fails for any reason, system 2 becomes the leader, and the database is promoted to the master. All other instances are designated secondary and stream from the new master (system 2). To initiate failover manually, see [Manual Failover](#).

12. After you have confirmed the Primary server's Authentication Manager and Database Service are active, repeat steps 2-7 for all additional servers included in this deployment. Be sure the ports and Server List entry is identical for each installation.


Enabling Secure Messaging

Enable secure messaging to set the 'use SSL' flag to true on each node and automatically import the SSL certificates into each node's Keystore.

NOTE: All instances should be installed before performing the certificate creation as the ActiveMQ Broker must be active on each node.


To enable secure messaging

1. In the Navigation pane, choose **Server Health and Failover**. The [Server Health and Failover screen appears](#).

A  icon indicates secure messaging is not enabled for a server.

2. Click **Enable Secure Messaging**. A message appears indicating that submitting this request will secure the messaging service on all servers that are currently using an insecure connection, and that this will restart the authentication managers.

NOTE: Authentication may be unavailable for a few seconds when enabling secure messaging.

3. Click **Yes** to confirm. A  icon in the Messaging Server column indicates secure messaging has been enabled for the server.

Installing the IBM i Agent

Ensure the following servers are available and running prior to installation:

- FTP Server
- Remote Command Server

Do the following to perform the installation or update:

1. Download the Powertech Multi-Factor Authentication installer (**setupPowertechMFA_IBMi.exe**) to your PC from the [Powertech Multi-Factor Authentication download page](#).
2. On the Choose Components panel, select which components you want to install. You can choose to install the Manuals and the Software for IBM i. Click **Next**.
3. If you are installing the Manuals only, the process completes and the installer closes. The Manuals have been installed. You can skip the rest of these steps.

NOTE: The manuals are installed to the following location:
C:\Program Files\PowerTech\Powertech MFA>manuals

4. On the IBM i Details panel:
 - a. Select or enter the IBM i system.
 - b. Enter a user profile and password that is a member of the user class *SECOFR and has at least the following special authorities: *ALLOBJ, *SECADM, *JOBCTL, *IOSYSCFG, and *AUDIT. The user profile should have Limit capabilities set to *NO.
 - c. (Optional) In the Advanced Settings section:
 - Enter a port number or use the arrows if you want to change the FTP port number to something other than the default of 21.
 - Select **Secure File Transfer** if you want to use FTPS (FTP over SSL) during the file transfer. The default FTPS secure port is 990, but it can be changed to the required secure port for your environment.

- In the **Timeout (seconds)** field, enter the number of seconds the session should be kept active during an FTP transfer. You can choose anywhere between 25 and 1800 seconds (30 minutes).

NOTE: If the transfer takes longer than the amount of time specified, the session will expire.

- d. Click **Next**.
5. You have two options on the Product Load Options panel:
 - a. Click **Immediate Load** if you'd like to load the product on the IBM i now.
 - b. Click **Staged Load** if you'd like to transfer the objects now and load them on the IBM i at a later time.

NOTE: See "Loading Staged Objects on the IBM i" (below) for instructions on how to load the staged objects on your selected IBM i system.

6. The Product Load Progress panel for Powertech Multi-Factor Authentication launches. If the Product Load Progress panel ends with an overall Failed message, the product upload could not complete properly. To find the reason the upload failed, click **View Logs** and review your logs. You can also use **Download** at the top of the logs to save the information for future review.

When the processing is complete, you have two choices:

- If this is the only installation or update of Powertech Multi-Factor Authentication that you're doing, click **Finish**.
- If you have installs or updates to do on other IBM i systems, click **Restart**. Then, return to step 4.

Loading Staged Objects on the IBM i

If you chose to stage your objects during step 5b of the installation or update process, do the following to manually load them on the IBM i you identified above.

1. On the IBM i, execute the following command to display the Work with Loads panel:
HSLOADMGR/HSWRKLOAD
2. Enter option **1**, Load, next to the Load Name for Powertech Multi-Factor Authentication and press Enter.

The installation program installs Powertech Multi-Factor Authentication, including the required user profiles and libraries (see table below for details).

The installation process displays the job log name, user, and job log number. Use the WRKSPLF command to display the job log for complete information on the Powertech Multi-Factor Authentication install.

Objects Installed on System

Installed on System	Description
Product Library	PTMALIB
User Profiles	PMAADMIN, which has special authorities *ALLOBJ, *AUDIT, *IOSYSCFG, *JOBCTL, *SAVSYS, *SECADM, *SERVICE, and *SPLCTL PMAUSER, which has no special authorities (These profiles are set to Password = *NONE so that they can't be used to sign on to the system.)
Authorization List	PMAADMIN - Powertech Multi-Factor Authentication Administrators
Subsystem	PMASBS
Job Queue Entries	PTMALIB/PMAJOBQ added to PMASBS
Objects in QGPL:	Depending on the exit points that are being monitored, there could be up to four programs starting with PMA created in QGPL.
Powertech-created Unregistered Exit Points:	POWERLOCK_AA

Configuring the IBM i Agent

After installation, you need to add any profiles that will require access to the IBM i agent's configuration settings to the PMAADMIN authorization list. Then, configure the IBM i agent to synchronize with Insite and the Authentication Manager.

1. Sign on to the IBM i system and add the product administrator's user profile to the PMAADMIN authorization list:

```
WRKAUTL PMAADMIN
```

2. Choose **2** to edit for the PMAADMIN authorization list.
3. Press **F6** and add the user profile. Object Authority should be set to *ALL.
4. Repeat steps 1-3 for any other product administrators.
5. Use the following command to open the Main Menu:

```
PTMALIB/WRKPTMA
```

6. Choose option **1** to open the [Insite Server Configuration panel](#).

7. Enter the IP address or DNS name (e.g. on Windows, the full computer name) and the port of the Insite server. The default port is 3030.

```

11/30/17      Multi-Factor Authentication      OSCAR
07:57:15     Insite Server Configuration        PMA3500
                                                QSECOFR

Address . . . . : mijohnson0786.helpsystems.com_

-----

Port . . . . . : 3030
Timeout . . . . : 5 (seconds)
SSL? . . . . . : N (Y=Yes, N=No)

F3=Exit

```

Press Enter to save changes.

8. Press **F3** to return to the Main Menu, then choose option 2. The [Work with Authentication Managers panel](#) appears. If you have already installed the Authentication Manager and Data Services, and added the Authentication Manager IP(s) to Insite, they appear here automatically.

```

12/01/17      Multi-Factor Authentication      OSCAR
08:26:40     Work with Authentication Managers  PMA3601
                                                QSECOFR

Options
 2=Change  4=Delete
Opt  IP Address      Port  SSL
--  -
 10.60.152.191      3040  N

Bottom

F3=Exit  F6=Add Manager

```



NOTE: If you have not yet installed/configured an Authentication Manager, you can press **F6** to add it here manually before it has been installed/added to Insite. (You will need to know the IP and port it will be installed on.)

9. Press **F3** to return to the Main Menu, then choose option 4. The [Emergency Override Setup panel](#) appears.

10. Enter any profiles that will be allowed to bypass authentication in case of an emergency. Press Enter. The IBM i agent has been configured.

NOTE: Choose option **3** to stop authentication on this IBM i system. See [Deactivate Authentication Verification panel](#) for details.

Next, you need to add the IBM i agent to Powertech Multi-Factor Authentication in Insite.

11. Open HelpSystems Insite and choose **Powertech Multi-Factor Authentication** from the navigation pane on the left, then choose **Agents**.
12. Ensure the IBM i system has been added as a product connection in Insite. See [Product Connections](#) in the Insite documentation.
13. If IBM i agent is Disabled, click  on the right side of the IBM i agent row and select **Enable**.
14. Click **IBM i agent**, then click **Add**. The [Agents > New System](#) screen appears.
15. For System, choose **Select System** and choose the system you just configured.
16. Configure any system settings and click **Save**. You return to the [Agents > IBM i agent screen](#).
17. To activate the system, click  (on the right side of the screen) and choose **Enable**.

When the necessary components have been installed, see [Administrator Setup Procedure](#) to begin configuring and using Powertech Multi-Factor Authentication.

Starting and Stopping the IBM i Agent for Backups

When started, the Powertech Multi-Factor Authentication IBM i agent places a lock on ptmalib, which can interfere with system backup procedures. For this reason, and also in order to facilitate the addition of Powertech Multi-Factor Authentication into the startup program, the following commands are available:

- **PMASTRMON** - Start Powertech Multi-Factor Authentication
- **PMAENDMON** - Stop Powertech Multi-Factor Authentication

When backing up your system, use PMAENDMON to deactivate the agent and remove the object lock. After the backup is complete, use PMASTRMON to start the agent. If you are performing a backup with IPL, you can incorporate these commands into your backup procedure either manually or using scripts in a backup tool like Robot Save or BRMS.

NOTE: When the Powertech Multi-Factor Authentication agent is ended, it is still fully configured, but inactive. While inactive, registered users are not asked to authenticate.

Upgrading Powertech Multi-Factor Authentication

These instructions guide you through the process of upgrading Powertech Multi-Factor Authentication.

NOTE: For system requirements, including IBM i Agent system values, see [Installing Powertech Multi-Factor Authentication](#).

WARNING: The Authentication Manager must be stopped in order to be upgraded, which means Powertech Multi-Factor Authentication will be out of service for a short period of time during the upgrade procedure. As such, we recommend scheduling the upgrade at a time with minimal server activity.

Upgrade Procedure Overview

Like installation, the Powertech Multi-Factor Authentication upgrade procedure on your network is a multi-step process. Perform the upgrade in the order listed below.

- **HelpSystems Insite.** This is the same as the installation process. See [HelpSystems Insite Documentation List](#) for instructions that describe how to install and use HelpSystems Insite. The latest version of HelpSystems Insite is required for compatibility with the latest Authentication Manager.
- **Powertech Multi-Factor Authentication Authentication Manager and Data Services.** The Authentication Manager must be stopped on the Primary and Secondary systems prior to installing the upgrade. See [Upgrading the Authentication Manager and Data Services](#).
- **Powertech Multi-Factor Authentication IBM i agent.** The latest IBM i agent software must be installed on all systems to be secured by Powertech Multi-Factor Authentication to ensure compatibility. See [Installing the IBM i Agent](#).

Upgrading the Authentication Manager and Data Services

The following instructions demonstrate how to upgrade the Authentication Manager and Data Services on a Primary and Secondary system in order to provide replication and failover capability. If you intend to upgrade on a single system only, use the initial steps of the following procedure for your platform (stopping when directed to repeat steps for a Secondary system).

As of Powertech MFA 1.5, the process used to support failover has changed. See [Installing the Authentication Manager and Data Services with Failover Support](#) for details.

To upgrade the Powertech Multi-Factor Authentication Authentication Manager and Data Services on Linux

1. Login as root on the server you want to use as your Primary installation. The installer must be run as root or with sudo.
2. Download the Powertech Multi-Factor Authentication for Linux file (installPowertechMFA.tgz) to a temporary directory on the system. To acquire the file, go to the [HelpSystems website](#) and click **My Account**. (The "Trial" download is the full product, which can be unlocked with a valid License Key.)
3. Use the following command to extract the contents of the file:

```
tar xvzf installPowertechMFA.tgz
```

Files are extracted to the directory installPowertechMFA.

4. Use the following commands to stop the Authentication Manager service:
 - If your Linux system supports systemctl, use:

```
systemctl stop  
HelpSystemsAccessAuthenticatorManager.service
```

- If your Linux system does not support systemctl, use:

```
/etc/init.d/HelpSystemsAccessAuthenticatorManager.sh stop
```

5. Use the following commands to start the installer:

```
cd installPowertechMFA  
./serverInstall
```

WARNING: If you need to terminate the installation process before finishing, delete the /opt/helpsystems/PowertechMFA directory and start the installer again.


6. When prompted to choose whether you want to use the default ports, either indicate **y** accept and proceed, or **n** to change the ports used.

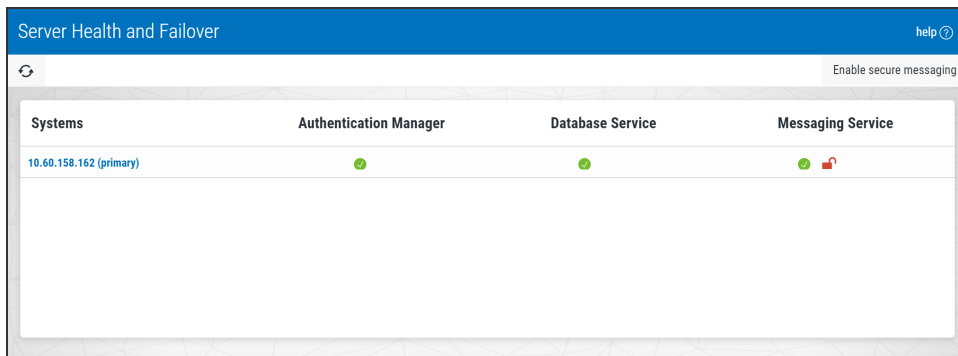
NOTE: In order to use Powertech MFA, your firewall must allow communication over the ports configured here.




7. When prompted to provide the ActiveMQ IP address list, enter the IP addresses of the servers being used for this implementation, separated by semicolons (;). The order of the IP addresses entered here must be the same for each Powertech MFA Authentication Manager installation included in this deployment.

EXAMPLE:

```
Configuring ActiveMQ addresses:  
ActiveMQ IP address list - the list should be delimited by a semi-colon  
(;)  
and should be entered in the same order on all systems:  
10.60.158.85;10.60.158.148;10.60.158.162
```

8. When prompted to verify the server IP, confirm it is correct. Or, if it is not correct, enter n, then enter the correct IP.
9. Powertech Multi-Factor Authentication creates the Primary database and starts the product. It installs to /opt/helpsystems/PowertechMFA.
10. Open HelpSystems Insite and open the Powertech MFA module.
11. In the Navigation Pane, click **Managers**.
12. Click **Add**. The [New Manager screen](#) appears. Enter the IP Address of the first server in this deployment, enter the license key, and click **Save**. Repeat this step for the additional servers in this deployment.
13. In the Navigation pane, choose **Server Health and Failover**. All servers configured should appear in this table. The Primary server's name is listed in blue. For a full description, see [Server Health and Failover screen](#). A  in the Authentication Manager and Database Service columns indicate the services are active and ready for you to proceed with the remaining secondary installations.



Systems	Authentication Manager	Database Service	Messaging Service
10.60.158.162 (primary)			

As mentioned previously, the application layer handles governance of the leader. The terms *leader* and *master* are basically synonymous. Leader pertains to the application layer, which determines the database master. The leader and master are synchronized with one another. If the leader changes, as does the master database, and vice versa. In our recommended three-system deployment, when system 1 fails for any reason, system 2 becomes the leader, and the database is promoted to the master. All other instances are designated secondary and stream from the new master (system 2). To initiate failover manually, see [Manual Failover](#).

14. After you have confirmed the Primary server's Authentication Manager and Database Service are active, repeat steps 2-8 for all additional servers included in this deployment. Be sure the ports and Server List entry is identical for each installation.

To secure the messaging service, see [Enabling Secure Messaging](#).

To upgrade the Powertech Multi-Factor Authentication Authentication Manager and Data Services on Windows

1. Login to the Windows server of your Primary installation.
2. Download the Powertech Multi-Factor Authentication installer ([setupPowertechMFA.exe](#)). To do so, go to the [HelpSystems website](#) and click **My Account**. (The "Trial" download is the full product, which can be unlocked with a valid License Key.)

3. Stop the Authentication Manager service. To do so:
 - a. In the search bar type "services.msc" and press Enter. Or, click the **Start** menu and choose **Run**, then type "services.msc".
 - b. Right-click HelpSystems Powertech Multi-Factor Authentication Manager and choose **Stop**.
 - c. Close the Services window.
4. Double-click the installer file to begin the installation process.


WARNING: If you need to terminate the installation process before finishing, delete the C:\Program Files\Help Systems\Powertech MFA folder and start the installer again.

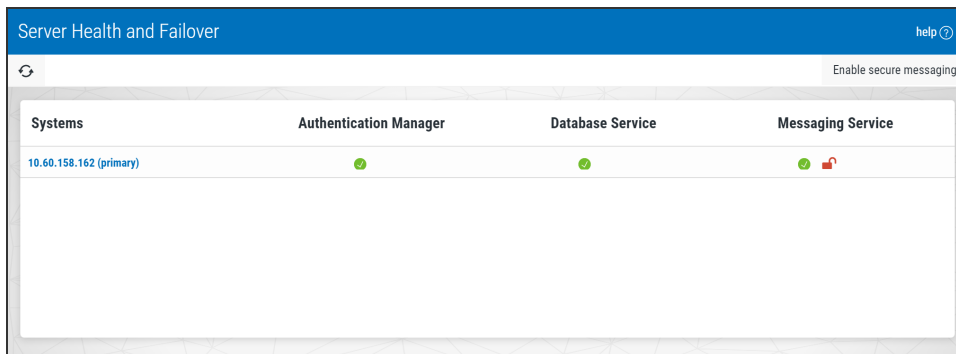
5. Follow the instructions to continue the installation.
6. When the HelpSystems Access Manager and Data Services Configuration Manager appears, configure ports for the manager and services.

NOTE: In order to use Powertech MFA, your firewall must allow communication over the ports configured here.

The installer informs you if the default ports are available. If a port is not available, enter a new port number and click **Test** to see if it is available.

7. For Server List, enter the IP addresses of the servers being used for this implementation, separated by semicolons (;). The order of the IP addresses entered here must be the same for each Powertech MFA Authentication Manager installation included in this deployment.
8. Click **OK** to save the ports and continue installation. See also [Port Descriptions](#).
9. Click **Finish** to complete installation on the Primary server.
10. Open HelpSystems Insite and open the Powertech MFA module.
11. In the Navigation Pane, click **Managers**.
12. Click **Add**. The [New Manager screen](#) appears. Enter the IP Address of the first server in this deployment, enter the license key, and click **Save**. Repeat this step for the additional servers in this deployment.

- In the Navigation pane, choose **Server Health and Failover**. The server you have just configured should appear in this table, and be marked "primary." For a full description, see [Server Health and Failover screen](#). A  in the Authentication Manager and Database Service columns indicate the services are active and ready for you to proceed with the remaining secondary installations.



As mentioned previously, the application layer handles governance of the leader. The terms *leader* and *master* are basically synonymous. Leader pertains to the application layer, which determines the database master. The leader and master are synchronized with one another. If the leader changes, as does the master database, and vice versa. In our recommended three-system deployment, when system 1 fails for any reason, system 2 becomes the leader, and the database is promoted to the master. All other instances are designated secondary and stream from the new master (system 2). To initiate failover manually, see [Manual Failover](#).

- After you have confirmed the Primary server's Authentication Manager and Database Service are active, repeat steps 2-7 for all additional servers included in this deployment. Be sure the ports and Server List entry is identical for each installation.
To secure the messaging service, see [Enabling Secure Messaging](#).

Implementing Powertech Multi-Factor Authentication

This guide describes how to configure and use Powertech Multi-Factor Authentication. It describes how administrators can tailor Powertech Multi-Factor Authentication to fit the security needs of their organization, how users can register devices to act as authentication factors, and how those users can authenticate using a registered device.

Administrator Setup Procedure

After installation, complete the following procedure to configure Powertech Multi-Factor Authentication.

NOTE: See [Installing Powertech Multi-Factor Authentication](#) for installation information.

To Configure Powertech Multi-Factor Authentication

Configure Powertech Multi-Factor Authentication in HelpSystems Insite by configuring the general Powertech Multi-Factor Authentication settings, adding and configuring IBM i agents in Insite, configuring email settings, then adding and/or importing users to Powertech Multi-Factor Authentication.

Configure Powertech Multi-Factor Authentication Settings

The Settings screen includes several important settings related to authentication and general management of Powertech Multi-Factor Authentication. Review and configure all options available on the Settings screen prior to deploying Powertech Multi-Factor Authentication. See [Settings Screen](#).

Add and Configure IBM i Agents in Insite



NOTE: The following instructions assume the Powertech Multi-Factor Authentication IBM i Agent software has been installed on the IBM i system. See [Installing the IBM i Agent](#).

1. Sign in to Insite and choose Powertech Multi-Factor Authentication from the Navigation Pane on the left.
2. Click **Systems Defaults** to configure default agent settings. The [Edit Default System screen](#) appears. Here, you can:
 - Choose whether or not to allow user profiles that have not been assigned to a user in Powertech Multi-Factor Authentication.
 - Choose whether to allow or deny individual profiles for exit point sign on.
 - Choose whether to activate Exit Points by default for new IBM i Agents when the agent is activated.
3. When you have finished configuring the defaults, click **Save**.
4. On the Navigation Pane, choose **Agents**, click **IBM i Agent**, then click **Add** to open the [New System screen](#), where you can add an agent. Do the following to setup the agent:

NOTE: Settings for individual systems in Edit Systems override the equivalent settings configured in [Edit Default System screen](#).

- a. Choose **Select System** and choose the IBM i system.
- b. Select whether or not to allow profiles that have not been assigned in Powertech Multi-Factor Authentication.
- c. Choose how to handle sign on of unassigned profiles. You can set Use Agent Defaults to **Off** in order to specify a profile to use for unassigned profile sign ons. Or, choose **On** to use the default settings defined in the [Edit Default System screen](#).
- d. Check the Exit Points you want to enable and click **Activate**.

NOTE: If you choose to require authentication for Exit Point sign on, users will need to download the Desktop Agent from the User Portal during User Setup. Instructions for doing so are included under [User Setup](#).

- e. Click **Save**.
5. To enable the system, click  and choose **Activate**.
6. Click **Agents** again in the navigation pane to show the IBM i agent option. If the "IBM i agent" row reads "Disabled", click  for this option (on the right side of the screen) and choose **Enable** to enable IBM i agent service with Powertech Multi-Factor Authentication. You are asked if you want to change the statuses (activated or deactivated) of all systems connected to the agent. Choose **Yes** to do so and **No** to change only this system.

Add Groups

Before you begin adding Powertech Multi-Factor Authentication users, it is a good idea to create any Groups you would like to organize your users into. When users are organized into a Group, they can, for example, be enabled, disabled, or sent an email all at once. They can also be configured to use their own authentication method(s). (Users not assigned to a Group when added are assigned to the default group.)

1. On the Navigation Screen, choose **Users**.
2. Choose **Add > Add Group**. The [New Group screen](#) appears.
3. Enter a Name and Description for the Group.
4. Choose whether to Enable, Disable, or Inherit the five authentication methods.
5. Click **Save**. This Group will not be available for selection when you add Powertech Multi-Factor Authentication Users.

Add Users

Powertech Multi-Factor Authentication must be added and linked to a profile on an IBM i agent system before registration or authentication can take place. Users can be added manually on an individual basis, or imported from Access Directory and created automatically.

NOTE: It is faster to import Active Directory users than create them manually, as they are created automatically upon import (see the next section, [Importing Users](#), for details).

WARNING: QSECOFR is an IBM-supplied profile that should not, in general, be configured for multi-factor authentication. IBM warns: "do not change values *[other than the password]* for IBM-supplied user profiles. Changing these profiles can cause system functions to fail." See "IBM-supplied user profiles" in the IBM Security Reference at <https://www.ibm.com/support/knowledgecenter/> for more details.

Adding Users Manually

Powertech Multi-Factor Authentication Users can be created individually using the following procedure:

1. In the Navigation Pane, choose **Users**, then **Add > Add User** to open the [New User screen](#).
2. Enter the Powertech Multi-Factor Authentication Name. This is the name the user will be instructed to use to, for example, login to the Powertech Multi-Factor Authentication User Portal during the registration procedure. It can be the same as the Active Directory account name or IBM i profile the user will be attached to.
3. Enter the Active Directory Username, if one exists for the user. Skip this step if the user has only an IBM i profile, and no Active Directory Username.
4. Enter the user's Full Name, email, and desired Group.
5. For 'User Status,' set Enabled to **Yes**, which activates the user within Powertech Multi-Factor Authentication.
6. For 'Authenticate User,' choose **Yes** if you want the user to be required to authenticate immediately, then next time they attempt to sign on to the IBM i. You can leave this set to **No** if you would rather wait and give the user time to register an authentication device before requiring them to authenticate.
7. For Authentication Methods, select whether you want to enable or disable each method, or inherit settings from the Group settings.
8. Link IBM i profiles with this Powertech Multi-Factor Authentication User:
 - a. Under 'IBM i Profiles and Systems,' click **Add**.
 - b. Select a system and choose **Next**.
 - c. Select one or more profiles and choose **Save**.
 - d. Repeat the above steps to add profiles from additional systems.
9. Click **Save** to save the User in Powertech Multi-Factor Authentication's database.

Importing Users

Import users to expedite the process of creating Powertech Multi-Factor Authentication users using the following procedure:

1. Import Active Directory users.

In order for Powertech Multi-Factor Authentication to authenticate a user, it must have its own record of the user enrolled in Powertech Multi-Factor Authentication's database. Powertech Multi-Factor Authentication can create these users automatically while importing Active Directory users. However, before importing IBM i user profiles, the Powertech Multi-Factor Authentication users must already exist.

Import Active Directory users first. This way, your Powertech Multi-Factor Authentication users can be created quickly for every Active Directory user. Then, you can import IBM i user profiles and use Powertech Multi-Factor Authentication's *Smart Match* feature to link them to the existing Powertech Multi-Factor Authentication users that were created when you imported from Active Directory.

Any individual who does not have an Active Directory account must be imported manually. See [Importing Users Manually](#).

- a. Configure LDAP using the [LDAP Settings screen](#). To do so, in the Navigation Pane, click **LDAP**.
- b. Once LDAP has been configured, in the Navigation Pane, choose **Users**, then select **Add > Import Users**. The [Import Users screen](#) appears.


- c. For Location, choose **Active Directory**. For LDAP Context, enter the LDAP attributes you would like to use.
- d. For **Group**, select a Group for the users you are about to import.

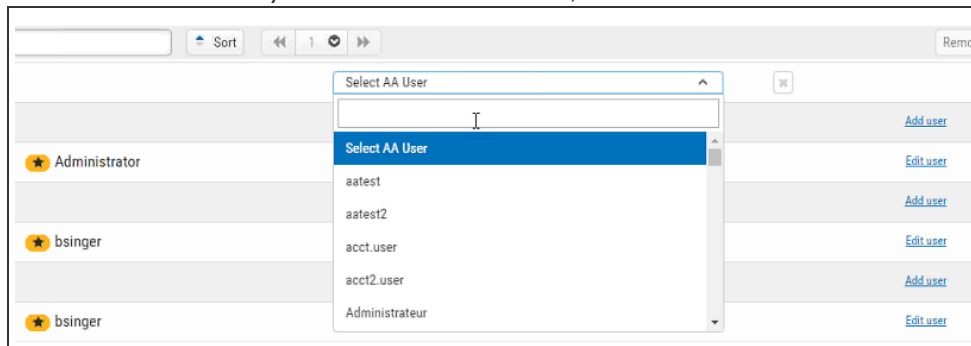
NOTE: To add a group, on the Users screen, click **Add > Add Group**. See [Users screen](#) for more details.

- e. Click **Start Import**. An Powertech Multi-Factor Authentication user is created for every Active Directory user.

2. **Import a list of IBM i user profiles and map them to the appropriate Powertech Multi-Factor Authentication users.**

WARNING: Powertech Multi-Factor Authentication does not prevent the possibility of system access using the Program/procedure field by a user during sign on. To disable the use of this field for users, set their Limit Capabilities user profile setting to *YES or *PARTIAL.

- a. In the Navigation Pane, choose **Users**, then select **Add > Import Users**. The [Import Users pane](#) appears.
- b. For Import Type, choose **IBM i Profiles**.
- c. For System, select the IBM system that includes the profiles you would like to import.
- d. You can filter results using a string of up to ten characters.
- e. Set Smart Match to **On** if you want Powertech Multi-Factor Authentication to attempt to match profiles with existing Powertech Multi-Factor Authentication users. (See [Import Users screen](#) for more details.)
- f. Click **Start Import** to begin importing profiles. After import, use the 'Assign Users to IBM i Profiles' section to link Powertech Multi-Factor Authentication users with imported IBM i profiles. Tips:
 - If Smart Match was enabled, use the  icon to help identify matching users.
 - If the IBM i user was already assigned to an Powertech Multi-Factor Authentication user, the Powertech Multi-Factor Authentication user name appears in the column to the right of the Smart Match results.
 - Click **Add User** to display a menu that allows you to select an Powertech Multi-Factor Authentication user for the imported IBM i profile. Click within the text box and type to quickly identify the Powertech Multi-Factor Authentication user you would like to select, or use the scroll bar.



- Click **Edit User** to open the [Edit User screen](#) where you can edit user settings.

Send Email to Users

After users have been added to Powertech Multi-Factor Authentication, they need to be informed how to register the device(s) they will be using for authentication. Powertech Multi-Factor Authentication provides administrators with a pre-configured (and customizable) email that can be used for this purpose. The email includes the Powertech Multi-Factor Authentication User name, and a link to the User Portal, which allows them to register devices.

Configuring Email Settings

1. In the Navigation Pane, click **Email** to configure email settings. See [Email Settings screen](#).
 - a. For 'Enabled,' choose **On** to allow emails to be sent from Powertech Multi-Factor Authentication.
 - b. For 'Host,' enter your organization's email server (e.g. smtp.yourcompany.com).
 - c. For 'Port,' select the email server port. (The default is 25, the usual default smtp port.)
 - d. Set 'Use SSL with Email' to **On** to secure the connection between Powertech Multi-Factor Authentication and your mail server.
 - e. For 'Email,' enter the account you want in the From field for outgoing messages.
 - f. Enter your login credentials.
 - g. If desired, enter a custom message. For example, if you intend to enable Exit Point authentication, you might inform users that they will need to download and install the Desktop Agent from the User Portal during the registration process in order to authenticate Exit Point Sign ons.
2. Click **Preview User Portal registration email** to preview the contents of the email. This is a representation of how the message will look to users.
3. Click **Save**.

Sending a 'Welcome' Email to Users

1. On the Navigation Pane, choose **Users** to go to the [Users screen](#).
2. Check the user(s) and/or group(s) you want to email.
3. Click **Send Email**. A confirmation message appears.
4. Click **Send**. An email is sent to the selected recipients.

Users will now be able to register devices using the User Portal and authenticate.

Configuring RADIUS Authentication

If you are using an existing RADIUS server to authenticate users, first complete the above steps: [To Configure Powertech Multi-Factor Authentication](#). Then, proceed with the following steps to configure your RADIUS server and Powertech Multi-Factor Authentication Users accordingly.

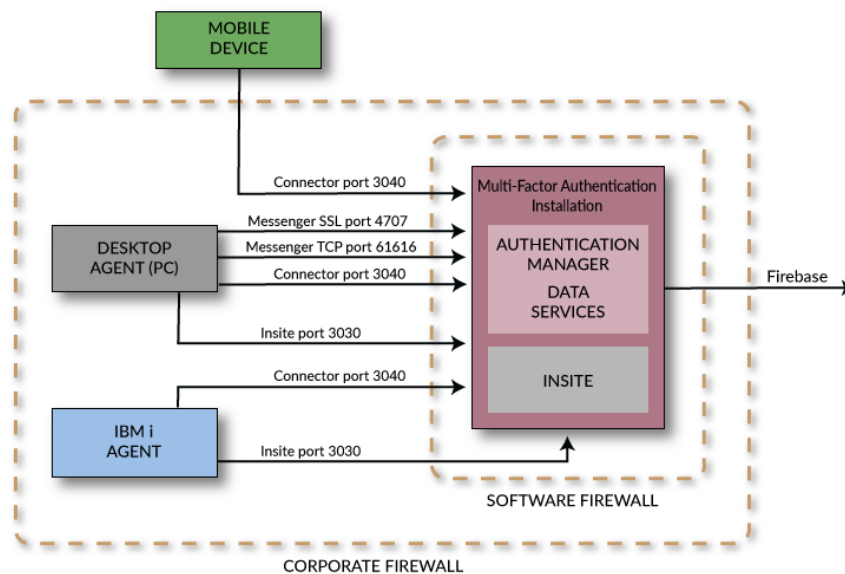
NOTE: Powertech Multi-Factor Authentication can use either its own authentication or RADIUS authentication, but not both at the same time.

1. In Insite's Navigation pane, choose **RADIUS Authentication**.
2. Toggle Authenticate Using Radius to **On**.
3. Enter the RADIUS Server Location, Port, Secret Key, and other requested information. See [RADIUS Authentication screen](#) for details.
4. Click **Save**. Now that you have configured your RADIUS server, you need to add the RADIUS user credentials to the Powertech Multi-Factor Authentication Users that will need to be authenticated.
5. In Insite's Navigation pane, choose **Users**.
6. Edit a User that will be authenticated with RADIUS. The [Edit User pane](#) appears.
7. In the RADIUS User Name field, enter the user name referred to by RADIUS.
8. Click **Save**.

Port/Server Configuration Diagrams

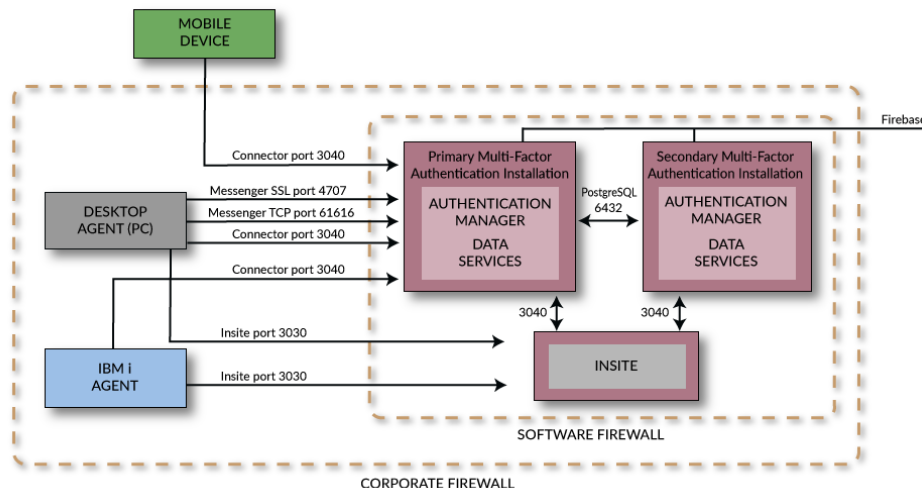
The following diagrams show two possible Powertech Multi-Factor Authentication system configurations.

Basic Configuration



Basic Configuration with Failover Support

For a dual server installation, the database port (6432 by default) also needs to be open.



User Setup Procedure

Use the following procedure to install and configure Powertech Multi-Factor Authentication in preparation for authenticating with your mobile device, YubiKey, or Soft Token.

NOTE: *Soft Token* refers to a one-time password accessible using a 4-digit PIN code on your PC.

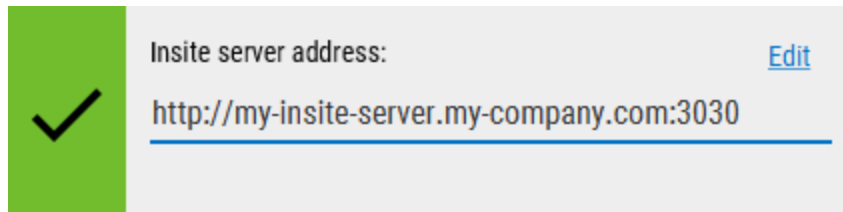
You will receive an email from your administrator when you are ready to begin. This email will include the links you need to get started.


1. Open the email sent by your administrator with the subject "Welcome to Powertech Multi-Factor Authentication." Read this email.
2. If you will be using a mobile device for authentication, download the HelpSystems Powertech Multi-Factor Authentication mobile app from your device's app store (iTunes App Store for iOS or Google Play for Android). Links to these apps are included in the email you received.

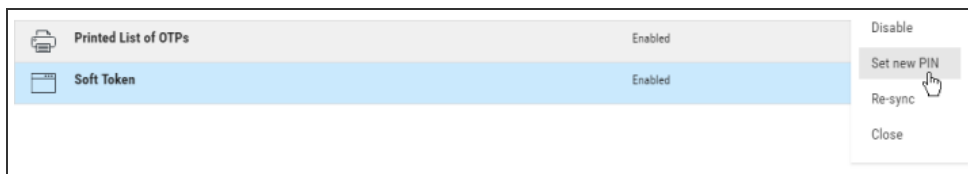


3. Click the **Go to Powertech Multi-Factor Authentication User Portal** link, complete the sign in form (using the Powertech Multi-Factor Authentication User Name specified in the email you received), and click **Login**. The [User Portal](#) appears. This is the page used to register and manage your device(s). The first time you access the User Portal, you are not required to authenticate.
4. If you will be using the Soft Token (authenticating with your PC), or Exit Point sign on (e.g. FTP), you will also need the Powertech Multi-Factor Authentication Desktop Agent installed on your desktop (Windows) workstation, and started (if the Desktop Agent has not already been installed by your IT staff).

- a. Click **Download the Desktop Agent** and follow the on-screen instructions to install it.
- b. Use your Windows Start Menu to start the Powertech Multi-Factor Authentication Desktop Agent program.
- c. Login to the Desktop Agent and specify the Insite server name and port (e.g. `http://yourinsiteservername:3030`). See [Desktop Agent](#) for more details.



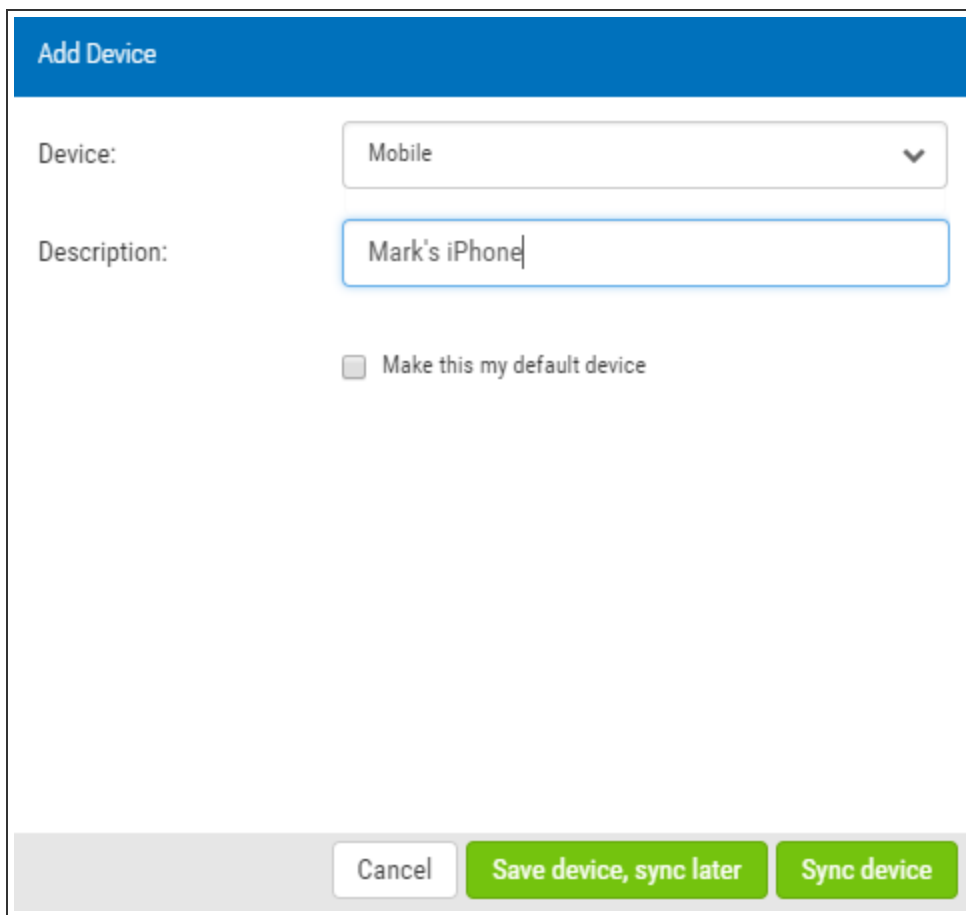
5. In the User Portal, if you will be using the Soft Token for authentication, click the  on the right side of the Soft Token option and choose **Set New Pin**.



6. Enter the desired 4-digit pin and click **Save**.

NOTE: If you are using the Soft Token or a printed list of OTPs (one-time passwords), registering a device is not required and you can skip ahead to [User Authentication](#).

7. In the User Portal, if you will be using a mobile device or YubiKey for authentication, click **Add Device**.



Add Device

Device: Mobile

Description: Mark's iPhone

Make this my default device

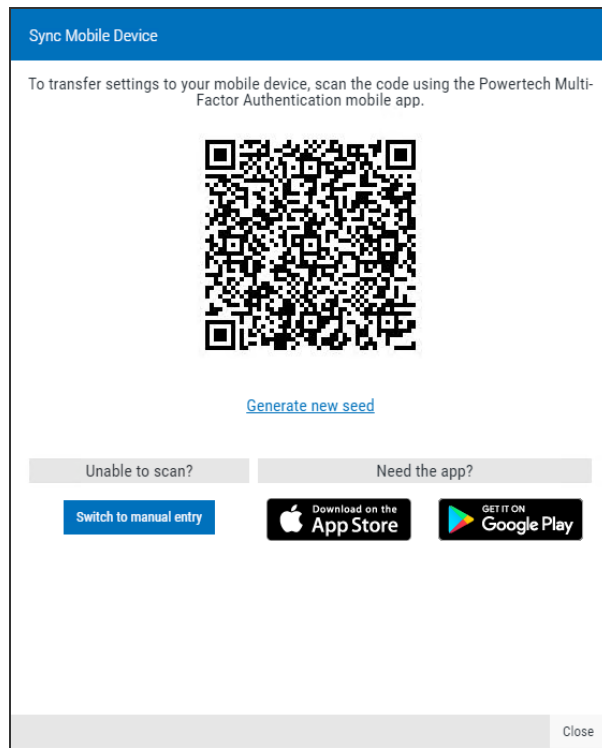
Cancel Save device, sync later Sync device

8. Select the type of device from the Device drop-down and add a description.
9. Check 'Make this my default device' if this is the device you will usually use to authenticate.
10. Complete the registration using the following steps:
 - To add a YubiKey, insert the YubiKey and press the button (a short press). This will authenticate it and add it as a device.

NOTE: If this is the first time the YubiKey has been inserted, it may take a few moments to install drivers. After installation, you may need to remove the YubiKey, re-insert, and re-press.

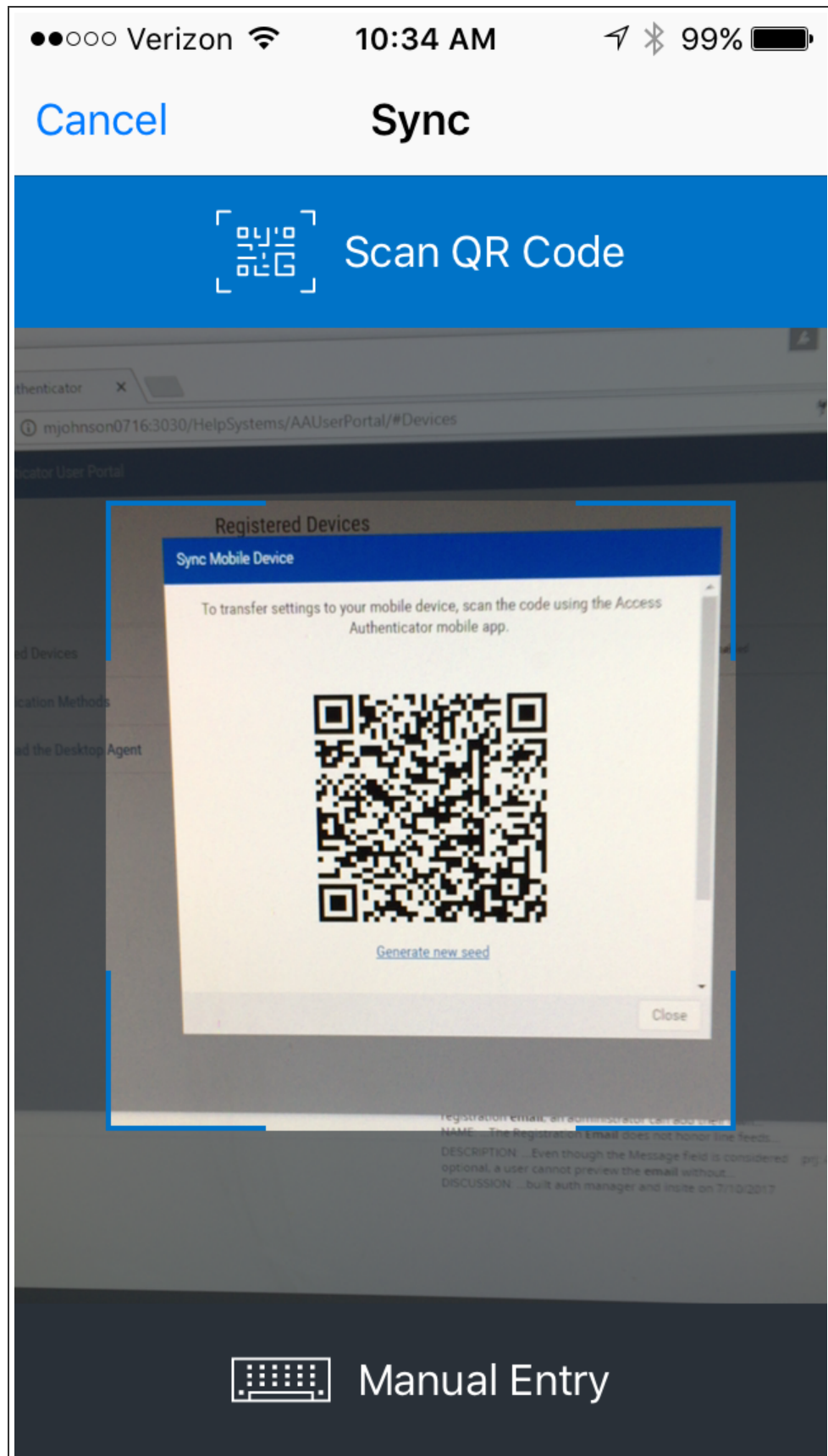
- To add a mobile device:
 - a. Click **Sync device**. The Sync Mobile Device screen appears.

NOTE: You can choose **Save device, sync later** to keep a record of the device in the User Portal, but synchronize it with Powertech Multi-Factor Authentication later.



- b. On your mobile device, open the Powertech Multi-Factor Authentication app. Click the gear icon in the upper right .

- c. Scan the on-screen QR code with your device's camera to sync. (When the QR code appears in the camera's range, it scans and closes automatically).



NOTE: If your camera is broken, you can click **Manual Entry** to type the string manually on your mobile device. In the Sync Mobile Device screen, scroll down and choose **Switch to manual entry** to acquire the Authentication Key to be entered.

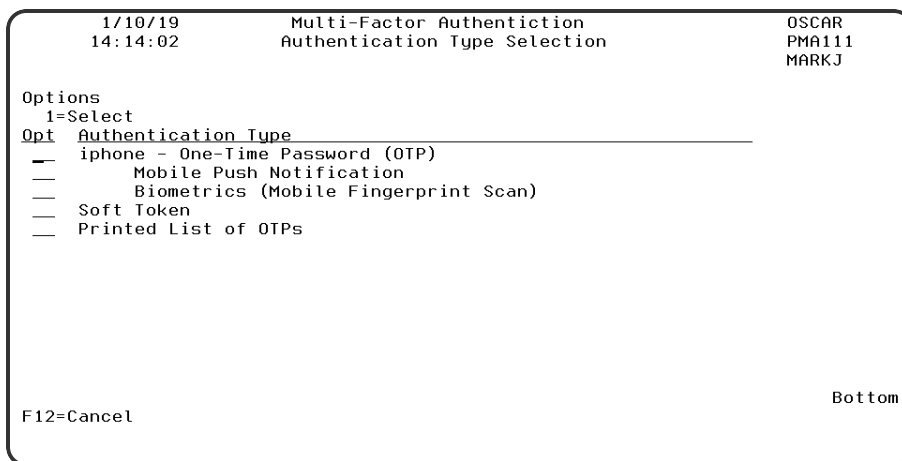
- d. Click **Close** to close the Sync Mobile Device window. Your device is registered.
- 11. An email with the subject "Powertech Multi-Factor Authentication - New Device Registration" appears in your inbox, which includes the type and description of the registered device. You are now ready to authenticate.

User Authentication

If you are using a mobile device or YubiKey, after you have registered the device, you are ready to authenticate. If you are using the Soft Token or Printed List of OTPs, registering a device is not required.

Authenticating an Interactive IBM i Sign On

1. Sign on to the IBM i system your administrator has configured with Powertech Multi-Factor Authentication. Or, run a program secured by your administrator. When you do, a screen with one or more of the possible authentication methods appears:




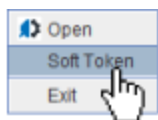
NOTE: If the above screen is accessed by calling a program, F12=Cancel appears instead of F3=Signoff.


2. Enter **1** next to the authentication method you would like to use, and do the following to authenticate:
 - For **One-Time Password (OTP)**, open the mobile app and enter the six-digit number from your mobile device into the IBM i prompt, then press Enter.
 - For **Mobile Push Notification**, open the notification using the Powertech Multi-Factor Authentication mobile app and tap **Accept**.
 - For **Biometrics (Mobile Fingerprint Scan)**, open the notification using the Powertech Multi-Factor Authentication mobile app and tap **Accept**, then scan your fingerprint.

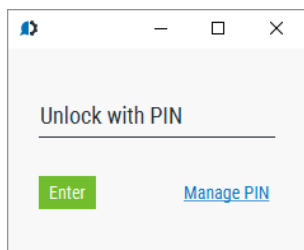
• **NOTE:** See [Troubleshooting Authentication with your Mobile Device](#) if you have difficulties authenticating with your mobile device.

- For **Printed list of backup OTPs**, enter a valid six-digit password, then press Enter.
- For **YubiKey ID**, insert the YubiKey and press (short press) the YubiKey button.
- For **Soft Token**:

- a. On your PC, click the HelpSystems icon  in the Windows System Tray and choose **Soft Token**.

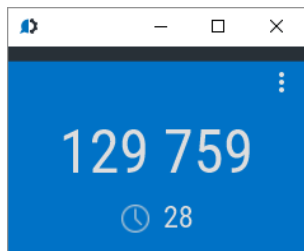


Alternatively, you can click the  button in the upper right of the Desktop Agent. The Soft Token entry panel appears.



NOTE: Here, you can click **Manage Pin** to login to the [User Portal](#) where you can set your pin.

- b. Enter the pin configured in step 6 of the [User Setup Procedure](#). The One-Time Password appears.



- c. Enter the six-digit number displayed on the Soft Token panel into the IBM i prompt, then press Enter.

3. If authentication is successful, you are allowed to sign on.

Authenticating an FTP IBM i Sign On

If you are signing on using an Exit Point, like FTP, the Powertech Multi-Factor Authentication Desktop Agent must be installed and running (See [User Setup](#)).

1. Connect to the IBM i via FTP and sign on.
2. The Powertech Multi-Factor Authentication Desktop Agent appears on your Windows workstation.



NOTE: If you do not see the above screen, click the arrow in the upper right corner of the Desktop Agent window:



3. To allow the connection, click **Allow**. For Device, click the drop-down arrow and select the device you will use to authenticate. You are presented with one or more authentication options. Use one of the following methods to authenticate:
 - Click **One-Time Password (OTP)**, then open the Powertech Multi-Factor Authentication mobile app. Enter the six-digit number from your mobile device into the Desktop Agent, then press Enter or click **Submit**.
 - Click **Push Notification**, then open the notification using the Powertech Multi-Factor Authentication mobile app and tap **Accept**.
 - Click **Mobile Biometrics**, then open the notification using the Powertech Multi-Factor Authentication mobile app and tap **Accept**, then scan your fingerprint.
 - For **YubiKey ID**, click **Not ready. Click here.** if shown. Insert the YubiKey and press (short press) the YubiKey button.
 - For **Printed list of backup OTPs**, enter a valid six-digit password, then press Enter (or click **Submit**).

NOTE: See [Troubleshooting Authentication with your Mobile Device](#) if you have difficulties authenticating with your mobile device.

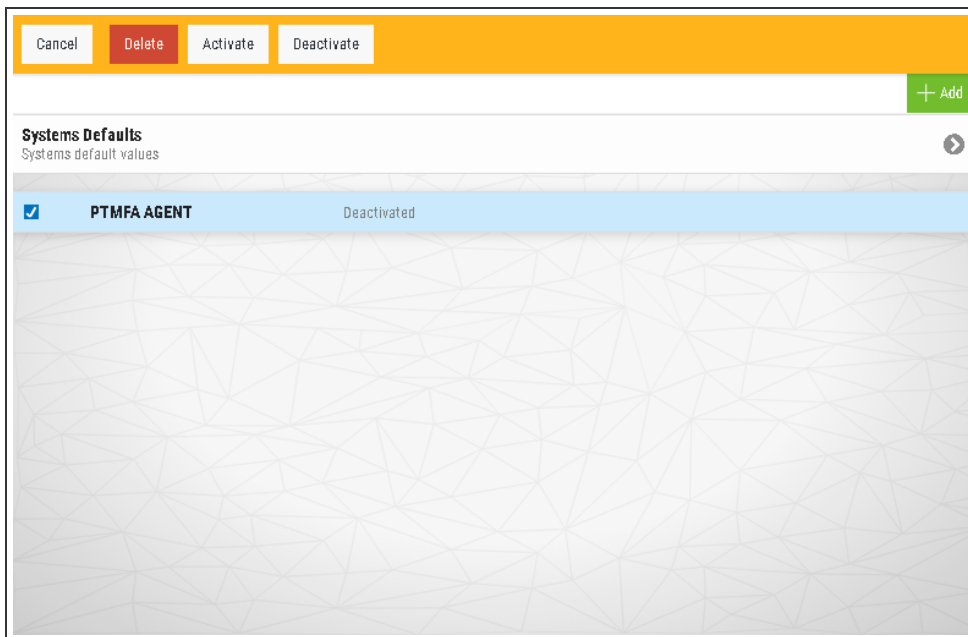
4. If authentication is successful, you are granted access.

Reference

The topics in this section include descriptions of Powertech Multi-Factor Authentication's options and controls.

Agents screen

Use these settings to add, remove, enable, disable Powertech Multi-Factor Authentication agents.



How to Get There

In the Navigation Pane, choose **Agents**, then select the Agent type (e.g. IBM i agent).

Options

Add

Click **Add** to open the [New Systems](#) page where you can define a new agent.


Systems Defaults

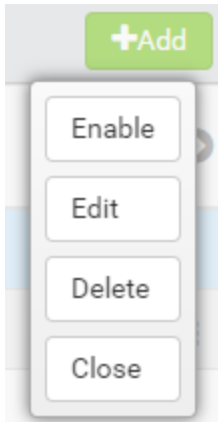
Select this option to open the [Edit Default System](#) page where you can change the default system values.

[agent list]; **Cancel** • **Delete** • **Enable Selected** • **Disable Selected**

Check the box to the left of one or more systems and additional buttons appear at the top of the screen.

- **Cancel.** Click **Cancel** to dismiss the buttons.
- **Delete.** Click **Delete** to remove the selected systems from Powertech Multi-Factor Authentication.
- **Enable Selected.** Click **Enable Selected** to begin authentication for the selected systems.
- **Disable Selected.** Click **Disable Selected** to end authentication for the selected systems.

Click the  icon to display the following context menu.



You can use these options to make changes to the system.

- **Enable.** Click **Enable** to begin authentication on the system.
- **Edit.** Click **Edit** to open the [Edit System](#) screen, where you can make changes to the system's settings.
- **Delete.** Click **Delete** to remove the system from Powertech Multi-Factor Authentication.
- **Close.** Click **Close** to dismiss the context menu.

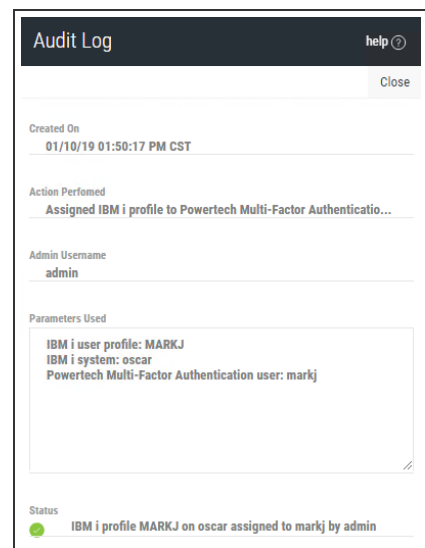
Audit Log screen

This screen displays the following information:

- **Created On:** The date and time the record was created.
- **Action Performed:** The action applied by the Powertech Multi-Factor Authentication administrator.
- **Admin Username:** The User logged in as the Powertech Multi-Factor Authentication administrator.
- **Parameters Used:** Extra information regarding the data submitted to Powertech Multi-Factor Authentication.
- **Status:** The state of Powertech Multi-Factor Authentication and/or additional information pertaining to the logged activity.

How to Get There

On the [Reports screen](#), click an Audit Log report.



Authentication Log screen

This screen displays the following information:

- **Created On:** The date and time the record was created.
- **Created By:** The user who attempted to authenticate.
- **Agent name:** The type of agent used (e.g. IBM i agent).
- **Attempt:** Displays x of y attempts.
- **Device:** The device used for the authentication attempt.
- **Rules used:** The rules used to validate the attempt (e.g. user disabled, IBM i profile not mapped).
- **System:** The system of the login attempt.
- **Status:** The state of Powertech Multi-Factor Authentication and/or additional information pertaining to the logged activity.

How to Get There

On the [Reports screen](#), click an Authentication Log report.

The screenshot shows the 'Authentication Log' screen with the following details:

- Created On:** 01/10/19 01:59:24 PM CST
- Created by:** markj
- Agent name:** IBM i agent
- Attempt:** Attempt 1 of 1
- Device:** Mobile (Mobile Device)
- Rules used:** OTP is invalid, Username provided = MARKJ
- System:** OSCAR
- Status:** User markj failed to authenticate as MARKJ (IBM i signon)


Copy/Move Configuration screen

See also [Copying or Moving an IBM i Agent Configuration](#).

These options allow you to create a copy of a Powertech Multi-Factor Authentication agent configuration on a different IBM i partition, or move a configuration to a new IBM i partition.

If the source system was active, the target system will also be active. The status of exit points and user profiles configured to be authenticated on the source are copied or moved to the target system. Details are logged in the audit log.

How to get there

In the Navigation Pane, choose **Agents**, then click **IBM i Agents**. Click  > **Copy/move configuration** for an IBM i agent.

The screenshot shows the 'Copy/move configuration' screen with the following options:

- Copy/move from:** OSCAR
- Copy/move to:** [Select System](#)
- Move configuration (remove source system):** off on

Options

Select System

Click **Select System** to open the [Select System screen](#), where you can choose the target system.

Move configuration (remove source system); Off • On

Set to **Off** to leave the configuration on the current system. Set to **On** to remove the configuration from the current system - the source system will no longer be registered as an IBM i agent system.

Cancel • Save

Click **Cancel** to dismiss the screen without making changes. Click **Save** to confirm your changes and copy or move the configuration based on your settings.

Powertech Multi-Factor Authentication Desktop Agent

The Desktop Agent allows you to authenticate using a desktop computer as an alternative to the IBM i green screen agent. It also allows you to access the Soft Token screen in order to view the Soft Token One-Time Password.

When prompted, you are presented with the authentication methods made available by your Powertech Multi-Factor Authentication administrator. If you select one of the One-Time Password methods, for example, a One-Time Password sent to a mobile device via SMS, you will be able to enter the One-Time Password into the Desktop Agent to be submitted to Powertech Multi-Factor Authentication for validation.

See also [User Authentication](#).

How to get there

The desktop agent appears when prompted by an Powertech Multi-Factor Authentication exit point authentication request.

Login Options

Login Type

Choose whether you are using Active Directory or an IBM i user profile for authentication.

Powertech Multi-Factor Authentication Username

This is your Powertech Multi-Factor Authentication user name.

The remaining login options change depending on your selection:

For Active Directory

Active Directory Username

This is the username of your Active Directory account.

Active Directory Password

This is the password for your Active Directory username. Click  to show/hide the password.

For IBM i


IBM i System

This is the IBM i system that is being used by your administrator for authentication.

IBM i User Profile

This is the IBM i user profile used for authentication.

IBM i Password

This is the password of your IBM i user profile. Click  to show/hide the password.

Login

Click **Login** to log in to the Powertech Multi-Factor Authentication Desktop Agent.

Settings

This screen displays your current configuration and allows you to configure your Powertech Multi-Factor Authentication Desktop Agent settings. At the top, the HelpSystems Insite server being used for authentication is listed, as well as your status including the user you are logged-in as, and whether you are using an Active Directory account or an IBM i user profile for authentication.

Click  in the upper right corner of the Desktop Agent screen to open the Soft Token panel.

Start Powertech Multi-Factor Authentication when PC is turned on

Move this slider to the right to indicate that you want the Powertech Multi-Factor Authentication Desktop Agent to start when your computer is started.

Remember me

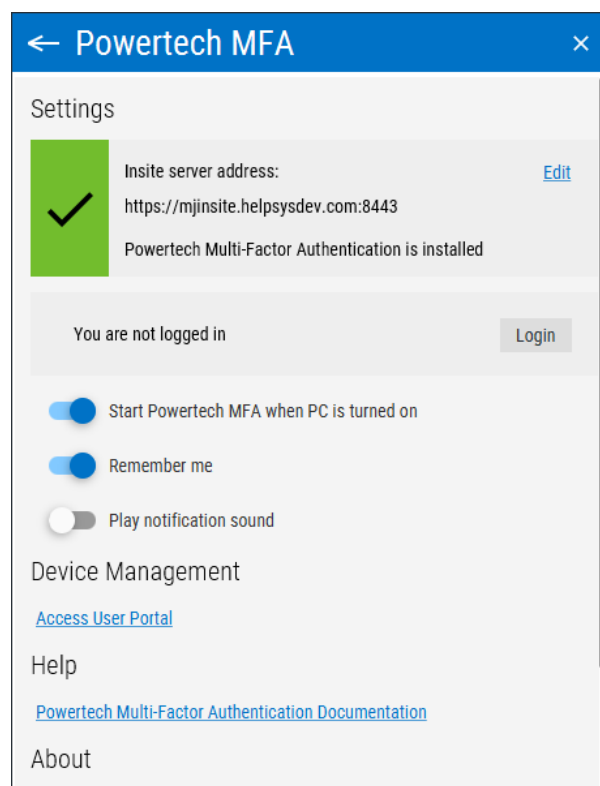
Move this slider to the right to indicate you want Powertech Multi-Factor Authentication to remember your login information.

Play notification sound

Move this slider to the right to indicate you want Powertech Multi-Factor Authentication to chime when prompted by an authentication request.

Device Management

Click Access User Portal to open the Powertech Multi-Factor Authentication User Portal, where you can manage the devices you are using as factors of authentication.



Edit Default System

The settings on this page allow Powertech Multi-Factor Authentication administrators to configure the default action to perform (allow or deny) for IBM i user profiles not allocated to an Powertech Multi-Factor Authentication user on systems that authentication is enabled on.

Upon signing on to a system secured by Powertech Multi-Factor Authentication with a user profile not attached to an Powertech Multi-Factor Authentication user, Powertech Multi-Factor Authentication first consults the settings for that system in its [Edit System screen](#). If 'Use Agent Defaults' is set to **On**, or the user profile is otherwise allowed by the individual system's settings, Powertech Multi-Factor Authentication defers to the settings on this screen.

Administrators can then allow or deny access for individual new user profiles as exceptions to the default action.

This page also allows administrators to change the default authentication status (enabled or disabled) for each exit point.

How to Get There

In the Navigation Pane, choose **Agents**, then **Systems Defaults**.

Options

Default Unassigned Profile Action: Deny users access • Allow users access

Choose 'Deny users access' to reject login attempts by IBM i user profiles unfamiliar to Powertech Multi-Factor Authentication. Choose 'Allow users access' to grant access to user profiles unfamiliar to Powertech Multi-Factor Authentication. Unassigned users that have been granted access will inherit the user settings of the Default Group. See [Users screen](#).

Unassigned Profile Action

If any of the profiles in this list come through one of the system's exit points, and Powertech Multi-Factor Authentication can't find an Powertech Multi-Factor Authentication user attached to that profile to challenge for authentication, Powertech Multi-Factor Authentication will check the Unassigned Profile Action setting for that user profile. If it is set to **Allow**, the user will not be challenged with an authentication request and will be permitted to sign on. If the user is set to **Deny**, they will be denied access.

Add Profile • Remove

Click **Add Profile** to open the Select Profiles screen, where you can choose a profile on the selected system. Select a user and click **Remove** to remove that user from the list.

The screenshot shows the 'Edit Default System' interface. At the top, there's a title bar with 'Edit Default System' and a 'help' icon. Below the title bar are 'Cancel' and 'Save' buttons. The main content area is organized into sections:

- Default Unassigned Profile Action:** A dropdown menu currently set to 'Deny Users Access'.
- Unassigned Profile Action:** A section with a text input field for a profile name, an 'Add Profile' button, and a message: 'No profiles have been added to this list. To set individual actions enter a profile name in the input above.'
- Authentication Suppression:** A section with a label 'Authentication suppression (minutes)' and a value of '30'. Below it is a note: 'Authentication suppression time period (1-999)'.
- Exit Points:** A section with a 'Select All' checkbox and 'Activate'/'Deactivate' buttons. It contains a list of system services, each with a checkbox and a note 'Deactivated when system is activated':
 - DDM/DRDA request access
 - Database Svr-Initiation
 - FTP Server Logon
 - FTP Server Raquests
 - File Server
 - REXEC Server Logon
 - Remote Command
 - Retrieve command exit programs
 - TCP Signon Server

[profile list]; Deny • Allow

Choose 'Deny' from the drop-down list adjacent to a user to reject login attempts by that user. Choose 'Allow' to grant access to the adjacent user.

Authentication Suppression

This parameter controls authentication suppression globally. Authentication suppression reduces the number of times authentication is required.

Authentication Suppression (minutes)

Specify the period of time, in minutes, authentication will be suppressed for each IBM i interactive session. After an initial authentication request, the user will not receive additional authentication requests during that session until the time period has expired. This is the global setting. This setting can be overridden for systems individually using the [Edit System page](#).

Exit Points; Activate • Deactivate

Check the exit points you would like to activate or deactivate. Whether the exit point is set to activated or deactivated initially depends on the system's default settings when added to Powertech Multi-Factor Authentication. Powertech Multi-Factor Authentication supports the following exit points:

- DDM/DRDA Server
- Database Svr-Initiation
- FTP Server Logon
- FTP Server Requests
- File Server
- REXEC Server Logon
- Remote Command
- Retrieve command exit programs
- TCP Signon Server

NOTE: See also [IBM i Exit Point Descriptions](#).

Click **Activate** to secure them with Powertech Multi-Factor Authentication. Click **Deactivate** to stop securing them with Powertech Multi-Factor Authentication.

For example, if the system is enabled, and you set an exit point to **Deactivate** and click **Save**, Powertech Multi-Factor Authentication sends a message to deregister the exit point program with Powertech Multi-Factor Authentication. If the system is not currently enabled in Powertech Multi-Factor Authentication, and this setting is changed, the setting is stored in the database so that when the system is enabled within Powertech Multi-Factor Authentication, Powertech Multi-Factor Authentication will apply the activate/deactivate setting as appropriate, and register/deregister the exit point program accordingly.

NOTE: In some cases, restarting the services (which Powertech Multi-Factor Authentication does when activating/deactivating exit points) is not sufficient for the Database Server and File Server exit points. In this case, restart QSERVER subsystem:

```
ENDSBS SBS(QSERVER)
STRSBS SBSD(QSERVER)
```

If after restarting the subsystem authentication still does not function properly, also restart the QUSRWRK subsystem:

```
ENDSBS SBS(QUSRWRK)
STRSBS SBSD(QUSRWRK)
```

Email Settings

Once users have been added to the Authentication Manager database, they can be sent an email to advise them of this fact (e.g. a welcome email informing them that they have been enrolled). Email server settings are required in order for Powertech Multi-Factor Authentication to send email messages to administrators and users, and settings must be enabled if you wish to allow Powertech Multi-Factor Authentication to send emails.

The email includes a link to the self-service portal where users can complete the registration process and maintain their account details. Use the settings on this screen to configure your email server settings and define the content of the message.

How to Get There

In the Navigation Pane, choose **Email**.

Options

Validate Email Connection

Use this button to test the email server connection. If the server requires validation, the specified User Name and Password is tested.

Enabled

Choose this option to enable email.

Host

This is the host name of your email server.

Port

This is the port used by your email server.

Enabled
off on

Host

Port
25

Use SSL with Email
off on

[Validate Email Connection](#)

Email Address of Sender

User Name
qsecofr

Password

Message (optional)

Note: Any custom message will be applied to user registration emails only.

[Preview User Portal registration email](#)

Use SSL with email

Choose this option to secure email correspondence with SSL.

Sender Email Address

This is the email address that will appear in the "From" field of the recipient's message.

Server Requires Validation

Set this slider to **On** to enable the User Name and Password fields. Use these fields to specify credentials for your email server, if your email server requires a User Name and Password. Use the **Validate Email Connection** button at the top of the screen to test the connection.

User Name

Enter the username required by mail server (if credentials are required by the mail server).

Password

Enter the password required by the mail server (if credentials are required by the mail server).

Message (optional):

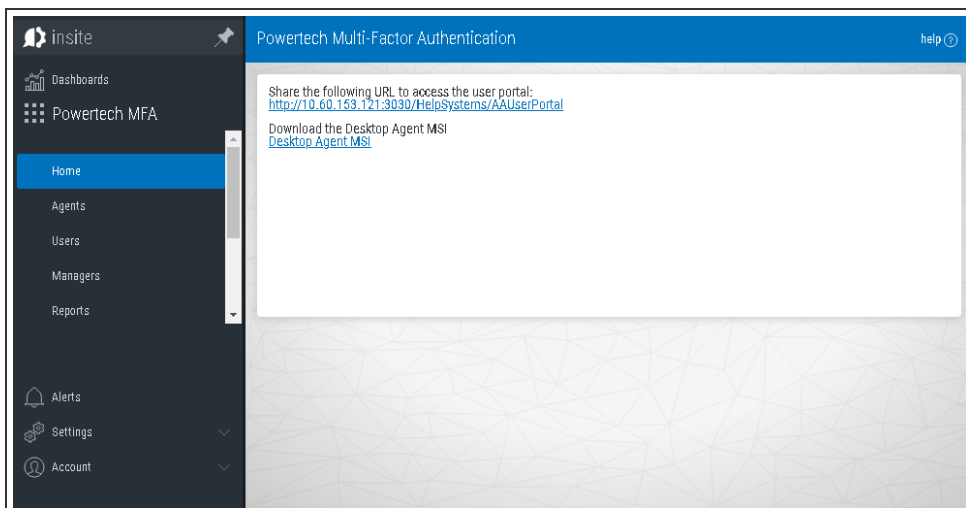
Enter a message to include for new users.

Preview User Portal registration email

Click this button to display a preview of the email that will be sent to users.

Powertech Multi-Factor Authentication Home

Share the URL on this screen with users in order for them to access the Powertech Multi-Factor Authentication User Portal.



Import Users

Use this screen to import users from an Active Directory or IBM i user database. See also [Adding and Importing Users](#).

How to Get There

In the Navigation Pane, choose **Users**. Click **Add > Import Users**.

Options

Cancel • Start Import

Click **Cancel** to return to the [Users screen](#) without importing users. Click **Start Import** to begin importing users based on your settings.

Import Type; MFA Users (import from Active Directory) • MFA users (Import from CSV) • IBM i profiles (import from the IBM i) • IBM i profiles (Import from CSV)

Choose MFA users (Import from CSV) or IBM i profiles (Import from CSV) to import multiple users specified in a .csv file. For more information, see [Importing Multiple Users Using a .CSV File](#).

If you are not importing from a .csv file, choose whether you would like to import records from Active Directory or user profiles from one or more IBM i systems. The options available depend on your selection:

[MFA Users (import from Active Directory)]

LDAP Context

Enter the LDAP context to specify the user you would like to import. LDAP Settings can be configured on the [LDAP screen](#).

Group

Specify the group you want to import the user into. See [New/Edit Group screen](#) for details on creating and editing Groups.

[IBM i profiles (import from the IBM i)]

System

Choose the system that includes the user profiles you would like to import.

Filter

Narrow import results based on input string. 10 character max limit.

Smart Match; On • Off

Smart Match cross-references the IBM i profiles that are being imported against the existing Powertech Multi-Factor Authentication user profiles and attempts to match them. It takes the Full Name (listed in the [New/Edit User screen](#)) and searches IBM i profiles that include:

- The first and last name with a space.
- The first and last name with no space.
- The first initial followed by the last name with no space.

The match looks for these strings in the IBM i profile's name and description fields. For example, for Powertech Multi-Factor Authentication user "Shirley Matchwell," Powertech Multi-Factor Authentication will match IBM i profiles that contain the following in either the user profile Name or Text description fields: "shirley matchwell," "shirleymatchwell," and "smatchwell."

NOTE: Smart Match disregards case during its comparison.

TIP: If network users have both Active Directory accounts and IBM i user profiles, import the Active Directory accounts first to create the Powertech Multi-Factor Authentication users, then import the IBM i user profiles using Smart Match to match them to the existing Powertech Multi-Factor Authentication users imported from Active Directory.

Start Import

Click this button to begin the import process.

Assign Users to IBM i Profiles

Profile ID	Name	Action
AA789108	Tim Jones - IT	Add user
ACEDTI	Agent for RSA SecurID Administrator	Add user
ADAMS		Add user
ADAMW	Adam Weigold	Add user
ADAMW1	Adam Weigold	Add user

Use this screen to link the imported IBM i users with existing Powertech Multi-Factor Authentication users, or add them as new Powertech Multi-Factor Authentication users.

LDAP Settings screen

Use these settings to configure Lightweight Directory Access Protocol (LDAP) settings in order to prepare Powertech Multi-Factor Authentication for profile import from Active Directory.

These settings are specific to the Powertech Multi-Factor Authentication module, and do not pertain to the Insite authentication settings configured on Insite's Authentication page.

How to Get There

In the Navigation Pane, choose **LDAP**.

Options

Enabled

Select **On** to enable the LDAP connection.

LDAP Host

This is the host name of your LDAP server.

LDAP Port

This is the port number used to communicate with the LDAP server. The default value, 389, is the standard number used for communicating with an LDAP server in plain text mode. Do not change this unless you communicate with your LDAP server on a non-standard port.

Use SSL with LDAP

Select **On** to use SSL (Secure Socket Layer). SSL provides cryptographically secure communication.

Validate LDAP Settings

Click this button to validate that Powertech Multi-Factor Authentication can communicate with the LDAP server without errors before saving your LDAP settings.

LDAP Administrator

Enter the username of the LDAP administrator.

Administrator Password

Enter the LDAP administrator's password.

Default Context

This is the command used by Powertech Multi-Factor Authentication to query LDAP directory records during import.

User ID Field Name

Enter the LDAP field used for the User ID.

The screenshot shows the LDAP Settings screen with the following fields and values:

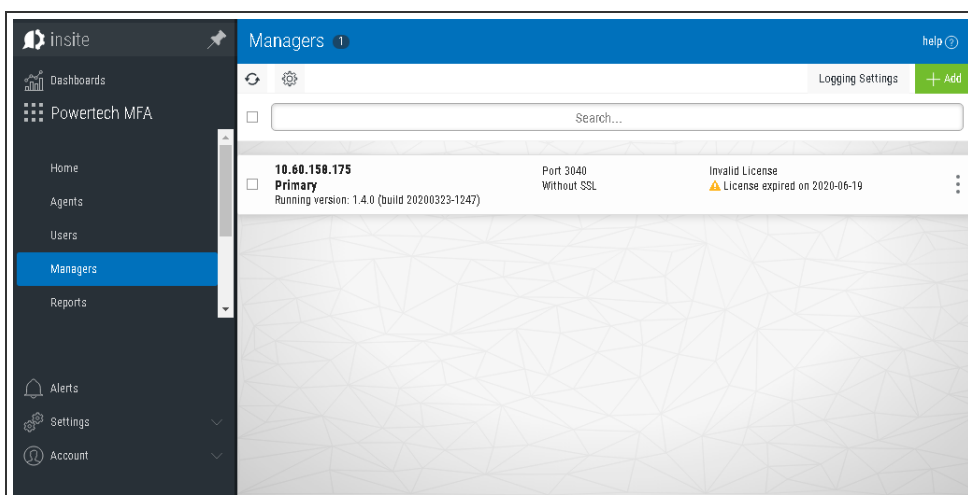
- Enabled:** off on
- LDAP Host:** ldap:fds.ldaphost.com
- LDAP Port:** 389
- Use SSL with LDAP:** off on
- Validate LDAP settings:** (button)
- LDAP Administrator:** (empty field)
- Administrator Password:** (empty field)
- Default Context:** (empty field)
- User ID Field Name:** samaccountname

Managers

This screen lists the Authentication Managers that have been added to Powertech Multi-Factor Authentication. You can use settings on this screen to view, add, and delete Authentication Managers. At least one Authentication Manager must be added before configuration settings can be made (using the [Settings screen](#)). The Authentication Manager set to Primary is the one used for configuration (see [Edit Manager screen](#)).

The Authentication Manager is Powertech Multi-Factor Authentication's central processing component. It houses all the configuration settings and user registration data, and is the software that users connect to when they authenticate. Administration of the Authentication Manager is controlled with HelpSystems Insite. See the [HelpSystems Insite User Guide](#) for more details on HelpSystems Insite.

Upon signing on to any system secured by Powertech Multi-Factor Authentication, an Authentication Manager is chosen at random to process the authentication request.



How to Get There

In the Navigation Pane, choose **Managers**.

Options

Logging Settings

Click this button to open the Logging Settings pane, where you can change the logging level in the Tomcat server logs.


Add

Click **Add** to open the [New Manager](#) page where you can define a new Authentication Manager.

[manager list]; Cancel • Delete

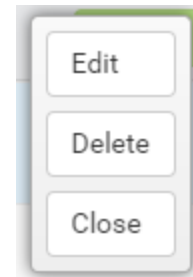
Check the box to the left of one or more Managers and additional buttons appear at the top of the screen.

- **Cancel.** Click **Cancel** to dismiss the buttons.
- **Delete.** Click **Delete** to remove the selected Managers from Powertech Multi-Factor Authentication.

Click the  icon to display the following context menu.

You can use these options to make changes to the Manager.

- **Edit.** Click **Edit** to open the [Edit Manager](#) screen, where you can make changes to the Manager's settings.
- **Delete.** Click **Delete** to remove the Manager from Powertech Multi-Factor Authentication.
- **Close.** Click **Close** to dismiss the context menu.




New/Edit Group

These settings allow Powertech Multi-Factor Authentication administrators to define Groups to use for different subsets of users. Each group can have its own authentication settings.

Administrators can select a Group for a user in the [New/Edit User screen](#).

How to Get There

In the Navigation Pane, choose **Users**. To add a new Group, choose **Add > Add Group**. To edit an existing Group, click  for a Group and select **Edit**.

Options

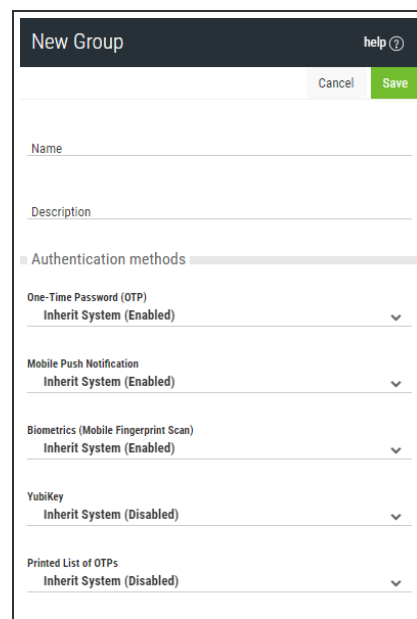
Authentication Methods

Here, specify authentication settings for the Group. All users in the Group will inherit these Authentication Settings, which override the Authentication Settings in [Settings](#). (The same five authentication options are available.)

- **Inherit.** Choose this option to use the setting configured in [Settings](#) for the authentication method.
- **Disabled.** Choose this option to turn the authentication method off for all users in the group.
- **Enabled.** Choose this option to turn the authentication method on for all users in the group.

Users

This is a list of users in the Group.



Delete • Cancel • Save


Choose Delete to remove the Group from Powertech Multi-Factor Authentication. Choose Cancel to dismiss the screen without making changes. Click Save to save the Group's settings and return to the [Users screen](#).

New/Edit Managers

This screen allows Powertech Multi-Factor Authentication administrators to add an Authentication Manager or edit an existing one. Powertech Multi-Factor Authentication does not limit the number of Authentication Managers that can be added.

How to Get There

To add a new Manager, in the Navigation Pane, choose **Managers**, then click **Add**.

To edit an existing Manager, in the Managers screen, double-click a Manager, or, click  for a Manager and choose **Edit**.

Options

Address

This is the IP address or name of the Manager system.

Port

This is the Connector Port number used to communicate with the Manager system (default is 3040).

Primary

Choose **On** to select this instance as the Primary Authentication Manager. The Primary Authentication Manager is used for configuration. See [Settings screen](#). Choose **Off** if you would not like to assign this instance as the Primary Authentication Manager.

UseSSL

Choose **On** to use SSL encryption for this connection. Choose **Off** if you do not intend to use SSL encryption for this connection. In order to use TLS security to encrypt an Authentication Manager Connection from Insite, you must create and configure a Digital Certificate (also called a *Certificate Authority*). See [Securing an Authentication Manager Connection](#).

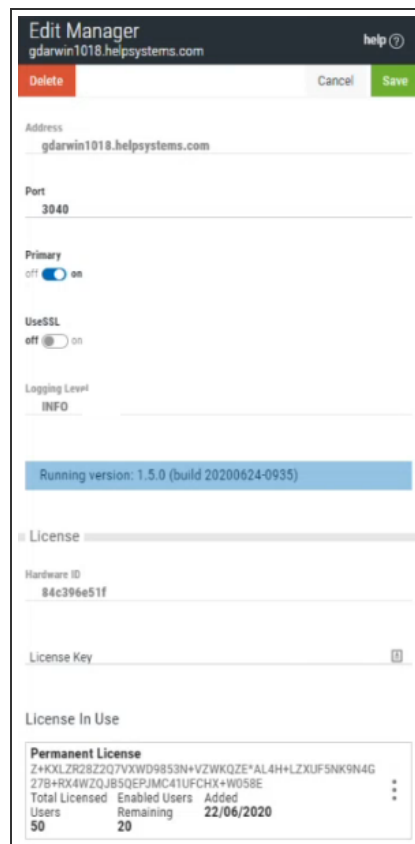
Logging Level

This is a display of the logging level (INFO, DEBUG, or TRACE) of the Authentication Manager server. The Logging Level can be changed in the [Logging Settings screen](#).

License

Hardware ID

This is the manager's unique ID.



Edit Manager
gdarwin1018.helpsystems.com

Delete Cancel Save

Address
gdarwin1018.helpsystems.com

Port
3040

Primary
off on

UseSSL
off on

Logging Level
INFO

Running version: 1.5.0 (build 20200624-0935)

License

Hardware ID
84c396e51f

License Key

License In Use

Permanent License		
Z+KXLZK2BZQ7VXWD9853N+VZWKQZE*AL4H+LZXUF5NK9N4G		
27B+RX4WZQJBSQEPJAC41UFCHX+W058E		
Total Licensed	Enabled Users	Added
Users	Remaining	22/06/2020
50	20	

License Key

This is the license key provided by HelpSystems. Contact keys@helpsystems.com if you need to request a new license key.

To delete the License Key, click  for a License and choose **Delete**.

New/Edit System

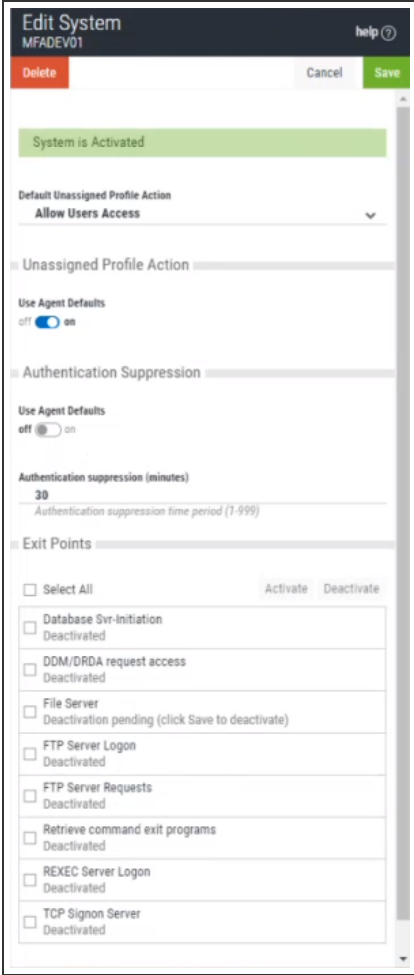
Use these settings to add a system to be authenticated with the IBM i agent. The system needs to have been added to Insite (see [Product Connections](#)), and have Powertech Multi-Factor Authentication installed.

The settings on this page allow Powertech Multi-Factor Authentication administrators to configure the action to perform (allow or deny) for IBM i user profiles on the system that are not allocated to an Powertech Multi-Factor Authentication user.

Upon signing on to a system secured by Powertech Multi-Factor Authentication with a user profile not attached to an Powertech Multi-Factor Authentication user, Powertech Multi-Factor Authentication first consults the settings on this screen to determine whether to allow or deny the user access. If 'Use Agent Defaults' is set to **On**, or the user profile is otherwise allowed by the settings on this screen, Powertech Multi-Factor Authentication defers to the settings on the [Edit Default System screen](#).

In other words, here, Powertech Multi-Factor Authentication administrators can allow or deny access to specific user profiles as exceptions to the default action specified on the Edit Default System screen.

This page also allows administrators to change the default authentication status (enabled or disabled) for each exit point.



How to Get There

In the Navigation Pane, choose **Agents**, then **IBM i Agent**, then click **Add**.

Options

System; Select System (New System only)

Click **Select System** to open the [Select System screen](#), where you can choose the system to be added.

Default Unassigned Profile Action

Choose **Deny users access** to reject login attempts by IBM i user profiles not connected to an Powertech Multi-Factor Authentication user. Choose **Allow users access** to grant access to user

profiles not connected to an Powertech Multi-Factor Authentication user. Unassigned users that have been granted access will inherit the user settings of the Default Group. The Default Group is listed on the [Users screen](#). Choose **Inherit user access** to use the setting defined in the [Edit Default System page](#).

Unassigned Profile Action

Use Agent Defaults; On • Off

Choose **On** to use the Unassigned Profile Action settings defined in the [Edit Default System page](#). Choose **Off** to use the Unassigned Profile Action settings defined on this page for this system.

Authentication Suppression

This parameter controls authentication suppression for an individual system. Authentication suppression reduces the number of times authentication is required.

Use Agent Defaults; On • Off

Choose **On** to use the Authentication Suppression settings defined in the [Edit Default System page](#). Choose **Off** to use the Authentication Suppression settings defined on this page for this system.

Authentication Suppression (minutes)

Specify the period of time, in minutes, authentication will be suppressed for each IBM i interactive session. After an initial authentication request, the user will not receive additional authentication requests during that session until the time period has expired.

Exit Points; Activate • Deactivate

Check the exit points you would like to activate or deactivate. Whether the exit point is set to activated or deactivated initially depends on the system's default settings when added to Powertech Multi-Factor Authentication. Powertech Multi-Factor Authentication supports the following exit points:

- DDM/DRDA Server
- Database Svr-Initiation
- FTP Server Logon
- FTP Server Requests
- File Server
- REXEC Server Logon
- Remote Command
- Retrieve command exit programs
- TCP Signon Server

NOTE: See also [IBM i Exit Point Descriptions](#).

Click **Activate** to secure them with Powertech Multi-Factor Authentication. Click **Deactivate** to stop securing them with Powertech Multi-Factor Authentication.

For example, if the system is enabled, and you set an exit point to **Deactivate** and click **Save**, Powertech Multi-Factor Authentication sends a message to deregister the exit point program with Powertech Multi-Factor Authentication. If the system is not currently enabled in Powertech Multi-Factor Authentication, and this setting is changed, the setting is stored in the database so

that when the system is enabled within Powertech Multi-Factor Authentication, Powertech Multi-Factor Authentication will apply the activate/deactivate setting as appropriate, and register/deregister the exit point program accordingly.

NOTE: In some cases, restarting the services (which Powertech Multi-Factor Authentication does when activating/deactivating exit points) is not sufficient for the Database Server and File Server exit points. In this case, restart QSERVER subsystem:

```
ENDSBS SBS(QSERVER)
STRSBS SBSD(QSERVER)
```

If after restarting the subsystem authentication still does not function properly, also restart the QUSRWRK subsystem:

```
ENDSBS SBS(QUSRWRK)
STRSBS SBSD(QUSRWRK)
```


New/Edit User

This screen allows Powertech Multi-Factor Authentication administrators to edit the properties of a user enrolled in the authentication manager. There is some overlap with some of the features provided by the self service portal for the user to edit their own profile. The administrator is able to edit some details that the user can't edit, though (and vice versa). The administrator is able to:

- Add/Edit/Remove IBM i profiles assigned to the user
- Add/Remove devices registered by the user

How to Get There

To add a new User, in the Navigation Pane, choose **Users**, then click **Add > Add User**.

To edit an existing user, in the Users screen, double-click a user, or, click  for a User and choose **Edit**.

Options

Delete

Click this button to delete the user in Powertech Multi-Factor Authentication.

Send Email

Click this button to send the user an email. See [Email Settings](#) for details.

You can also send an email to several users at once, or groups of users, from the [Users screen](#).

Powertech Multi-Factor Authentication Name

The user profile name. This is the name that will be emailed to users so that they can access the User Portal.

Active Directory User Name

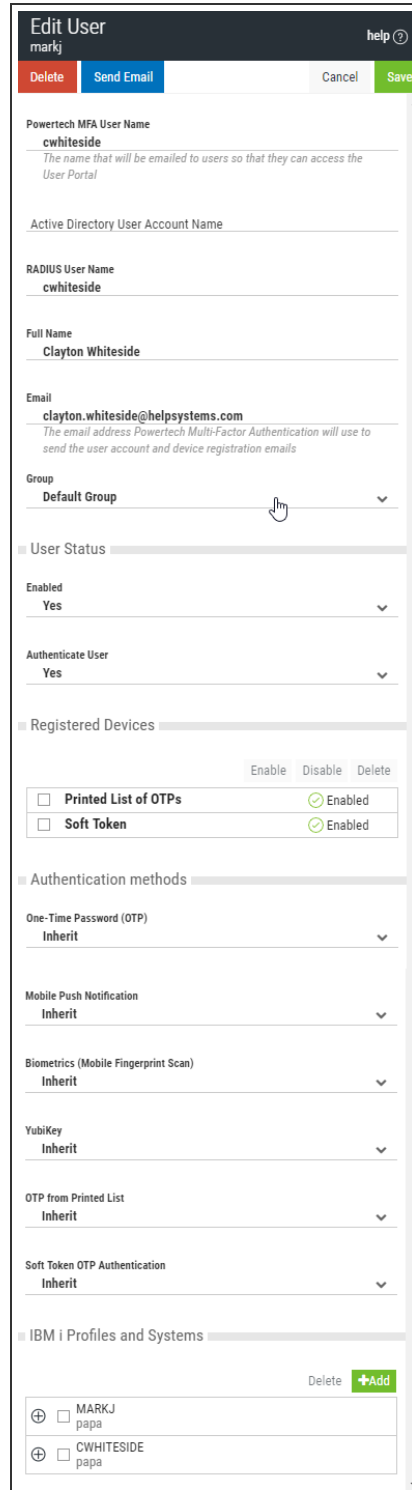
The user name of the User in Active Directory.

RADIUS User Name

The RADIUS user name used for the RADIUS server.

Full Name

The full name of the user, used only to identify the user in Powertech Multi-Factor Authentication.



The screenshot shows the 'Edit User' interface for user 'markj'. At the top, there are buttons for 'Delete', 'Send Email', 'Cancel', and 'Save'. The user's name is 'markj' and there is a 'help' icon. The form contains several sections:

- Powertech MFA User Name:** 'cwhiteside'. A note below says: 'The name that will be emailed to users so that they can access the User Portal'.
- Active Directory User Account Name:** (empty field)
- RADIUS User Name:** 'cwhiteside'.
- Full Name:** 'Clayton Whiteside'.
- Email:** 'clayton.whiteside@helpsystems.com'. A note below says: 'The email address Powertech Multi-Factor Authentication will use to send the user account and device registration emails'.
- Group:** 'Default Group' (dropdown menu).
- User Status:**
 - Enabled:** 'Yes' (dropdown menu).
 - Authenticate User:** 'Yes' (dropdown menu).
- Registered Devices:**
 - Buttons: Enable, Disable, Delete.
 - Printed List of OTPs** (Enabled)
 - Soft Token** (Enabled)
- Authentication methods:**
 - One-Time Password (OTP):** 'Inherit' (dropdown menu).
 - Mobile Push Notification:** 'Inherit' (dropdown menu).
 - Biometrics (Mobile Fingerprint Scan):** 'Inherit' (dropdown menu).
 - YubiKey:** 'Inherit' (dropdown menu).
 - OTP from Printed List:** 'Inherit' (dropdown menu).
 - Soft Token OTP Authentication:** 'Inherit' (dropdown menu).
- IBM i Profiles and Systems:**
 - Buttons: Delete, +Add.
 - MARKJ (papa)
 - CWHITESIDE (papa)

Email

The email address Powertech Multi-Factor Authentication will use to send the user account and device registration emails.

Group

The Group the User is assigned to.

User Status

Enabled

Choose **Yes** to enable the user within Powertech Multi-Factor Authentication. Choose **No** to disable the user. Yes must be selected in order for the user to log in.

Authenticate User

If **Yes** is selected, (and the user is enabled), the user will be challenged to provide the second authentication factor. If **No** is selected, the user will be able to log in without providing a second authentication factor.

Registered Devices

Devices registered by the user that can be used for authentication are listed here. An administrator can enable, disable, or delete any of the user's devices.

Authentication Methods

For each of the authentication methods, one of the following three settings is possible:

- **Disabled.** Choose Disabled to turn the authentication method off.
- **Enabled.** Choose Enabled to turn the authentication method on.
- **Inherit.** Choose Inherit to use the authentication method defined for the User's [Group](#). If the user's Group setting for an authentication method is set to Inherit, the user will acquire the setting specified in [Settings](#).

NOTE: Descriptions of the authentication methods are available in the [Settings](#) topic.

IBM i Profiles and Systems

Click **Add** to begin the process of importing profiles from an IBM i system.

Cancel • Save

Click **Cancel** to dismiss the screen without making changes. Click **Save** to create or update the user.

Reports screen

Use report to view Powertech Multi-Factor Authentication system activities, including authentication data, system event information, and an audit log of Powertech Multi-Factor Authentication configuration information.

Reports			help ⓘ
◀ 1 ▶	🔄	🗑️	
Search...			
🟢	Authentication Log User markj authenticated successfully (IBM i signon)	02/07/18 09:46:49 AM CST	
🟢	Authentication Log User markj authenticated successfully (IBM i signon)	02/07/18 09:46:13 AM CST	
🟢	Audit Log User markj updated by admin	02/07/18 09:45:39 AM CST	
🟢	Audit Log IBM i profile MARKJ on OSCAR assigned to markj by admin	02/07/18 09:45:35 AM CST	
🟢	Audit Log IBM i agent system OSCAR activated by admin	02/07/18 09:42:36 AM CST	
🟢	Audit Log IBM i agent system OSCAR updated by admin	02/07/18 09:42:32 AM CST	
🔴	Authentication Log IBM i profile MARKJ (IBM i profile) denied access without authenticating (IBM i signon)	02/07/18 09:32:31 AM CST	
🟢	Audit Log User markj updated by admin	02/07/18 09:32:25 AM CST	
🔴	Authentication Log IBM i profile MARKJ (IBM i profile) denied access without authenticating (IBM i signon)	02/07/18 09:29:54 AM CST	
🟢	Audit Log IBM i agent system OSCAR activated by admin	02/07/18 09:26:11 AM CST	
🟢	Audit Log IBM i agent system OSCAR updated by admin	02/07/18 09:26:07 AM CST	
🟢	Audit Log User mikew updated by [unknown]	02/02/18 12:35:27 PM CST	
🟢	Audit Log User adams created by [unknown]	02/02/18 12:34:39 PM CST	
🟢	Audit Log	02/02/18 12:33:09 PM CST	

How to Get There

In the Navigation Pane, choose **Reports**.



Options



Click this button to display sorting and filtering options. Use the Sort By options to sort log records by Status, Timestamp, and Log entry.

Sort By



Click these icons to indicate whether you want to display the Status/Timestamp/Log entry in ascending  or descending  order.

Filter By

Use this menu to indicate the types of logs you want to show, All logs, Audit logs, Authentication logs, System Event logs, or User Portal logs.



Click this button to dismiss the Sort By and Filter By options.

[Search field]

Start typing in the Search field to limit the log list to show only records that contain the text typed.

[Log list]

There are three types of reporting logs displayed on this screen: Administration logs, the Authentication logs, and the System Events logs. Click an entry to view the log report.

Select a Group

Use this screen to select a Group for one or more selected users.

How to Get There

Select one or more users on the Users screen and click **Add to Group**.

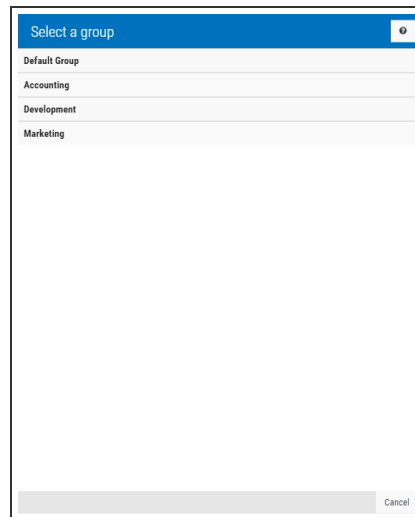
Options

[Group selection]

Choose the group you would like to add the selected users to. Groups can be created on the [Users screen](#), by choosing **Add > Add Group**.

Cancel

Click **Cancel** to dismiss this screen.



Select IBM i Profiles

Use this screen to select one or more IBM i profiles.

How to Get There

After selecting a system in the [Select Systems screen](#) (by, for example, clicking **Add** the [Edit User screen](#)), click **Next** to advance to this screen.

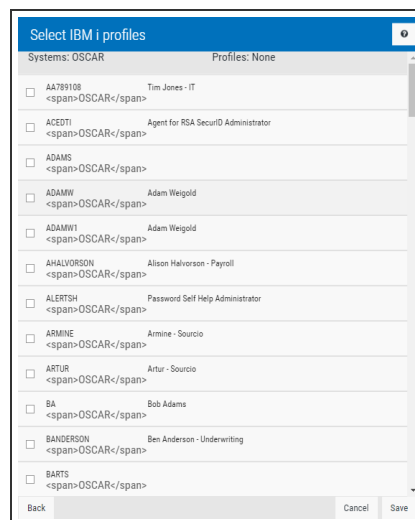
Options

[Search box]

Enter a value in the search field to quickly identify profiles on the system. The list is filtered as you type.

Cancel • Next

Click **Cancel** to dismiss this screen without selecting one or more profiles. Click **Save** to save your selection.



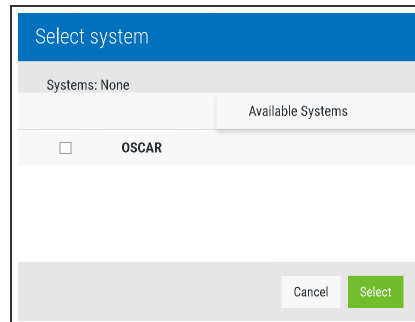
Select Systems

Use this screen to select one or more IBM i systems.

Options

[System list]

This list includes all systems that have been added as a Product Connection in HelpSystems Insite. Use the check box to the left of a system to select it. See [Product Connections](#) in the Insite User Guide.



Cancel • Select

Click **Cancel** to dismiss this screen without selecting one or more systems. Click **Select** to confirm your selection.

Server Health and Failover screen

These options allow you to see the health of Powertech Multi-Factor Authentication's environment and manage the failover process.

Systems	Authentication Manager	Database Service	Messaging Service
10.60.158.162 (primary)	✔	✔	✔ 🔒
10.60.158.148	✔	✔	✔ 🔒
10.60.158.85	✔	✔	✔ 🔒

How to Get There



In the Navigation Pane, choose **Server Health and Failover**.

Options

Enable Secure Messaging

Submitting this request will secure the messaging service on all servers that are currently using an insecure connection.

This restarts the Authentication Managers. Authentication may be unavailable for a few seconds.




A  icon in the Messaging Server column indicates secure messaging has been enabled for the server. A  icon indicates secure messaging is not enabled for the server.

[Refresh]

Click this button to refresh the page in order to display the most current data.

[Server Health Table]

This table includes the systems connected to Powertech MFA with the following possible status indicators for each system.


-  Service is active
-  Service is inactive
-  Authentication manager version is invalid

A blue question mark indicates the service status is unknown

Column Descriptions

- **Systems.** This column includes the name of the connected system. The Primary system is blue, and indicated with the suffix "(Primary)".
- **Authentication Manager.** This column includes the status of the Authentication Manager on the connected system.
- **Database Service.** This column includes the status of the Database Service on the connected system.
- **Messaging Service.** This column includes the status of the Messaging Service on the connected system.

Row Actions

The row action menu does not appear next to the primary server. For one of the other servers, click  to show the option **Fail over to this server**. Choose this option to trigger the failover process, making this server Primary.

You are prompted to restart all services on all servers. If you choose to continue, a call is made to initiate failover. A "failover in progress" indicator is displayed.

Settings screen

Use these settings to allow an Powertech Multi-Factor Authentication administrator to define which authentication methods are authorized, and configure other settings pertaining to Powertech Multi-Factor Authentication's user interactions.

How to Get There

In the Navigation Pane, choose **Settings**. At least one Authentication Manager must exist before settings can be configured. See [Managers screen](#).

Options

Authentication Methods

Note: When RADIUS authentication is turned on, these settings are unavailable in favor of the RADIUS authentication settings. See [RADIUS Authentication screen](#) for more details.

Choose the authentication methods available to network users.

- **One-Time Password (OTP).** The Powertech Multi-Factor Authentication agent software prompts the user to enter a one-time password. Network users use their mobile app to generate the one-time password and they enter the value generated. This value is authenticated with the authentication manager.

Note: Powertech Multi-Factor Authentication uses time-based one-time passwords (TOTP) for authentication. If this method is being used, the time on the user's mobile device must be in sync with the time on the authentication manager server. Time differences of more than one minute will cause validation of TOTPs to fail.

- **Mobile Push Notification.** A push notification is sent to the network user's mobile app, which displays a notification on-screen. The user is presented with the profile that is 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 that the sign-in attempt is legitimate, a message is returned to the authentication manager to authenticate and the user is allowed to sign in. If the user denies the sign-in attempt, authentication fails and the user is not allowed to sign in. The authentication manager alerts an administrator to a possible hacking attempt.



WARNING: In order for Powertech Multi-Factor Authentication to send Push Notifications to a mobile device outside the private network, the Authentication Manager's Connector Port (port 3040 by default) must be accessible to the public.

- **Biometrics (Mobile Fingerprint Scan).** This feature is available on mobile devices that contain a fingerprint scanner (e.g. the Google Nexus 5X and 6P, or the iPhone 5S and up). Similar to the push notification processing, a notification is sent to the mobile device prompting the user to authenticate using the fingerprint scanner. If the sign-in attempt is legitimate, the user can authenticate using the fingerprint scanner. If it isn't, they will have the option to deny the request (as per push notifications).

WARNING: In order for Powertech Multi-Factor Authentication to send Fingerprint Scan prompts to a mobile device outside the private network, the Authentication Manager's Connector Port (port 3040 by default) must be accessible to the public.

- **YubiKey.** The YubiKey is a FIDO certified U2F USB authentication device that can be used as an alternative to the Powertech Multi-Factor Authentication mobile app. When the Powertech Multi-Factor Authentication agent software prompts for the second factor, the user selects the YubiKey authentication option, inserts the YubiKey into a USB port on their PC/laptop, and presses a button on the YubiKey.
- **OTP from Printed List.** This is a printed list of one-time passwords, and is a backup authentication method for the user if they lose their smart phone.
- **Soft Token OTP Authentication.** You can choose to authenticate using a one-time password (OTP) generated by the soft token. The soft token is launched from the desktop agent and is PIN protected. See [Desktop Agent](#).

Authentication Attempts

NOTE: When RADIUS authentication is turned on, this setting is unavailable in favor of the RADIUS authentication settings. See [RADIUS Authentication screen](#) for more details.

Allowed Attempts

Enter the number of authentication request attempts can be made before the user is rejected.

Printed Backup OTP Expiration

NOTE: When RADIUS authentication is turned on, these settings are unavailable in favor of the RADIUS authentication settings. See [RADIUS Authentication screen](#) for more details.

Backup List Expiration

Enter the number of days a printed list of one-time passwords will be valid.

New User Action

This drop-down menu allows you to configure Powertech Multi-Factor Authentication's authentication settings upon user creation.

When a new user is created:

- **Set User to Authenticate Immediately.** Require authentication at next user sign on. If you choose this option, new users enrolled in Powertech Multi-Factor Authentication will be required to authenticate using a registered device the first time they sign on. This means they will need to register a device with Powertech Multi-Factor Authentication prior to their next sign on attempt in order to gain access.

WARNING: If this option is selected, users will be locked out of the system until they have registered a device with Powertech Multi-Factor Authentication.

- **Set User to Authenticate only after Device Registration.** Require authentication after user registers a device. If you choose this option, new users enrolled in Powertech Multi-Factor Authentication will not be prompted to authenticate upon sign on until after they have registered a device.
- **Manually Set Authentication Option for User.** Administrator is responsible for activating or deactivating authentication on an individual user basis using the 'Authenticate User' option in the [Edit User settings](#) for each new user (regardless of whether a device has been registered or not).

User Portal

User Portal Session Timeout

Enter the number of minutes an idle User Portal session will remain active before timing out and requiring the user to sign on again.

Log successful User Portal logins in User Portal Log; On • Off

This option allows you to specify whether or not to log successful user portal logins. It is disabled (set to **Off**) by default. HelpSystems recommends that this option remains off unless audit requirements dictate that successful user portal logins must be logged. Toggle to **On** to activate logging of successful portal logins.

Log Output

Output to Syslog; On • Off

Set to **On** in order to log output report data to a syslog server, or **Off** if you do not wish to log report data to a syslog server.

Output to Syslog

Enter the IP address or DNS name and port of the syslog server you would like to output log data to. (The default syslog port is 514.)

EXAMPLE:
10.60.153.12:514

License Expiry Notification

Enabled

Set Enabled to **On** to receive a notification when the current license is approaching its expiration date.

If enabled, a service runs once per day at 12 noon to check license expiration and send notifications. A notification is sent to the email address specified if a temporary or subscription license is due to expire within 15 days, or if it has already expired.

The notification email is sent once.

Set Enabled to **Off** if you do not wish to receive a notification in the circumstances listed above.

Email Address to Notify

If License Expiry Notification is enabled, the expiry notification will be sent to the email address specified here.

Name of Person to Notify

Here you can specify the name of the person to be addressed in the body of the email message.

Purging Report Data

Automatically Purge Report Data

Set this option to **On** if you would like to enable automatic purging of report data. If enabled, a service runs every day at midnight and deletes from the database all report data older than the number of days specified in the 'Days' Worth of Data to Retain' field.

NOTE: The processing runs at midnight as observed by the Authentication Manager, not the server hosting the Data Services. If you are in a different time zone from your Authentication Manager, report data may appear to have been purged earlier or later than expected because of this.

A record is written into the system event log to record the fact that a purge has run.

Set this option to **Off** to disable purging. When disabled, no data is deleted from the database.

Disable Inactive Users

Use these options to specify whether user accounts are automatically disabled if the user fails to authenticate within a specific number of days.

Disable Users Who Have Not Authenticated in x Days; Off • On

Toggle to **On** to disable users who are inactive for the specified number of days. Toggle to **Off** to disable this feature.

Inactive Days Threshold

Specify the number of days without an authentication to be allowed before users are disabled (1-999).

Email User When Account is Disabled; Off • On

Toggle to **On** to automatically send an email notification to users who are disabled. Toggle to **Off** to disable the email notification.

Intrusion Detection, Notification, and Lockdown

Use these settings to automatically disable user accounts that repeatedly fail authentication.

Enabled; Off • On

Toggle to **On** to activate a maximum number of authentication attempts.

Consecutive Invalid Authentication Attempts to Trigger

Enter the number of consecutive invalid authentication attempts to be allowed of users (1-999). If the user exceeds this threshold an email can be sent to the administrator, or the user account can be disabled, or both (depending on the status of subsequent options).

Notify Administrator on Intrusion Detection/Lockdown; Off • On • Administrator Email Address

Toggle to **On** to automatically send an email notification to the administrator indicating the user account that has been disabled. Toggle to **Off** to disable the email notification. In the field provided, specify the administrator's email address to be used for the notification. Email server settings can be configured on the [Email screen](#).

Administrator Email Address

With Intrusion Detection, Notification, and Lockdown Enabled, use the following options to specify the action to be taken in response to a user meeting the maximum number of failed authentication attempts.

Email User on Intrusion Detection/Lockdown; Off • On

Toggle to **On** to automatically send an email notification to the user indicating their user account that has been disabled. Toggle to **Off** to disable the user email notification.

Disable User Following Intrusion Detection; Off • On

Toggle to **On** to disable users who exceed the specified maximum number of authentication attempts. Toggle to **Off** to disable this feature.

Failover Notifications

Send Notification Email when Failover Occurs; Off • On

Toggle to **On** to automatically send an email notification to the specified email address upon failover to the secondary server. Toggle to **Off** to disable the sending of these email notifications.

Email must be configured in Powertech Multi-Factor Authentication to use this feature. See [Email Settings](#).

Email Address to Notify

This is the email address that will be used for server failover notifications

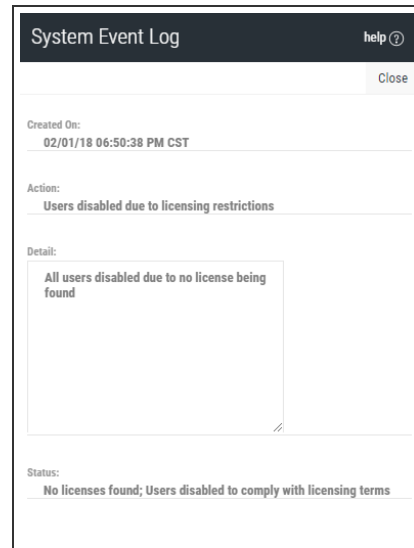
System Event Log screen

Displays the following information regarding an Powertech Multi-Factor Authentication system event:

- **Created On:** The date and time the record was created.
- **Action:** A brief description of the action that was applied.
- **Detail:** Details regarding the action that was applied.
- **Status:** The state of Powertech Multi-Factor Authentication and/or additional information pertaining to the logged activity.

How to Get There

On the [Reports screen](#), click a System Event Log report.



Troubleshooting Authentication with your Mobile Device

The Powertech Multi-Factor Authentication mobile app uses features of your mobile device to facilitate authentication, including:

- Your biometric touch sensor (required for biometric authentication)
- Your camera (required to scan QR code)
- Push Notifications (required for One-Time Passwords)

Do the following to ensure these features are active and available for use with Powertech Multi-Factor Authentication.

NOTE: If your mobile device is configured properly, connected to the Internet (or, if required, your organization's private wi-fi network), and you are still unable to authenticate, contact your administrator for assistance.

Enable your fingerprint touch sensor

Your touch sensor must be configured and enabled in order to authenticate with Powertech Multi-Factor Authentication. In order to do this, your mobile device must learn your unique fingerprint and store this information for comparison later. If you already use your touch sensor for security (e.g. to unlock your phone), your touch sensor is functional and is ready for use with Powertech Multi-Factor Authentication. Otherwise, refer to the following to learn how to enable your biometric touch sensor on your device.

Enabling Touch ID on your iPhone or iPad

Refer to [Use Touch ID on iPhone and iPad](#).


Enabling Fingerprint Security on your Android device

Refer to the instructions that pertain to your device. If your device is not listed below, refer to the device's manufacturer's documentation.

For Samsung Galaxy

1. Go to the **Settings** menu.
2. Slide over the **Personal** tab.
3. Select **Lock screen and security**.
4. Under the Security category, choose **Fingerprints**.
5. Select **Add fingerprint**.
6. Place your finger on the Home button. You'll need to place your finger on the home button multiple times in order for Samsung to learn your fingerprint from multiple angles.

For Pixel or Nexus

1. Open your device's Settings app .
2. Under **Personal**, tap **Security** and then **Pixel Imprint** or **Nexus Imprint**.
3. Follow the on-screen directions.
4. If you don't already have a screen lock, you'll be asked to add a backup PIN, pattern, or password to unlock your device.
5. Scan your first fingerprint.

TIP: Place your finger on your device's sensor (not its screen). Hold your phone in the same way that you'd normally hold it when unlocking. For example, hold your phone with its screen facing you.

See [Unlock with your fingerprint](#) for more details.

Allow Powertech Multi-Factor Authentication to use your camera

Powertech Multi-Factor Authentication needs access to your mobile device's camera in order to scan the QR code used to sync your device with the Authentication Manager.

Granting Powertech Multi-Factor Authentication access to your camera on iPhone or iPad

1. Go to **Settings > Privacy > Camera**.
2. Ensure Powertech Multi-Factor Authentication is allowed access.


Granting Powertech Multi-Factor Authentication access to your camera on your Android device

Refer to the instructions that pertain to your device. If your device is not listed below, refer to the device's manufacturer's documentation.

For Samsung Galaxy

1. From a Home screen, navigate: **Apps > Settings > Applications**.
2. Tap the Powertech Multi-Factor Authentication app.
3. If available, tap **Permissions**.
4. Tap **Camera** to turn it on.

For Pixel or Nexus

1. Open your device's Settings app .
2. Tap **App permissions**.
3. Tap the Powertech Multi-Factor Authentication app.
4. Tap **Camera**.

Allow Powertech Multi-Factor Authentication to send push notifications

Powertech Multi-Factor Authentication needs access to your mobile device's messaging capabilities in order to send One-Time Passwords.

Enabling push notifications on your iPhone or iPad

To get notifications, connect to a Wi-Fi or cellular network. Then do the following:

1. Go to **Settings > Notifications**, select the Powertech Multi-Factor Authentication app, and make sure that Notifications are turned on.
2. If you have notifications turned on, but you're not receiving alerts, the alert style might be set to None. Go to **Settings > Notifications** and check that your Alert Style is set to **Banners** or **Alerts**.
3. Make sure that you're signed in to your Apple ID. Go to **Settings > iTunes & App Stores** and enter your Apple ID and password.
4. Make sure that Do Not Disturb is turned off. Go to **Settings > Do Not Disturb** and tap **Manual** if it's turned on.


Enabling push notifications on your Android Device

Refer to the instructions that pertain to your device. If your device is not listed below, refer to the device's manufacturer's documentation.

For Samsung Galaxy

1. From the home screen, tap **Apps**.
2. Scroll to and tap **Settings**.
3. Scroll to and tap **Notifications**.
4. Tap to enable for the Powertech Multi-Factor Authentication app.

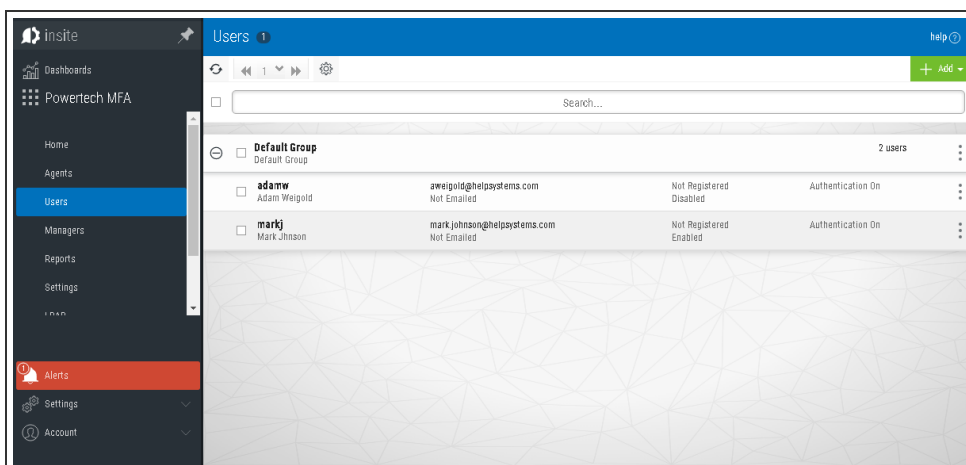
For Pixel or Nexus

1. Open your device's Settings app .
2. Tap **Notifications**.
3. Tap Powertech Multi-Factor Authentication.
4. Tap the options that will allow you to see notifications for Powertech Multi-Factor Authentication. For example:
 - Disable Block all
 - Override Do Not Disturb

Users screen

Use these settings to view, add, and remove Powertech Multi-Factor Authentication users and user groups.

A Default Group is always available to house users that do not belong to any other group. Administrators can create multiple groups for different subsets of users.



How to Get There

In the Navigation Pane, choose **Users**.

Options

Add

Use the options here to add users, import user profiles, or add user groups.

- Click **Add User** to open the [New User](#) page where you can define a new user to add.
- Click **Import Users** to open the [Import Users](#) screen where you can import user profiles from Active Directory database or IBM i system.
- Click **Add Group** to open the [New Group](#) screen where you can add a new User Group.

[user list]; Delete • Enable Selected • Disable Selected • Authenticate on • Authenticate off • Add to group

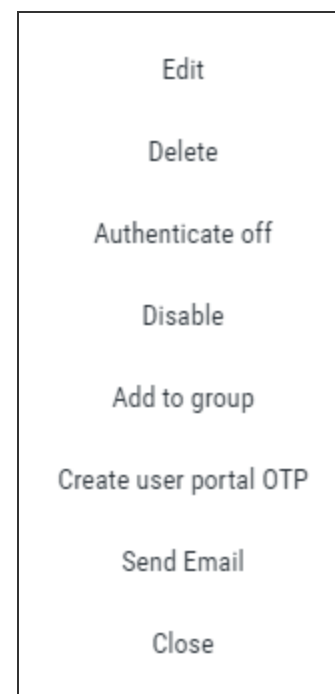
Check the box to the left of one or more Users and/or Groups and additional buttons appear at the top of the screen.

- **Delete.** Click **Delete** to remove the selected Users from Powertech Multi-Factor Authentication.
- **Enable.** Click **Enable** to begin authentication for the selected Users.
- **Disable.** Click **Disable** to end authentication for the selected Users.
- **Authenticate on.** Click **Authenticate on** to set the Authenticate User status to Yes.
- **Authenticate off.** Click **Authenticate off** to set the Authenticate user status to No.
- **Add to group.** Click **Add to group** to open the Select a group screen, where you can choose a Group in which you would like to include the selected users.

Click the  icon for a User to display the following row actions.

You can use these options to make changes to the system.

- **Edit.** Use this option to open the [Edit User](#) screen, where you can make changes to the system's settings.
- **Delete.** Use this option to remove the User from Powertech Multi-Factor Authentication.
- **Authentication off/on.** Use these options to toggle the User's authentication status.
- **Enable/Disable.** Use these options to enable or disable the user within Powertech Multi-Factor Authentication.
- **Add to Group.** Use this option to add the User to an Powertech Multi-Factor Authentication User Group.
- **Create User Portal OTP.** Use this option to create a one-time password for the user. This option can be used to grant a user access to the [User Portal](#) when, for example, the user's usual second factor is not available.
- **Send Email.** Use this option to send an email to the user that informs them that they have been enrolled. The email includes a link to the [User Portal](#), where users can complete the registration process and maintain their account details. Use the settings on the [Email Settings screen](#) to configure your email server settings and define the content of the message.
- **Close.** Use this option to dismiss the context menu.



IBM i Agent Reference

The topics in this section include descriptions of Powertech Multi-Factor Authentication's IBM i Agent options and controls.

Change Initial Program panel

This panel allows you to change the supplemental initial program for active Powertech Multi-Factor Authentication users.

```

1/07/19 Powertech Multi-Factor Authentication Agent      OSCAR
12:57:34 User Own Initial Program Configuration        PMA3604
                                                    QSEC0FR

User Profile . . : MARKJ_____

Initial program : *NONE_____      Name, *NONE
Library . . . . : _____      Name, *LIBL, *CURLIB

F3=Exit

```

How to Get There

On the [Powertech Multi-Factor Authentication Main Menu](#), choose option 5, then, on the [Work with User Initial Program panel](#), choose option 2 for a user.

Or, on the command line, run CHGAAINITP. To run from the command line, ensure the Powertech Multi-Factor Authentication library has been added to the library list.

Options

Profile Name

The profile or profiles for which the supplemental initial program should be changed.

Name

Updates this user's initial program reference within Powertech Multi-Factor Authentication.

generic*

A generic name is a character string that contains one or more characters followed by an asterisk (*). If a generic name is specified, all user profiles that have names with the same prefix as the generic name will be changed with new initial program mentioned in the command.

*ALLUSER

Updates all users' initial program reference within Powertech Multi-Factor Authentication.

Initial Program • Library

This is the name and library of the desired Powertech Multi-Factor Authentication supplemental initial program.

Command Keys

F3=Exit

Dismisses the panel.

Deactivate Authentication Verification panel

The Deactivate Authentication Verification panel allows you to deactivate authentication on the system.

```
PMA3985          Deactivate Authentication          17:10:50
                  Verification                      OSCAR

Are you certain you wish to Deactivate Authentication?

  It will do the following commands:
  - ENDHOSTSVR SERVER(*SIGNON)
  - ENDTCPSVR  SERVER(*FTP)
  - STRHOSTSVR SERVER(*SIGNON)
  - STRTCPSVR SERVER(*FTP)

Select one of the following:
_ No, do not deactivate Authentication.
_ Yes, deactivate Authentication.

F12=Cancel
```

How to Get There

On the [Powertech Multi-Factor Authentication Main Menu](#), choose option 3.

Options

No, do not deactivate Authentication • Yes, deactivate Authentication.

Choose No, to continue authenticating. Choose Yes to deactivate authentication on this system.

Command Keys

F12=Cancel

Cancels this panel.

Emergency Override Setup panel

The Emergency Override Setup panel allows you to configure options for the Emergency Override.

```

1/10/19 Powertech Multi-Factor Authentication Agent OSCAR
13:57:33 Emergency Override Setup PMA3700
QSECOFR

Allow Emergency Override . . . : N (Y=Yes, N=No)
Users Authenticated with Emergency Override rules:

____
____
____
____

____
____
____
____

F3=Exit

```

How to Get There

On the [Powertech Multi-Factor Authentication Main Menu](#), choose option 4.

Options

Allow Emergency Override

Option which pertain to allow the Emergency Overrride.

Emergency override Users

The Users that are allowed to bypass Authentication in case of an Emergency.

Command Keys

F12=Cancel

Cancels this panel.

Insite Server Configuration panel

The Insite Server Configuration panel allows you to configure options for email notifications.

```

1/10/19 Powertech Multi-Factor Authentication Agent OSCAR
13:58:25 Insite Server Configuration PMA3500
QSECOFR

Address . . . . . : 10.60.36.126

____
____

Port . . . . . : 3030
Timeout . . . . . : 5 (seconds)
SSL? . . . . . : N (Y=Yes, N=No)

F3=Exit

```

How to Get There

On the [Powertech Multi-Factor Authentication Main Menu](#), choose option **1**.

Options

SMTP Server Options

Options which pertain to communicating with an SMTP Server.

Address

The IP address or DNS name for the Insite Server. This can be the full Windows computer name of the system running the Insite server.

Port

The port number on the Insite server that will be used for communications.

Timeout

Number of seconds before a timeout occurs.

SSL

Indicates whether SSL (Secure Sockets Layer) is used.

Command Keys

F12=Cancel

Cancels this panel.

Powertech Powertech Multi-Factor Authentication Main Menu

This menu allows you to configure the IP of the Insite server and Authentication Manager used with Powertech Multi-Factor Authentication. It also allows you to deactivate authentication.

```

PMA3000          Powertech Multi-Factor Authentication Agent      13:59:28
R01M061190102          Main Menu                                OSCAR

Select one of the following:                                     Authentication: ACTIVE
                                                                Activation Jobs: ACTIVE

  1. Insite Server Configuration
  2. Authentication Manager Configuration
  3. Deactivate Authentication
  4. Emergency Override Setup.
  5. Maintain Supplemental Initial Programs.

Selection or command
===> _____

F3=Exit   F4=Prompt   F9=Retrieve   F13=Information Assistant

```

How to Get There

Enter command `wrkptma`.

Options

1. Insite Server Configuration

The Insite Server Configuration allows maintaining the Insite Server settings.

2. Authentication Manager Configuration

The Authentication Manager Configuration allows maintaining the Authentication Manager settings.

3. Deactivate Authentication

The Deactivate Authentication allows you to Deactivate Authentication in the event that Insite cannot communicate.

4. Emergency Override Setup

The Emergency Override Setup option allows you to configure options for the Emergency Override. See [Emergency Override Setup panel](#).

5. Maintain Supplemental Initial Programs

The Maintain Supplemental Initial Programs option allows you to change the supplemental initial program for active Powertech Multi-Factor Authentication users. See [Work with User Initial Programs panel](#).

Selection or Command Entry

Selection or Command entry allows you to enter menu options or commands to be processed by the system.

To run a command, type the command and press Enter. For assistance in selecting a command, press F4 (Prompt) without typing anything. For assistance in entering a command, type the command and press F4 (Prompt). To see a previous command you entered, press F9 (Retrieve).

Command Keys

F1=Help

Provides additional information about using the display or a specific field on the display.

F3=Exit

Ends the current task and returns to the display from which the task was started.

F9=Retrieve

Displays the last command you entered on the command line and any parameters you included. Pressing this key once, shows the last command you ran. Pressing this key twice, shows the command you ran before that and so on.

User Own Initial Program Configuration panel

This panel allows you to specify the initial program and library for a specific active Powertech Multi-Factor Authentication user.

```

1/10/19 Powertech Multi-Factor Authentication Agent OSCAR
14:20:58 User Own Initial Program Configuration PMA3604
                                                QSEC0FR

User Profile . . : MARKJ_____

Initial program : *NONE_____ Name, *NONE
Library . . . . : _____ Name, *LIBL, *CURLIB

F3=Exit

```

How to Get There

On the [Work with User Initial Programs screen](#), choose option 2 for a user.

Options

User Profile

The Profile name to change the user own Initial Program.

Initial Program • Library

This is the name and library of the desired Powertech Multi-Factor Authentication supplemental initial program.

Command Keys

F12=Cancel

Cancels this panel.

Work with Authentication Managers panel

The Work with Authentication Managers panel allows you to view the IP addresses for the Authentication Manager.

```

7/27/17          Multi-Factor Authentication          OSCAR
17:09:27        Work with Authentication Managers    PMA3601
                                                       QSECOFR

Options
2=Change  4=Delete
Opt  IP Address          Port  SSL
---  10.60.129.234      3040  N
---  10.60.129.240      3040  N

Bottom

F3=Exit  F6=Add Manager

```

How to Get There

On the [Powertech Multi-Factor Authentication Main Menu](#), choose option 2.

Options

IP Address

The IP address or DNS name for the Authentication Manager.

Port

The port number that will be used. for communications.

SSL

Indicates whether SSL (Secure Sockets Layer) is used.

Timeout

Number of seconds before a timeout occurs.

Option

Enter a valid option from the list of options provided on the panel.

Work with User Initial Programs panel

When an IBM i user profile is assigned to an Powertech Multi-Factor Authentication user and the IBM i agent is activated, the user's existing initial program is replaced with the Powertech Multi-Factor Authentication authentication program. The program that was replaced is called once the authentication program call has completed.

The user's old initial program is encrypted and stored in a reference file and cannot be maintained without deactivating and reactivating the user profile in Powertech Multi-Factor Authentication. This change warranted the addition of the Maintain Supplemental Initial Programs option in the [Main Menu](#). This option allows administrators to make changes to the initial programs stored in the configuration file for each user profile that is being authenticated by Powertech Multi-Factor Authentication (without requiring user deactivation).


```

9/17/18      Multi-Factor Authentiction      HOTEL2
13:39:53    Work with User Initial Programs  PMA3603
                                                    QSECOFR

Options
2=Change
Opt  User Profile           User Initial Program
  _  GREGDARWIN             TEST/TNONE
  _  GDARWIN                TEST/TNONE

                                                    Bottom

F3=Exit      F7=View Sort      F14=Bulk update

```

How to Get There

On the [Powertech Multi-Factor Authentication Main Menu](#), choose option 5.

Field Descriptions

User Profile

The name of the Profile that has authentication turned on.

User Initial Program

The original/actual initial program attached to the user profile.

Option

Enter a valid option from the list of options provided on the panel.

Options

2=Change

Choose this option for a user to open the [User Own Initial Program Configuration panel](#) where you can change the initial program for a user individually.

Command Keys

F3=Exit

Cancels this panel.

F14=Bulk update

Opens the [Change Initial Program panel](#), which allows you to change the supplemental initial program for several users at once.

F7=View Sort

To sort the data within the view. To sort the data you need to take the cursor on top of the field that you want to sort or place the cursor on top of field caption and then press this function key. Sort always performs in ascending order. This key is only valid and will be visible when there are some data to show.

F14=Bulk update

To change the user own initial program in bulk. This function will run an internal command where specific name , generic name or all can be used for user name to change user(s) own initial program setup within Powertech Multi-Factor Authentication. This key is only valid and will be visible when there are some data to show.

Work with User Own Exit Point Programs panel

Exit programs that were registered against exit points before Powertech Multi-Factor Authentication control for those exit points was activated can be changed.

When Powertech Multi-Factor Authentication is set to control an exit point, it registers the Powertech MFA exit program against that exit point. If an exit program was already registered (for example, Powertech Exit Point Manager) then that is written into a file and associated with the exit program. This is done for the following reasons:

- If Powertech Multi-Factor Authentication is deactivated (or no longer controlling that exit point) the former exit program is restored (registered against that exit point).
- Once the Powertech Multi-Factor Authentication program has been called, it will call the program that was formerly registered against the exit point.

```

4/24/19      Powertech Multi-Factor Authentication      PAPA
12:56:26    Work with User Own Exit Point Programs      PMA3607
                                                    QSECOFR

Options
2=Change
Opt  Exit Point      Format      Exit Point Program
  _  QIBM_QTMF_SVR_LOGON  TCPL0300  PTMALIB/PMA102

                                                    Bottom

F3=Exit      F7=View Sort

```

How to Get There

On the [Powertech Multi-Factor Authentication Main Menu](#), choose option 6.

Field Descriptions

Exit Point

The name of the exit point where your own program is registered.

Format

The format of the exit point where user program is registered.

Exit Point Program

The user own program that has been registered against the exit point.

Command Keys

F3=Exit

Cancels this panel.

F7=View Sort

To sort the data within the view. To sort the data you need to take the cursor on top of the field that you want to sort or place the cursor on top of field caption and then press this function key. Sort always performs in ascending order. This key is only valid and will be visible when there are some data to show.

Appendix


The topics in this section include additional information about Powertech Multi-Factor Authentication.

Copying or Moving an IBM i Agent Configuration

Powertech Multi-Factor Authentication allows you to copy or move an IBM i configuration including all settings (users, exit point status, etc.) between two IBM i systems—an existing one and one being added—with the option of *copying* the configuration while retaining the existing system, or *moving* the configuration and deleting the existing system from Powertech MFA. All settings from the agent's source configuration are transferred to the target system's agent configuration.

In order to copy or move configurations, the target IBM i system needs to have been added to Insite (see [Product Connections](#)), and have Powertech Multi-Factor Authentication installed.

To copy or move an IBM i agent configuration

1. In the Navigation Pane, choose **Agents**, then click **IBM i Agents**. Click  > **Copy/move configuration** for an IBM i agent. The [Copy/move configuration screen](#) appears.
2. Click **Select System**. The [Select System screen](#) appears. Choose the target IBM i system. If the system does not exist, be sure it has been added to Insite (see [Product Connections](#)).
3. Check the target system and click **Select**.
4. Set Move Configuration (Remove Source System) to **On** if, after the move, the agent configuration should be removed from the source system. If the agent configuration should exist on both systems after the procedure, set this to **Off**.
5. Click **Save**. The configuration is moved or copied based on your settings.

Adding and Importing Users

Users can be added to Powertech Multi-Factor Authentication individually, or imported using a .csv file. Users who do not have an Active Directory account must be imported manually.

Adding Users Manually

To add users manually, add an Powertech Multi-Factor Authentication user, Import IBM i user profiles, then link them to the Powertech Multi-Factor Authentication you added:

1. On the Navigation Pane, click **Users**.
2. Click **Add > Add User**. The [New User screen](#) appears.
3. Enter the user's details. If you want Powertech Multi-Factor Authentication's Smart Match feature to automatically match the user to imported IBM i users, set the Powertech Multi-Factor Authentication Name to the IBM i User Profile Name. Or, you can use the 'IBM i Profiles and Systems' section at the bottom to specify the attached IBM i profiles manually.
4. Click **Save**. Repeat for additional IBM i users.

Importing Multiple Users Using a .CSV File

1. On the Navigation Pane, click **Users**.
2. Click **Add > Import Users**. The [Import Users screen](#) appears.
3. Under Import Type, choose either MFA users (Import from CSV)) or IBM i profiles (Import from CSV), depending on the users being imported.

The CSV documents used to import must contain the user information in a very specific order.

The documents themselves must be comma separated documents (that is, in .csv format). The column orders are as follows:

Column order for Powertech Multi-Factor Authentication user import

- Username (must be unique)
- LDAP username (can be blank)
- Full name (required)
- Email address (required)
- RADIUS username (can be blank - if RADIUS authentication is enabled, the MFA user name will be used to set a value for this field)
- Group name (group must exist)
- Enabled (T or F for "true" or "false")
- Authenticate user (T or F for "true" or "false")

NOTE: For Powertech Multi-Factor Authentication users, the license terms are checked during import. The number of enabled users you will be allowed to import is limited the the amount authorized by your license.

Column order for IBM i profile import

- IBM i alias (required – IBM i agent system alias displayed in Insite)
- IBM i user profile (required)
- MFA user name (must be a valid MFA user name)

NOTE: If Powertech Multi-Factor Authentication is active on the IBM i server conducting the import, the imported users will automatically be activated.

4. Click **Choose File**.
5. Select the .csv file containing the user information.
6. Click **Upload**.

Invoking Authentication from an IBM i Function

If, as a developer, you would like to integrate Powertech Multi-Factor Authentication into your own product and/or processes so, for example, authentication is invoked when calling the program, you can use Powertech Multi-Factor Authentication's PMA300i integration program.

Powertech Multi-Factor Authentication Integration - PMA300i

Required Parameters:

1.	Profile to authenticate	Input	char(10)
2.	Source of authentication	Input	char(50) <i>[free format text]</i>
3.	Authentication Type	Input	char(1) <i>['N' = Native, 'D' = Desktop]</i>

The Powertech Multi-Factor Authentication integration program, PMA300i, allows you to authenticate with your product interactively (via the green screen).

NOTE: IBM i user profiles to be authenticated must be mapped to an Powertech Multi-Factor Authentication user. See [Add Users](#) in the Administrator Setup Procedure topic.

Required Parameters

Profile to authenticate

The name of the profile you want to authenticate.

Source of authentication

The source from which the authentication is taking place, such as the 3rd party program. Text entered here will appear in the Desktop Agent upon remote authentication.

Authentication Type

Whether you are authenticating via a native installation, or via the Desktop Agent.

The possible values for this parameter are:

Value	Description
N	Native
D	Desktop

Example

The API's can be called from the command line, like the following:


```
CALL PMA300i PARM('profile' 'source' 'authentication type - N or D')
```

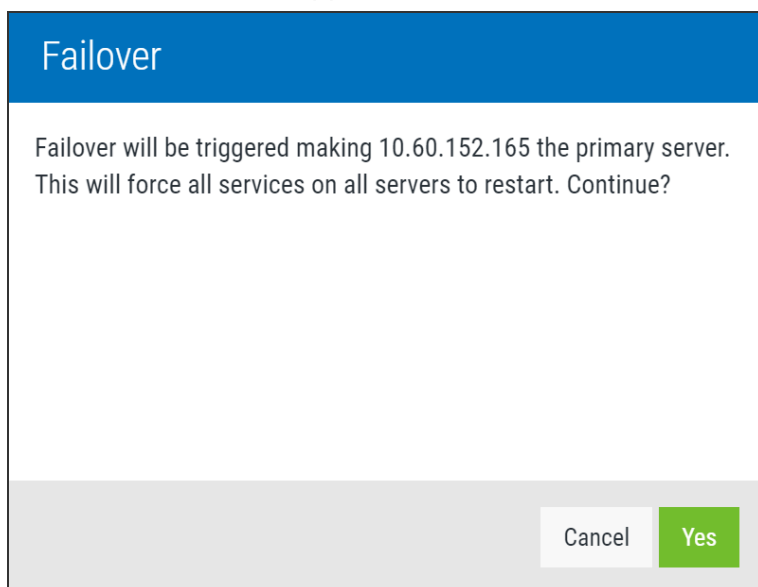
Manual Failover

In a multi-server deployment (see [Installing the Authentication Manager and Data Services](#)), Powertech MFA automatically initiates failover to a secondary server when the Authentication Manager or Database Services fail on the Primary server. If maintenance is required on the Primary server, or if, for any reason, the Primary server must be removed from service, Powertech Multi-Factor Authentication allows you to force a specific node/system to be promoted to Primary (the master/leader database).

NOTE: When failover is triggered, Powertech MFA's authentication service will be interrupted for several seconds, up to a minute. This delay is the amount of time required for the services to restart on the new Primary server.

To promote a Secondary system to Primary

1. In the Navigation pane, choose **Server Health and Failover**. The [Server Health and Failover screen](#) appears.
2. For the server to be designated Primary, click  (**Show Actions**) > **Fail Over to This Server**. A confirmation screen appears.



3. Click **Yes** to begin the failover procedure.

Securing Powertech Multi-Factor Authentication Connections

Powertech Multi-Factor Authentication supports TLS (Transport Layer Security/Secure Sockets Layer) communications to and from the Authentication Manager for both HelpSystems Insite and the IBM i Agent. The instructions in this topic describe how to configure these connections.

NOTE: In order to secure all HelpSystems Insite transactions, if you haven't already, complete the following instructions to secure your Insite installation and Insite Product Connections:

- [Securing an IBM i Product Connection](#)

Users who have already configured the [Desktop Agent](#) will need to update their Insite Server Address (to the new HTTPS address with the new port) after the HelpSystems Insite connection has been secured. See step 4c under [User Setup Procedure](#).

Securing the IBM i Agent

Upon installation of the IBM i Agent software, Powertech Multi-Factor Authentication is registered as a Client Application within the IBM Digital Certificate Manager (DCM). A valid certificate must be imported into the IBM DCM to ensure the appropriate protection is used.

The following values are used during the registration process:

- Application ID: PTECHMULTIFACTORAUTH
- Application description: Powertech Multi-Factor Authentication

Once your Certificate Authority has been configured in the IBM DCM, no additional steps are required to configure the IBM i Agent connection. If the Powertech Multi-Factor Authentication Client Application is removed from the DCM, it can be restored using the program PMA3501. Use the following command to call this program (requires profile with QSECOFR authority):

```
call ptmalib/pma3501
```

NOTE: If your organization does not already have a signed Certificate Authority, see [Securing an IBM i Product Connection](#) for help generating and importing a self-signed certificate.

Securing the Authentication Manager

The procedure for securing the Authentication Manager is almost identical to the procedure for securing HelpSystems Insite.

NOTE: After securing the Authentication Manager using these steps, users who authenticate using a mobile device will need to re-sync their Powertech Multi-Factor Authentication Mobile App.

1. If you haven't yet installed the Powertech Multi-Factor Authentication Authentication Manager, do so now. See [Installing the Authentication Manager and Data Services](#).
2. Stop the Access Authentication Manager service. On Windows, run services.msc to open the Services Manager. Right-click Help Systems Powertech Multi-Factor Authentication Manager and choose **Stop**.
3. Copy your Certificate Authority file to the Authentication Manager server. Do not store the Certificate Authority file within the Powertech Multi-Factor Authentication folder (as files within Powertech Multi-Factor Authentication folders are deleted and replaced while installing upgrades).

4. Open the "server.xml" file located at C:\Program Files\Help Systems\Access Authenticator\AuthenticationManager\conf and edit it as follows:

NOTE: You can edit the server.xml file with any text editor. Be sure to create a backup a copy of the original file before editing. If you are not familiar with the XML format, we recommend using an XML-aware editor such as XML Notepad or Notepad++.

- a. Comment out the code block for protocol="HTTP/1.1":

```
Connector SSLEnabled="false" compression="force"
connectionTimeout="20000" port="3040" protocol="HTTP/1.1"
scheme="http" secure="false"/
```

- b. Add the following code block, replacing the italicized text with information specific to your configuration:

```
Connector SSLEnabled="true" clientAuth="false"
compression="force" keystoreFile="your-ca-path/filename"
keystorePass="your-ca-password" keystoreType="your-keystore-type"
maxHttpHeaderSize="32768" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https" secure="true" sslEnabledProtocols="TLSv1,
TLSv1.1, TLSv1.2"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_
SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_
AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_
WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA" /
```

5. Save your changes to server.xml.
6. Restart the Authentication Manager service.
7. In Insite, navigate to the Powertech Multi-Factor Authentication Managers screen.
8. Choose the Authentication Manager instance you have just configured and click **Edit**.
 - a. Set the Port to 8443.
 - b. Set UseSSL to **On**.
9. Click **Save** to update the Authentication Manager settings.

Use of Firebase Third-Party Service

Powertech Multi-Factor Authentication uses the following third-party service while sending notifications to mobile devices (phones/tablets) that are running the Powertech Multi-Factor Authentication mobile app:

- Name of service: Firebase Cloud Messaging
- Service provider: Google, LLC

The following Terms of Service apply:

- [Google APIs Terms of Service](#)
- [Firebase Data Processing and Security Terms](#)

Data processed by the service provider in the provision of the service may include, without limitation, the following types of data:

- IP addresses.
- Mobile device UUID (unique identifier, so that Google/Firebase knows where to route the message). This ID is provided by the device when the user performs a sync. It is the same ID that is used by all mobile devices that use Firebase Cloud Messaging to perform push notifications.
- The user's Powertech Multi-Factor Authentication ID.
- Authentication prompt (i.e. information about the authentication attempt, for example "User XYZ is trying to authenticate on system ABC. Press Accept to authenticate.").
- A function ID that identifies whether the push notification requires biometric validation on the mobile phone in order to proceed (this differentiates between a push notification and a biometric notification).

NOTE: The function ID does not contain biometric data.

Some or all of the types of data processed by the service provider in the provision of the service may be considered personal data/personally identifiable information under the data processing laws and regulations that apply to your organization.

If you are not redirected automatically, follow this [link](#) to the Insite Other Help topic.