helpsystems

Reference Manual

Access Authenticator

1.3.2

Copyright Terms and Conditions

201811080144

Welcome to Access Authenticator

Access Authenticator 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*. Access Authenticator 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.

Access Authenticator 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 Access Authenticator.
- **The *Authentication Manager* Server.** The Authentication Manager is Access Authenticator's central processing component.
- **The *Data Services* Server.** The Data Services includes Access Authenticator'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 administrating Access Authenticator.

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 Access Authenticator 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 Access Authenticator.

See User Setup Procedure for details on setting up Access Authenticator for authentication.

See User Authentication for details on how to authenticate using Access Authenticator as an end user.

Installing Access Authenticator

These instructions guide you through the process of installing Access Authenticator.

System Requirements

Compatibility with HelpSystems Insite

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 4.4 or higher using Chrome Windows: OS 10 using Edge
IBM i	V7R1 or higher operating system

For more details, see Insite System Requirements.

Authentication Manager System Requirements

- For Linux, the /opt drive must have at least 20 GB of disk space.
- Version R01M04 of the Access Authenticator IBM i Agent (shipped with Access Authenticator 1.3.2).

The remaining system requirements for the Authentication Manager are the same as HelpSystems Insite. See Insite System Requirements.

IBM i Agent System Requirements

Access Authenticator requires IBM i (i5/OS, OS/400) version V7R1 or higher.

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 Access Authenticator 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 Access Authenticator 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 Access Authenticator install library (PTMALIB) for the product to function properly.
- Set QVFYOBJRST to 1, 2, or 3. This allows Access Authenticator to restore all objects regardless of their signature. (Note: If you normally check signatures, remember to check this system value after the Access Authenticator install process completes.)
- Set QFRCCVNRST (Force conversion on restore) to 0, Do not convert anything.

Desktop Agent System Requirements

- Windows 7 64-bit or Windows 10 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 Access Authenticator users upgrade to the latest Desktop Agent as soon as possible. See User Setup Procedure.

Mobile App System Requirements

Biometric authentication on Android to devices requires Android 6.0 Marshmallow or newer.

Installation Overview

Access Authenticator 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 Access Authenticator. See Profiles in the HelpSystems Insite User Guide.

- **Access Authenticator Authentication Manager and Data Services.** The Authentication Manager is Access Authenticator'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.
- **Access Authenticator IBM i agent.** The IBM i agent software must be installed on all systems to be secured by Access Authenticator. See Installing the IBM i Agent.

After Access Authenticator 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):

- **Access Authenticator 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.)
- **Access Authenticator 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

Access Authenticator can run in two modes:

- **Single System:** The Authentication Manager and Data Services are installed on the same system. This is the easiest installation that requires the smallest footprint. This is the recommended configuration for the first system.
- **Multiple Systems with Manual Failover:** In this configuration, the Authentication Manager and Data Services are installed on a second system (same as the first), but the installation points back to the Primary system to replicate its data. The second system can be switched to the Primary system in the event of a system failure, or for maintenance on the Primary system.

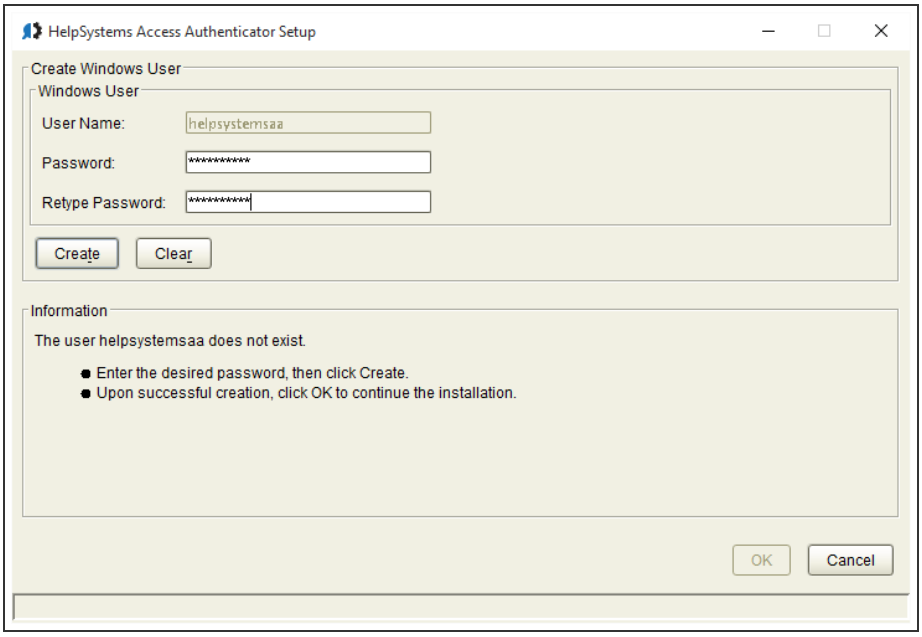
The following instructions demonstrate how to install the Authentication Manager and Data Services on a Primary and Secondary system in order to provide replication and failover capability. If you intend to install on a single system only, use the initial steps of the following procedure for your platform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

To install the Access Authenticator Authentication Manager and Data Services on Windows

1. Login to the Windows server you would like to use for your Primary installation.
2. Download the Access Authenticator installer (**setupAccessAuthenticator.exe**) from the Access Authenticator download page. (The "Trial" download is the full product, which can be unlocked with a valid License Key.)
3. 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\Access Authenticator` folder and start the installer again.

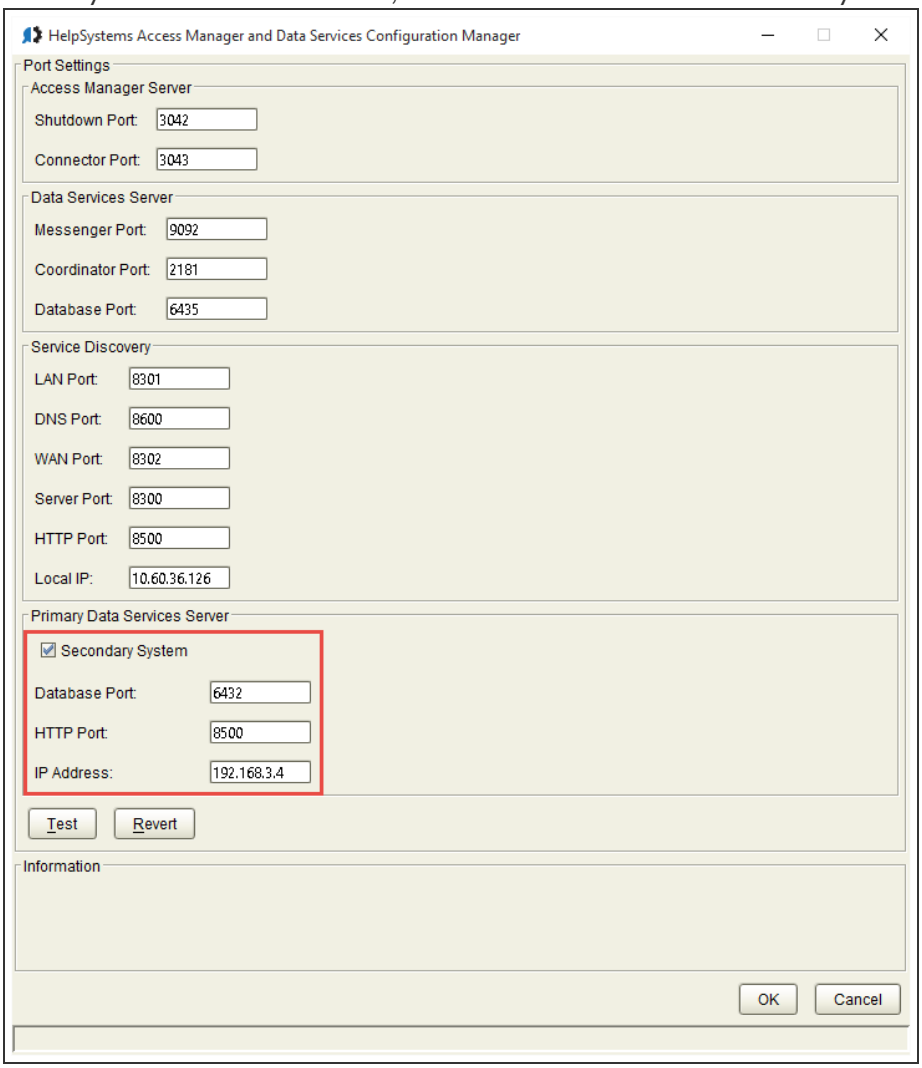
4. Follow the instructions to continue the installation.
5. The Access Authenticator Create Windows User window prompts you to create a new Windows user named helpsystemsaa. Enter a password for the new user and click **Create**. Once the password is accepted, click **OK** to continue installation.



   NOTE: If you are reinstalling Access Authenticator over a previous version, you will not see this window.

6. The HelpSystems Access Manager and Data Services Configuration Manager appears. You must configure ports for the manager and services. The installer lets you know 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. Make note of the Database Port and HTTP Port. Also note the Local IP address. These will need to be entered later.
   Once all ports are available, click **OK** to save the ports and continue installation. See also Port Descriptions.
7. Click **Finish** to complete installation on the Primary server.

8. Login to the Windows server you would like to use for your Secondary installation.
9. Repeat the installation process on this server until you reach the HelpSystems Access Manager and Data Services Configuration Manager screen (steps 1-5).
   Check **Secondary System**. Then, enter the Database Port and HTTP port specified for the Primary server. For IP Address, enter the IP address of the Primary server.



   If a port is not available, enter a new port number and click **Test** to see if it is available. Once all ports are available, click **OK** to save the ports and continue installation.

10. Click **Finish** to complete installation on the Secondary system.
11. On the Secondary system, open a command line and run the following command in the Access Authenticator directory (`C:\Program Files\Help Systems\Access Authenticator` by default):

    `master2standby.bat -a` *`ip address of primary system`* `-p` *`database port of primary system`*

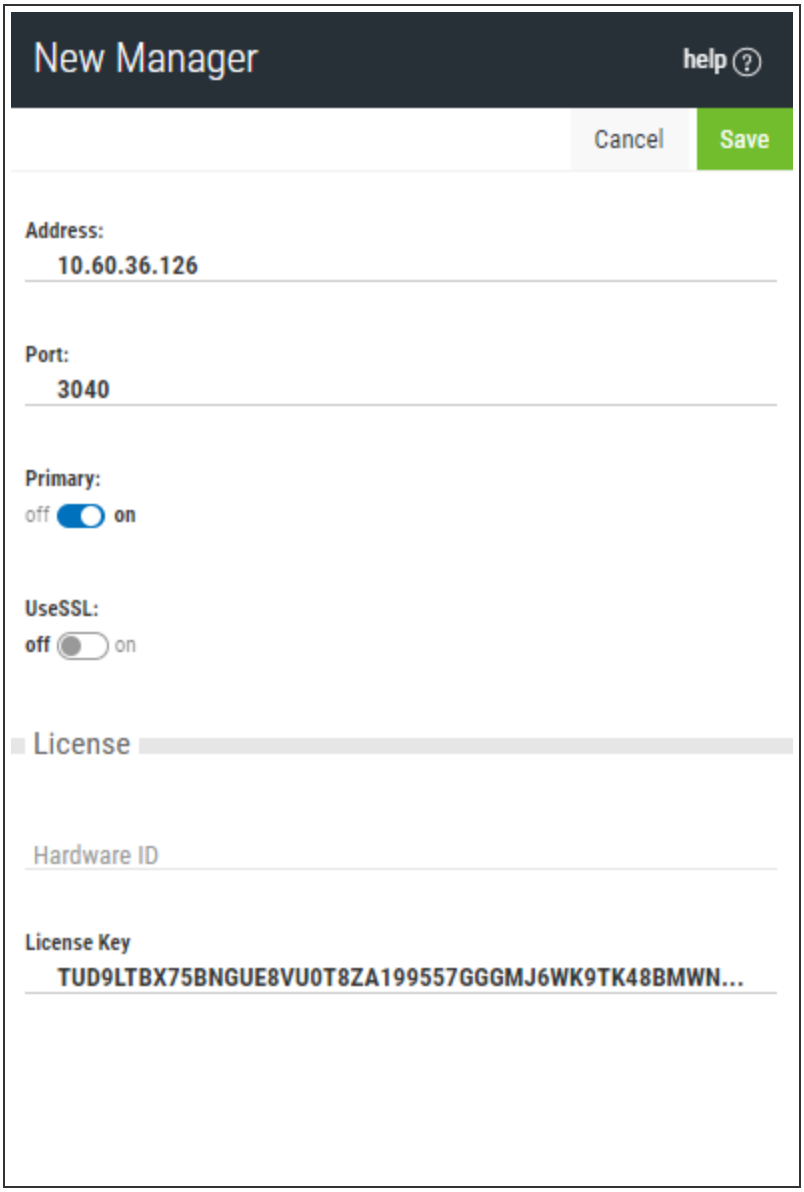
    This tells Access Authenticator to begin replicating data from the Primary system.

> **NOTE:** You can look at the "PortConfig.txt" file on the Primary system to view the port configuration, including the Database Port. This file is located at `C:\Program Files\Help Systems\Access Authenticator`.

Next, you need to add the IP addresses and ports of the Primary and Secondary systems you have just installed in HelpSystems Insite, which is the browser interface used to administer Access Authenticator.

12. Open HelpSystems Insite and choose **Access Authenticator** from the Navigation Pane. (See HelpSystems Insite Documentation List for Insite installation instructions if you have not yet installed Insite.)
13. Choose **Managers** from the Navigation Pane and click **Add** to add an Authentication Manager. Or, if you have already added the Primary Manager (e.g. for licensing), click ⋮ next to the Manager and choose **Edit**.

14. Specify the Address and Port of the Primary system (recorded earlier), then set Primary to **On**. Enter a valid License Key if you have not already.



TIP: To verify a system is configured to be the Primary Authentication Manager instance, you can run the command `is-master.bat` (located in the Access Authenticator folder). If it is Primary, the command will return `POSTGRES_MASTER=TRUE`.

15. Click **Save**. The Primary system is added to the list of Managers.
16. Click **Add**. Or, if you have already added the Secondary Manager, click ⋮ next to the Manager and choose **Edit**. Now, enter the IP address and Port of the Secondary Authentication Manager system. Leave the Primary setting at **Off**. Enter a valid License Key if you have not already.
17. Click **Save**. The Secondary system is added to the list of Managers. To promote a Secondary Authentication Manager to Primary in case of a system failure or maintenance, see Promoting a Secondary Authentication Manager to Primary.

> **NOTE:** You can view the IP addresses and ports of Primary (master) and Secondary databases in the pckz.properties file located in the `Access Authenticator/properties` folder.

To install the Access Authenticator 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 Access Authenticator for Linux file (installAccessAuthenticator.tgz) to a temporary directory on the system from the Access Authenticator download page. (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 installAccessAuthenticator.tgz
   ```

   Files are extracted to the directory installAccessAuthenticator.
4. Use the following commands to start the installer:

   ```
   cd installAccessAuthenticator
   ./serverInstall
   ```

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

5. When prompted to choose whether you want to install the Authentication Manager and Data Services, choose **y**.
6. When asked if this is the primary data services server, indicate **y**.
7. When prompted to verify the server IP, confirm it is correct. Or, if it is not correct, enter **n**, then enter the correct IP.
8. Next you are prompted to confirm a series of ports Access Authenticator uses for communication. Verify the ports are correct. Record the LAN port number and the Database port number, as you will need to enter these later if you are installing a Secondary instance.
9. Access Authenticator creates the Primary database and starts the product. It installs to /opt/helpsystems/AccessAuthenticator.
10. Login to the server you want to use for your Secondary installation and repeat the above process through step 4.
11. When asked if this is the primary data services server, indicate **n**. The Data Services must be running for the following steps to work.
12. Enter the IP of the primary system (the one just installed).
13. Enter the port number of the primary database (recorded earlier).

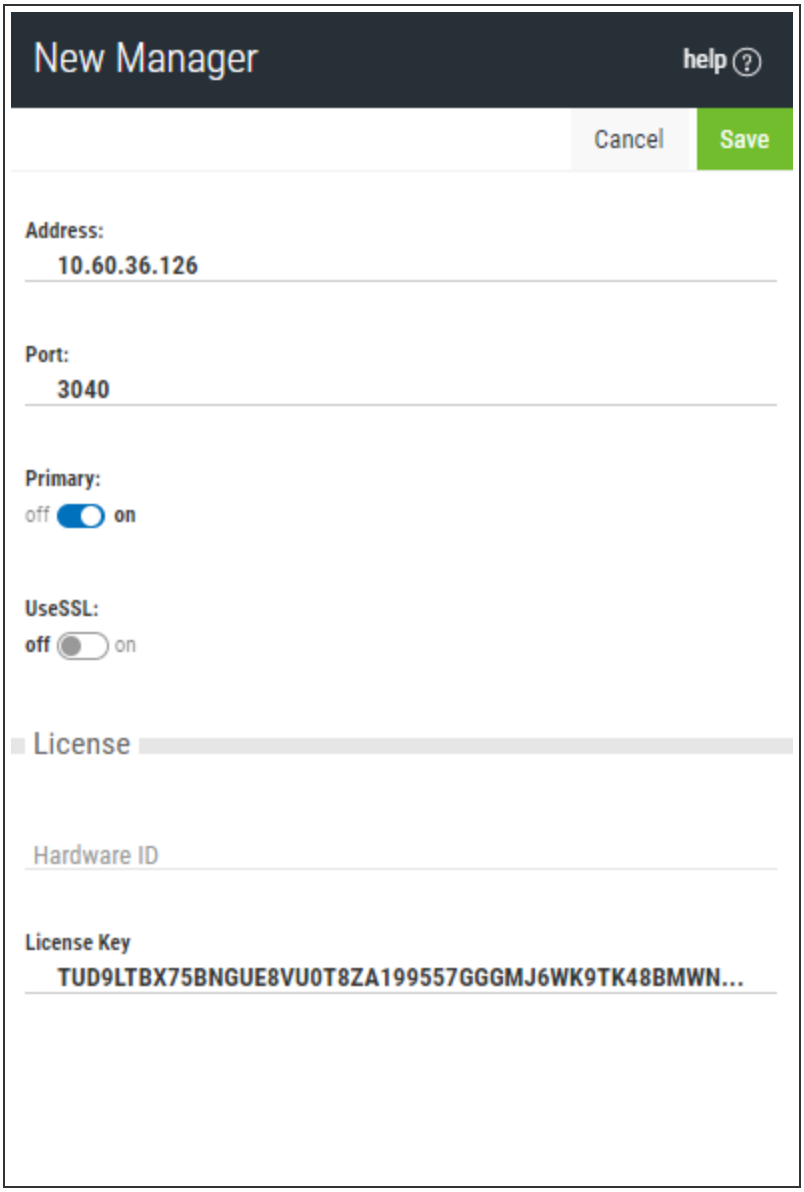
    > **NOTE:** You can look at "PortConfig.log" in the installAccessAuthenticator directory on the Primary system to view the port configuration, including the Database Port.

14. Enter the port number for the primary Discovery LAN (recorded earlier).

    > **NOTE:** If a firewall is preventing communication between the servers, create rules in the firewall to allow the required traffic.

15. When prompted to verify the server IP, confirm it is correct. Or, if it is not correct, enter **n**, then enter the correct IP.
16. You are prompted to confirm a series of ports Access Authenticator uses for communication. Verify the ports are correct.
17. Access Authenticator creates the Secondary database and starts the product. It installs to /opt/helpsystems/AccessAuthenticator.
    Next, you need to add the IP addresses and ports of the Primary and Secondary systems you have just installed in HelpSystems Insite, which is the browser interface used to administer Access Authenticator.
18. Open HelpSystems Insite and choose **Access Authenticator** from the Navigation Pane. (See HelpSystems Insite Documentation List for Insite installation instructions if you have not yet installed Insite.)
19. Choose **Managers** from the Navigation Pane and click **Add** to add an Authentication Manager. Or, if you have already added the Primary Manager (e.g. for licensing), click ⋮ next to the Manager and choose **Edit**. The New Managers screen appears.

20. Specify the Address and Port of the Primary system (recorded earlier), then set Primary to **On**. Enter a valid License Key if you have not already.



21. Click **Save**. The Primary system is added to the list of Managers.
22. Click **Add**. Or, if you have already added the Secondary Manager, click ⋮ next to the Manager and choose **Edit**. Now, enter the IP address and Port of the Secondary Authentication Manager system. Leave the Primary setting at **Off**. Enter a valid License Key if you have not already.
23. Click **Save**. The Secondary system is added to the list of Managers. To promote a Secondary Authentication Manager to Primary in case of a system failure or maintenance, see Promoting a Secondary Authentication Manager to Primary.

Installing the Access Authenticator 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 Access Authenticator installer (**setupAccessAuthenticatorIBMi.exe**) to your PC from the Access Authenticator 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\Access Authenticator\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 Access Authenticator 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 Access Authenticator 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 Access Authenticator and press Enter.
   The installation program installs Access Authenticator, 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 Access Authenticator install.

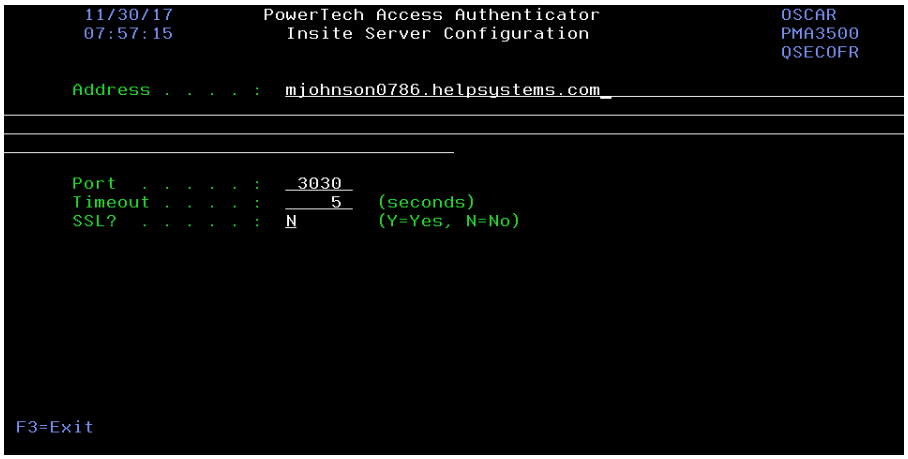
Objects Installed on System

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 - Access Authenticator 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

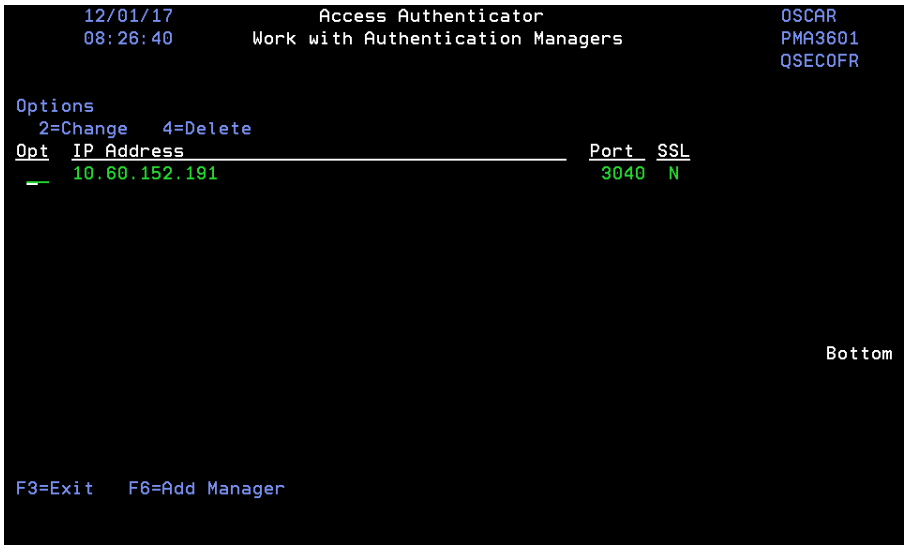
After installation, you need to add any profiles that will require access to the IBM i agent's configuration settings to the PMAADMIN authorization list. Then, configure the IBM i agent to synchronize with Insite and the Authentication Manager.

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.



   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.



> **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 Access Authenticator in Insite.

11. Open HelpSystems Insite and choose **Access Authenticator** 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. Click **IBM i agent**, then click **Add**. The Agents > New System screen appears.
14. For System, choose **Select System** and choose the system you just configured.
15. Configure any system settings and click **Save**. You return to the Agents > IBM i agent screen.
16. To activate the system, click ⋮ (on the right side of the screen) and choose **Activate**.

When the necessary components have been installed, see Administrator Setup Procedure to begin configuring and using Access Authenticator.

Starting and Stopping the IBM i Agent for Backups

When started, the Access Authenticator 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 Access Authenticator into the startup program, the following commands are available:

- **PMASTRMON** - Start Access Authenticator
- **PMAENDMON** - Stop Access Authenticator

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 Access Authenticator agent is ended, it is still fully configured, but inactive. While inactive, registered users are not asked to authenticate.

Upgrading Access Authenticator

These instructions guide you through the process of upgrading Access Authenticator.

> **NOTE:** For system requirements, including IBM i Agent system values, see Installing Access Authenticator.

> **WARNING:** The Authentication Manager must be stopped in order to be upgraded, which means Access Authenticator 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 Access Authenticator 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.
- **Access Authenticator 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.
- **Access Authenticator IBM i agent.** The latest IBM i agent software must be installed on all systems to be secured by Access Authenticator 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).

To upgrade the Access Authenticator Authentication Manager and Data Services on Windows

1. Login to the Windows server of your Primary installation.
2. Download the Access Authenticator installer (**setupAccessAuthenticator.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 Access Authenticator 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\Access Authenticator` folder and start the installer again.

5. Follow the instructions to continue the installation.
6. Click **Finish** to complete installation on the Primary server. The Authentication Manager service starts automatically. If you are upgrading one or more Secondary systems as well, continue with the next step. (If you are only using a Primary server complete the upgrade by installing the latest version of the remaining Access Authenticator components (see Installing Access Authenticator).
7. Login to the Windows server you would like to use for your Secondary installation.
8. Click **Finish** to complete installation on the Secondary system. The Access Authenticator service starts automatically.

To upgrade the Access Authenticator 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 Access Authenticator for Linux file (installAccessAuthenticator.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 installAccessAuthenticator.tgz
    ```

    Files are extracted to the directory installAccessAuthenticator.

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 installAccessAuthenticator
   ./serverInstall
   ```

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

6. When prompted to choose whether you want to install the Authentication Manager and Data Services, choose **y**.
7. When asked if this is the primary data services server, indicate **y**.
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. Next you are prompted to confirm a series of ports Access Authenticator uses for communication. Verify the ports are correct. Record the LAN port number and the Database port number, as you will need to enter these later if you are installing a Secondary instance.
10. Access Authenticator creates the Primary database and starts the product. It installs to /opt/helpsystems/AccessAuthenticator.
11. Login to the server you want to use for your Secondary installation and repeat the above process through step 4.
12. When asked if this is the primary data services server, indicate **n**. The Data Services must be running for the following steps to work.
13. Enter the IP of the primary system (the one just installed).
14. Enter the port number of the primary database (recorded earlier).

    NOTE: You can look at "PortConfig.log" in the installAccessAuthenticator directory on the Primary system to view the port configuration, including the Database Port.

15. Enter the port number for the primary Discovery LAN (recorded earlier).

    NOTE: If a firewall is preventing communication between the servers, create rules in the firewall to allow the required traffic.

16. When prompted to verify the server IP, confirm it is correct. Or, if it is not correct, enter **n**, then enter the correct IP.
17. You are prompted to confirm a series of ports Access Authenticator uses for communication. Verify the ports are correct.
18. Access Authenticator creates the Secondary database and starts the product. It installs to /opt/helpsystems/AccessAuthenticator.

After HelpSystems Insite and the Authentication Manager have been upgraded, use the Installation Instructions to upgrade to the latest versions of the IBM i Agent, Desktop Agent, and mobile apps (for these components, the upgrade and installation procedures are identical).

Implementing Access Authenticator

This guide describes how to configure and use Access Authenticator. It describes how administrators can tailor Access Authenticator 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 Access Authenticator.

> **NOTE:** See Installing Access Authenticator for installation information.

To Configure Access Authenticator

Configure Access Authenticator in HelpSystems Insite by configuring the general Access Authenticator settings, adding and configuring IBM i agents in Insite, configuring email settings, then adding and/or importing users to Access Authenticator.

Configure Access Authenticator Settings

The Settings screen includes several important settings related to authentication and general management of Access Authenticator. Review and configure all options available on the Settings screen prior to deploying Access Authenticator. See Settings Screen.

Add and Configure IBM i Agents in Insite

> **NOTE:** The following instructions assume the Access Authenticator 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 Access Authenticator 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 Access Authenticator.
   - 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 Access Authenticator.
   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 Access Authenticator. 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 Access Authenticator 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 Access Authenticator Users.

Add Users

Access Authenticator 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).

Adding Users Manually

Access Authenticator 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 Access Authenticator Name. This is the name the user will be instructed to use to, for example, login to the Access Authenticator 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 Access Authenticator.
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 Access Authenticator 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 Access Authenticator's database.

Importing Users

Import users to expedite the process of creating Access Authenticator users using the following procedure:

1. **Import Active Directory users.**
   In order for Access Authenticator to authenticate a user, it must have its own record of the user enrolled in Access Authenticator's database. Access Authenticator can create these users automatically while importing Active Directory users. However, before importing IBM i user profiles, the Access Authenticator users must already exist.

   Import Active Directory users first. This way, your Access Authenticator users can be created quickly for every Active Directory user. Then, you can import IBM i user profiles and use Access Authenticator's *Smart Match* feature to link them to the existing Access Authenticator 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.

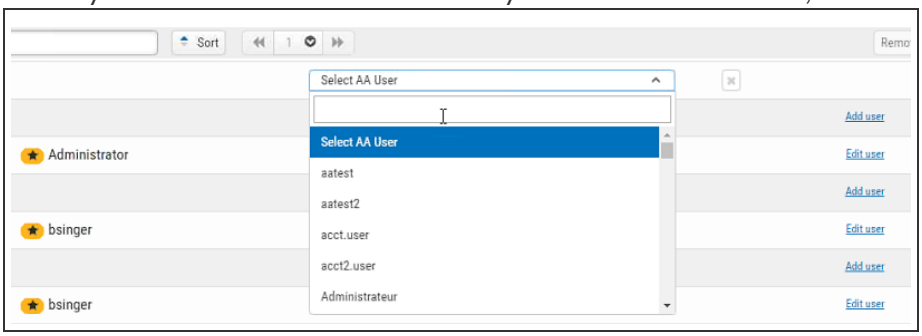
> **NOTE:** To add a group, on the Users screen, click **Add > Add Group**. See Users screen for more details.

e. Click **Start Import**. An Access Authenticator user is created for every Active Directory user.

2. **Import a list of IBM i user profiles and map them to the appropriate Access Authenticator users.**

> **WARNING:** Access Authenticator 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 Access Authenticator to attempt to match profiles with existing Access Authenticator 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 Access Authenticator 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 Access Authenticator user, the Access Authenticator 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 Access Authenticator user for the imported IBM i profile. Click within the text box and type to quickly identify the Access Authenticator 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 Access Authenticator, they need to be informed how to register the device(s) they will be using for authentication. Access Authenticator provides administrators with a pre-configured (and customizable) email that can be used for this purpose. The email includes the Access Authenticator 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 Access Authenticator.
    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 Access Authenticator 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

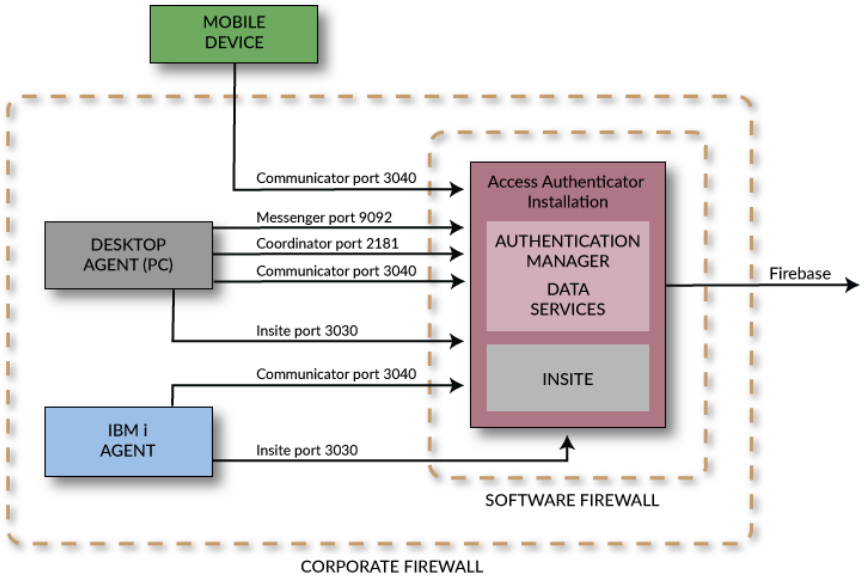
1. On the Navigation Pane, choose **Users** to go to the Users screen.
2. Check the user(s) and/or group(s) you want to email.
3. Click **Send Email**. A confirmation message appears.
4. Click **Send**. An email is sent to the selected recipients.

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

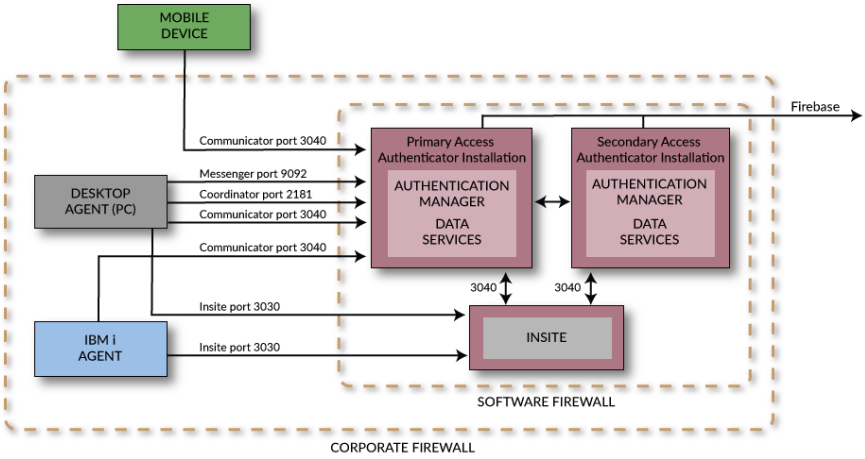
Port/Server Configuration Diagrams

The following diagrams show two possible Access Authenticator system configurations.

Basic Configuration



Basic Configuration with Failover Support



User Setup Procedure

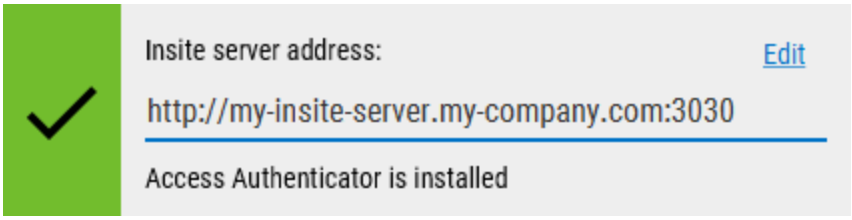
Use the following procedure to install and configure Access Authenticator in preparation for authenticating with your mobile device, YubiKey, or Soft Token.

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

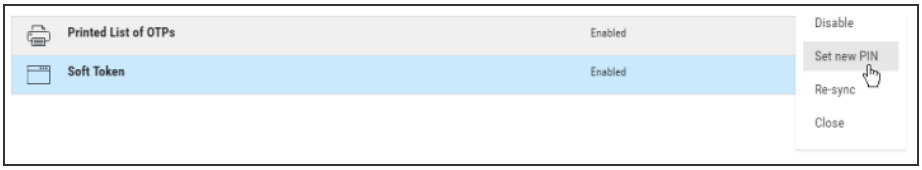
You will receive an email from your administrator when you are ready to begin. This email will include the links you need to get started.

1. Open the email sent by your administrator with the subject "Welcome to Access Authenticator." Read this email.
2. If you will be using a mobile device for authentication, download the HelpSystems Access Authenticator 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 Access Authenticator User Portal** link, complete the sign in form (using the Access Authenticator 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).
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 Access Authenticator 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 Access Authenticator 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.



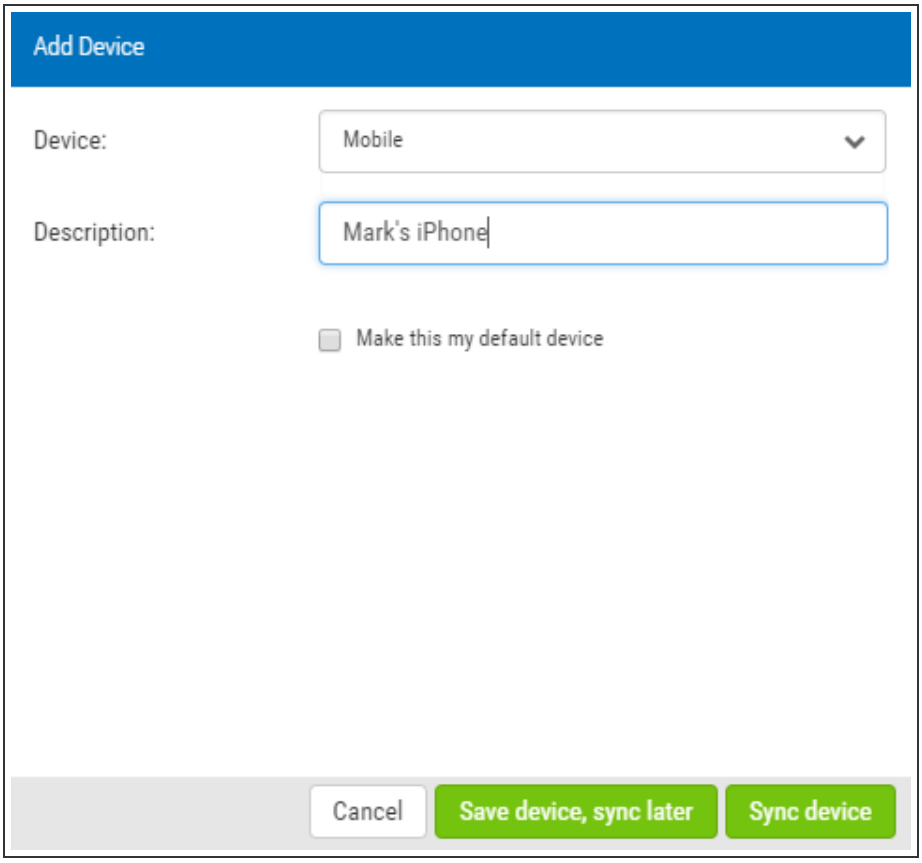
5. In the User Portal, if you will be using the Soft Token for authentication, click the ⋮ on the right side of the Soft Token option and choose **Set New Pin**.



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**.

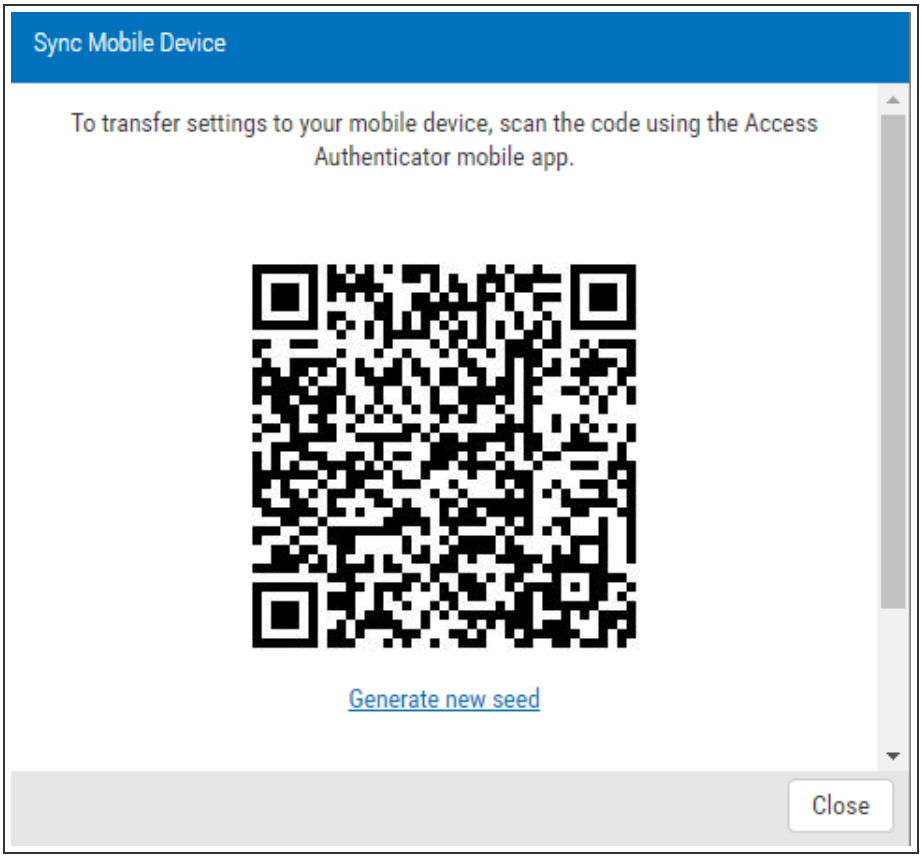


8. Select the type of device from the Device drop-down and add a description.
9. Check 'Make this my default device' if this is the device you will usually use to authenticate.
10. Complete the registration using the following steps:
    - To add a YubiKey, insert the YubiKey and press the button (a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

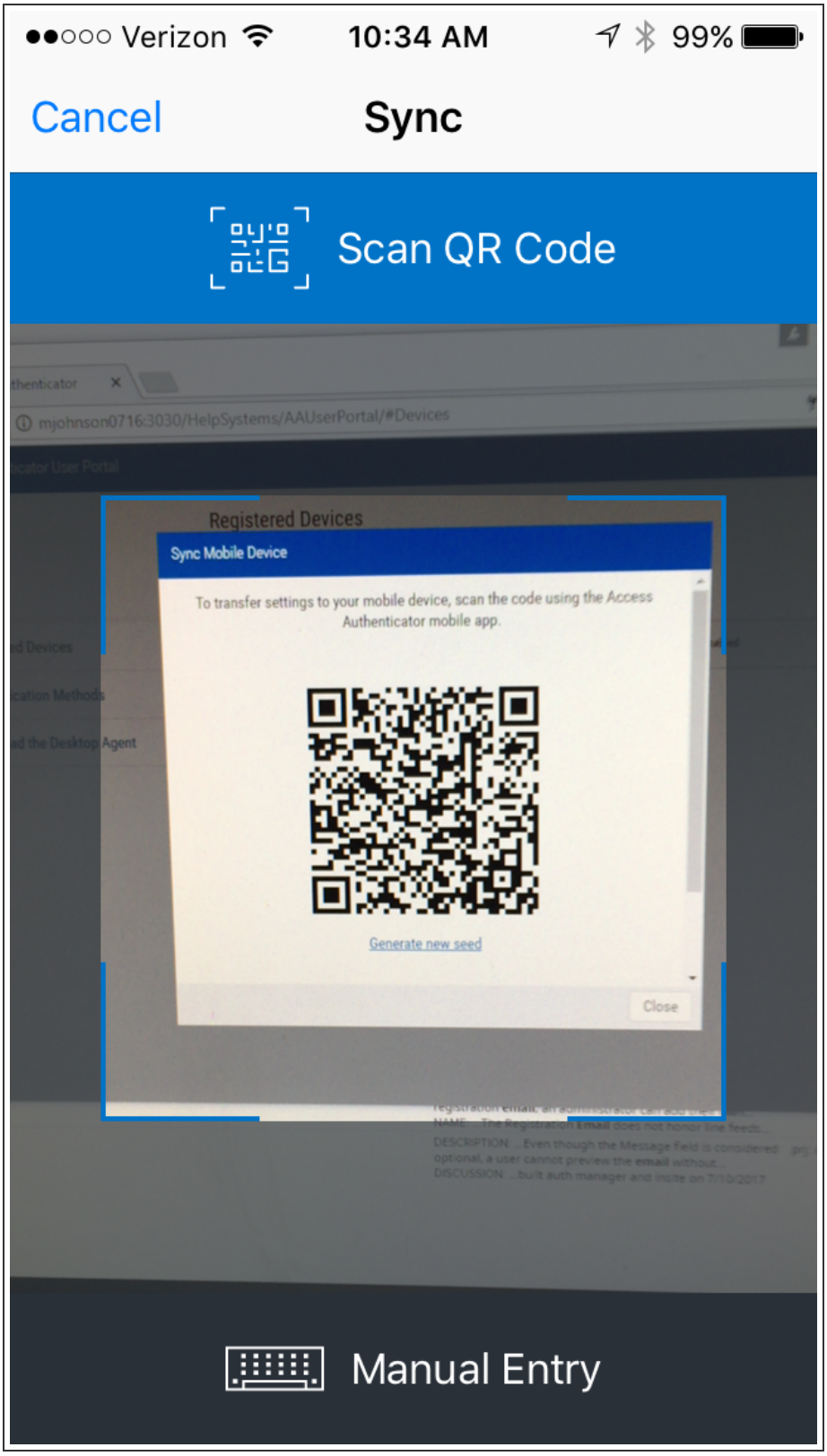
    - To add a mobile device:
        a. Click **Sync device**. The Sync Mobile Device screen appears.

           > **NOTE:** You can choose **Save device, sync later** to keep a record of the device in the User Portal, buy synchronize it with Access Authenticator later.



b. On your mobile device, open the Access Authenticator 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).


Verizon
10:34 AM
99%
Cancel
Sync
Scan QR Code
mjohnson0716:3030/HelpSystems/AAUserPortal/#Devices
Registered Devices
Sync Mobile Device
To transfer settings to your mobile device, scan the code using the Access Authenticator mobile app.
Generate new seed
Close
Manual Entry

> **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.

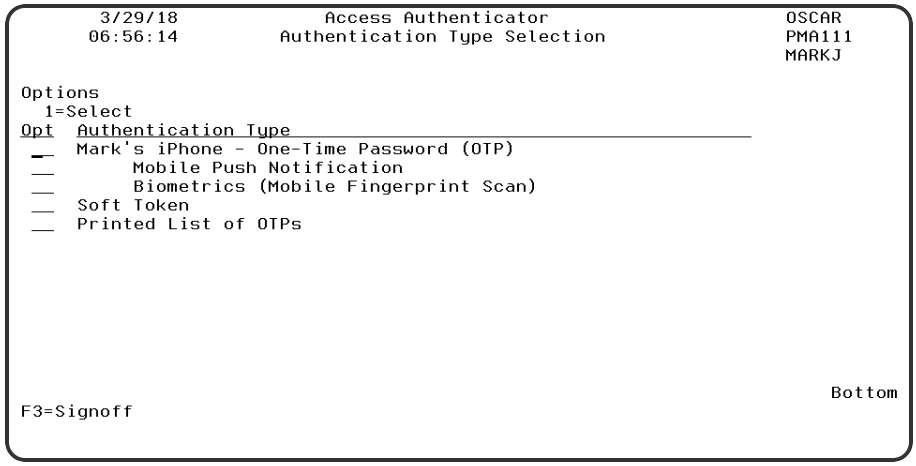
11. An email with the subject "Access Authenticator - New Device Registration" appears in your inbox, which includes the type and description of the registered device. You are now ready to authenticate.

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 Access Authenticator. 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.

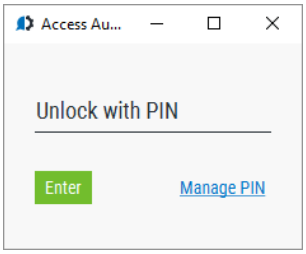
2. Enter **1** next to the authentication method you would like to use, and do the following to authenticate:
   - For **One-Time Password (OTP)**, open the mobile app and enter the six-digit number from your mobile device into the IBM i prompt, then press Enter.
   - For **Mobile Push Notification**,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

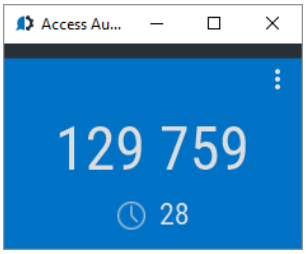
a. On your PC, click the HelpSystems icon in the Windows System Tray and choose **Soft Token**.

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.



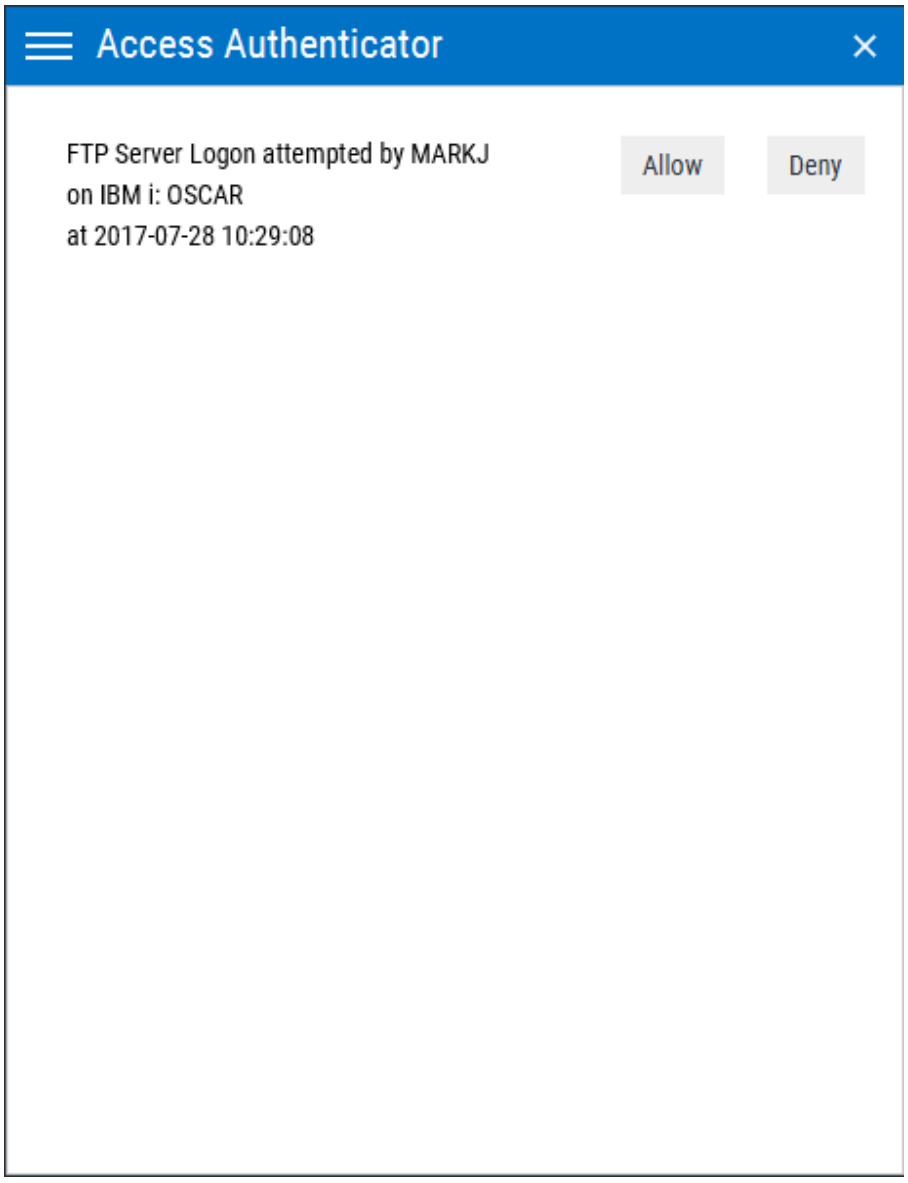
c. Enter the six-digit number displayed on the Soft Token panel into the IBM i prompt, then press Enter.

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

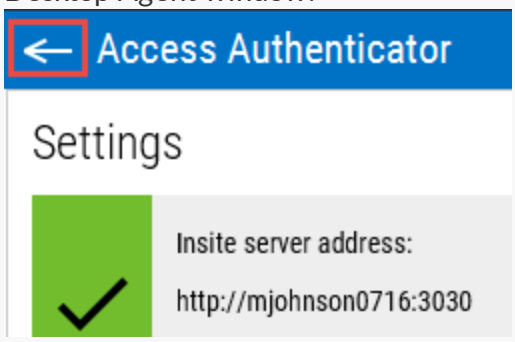
Authenticating an FTP IBM i Sign On

If you are signing on using an Exit Point, like FTP, the Access Authenticator Desktop Agent must be installed and running (See User Setup).

1. Connect to the IBM i via FTP and sign on.
2. The Access Authenticator 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 Access Authenticator mobile app. Enter the six-digit number from your mobile device into the Desktop Agent, then press Enter or click **Submit**.
   - Click **Push Notification**, the open the notification using the Access Authenticator mobile app and tap **Accept**.
   - Click **Mobile Biometrics**, then open the notification using the Access Authenticator 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**).

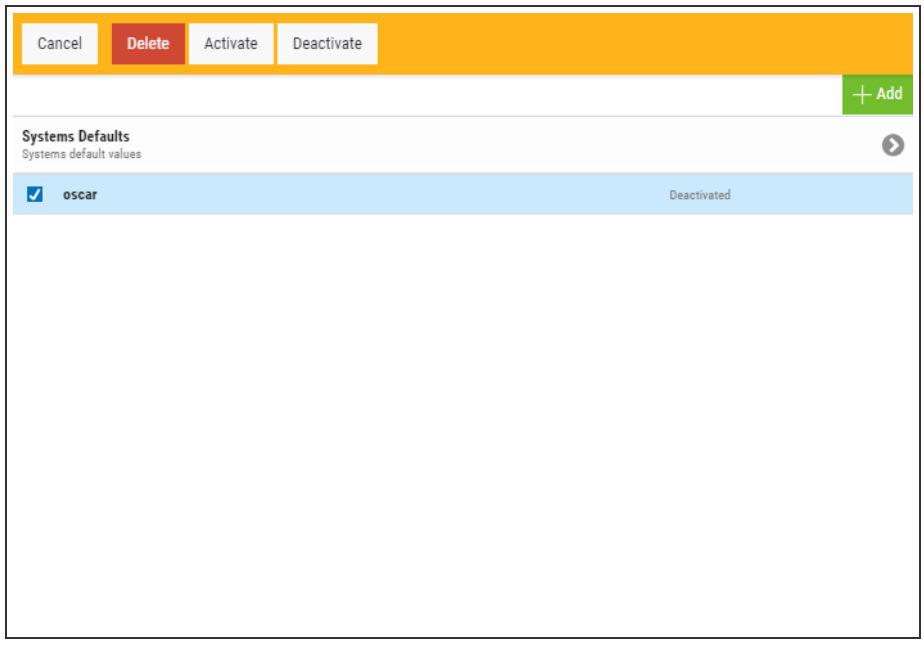
   > **NOTE:** See Troubleshooting Authentication with your Mobile Device if you have difficulties authenticating with your mobile device.

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

Reference

The topics in this section include descriptions of Access Authenticator's options and controls.

Agents screen



How to Get There

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

What it Does

Use these settings to add, remove, enable, disable Access Authenticator agents.

Options

Add

Click **Add** to open the New Systems page where you can define a new agent.

Systems Defaults

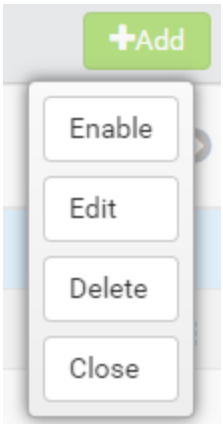
Select this option to open the Edit Default System page where you can change the default system values.

[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 Access Authenticator.
- **Enable Selected.** Click **Enable Selected** to begin authentication for the selected systems.
- **Disable Selected.**Click **Disable Selected** to end authentication for the selected systems.

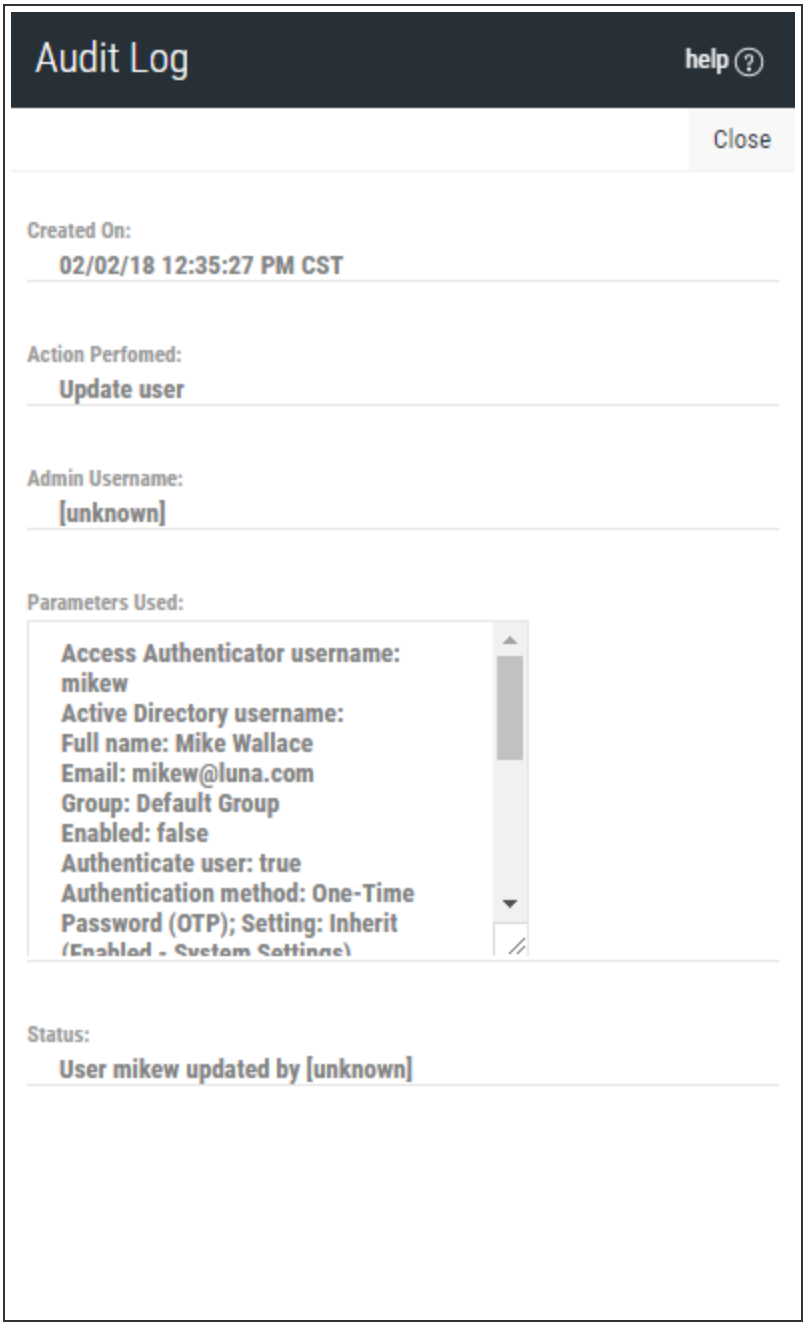
Click the icon to display the following context menu.



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 Access Authenticator.
- **Close.** Click **Close** to dismiss the context menu.

Audit Log screen



How to Get There

On the Reports screen, click an Audit Log report.

What it Does

Displays the following information:

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

Authentication Log screen

How to Get There

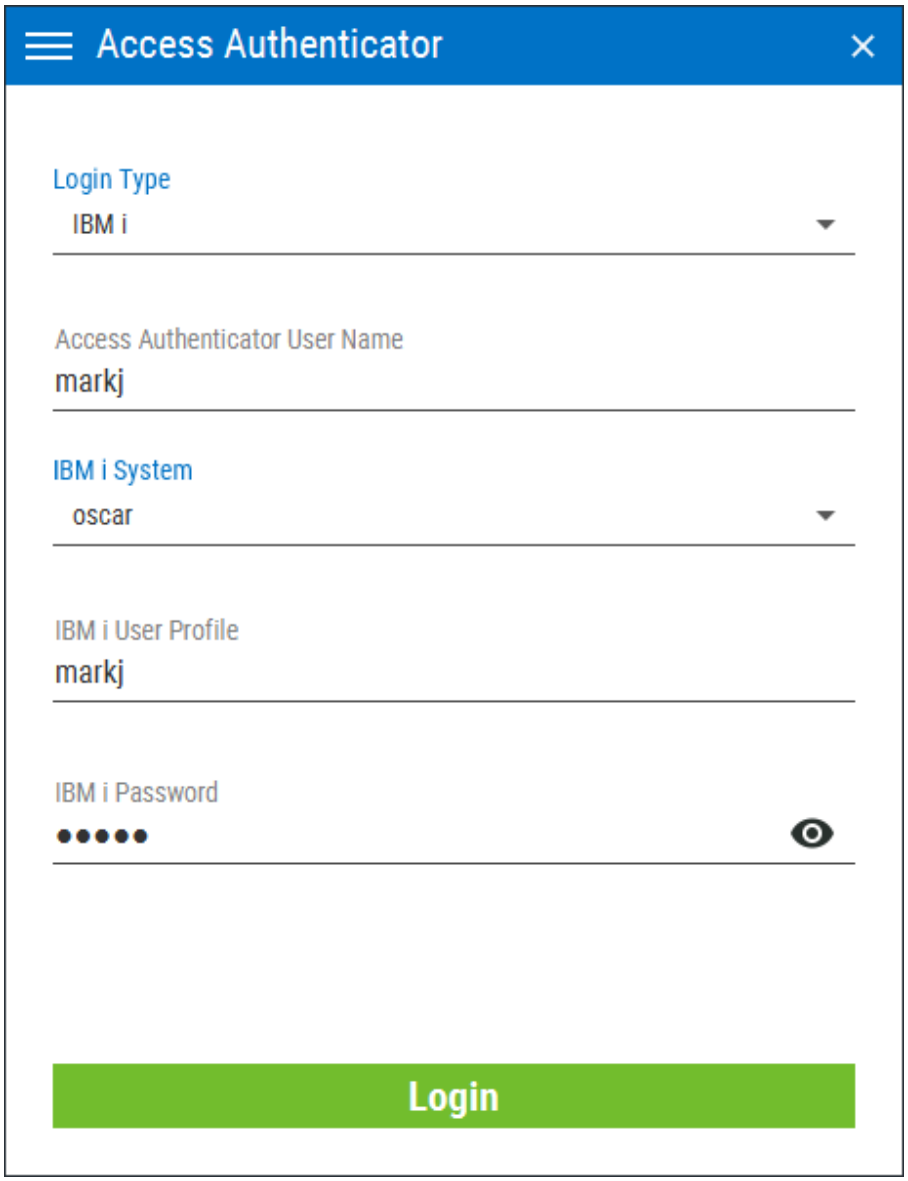
On the Reports screen, click an Authentication Log report.

What it Does

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 Access Authenticator and/or additional information pertaining to the logged activity.

Access Authenticator Desktop Agent



How to get there

The desktop agent appears when prompted by an Access Authenticator exit point authentication request.

What it does

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 Access Authenticator 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 Access Authenticator for validation.

See also User Authentication.

Login Options

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

Access Authenticator Username
This is your Access Authenticator 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.

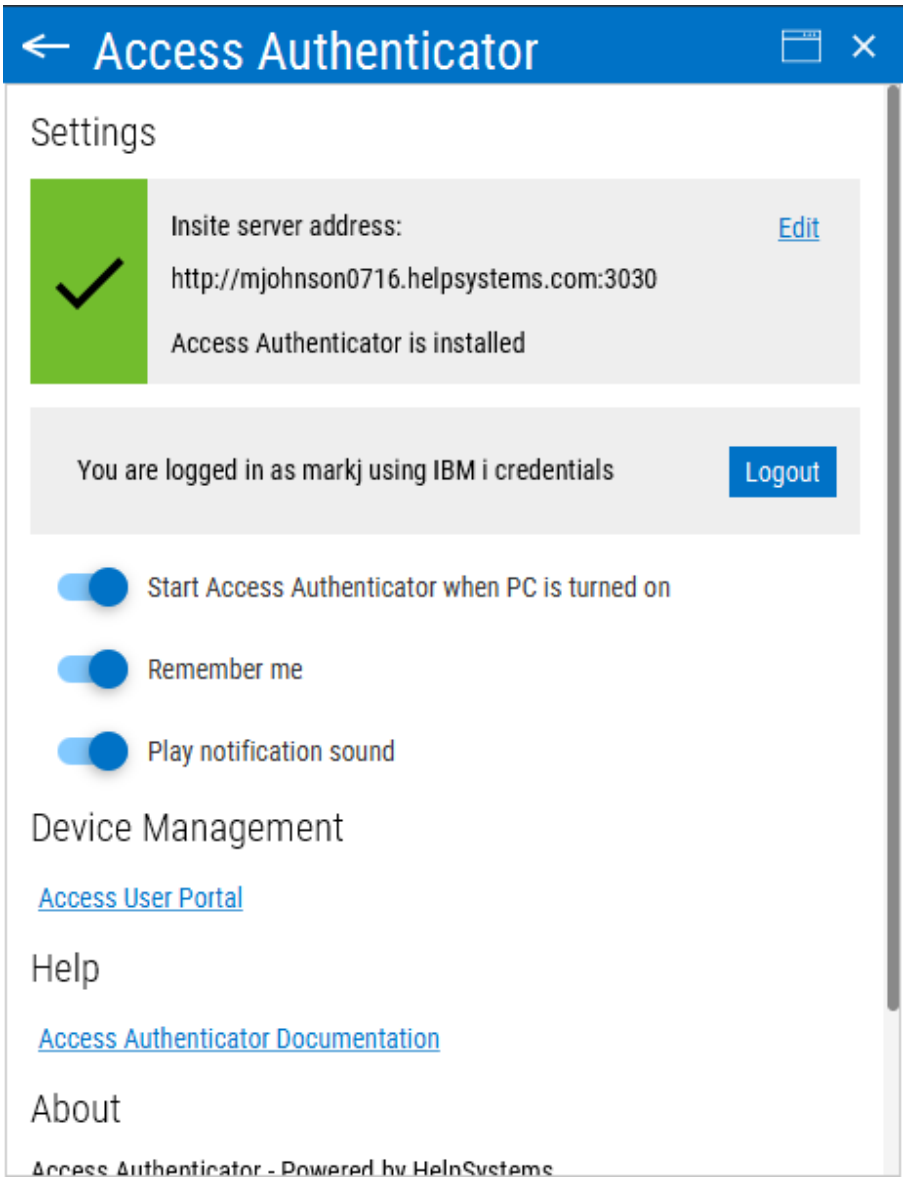
IBM i User Profile
This is the IBM i user profile used for authentication.

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 Access Authenticator Desktop Agent.

Settings

This screen displays your current configuration and allows you to configure your Access Authenticator 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.



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

Start Access Authenticator when PC is turned on

Move this slider to the right to indicate that you want the Access Authenticator Desktop Agent to start when your computer is started.

Remember me

Move this slider to the right to indicate you want Access Authenticator to remember your login information.

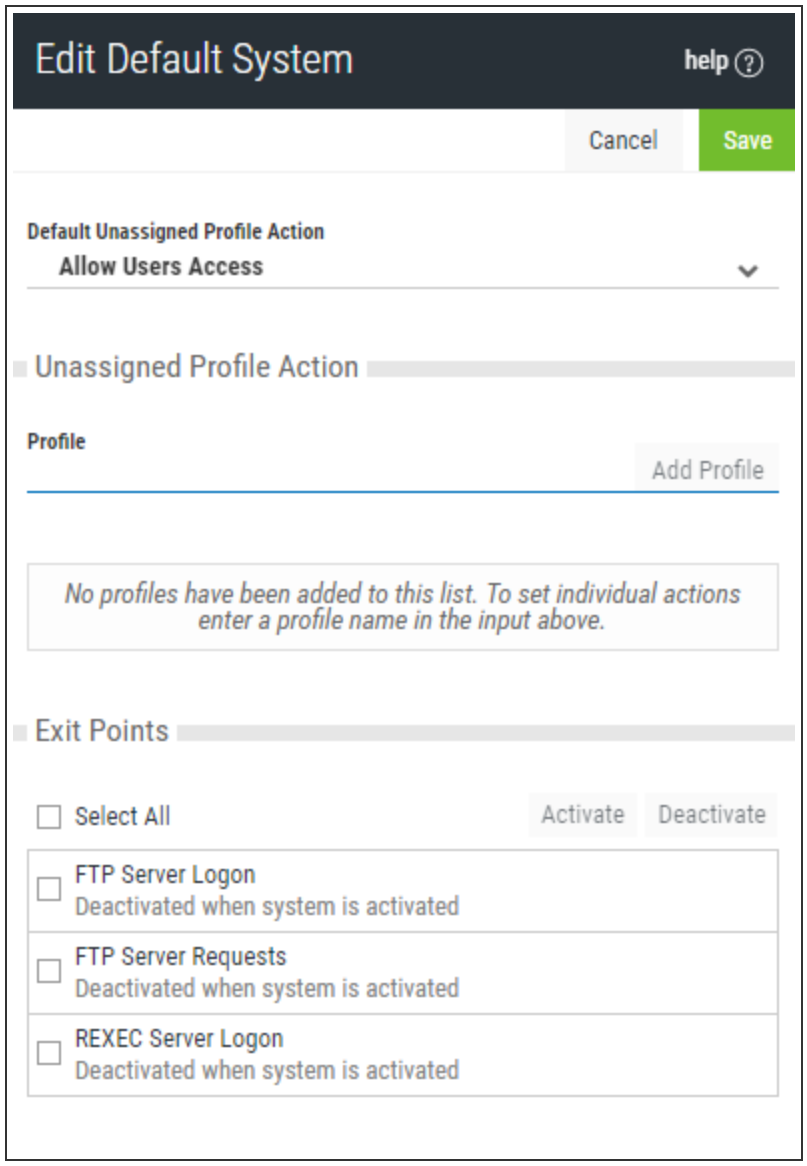
Play notification sound

Move this slider to the right to indicate you want Access Authenticator to chime when prompted by an authentication request.

Device Management

Click Access User Portal to open the Access Authenticator User Portal, where you can manage the devices you are using as factors of authentication.

Edit Default System



How to Get There

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

What it Does

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

Upon signing on to a system secured by Access Authenticator with a user profile not attached to an Access Authenticator user, Access Authenticator 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, Access Authenticator 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.

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 Access Authenticator. Choose 'Allow users access' to grant access to user profiles unfamiliar to Access Authenticator. 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 Access Authenticator can't find an Access Authenticator user attached to that profile to challenge for authentication, Access Authenticator 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.

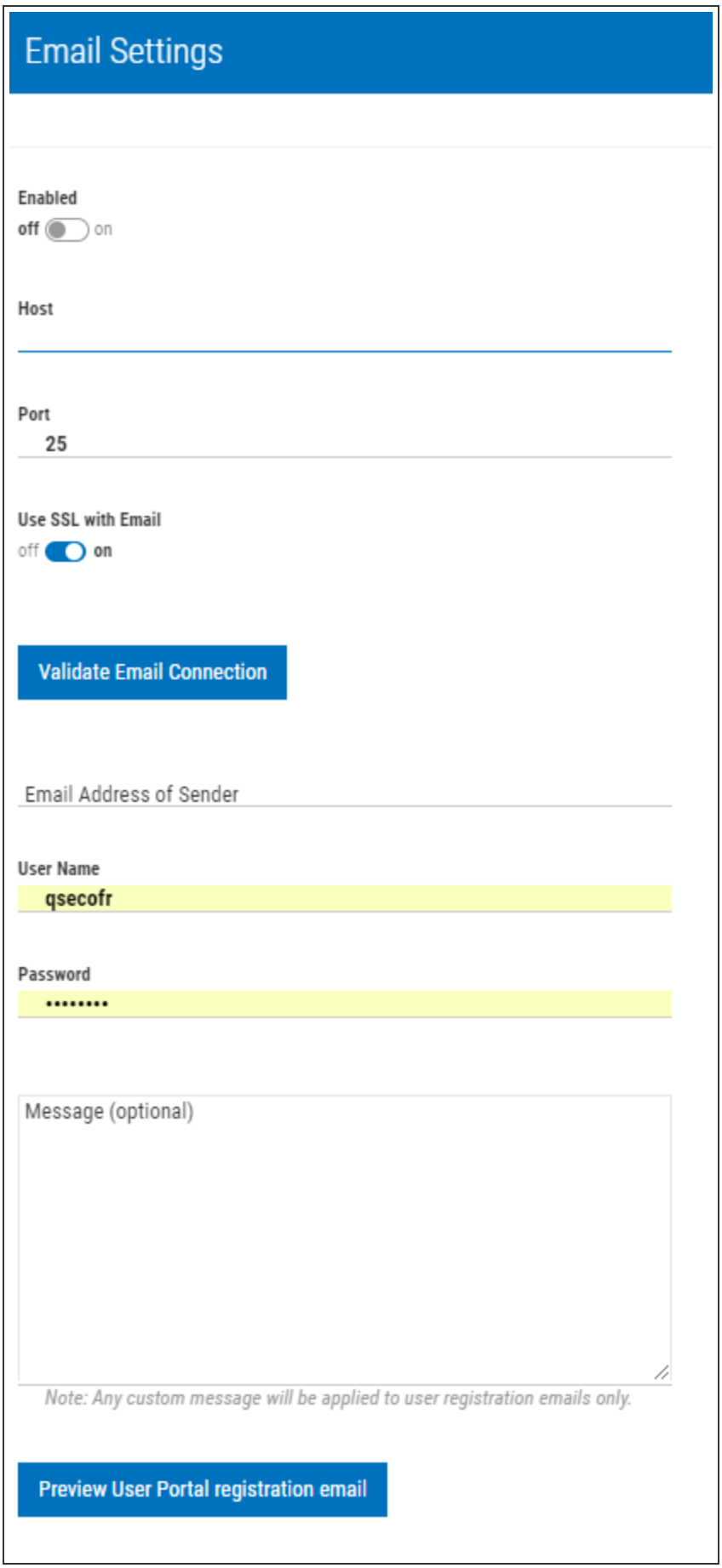
[profile list]; Deny • Allow

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.

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 Access Authenticator. Access Authenticator supports the TCP Signon Server, REXEC Server Logon, FTP Server Logon, and FTP Server Requests exit points. Click **Activate** to secure them with Access Authenticator. Click **Deactivate** to stop securing them with Access Authenticator.

Email Settings


Email Settings
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

How to Get There

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

What it Does

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 Access Authenticator to send email messages to administrators and users, and settings must be enabled if you wish to allow Access Authenticator 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.

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.

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).

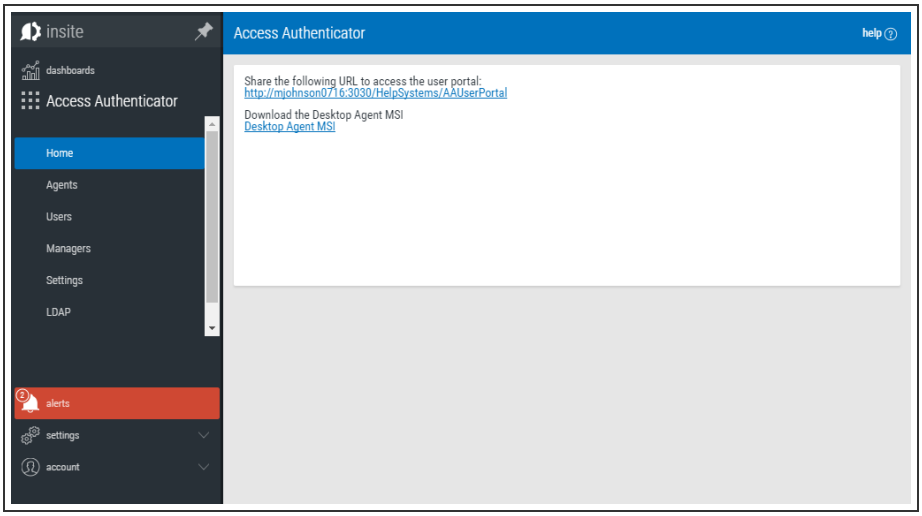
Password

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.

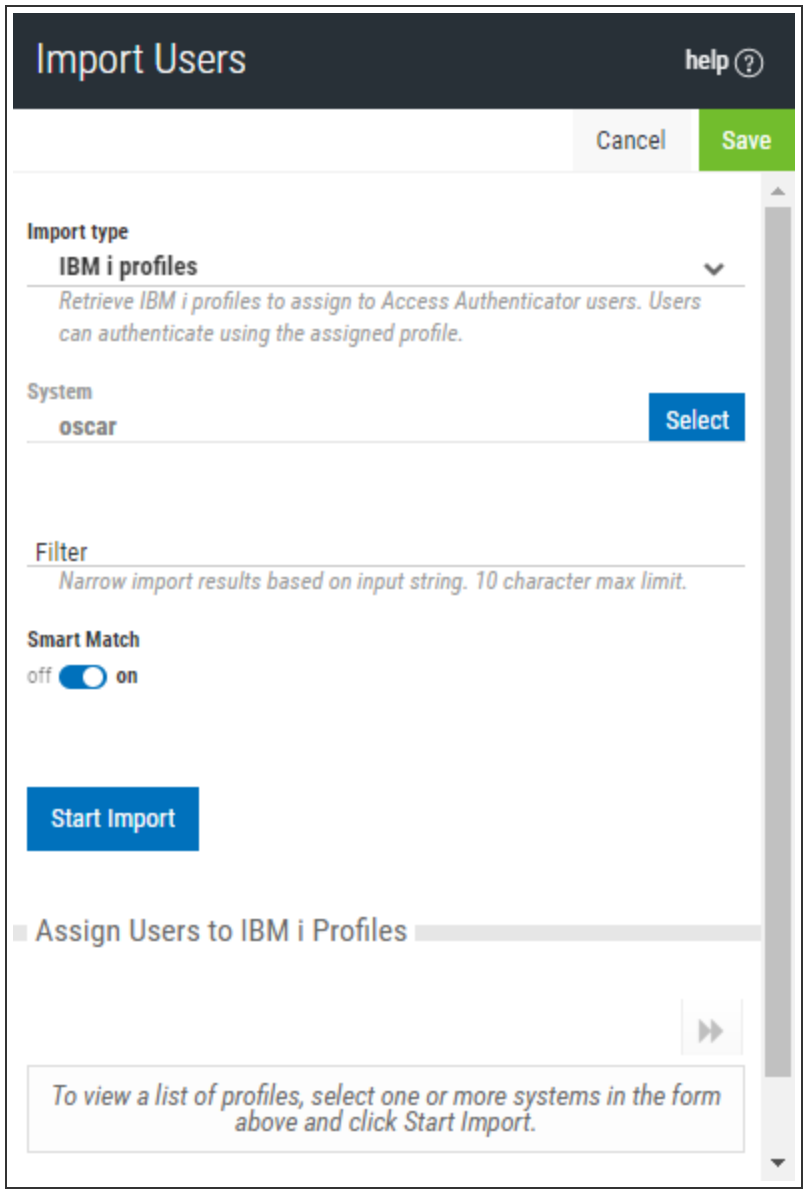
Preview User Portal registration email
Click this button to display a preview of the email that will be sent to users.

Access Authenticator Home



Share the URL on this screen with users in order for them to access the Access Authenticator User Portal.

Import Users



How to Get There

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

What it Does

Use this screen to import users from an Active Directory or IBM i user database. See also Importing 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

Choose whether you would like to import records from Active Directory or user profiles from one or more IBM i systems.

[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]

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 Access Authenticator 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 Access Authenticator user "Shirley Matchwell," Access Authenticator will match IBM i profiles that contain the following in either the user profile Name or Text description fields: "shirley matchwell," "shirleymatchwell," and "smatchwell."

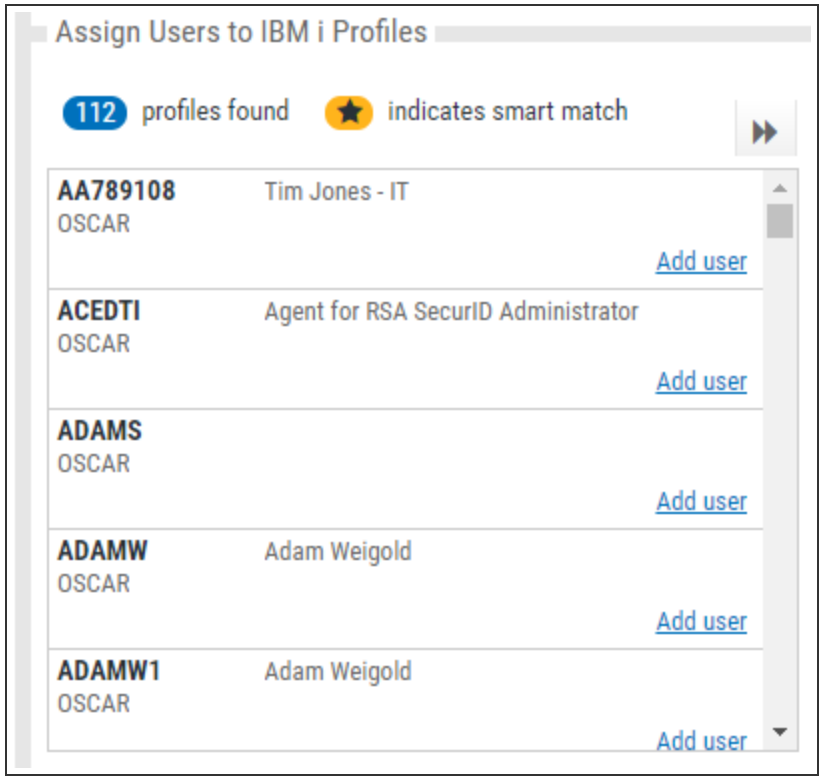
> **NOTE:** Smart Match disregards case during its comparison.

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

Start Import

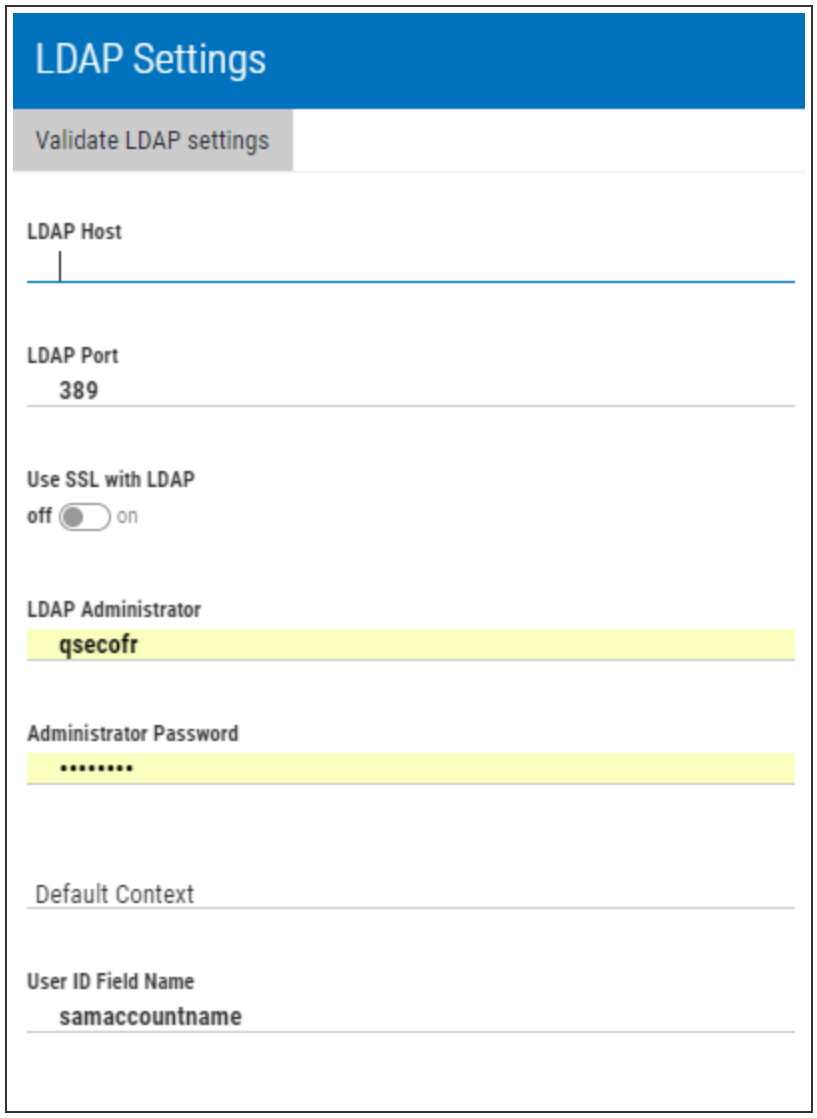
Click this button to begin the import process.

Assign Users to IBM i Profiles



Use this screen to link the imported IBM i users with existing Access Authenticator users, or add them as new Access Authenticator uses.

LDAP Settings screen



How to Get There

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

What it Does

Use these settings to configure Lightweight Directory Access Protocol (LDAP) settings in order to prepare Access Authenticator for profile import from Active Directory.

> **NOTE:** These settings are specific to the Access Authenticator module, and do not pertain to the Insite authentication settings configured on Insite's Authentication page.

Options

Validate LDAP Settings
Click this button to validate that Access Authenticator can communicate with the LDAP server without errors before saving your LDAP settings.

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.

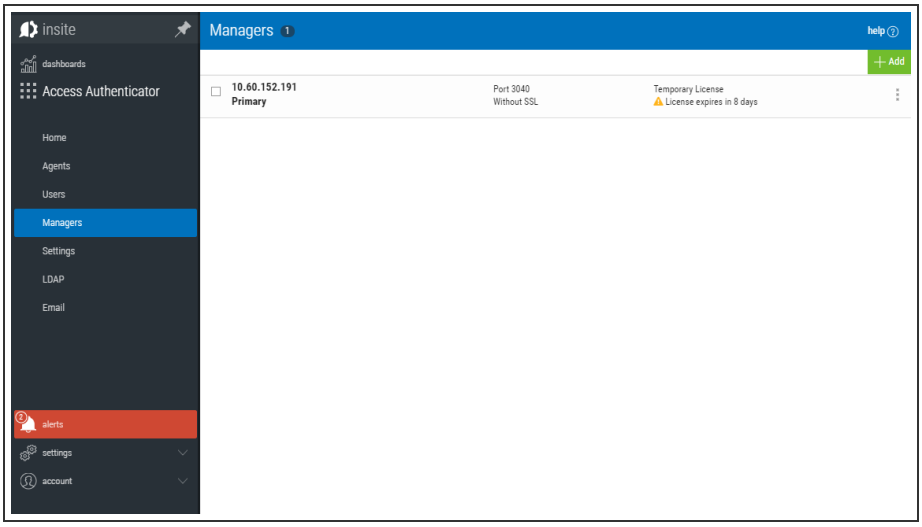
LDAP Administrator
Enter the username of the LDAP administrator.

Administrator Password
Enter the LDAP administrator's password.

Default Context
This is the command used by Access Authenticator to query LDAP directory records during import.

User ID Field Name
Enter the LDAP field used for the User ID.

Managers



How to Get There

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

What it Does

This screen lists the Authentication Managers that have been added to Access Authenticator. 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 Access Authenticator'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 Access Authenticator, an Authentication Manager is chosen at random to process the authentication request.

Options

Add

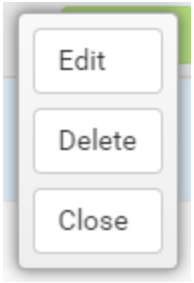
Click **Add** to open the New Manager page where you can define a new Authentication Manager.

[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 Access Authenticator.

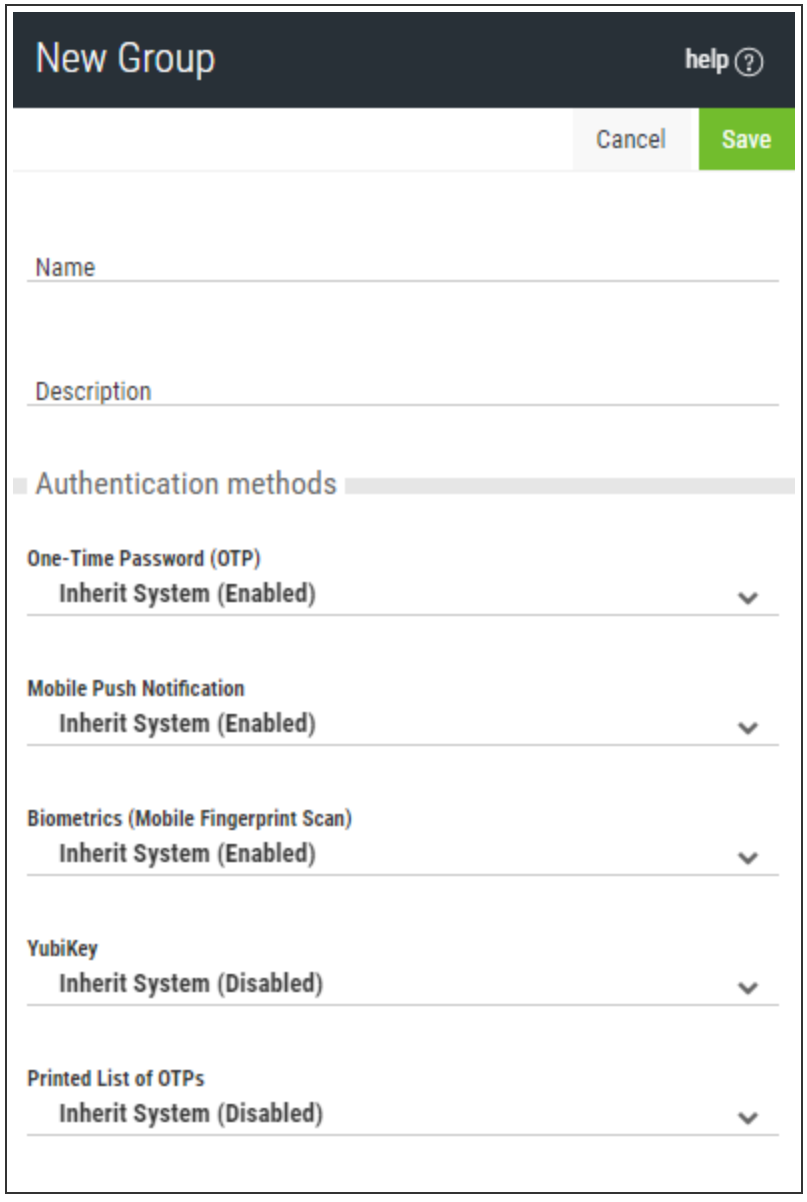
Click the icon to display the following context menu.



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 Access Authenticator.
- **Close.** Click **Close** to dismiss the context menu.

New/Edit Group



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**.

What it Does

These settings allow Access Authenticator 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.

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.

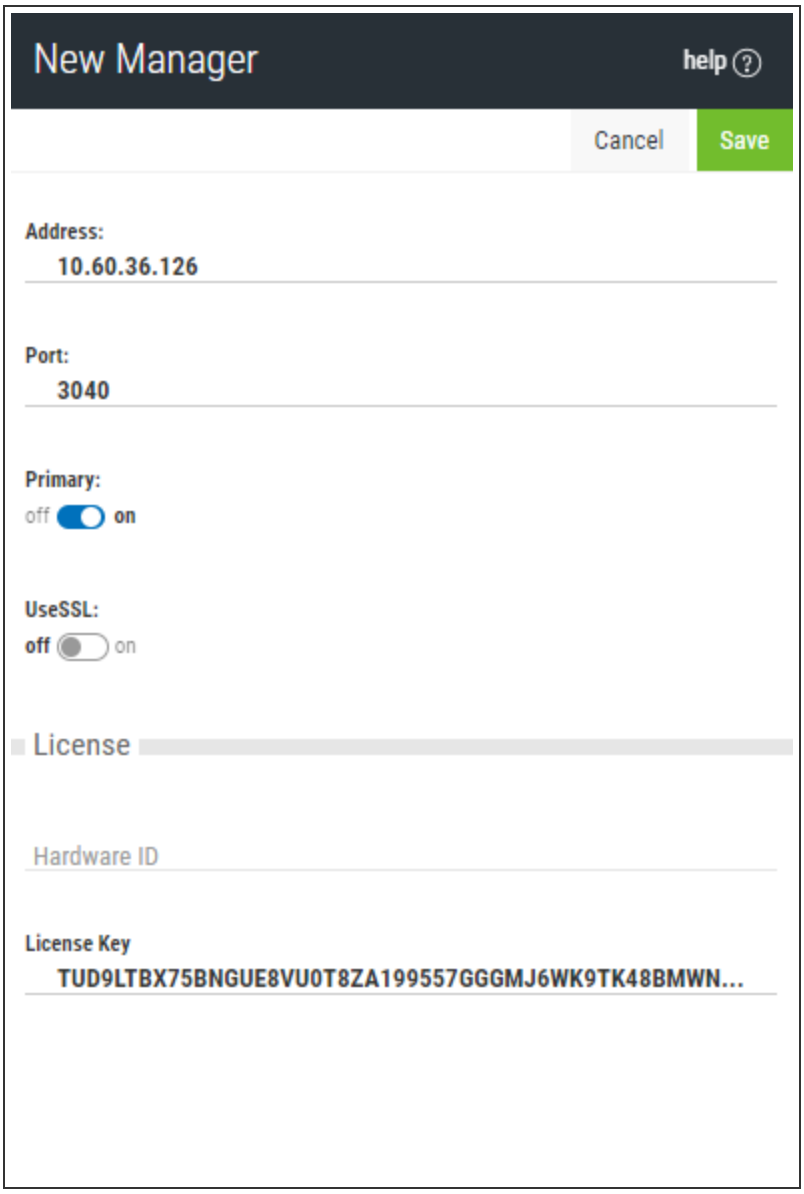
Users

This is a list of users in the Group.

Delete • Cancel • Save

Choose Delete to remove the Group from Access Authenticator. 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



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**.

What it Does

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

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.

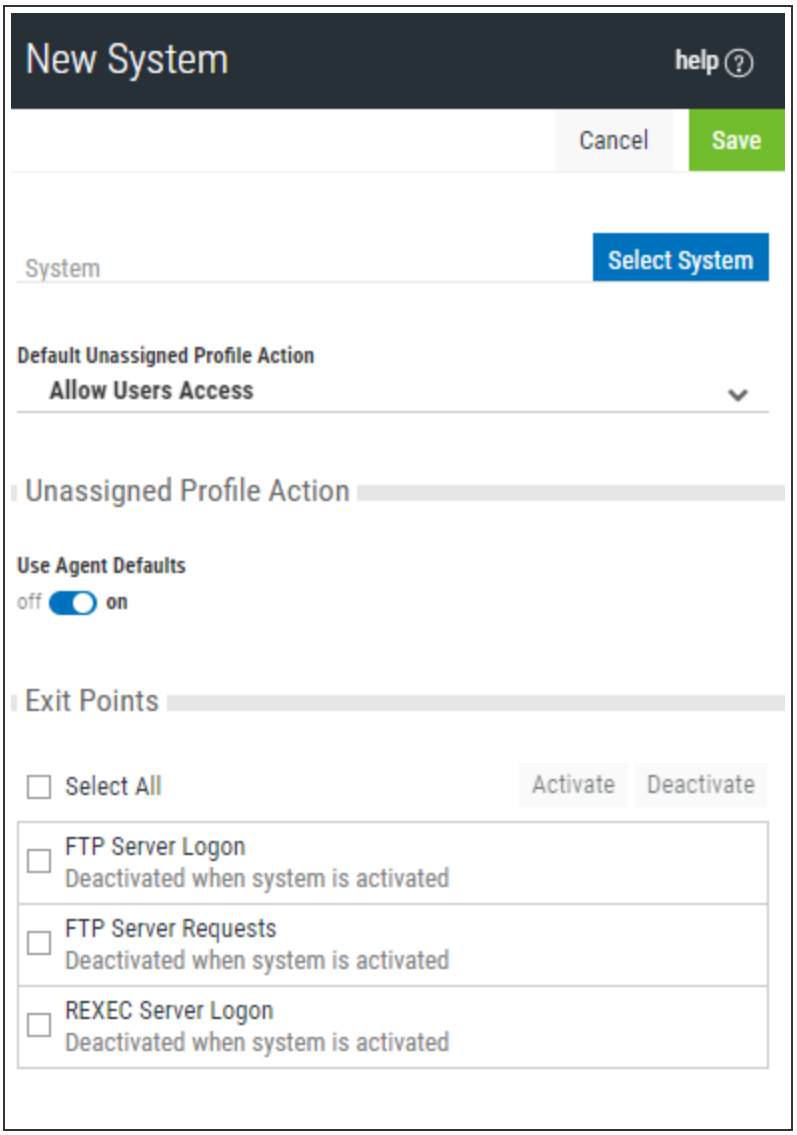
License

Hardware ID
This is the manager's unique ID.

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



How to Get There

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

What it Does

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 Access Authenticator installed.

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

Upon signing on to a system secured by Access Authenticator with a user profile not attached to an Access Authenticator user, Access Authenticator 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, Access Authenticator defers to the settings on the Edit Default System screen.

In other words, here, Access Authenticator 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.

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 Access Authenticator user. Choose **Allow users access** to grant access to user profiles not connected to an Access Authenticator 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

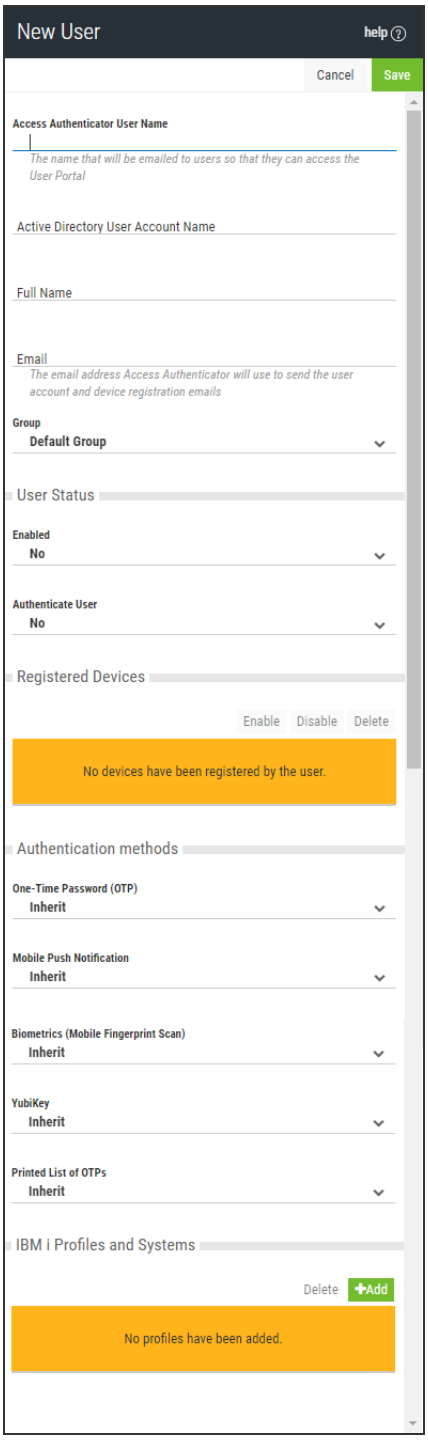
Use Agent Defaults; On • Off

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.

Exit Points; Activate • Deactivate

Check the exit points you would like to activate or deactivate. Click **Activate** to secure them with Access Authenticator. Click **Deactivate** to stop securing them with Access Authenticator. For example, if the system is enabled, and you set an exit point to **Deactivate** and click **Save**, Access Authenticator sends a message to deregister the exit point program with Access Authenticator. If the system is not currently enabled in Access Authenticator, and this setting is changed, the setting is stored in the database so that when the system is enabled within Access Authenticator, Access Authenticator will apply the activate/deactivate setting as appropriate, and register/deregister the exit point program accordingly.

New/Edit 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**.

What it Does

This screen allows Access Authenticator 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

Options

Delete

Click this button to delete the user in Access Authenticator.

Send Email

Click this button to send the user an email. See Email Settings for details.

> **NOTE:** You can also send an email to several users at once, or groups of users, from the Users screen.

Access Authenticator 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.

Full Name

The full name of the user, used only to identify the user in Access Authenticator.

Email

The email address Access Authenticator 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 Access Authenticator. 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.

Promoting a Secondary Authentication Manager to Primary

If the Primary Authentication Manager is down due to a system failure, you can use the steps in this section to resume authentication services by promoting a Secondary Authentication Manager to Primary. These steps can also be used if a Primary system needs to be taken offline for some reason, such as for maintenance.

> **NOTE:** These steps require that you have installed the Access Authenticator Authentication Manager and Data Services on both a Primary and Secondary system, and initiated replication of the Primary on the Secondary (see Installing the Authentication Manager and Data Services).

Promoting a Manager to Primary on Windows

1. If the Primary system has crashed, and the purposes of promotion are for recovery, skip to step 2. If the Primary database needs to be taken offline, on the system running the Primary database, stop the service HSAccessAuthenticatorDB.
2. Login to the system running a/the Secondary Authentication Manager. (You will need to know its IP address.)
3. Run the following command in `C:\Program Files\Help Systems\Access Authenticator`:

   ```
   standby2master
   ```

   This command sets postgres to stop replicating data and become the Primary Manager.
4. Run the following command in `C:\Program Files\Help Systems\Access Authenticator\consul`:

   ```
   set_ds_primary -ip current ip -port discovery port
   ```

   NOTE: The default discovery port is 8500.

   This command sets some internal variables that tells Access Authenticator where the new postgres master (Primary) is located.
5. Start the service 'HSAccessAuthenticatorDB' on the new Primary system.
6. If one or more additional Secondary installations are available, they need to be instructed to begin replicating from the new Primary system. Login to those systems and run the following command (in `C:\Program Files\Help Systems\Access Authenticator`):

   ```
   switchmaster new Primary system ip
   ```

   If no additional Secondary system is available, you can install the Authentication Manager and Data Services (as described in Installing the Authentication Manager and Data Services) on one or more Secondary systems, and run **master2standby**, to restore failover/recovery capability. Next, the new Primary system needs to be identified in Insite.
7. Open Insite and select **Access Authenticator** from the Navigation Pane, then choose **Managers**.
8. Click the system that was just promoted to Primary (it will still be listed as a Backup). The Edit Managers screen appears.
9. Set Primary to **On**.
10. Click **Save**.

Promoting a Manager to Primary on Linux

1. If the Primary system has crashed, and the purposes of promotion are for recovery, skip to step 2. If the Primary database needs to be taken offline, on the system running the Primary database, stop the service 'HelpSystemsAccessAuthenticatorDatabase'.
2. Login to the system running a/the Secondary Authentication Manager. (You will need to know its IP address.)
3. Run the following command in `opt\helpsystems\AccessAuthenticator`:

   ```
   standby2master
   ```

This command sets postgres to stop replicating data and become the Primary Manager.

4. Run the following command in `opt\helpsystems\AccessAuthenticator\consul`:

   ```
   set_ds_primary -ip current ip -port discovery port
   ```

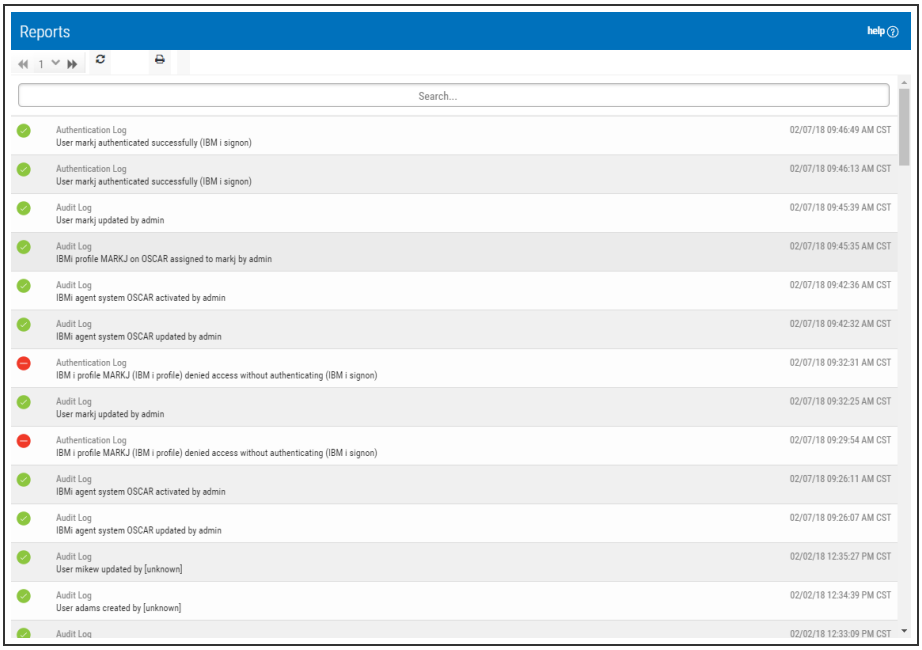
   NOTE: The default discovery port is 8500.

   This command sets some internal variables that tells Access Authenticator where the new postgres master (Primary) is located.
5. Start the service 'HelpSystemsAccessAuthenticatorDatabase' on the new Primary system.
6. Start the service 'HelpSystemsAccessAuthenticatorManager' on the new Primary system.
7. If one or more additional Secondary installations are available, they need to be instructed to begin replicating from the new Primary system. Login to those systems and run the following command (in `opt\helpsystems\AccessAuthenticator`):

   ```
   switchmaster new Primary system ip
   ```

   If no additional Secondary system is available, you can install the Authentication Manager and Data Services (as described in Installing the Authentication Manager and Data Services) on one or more Secondary systems, and run **master2standby**, to restore failover/recovery capability. Next, the new Primary system needs to be identified in Insite.
8. Open Insite and select **Access Authenticator** from the Navigation Pane, then choose **Managers**.
9. Click the system that was just promoted to Primary (it will still be listed as a Backup). The Edit Managers screen appears.
10. Set Primary to **On**.
11. Click **Save**.

Reports screen



How to Get There

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

What it Does

Use report to view Access Authenticator system activities, including authentication data, system event information, and an audit log of Access Authenticator configuration information.

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, or System Event Logs.

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

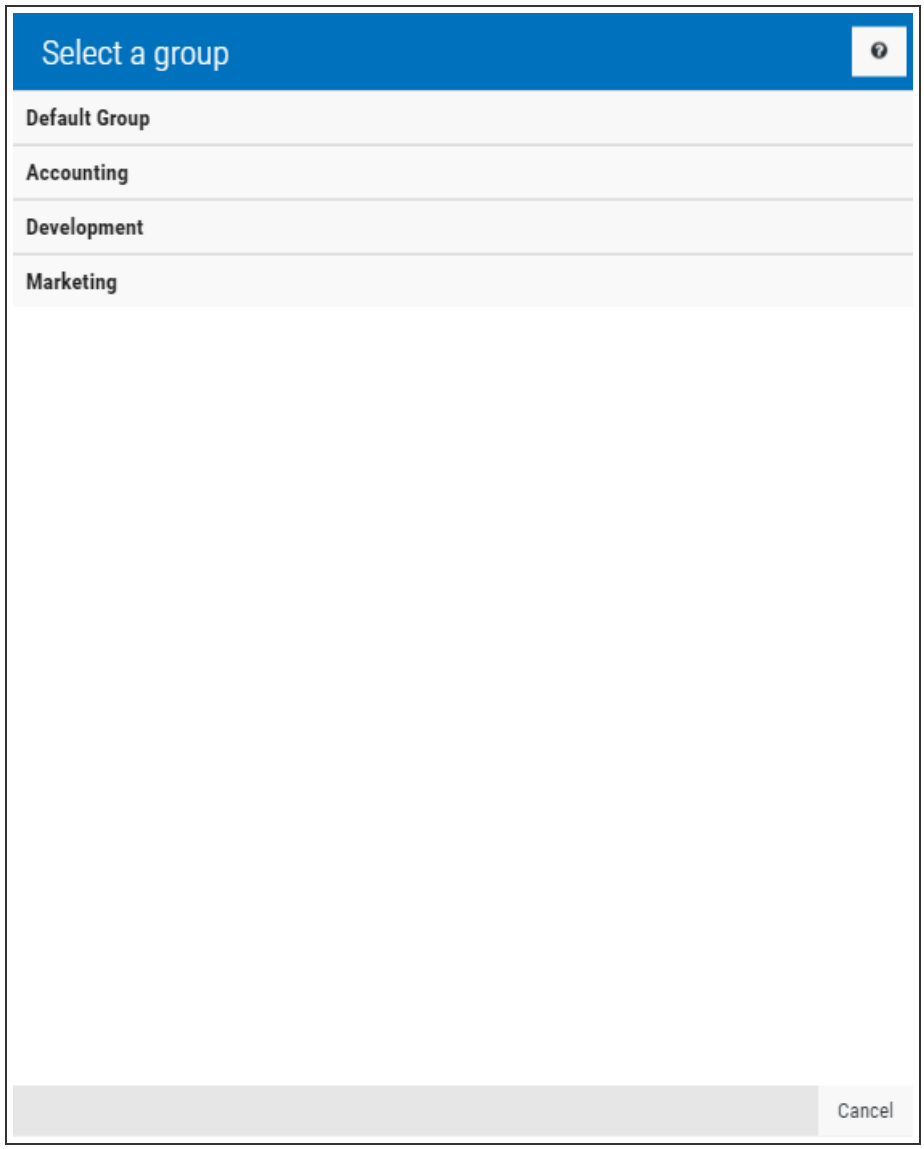
[Search field]

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

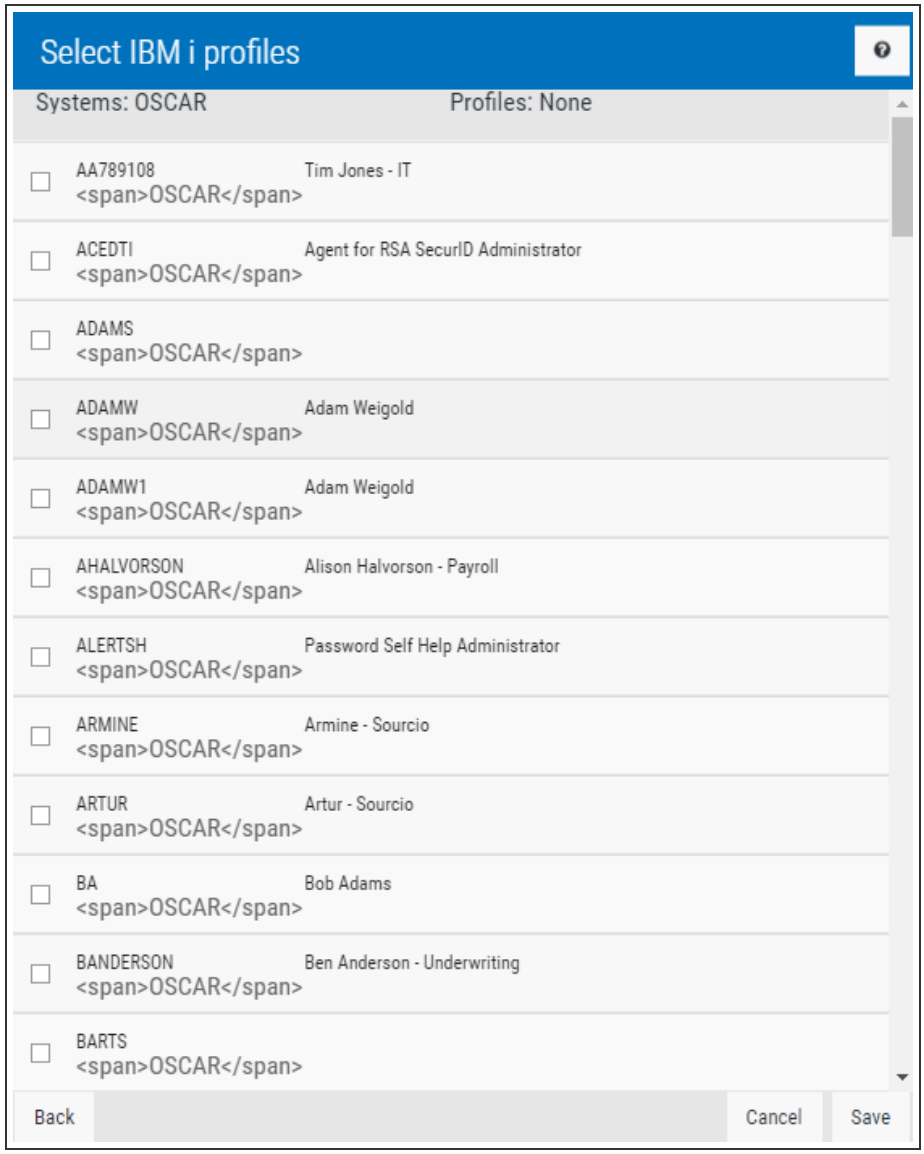
[Group selection]

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.

What it Does

This screen displays the profiles on the chosen IBM i system, and allows you to make your selection.

Options

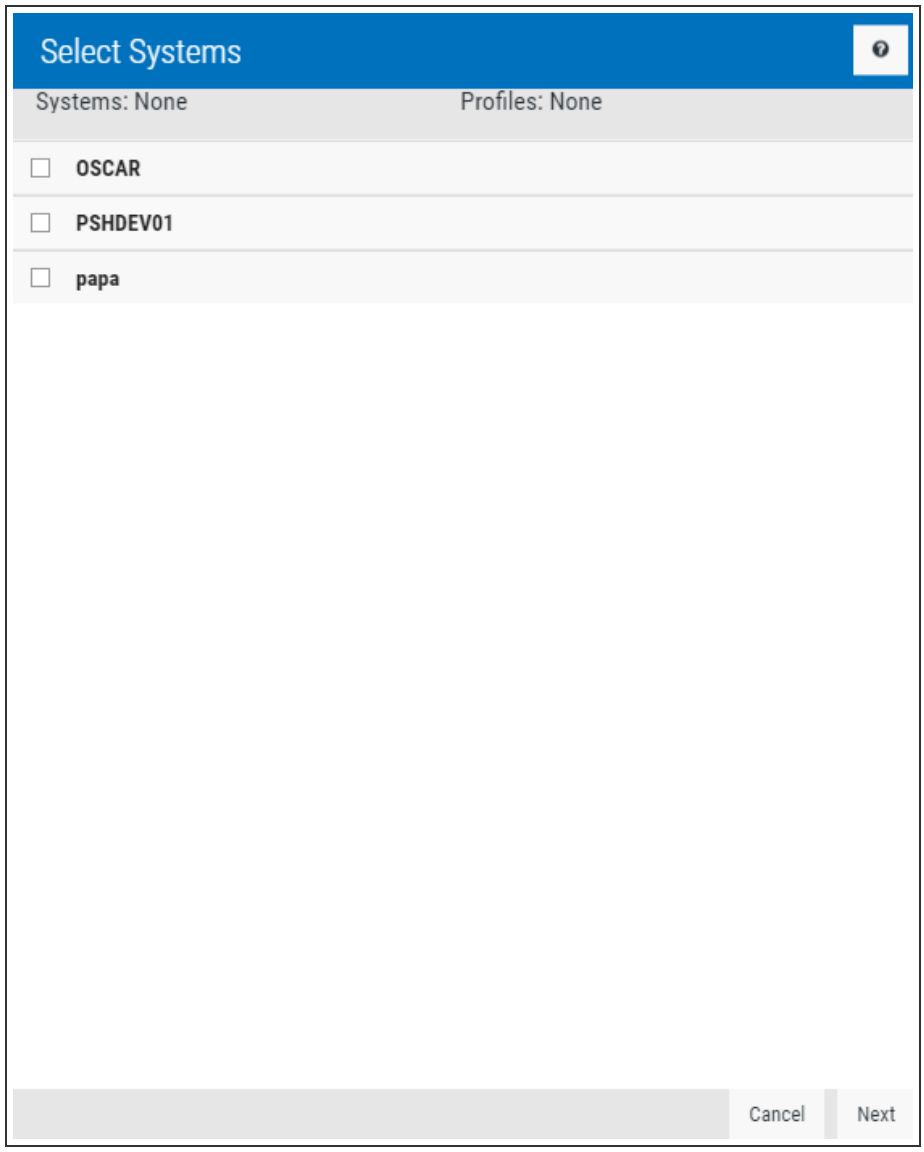
[Search box]

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

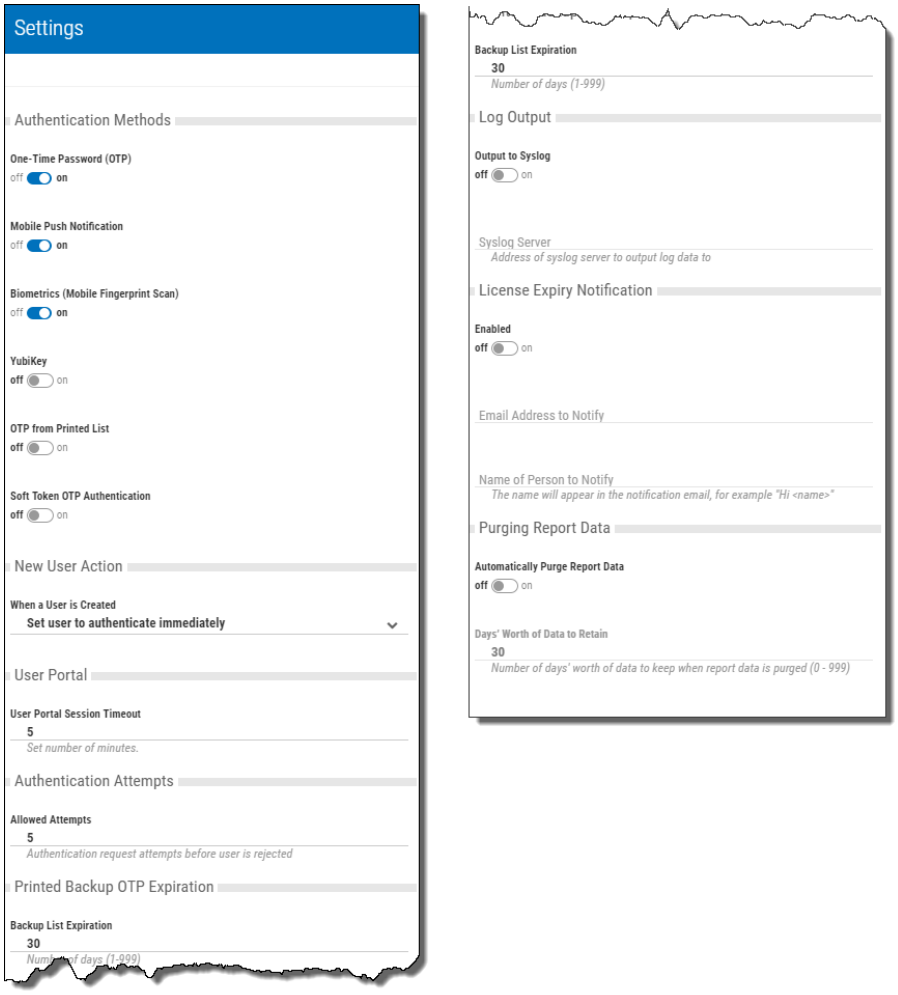
[Search box]

Enter a value in the search field to quickly identify systems that have been added. The list is filtered as you type. In order for systems to appear in this list, they must first be added in Insite. See Product Connections in the Insite User Guide.

Cancel • Next

Click **Cancel** to dismiss this screen without selecting one or more systems. Click **Next** to advance. See also Select IBM i profiles.

Settings screen



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.

What it Does

Use these settings to allow an Access Authenticator administrator to define which authentication methods are authorized, and configure other settings pertaining to Access Authenticator's user interactions.

Options

Authentication Methods

Choose the authentication methods available to network users.

- **One-Time Password (OTP).** The Access Authenticator 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.
- **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 Access Authenticator 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 Access Authenticator 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 Access Authenticator mobile app. When the Access Authenticator 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.

New User Action

This drop-down menu allows you to configure Access Authenticator'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 Access Authenticator 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 Access Authenticator 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 Access Authenticator.

- **Set User to Authenticate only after Device Registration.** Require authentication after user registers a device. If you choose this option, new users enrolled in Access Authenticator 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.

Authentication Attempts

Allowed Attempts

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

Printed Backup OTP Expiration

Backup List Expiration

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

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.

Syslog Server

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

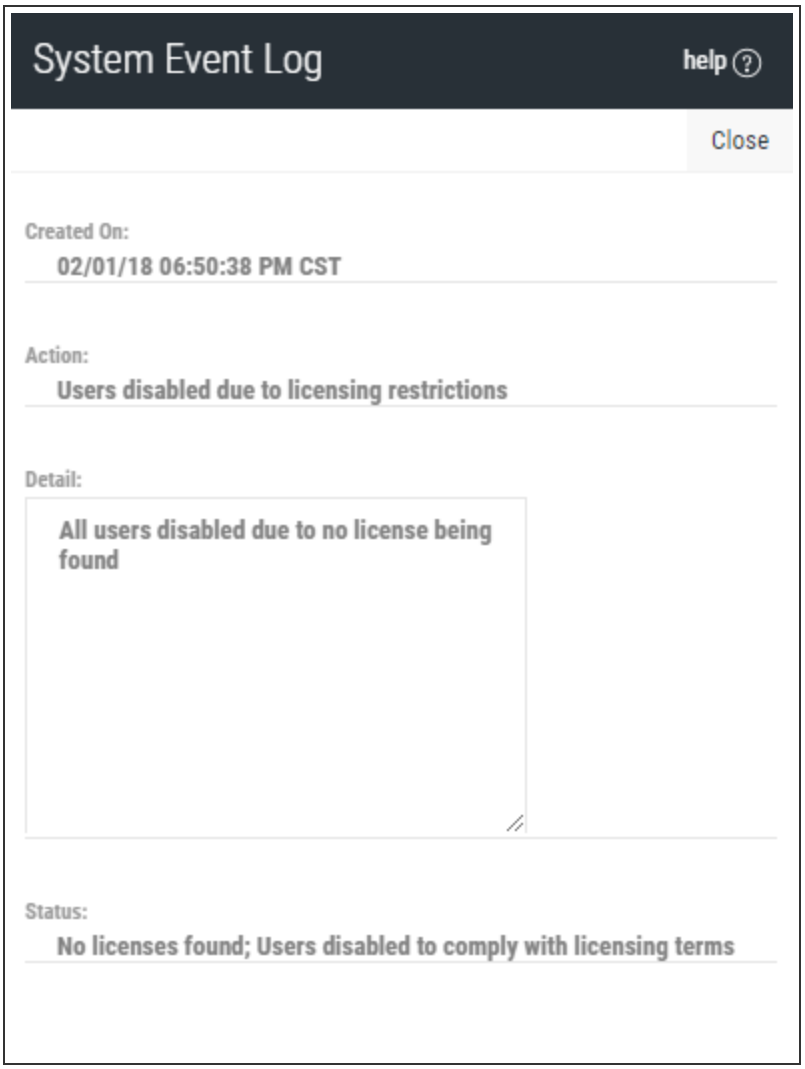
Set this option to **On** if you would like to enable automatic purging of report data. If enabled, a service runs every day at midnight and deletes from the database all report data older than the number of days specified in the 'Days' Worth of Data to Retain' field.

> **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.

System Event Log screen



How to Get There

On the Reports screen, click a System Event Log report.

What it Does

Displays the following information regarding an Access Authenticator 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 Access Authenticator and/or additional information pertaining to the logged activity.

Troubleshooting Authentication with your Mobile Device

The Access Authenticator 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 Access Authenticator.

> **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 Access Authenticator. 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 Access Authenticator. 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 Access Authenticator to use your camera

Access Authenticator 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 Access Authenticator access to your camera on iPhone or iPad

1. Go to **Settings > Privacy > Camera**.
2. Ensure Access Authenticator is allowed access.

Granting Access Authenticator 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 Access Authenticator 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 Access Authenticator app.
4. Tap **Camera**.

Allow Access Authenticator to send push notifications

Access Authenticator 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 Access Authenticator 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

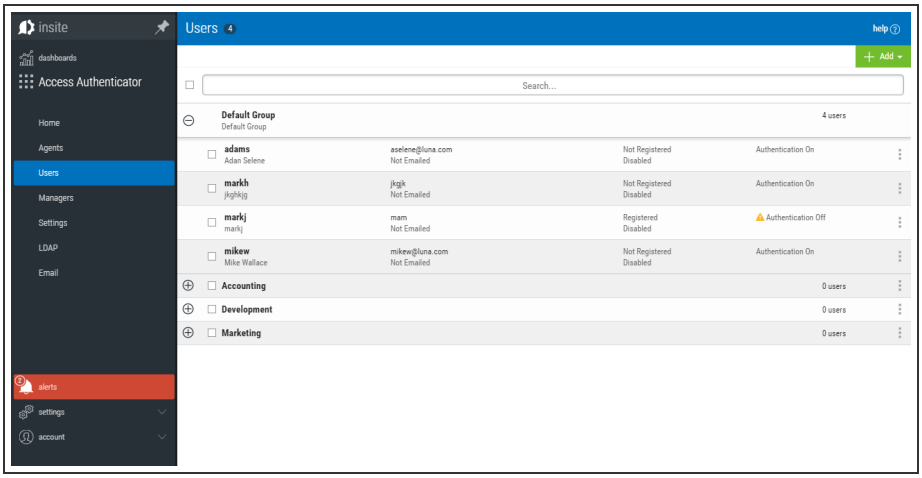
1. From the home screen, tap **Apps**.
2. Scroll to and tap **Settings**.
3. Scroll to and tap **Notifications**.
4. Tap to enable for the Access Authenticator app.

For Pixel or Nexus

1. Open your device's Settings app  .
2. Tap **Notifications**.
3. Tap Access Authenticator.

4. Tap the options that will allow you to see notifications for Access Authenticator. For example:
   - Disable Block all
   - Override Do Not Disturb

Users screen



How to Get There

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

What it Does

Use these settings to view, add, and remove Access Authenticator 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.

Options

Add

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

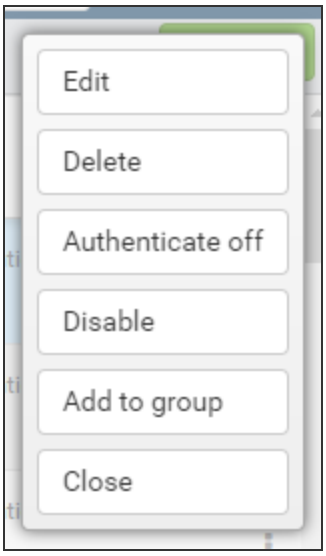
- Click **Add User** to open the New User page where you can define a new user to add.
- Click **Import Users** to open the Import Users screen where you can import user profiles from Active Directory database or IBM i system.
- Click **Add Group** to open the New Group screen where you can add a new 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 Access Authenticator.
- **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 context menu.



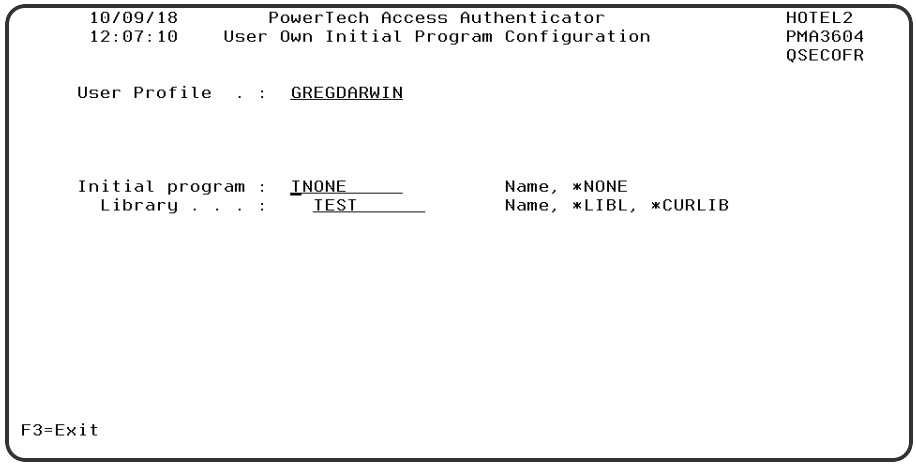
You can use these options to make changes to the system.

- **Edit.** Click **Edit** to open the Edit User screen, where you can make changes to the system's settings.
- **Delete.** Click **Delete** to remove the User from Access Authenticator.
- **Authentication off/on.** Click **Authenticate off** or **Authenticate on** to toggle the User's authentication status.
- **Enable/Disable.** Click **Enable** or **Disable** to enable or disable the user within Access Authenticator.
- **Add to Group.** Click **Add to Group** to add the User to an Access Authenticator User Group.
- **Close.** Click **Close** to dismiss the context menu.

IBM i Agent Reference

The topics in this section include descriptions of Access Authenticator's IBM i Agent options and controls.

Change Initial Program in AA panel



How to Get There

On the Access Authenticator 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 Access Authenticator library has been added to the library list.

What it Does

This panel allows you to change the supplemental initial program for active Access Authenticator users.

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 Access Authenticator.

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 Access Authenticator.

Initial Program • Library
This is the name and library of the desired Access Authenticator supplemental initial program.

Command Keys

F3=Exit
Dismisses the panel.

Deactivate Authentication Verification panel

```
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 Access Authenticator Main Menu, choose option **3**.

What it Does

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

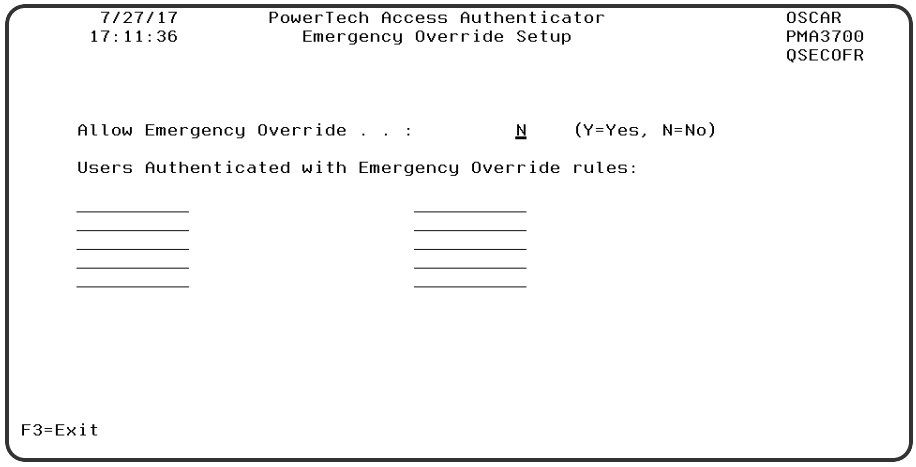
Options

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



How to Get There

On the Access Authenticator Main Menu, choose option **4**.

What it Does

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

Options

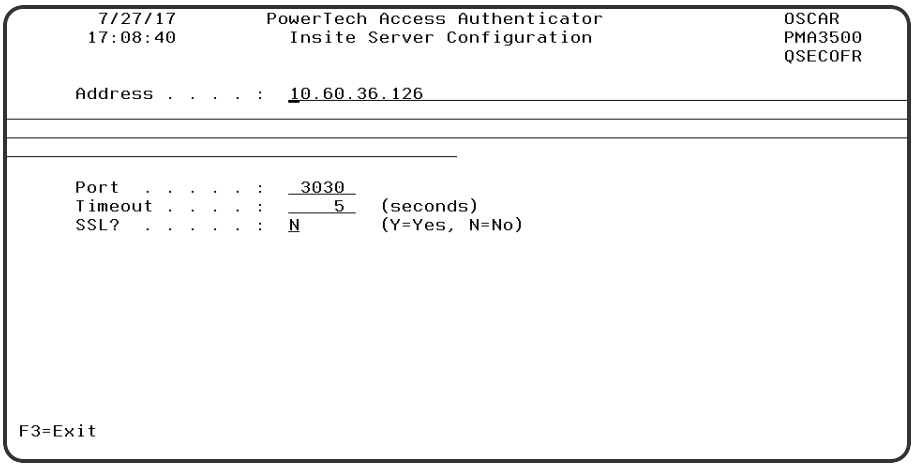
Allow Emergency Override
Option which pertain to allow the Emergency Overrride.

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



How to Get There

On the Access Authenticator Main Menu, choose option **1**.

What it Does

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

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

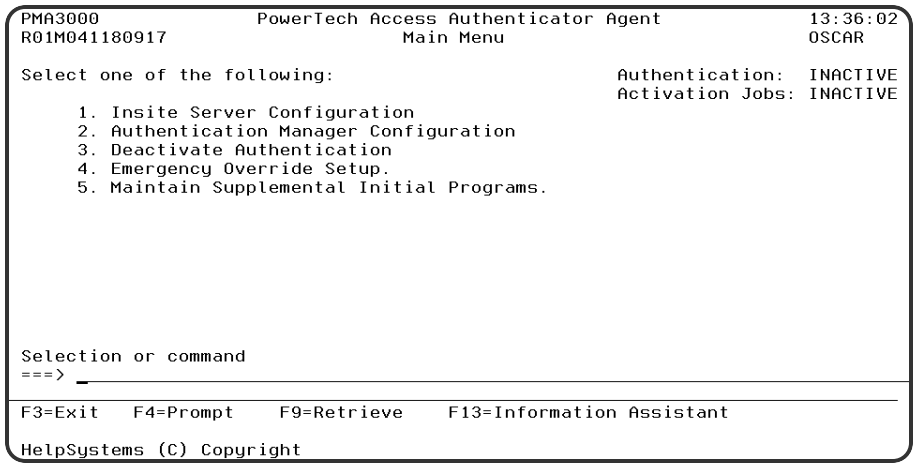
Indicates whether SSL (Secure Sockets Layer) is used.

Command Keys

F12=Cancel

Cancels this panel.

Powertech Access Authenticator Main Menu



How to Get There

Enter command **wrkptma**.

What it Does

This menu allows you to configure the IP of the Insite server and Authentication Manager used with Access Authenticator. It also allows you to deactivate authentication.

Options

1. Insite Server Configuration

The Insite Server Configuration allows maintaining the Insite Server settings.

2. Authentication Mananger Configuration

The Authentication Mananger 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 Access Authenticator 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.

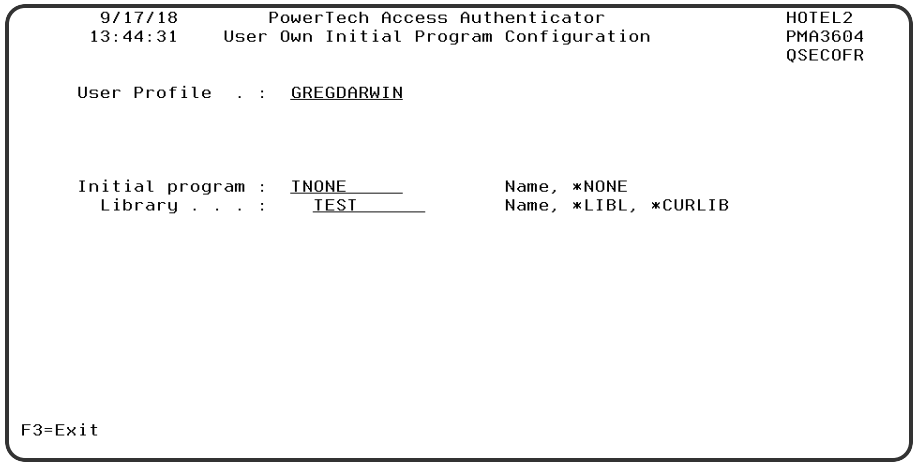
F3=Exit

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



How to Get There

On the Work with User Initial Programs screen, choose option **2** for a user.

What it Does

This panel allows you to specify the initial program and library for a specific active Access Authenticator user.

Options

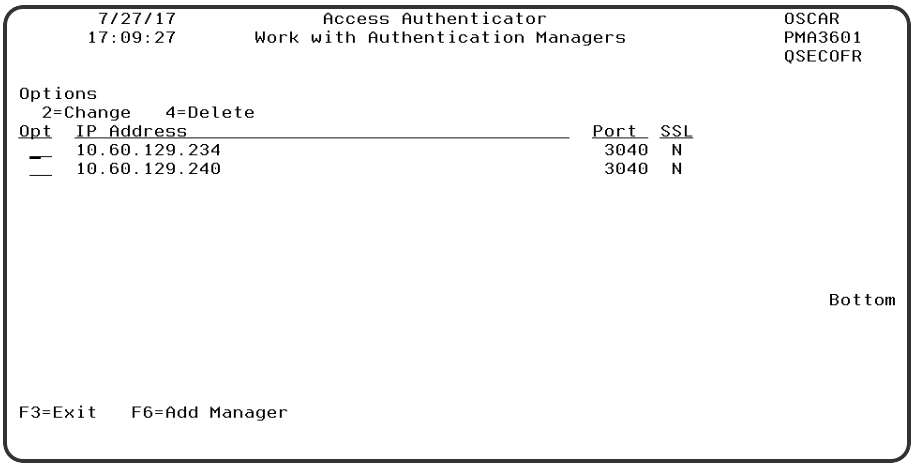
User Profile
The Profile name to change the user own Initial Program.

Initial Program • Library
This is the name and library of the desired Access Authenticator supplemental initial program.

Command Keys

F12=Cancel
Cancels this panel.

Work with Authentication Managers panel



How to Get There

On the Access Authenticator Main Menu, choose option **2**.

What it Does

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

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

```
      9/17/18            Access Authenticator                    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 Access Authenticator Main Menu, choose option **5**.

What it Does

When an IBM i user profile is assigned to an Access Authenticator user and the IBM i agent is activated, the user's existing initial program is replaced with the Access Authenticator 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 Access Authenticator. 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 Access Authenticator (without requiring user deactivation).

Field Descriptions

User Profile
The name of the Profile that has authentication turned on.

User Initial Program
The original/actual intial 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 Access Authenticator. 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 Access Authenticator.

API Help - Invoking Authentication from an IBM i Function

If, as a developer, you would like to integrate Access Authenticator into your own product and/or processes so, for example, authentication is invoked when calling the program, you can use the following APIs included with Access Authenticator. The first allows the user to authenticate interactively. The second forwards the request to the desktop agent.

Access Authenticator integration – Native (PMA300) API

Required Parameters:

1.	Profile to authenticate	Input	char(10)
2.	Source of authentication	Input	char(50)
3.	Return Code	I/O	binary(4)

The native Access Authenticator integration API (PMA300) 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 Access Authenticator user. See Add Users in the Administrator Setup Procedure topic.

Required Parameters

Profile to authenticate

INPUT; CHAR(10)

The name of the profile you want to authenticate.

Source of authentication

INPUT; CHAR(50)

The source where the authentication is taking place.

Return Code

I/O; BINARY(4)

The return code allows you to check for the success or failure of the authentication method.

The possible values for this parameter are:

Value	Description
1	Authentication successful
Other Value	Authentication failed

Access Authenticator integration – Desktop (PMA301) API

Required Parameters:

1.	Profile to authenticate	Input	char(10)
2.	Source of authentication	Input	char(50)
3.	Return Code	I/O	binary(4)

The desktop Access Authenticator integration API (PMA301) allows you to integrate Access Authenticator with another product. This program allows you to authenticate using the Desktop Agent. The response is returned to the calling program when the Desktop Agent authentication has completed.

> **NOTE:** IBM i user profiles to be authenticated must be mapped to an Access Authenticator user. See Add Users in the Administrator Setup Procedure topic.

Required Parameters:

Profile to authenticate

INPUT; CHAR(10)

The name of the profile you want to authenticate.

Source of authentication

INPUT; CHAR(50)

The source where the authentication is taking place.

Return Code

I/O; BINARY(4)

The return code allows you to check for the success or failure of the authentication method.

The possible values for this parameter are:

Value	Description
1	Authentication successful
Other Value	Authentication failed

Examples

The API's can be called from the command line. Like the following.

```
CALL PGM(PTMALIB/PMA300) PARM('AHABIB' NATIVE' 0)
```

NOTE: When you call from the command line, ensure the parameters are the correct length.

The API is called from a program in order to invoke the authentication. For example:

```
*
* Variable Definition
*

D Passed_user     s             10
D From_Source     s             50
D Error_code      s             10i 0

//
//  external calls
//

d $Native_Ath     pr                  extpgm('PTMALIB/PMA300')
d   User                        10
d   Source                      50
d   Error                       10i 0

 /Free
    $Native_Ath(Passed_user
                :From_Source
                :Error_code);
    If (Error_Code = 1);  //Successful Authentication
    // do your work here
    Endif;

    *inlr = *on;
 /End-Free
```

Promoting a Secondary Authentication Manager to Primary

If the Primary Authentication Manager is down due to a system failure, you can use the steps in this section to resume authentication services by promoting a Secondary Authentication Manager to Primary. These steps can also be used if a Primary system needs to be taken offline for some reason, such as for maintenance.

> **NOTE:** These steps require that you have installed the Access Authenticator Authentication Manager and Data Services on both a Primary and Secondary system, and initiated replication of the Primary on the Secondary (see Installing the Authentication Manager and Data Services).

Promoting a Manager to Primary on Windows

1. If the Primary system has crashed, and the purposes of promotion are for recovery, skip to step 2. If the Primary database needs to be taken offline, on the system running the Primary database, stop the service HSAccessAuthenticatorDB.
2. Login to the system running a/the Secondary Authentication Manager. (You will need to know its IP address.)
3. Run the following command in `C:\Program Files\Help Systems\Access Authenticator`:

   ```
   standby2master
   ```

   This command sets postgres to stop replicating data and become the Primary Manager.
4. Run the following command in `C:\Program Files\Help Systems\Access Authenticator\consul`:

   ```
   set_ds_primary -ip current ip -port discovery port
   ```

   > **NOTE:** The default discovery port is 8500.

   This command sets some internal variables that tells Access Authenticator where the new postgres master (Primary) is located.
5. Start the service 'HSAccessAuthenticatorDB' on the new Primary system.
6. If one or more additional Secondary installations are available, they need to be instructed to begin replicating from the new Primary system. Login to those systems and run the following command (in `C:\Program Files\Help Systems\Access Authenticator`):

   ```
   switchmaster new Primary system ip
   ```

   If no additional Secondary system is available, you can install the Authentication Manager and Data Services (as described in Installing the Authentication Manager and Data Services) on one or more Secondary systems, and run **master2standby**, to restore failover/recovery capability. Next, the new Primary system needs to be identified in Insite.
7. Open Insite and select **Access Authenticator** from the Navigation Pane, then choose **Managers**.
8. Click the system that was just promoted to Primary (it will still be listed as a Backup). The Edit Managers screen appears.
9. Set Primary to **On**.
10. Click **Save**.

Promoting a Manager to Primary on Linux

1. If the Primary system has crashed, and the purposes of promotion are for recovery, skip to step 2. If the Primary database needs to be taken offline, on the system running the Primary database, stop the service 'HelpSystemsAccessAuthenticatorDatabase'.

2. Login to the system running a/the Secondary Authentication Manager. (You will need to know its IP address.)
3. Run the following command in `opt\helpsystems\AccessAuthenticator`:

   ```
   standby2master
   ```

   This command sets postgres to stop replicating data and become the Primary Manager.
4. Run the following command in `opt\helpsystems\AccessAuthenticator\consul`:

   ```
   set_ds_primary -ip current ip -port discovery port
   ```

   NOTE: The default discovery port is 8500.

   This command sets some internal variables that tells Access Authenticator where the new postgres master (Primary) is located.
5. Start the service 'HelpSystemsAccessAuthenticatorDatabase' on the new Primary system.
6. Start the service 'HelpSystemsAccessAuthenticatorManager' on the new Primary system.
7. If one or more additional Secondary installations are available, they need to be instructed to begin replicating from the new Primary system. Login to those systems and run the following command (in `opt\helpsystems\AccessAuthenticator`):

   ```
   switchmaster new Primary system ip
   ```

   If no additional Secondary system is available, you can install the Authentication Manager and Data Services (as described in Installing the Authentication Manager and Data Services) on one or more Secondary systems, and run **master2standby**, to restore failover/recovery capability. Next, the new Primary system needs to be identified in Insite.
8. Open Insite and select **Access Authenticator** from the Navigation Pane, then choose **Managers**.
9. Click the system that was just promoted to Primary (it will still be listed as a Backup). The Edit Managers screen appears.
10. Set Primary to **On**.
11. Click **Save**.

Securing an Authentication Manager Connection on Windows

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*). To do so requires the following steps:

- **Create a Certificate.** Create the certificate on the Windows server running the Authentication Manager.
- **Enable the Certificate.** Enable the Certificate on the Authentication Manager server.
- **Import the Certificate into Insite.** Import the Certificate into Insite's Java Runtime Environment.

Creating a Certificate on a Windows Server

You must first generate a .keystore file. Make sure to note the password you enter, as you'll need this later. The Authentication Manager comes packaged with its own JVM. To generate the .keystore file on Windows, do the following:

1. On the Server that the Authentication Manager is installed, open the Command Prompt and go to the following directory:
   ```
   C:\Program Files\Help Systems\Access Authenticator\jvm\bin
   ```
2. Enter the following command to generate the key using the keytool:
   ```
   keytool -keysize 2048 -genkey -alias FullDomainName -keyalg RSA -
   keystore authmgr.keystore
   ```
   After creating a password, you'll be prompted for your organization's information. When asked for your first and last name, specify the domain name of the server that users will enter in order for their Authentication Manager name to help ensure that their certificates are valid when connecting to the server. We recommend not using an IP Address.
3. After you have filled in the requested fields, press Enter. The resulting authmgr.keystore file is located in your working directory (C:\Program Files\Help Systems\Access Authenticator\jvm\bin).
4. Export the certification from the keystore you just created so that you can import it into your Insite server's cacerts file in a later step.
   ```
   keytool -export -alias FullDomainName -file Domain.crt -keystore
   authmgr.keystore
   ```
5. Copy the .crt file to the Insite Server system.

Enabling the Certificate

1. Stop the Access Authentication Manager service. On Windows, run services.msc to open the Services Manager. Right-click Access Authenticator Manager and choose Stop.
2. Still on the Authentication Manager sever, open the Command Prompt and go to the following directory:
   ```
   C:\Program Files\Help Systems\Access
   Authenticator\AuthenticationManager\conf
   ```
3. Copy the authmgr.keystore file created into this directory.
4. Open and edit the server.xml file as follows. This file's location depends on the directory where the portal server is installed (see step 2).

   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++.

5. 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"/
   ```

6. Add in code block :

```
Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
SSLEnabled="true" scheme="https" secure="true"
keystoreFile="conf/authmgr.keystore" keystorePass="password used
when creating the keystore"
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" /
```

Import the Certificate Authority into Insite

1. On the Insite server, stop the HelpSystems Insite service.
   a. On Windows, run services.msc to open the Services Manager.
   b. Right-click Access HelpSystems Insite Server and choose **Stop**.
2. Open a command prompt in java 'bin' folder:

```
c:\Program Files (x86)\Help Systems\HelpSystems Insite\jvm\bin
```

3. Run the import command:

```
keytool -import -alias Server Alias -file Certificate Path -
keystore Keystore Path
```

EXAMPLE:

```
keytool -import -alias Server2012RAuth.domain.com -file
c:\helpsys\Server2012RAuth.crt -keystore "C:\Program Files
(x86)\Help Systems\HelpSystems Insite\jvm\lib\security\cacerts
```

4. Enter the keystore password, "changeit" by default.
5. Type `yes` and press **Enter**.
6. Restart the Insite server

After completing these steps, see Installing the Authentication Manager and Data Services in order to add a new Authentication Manager. Set UseSSL to **On** in the New Managers screen when adding a New Authentication Manager.

NOTE: The Insite Sever needs to “see” the full domain name of the Authentication Manager server. The windows Hosts file may need to be updated.

Other Help

For help with other Insite components and products supported by HelpSystems Insite, refer to the following resources:

Authority Broker Administrator's Guide

AutoMate Ops Console User Guide

AutoMate Schedule Ops Console User Guide

Crypto Complete for Insite User Guide

Deployment Manager User Guide

Event Manager for Insite User Guide

GoAnywhere MFT for Insite User Guide

HelpSystems Insite User Guide

Insite Analytics User Guide

Network Security Administrator's Guide

Password Self Help for Insite User Guide

Robot Network for Insite User Guide

Robot Schedule for Insite User Guide

Vityl IT & Business Monitoring for Insite User Guide