IBM i
7.6

Security
Multi-factor authentication (MFA)

Note

Before using this information and the product it supports, read the information in “Notices” on page 23.

This edition applies to IBM i 7.6 (product number 5770-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Multi-factor authentication (MFA)

This topic collection provides information about planning and setting up MFA on your IBM i platform.

This topic collection provides MFA configuration examples using CL commands and IBM Navigator for i. For more information on using IBM Navigator for i, refer to Using IBM Navigator for i to Manage MFA

PDF file for Multi-factor authentication (MFA)

You can view and print a PDF file of this information.

To view or download the PDF version of this document, select Multi-factor authentication (MFA).

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

MFA overview

Multi-factor authentication (MFA) extends password authentication to include an additional authentication factor used to verify your identity.

The IBM i integrated MFA solution incorporates a time-based one-time password (TOTP) key which is stored in the user profile and is architecturally protected similar to the password. The TOTP key is used, along with the system time, to generate a TOTP value. The TOTP value is presented as an additional factor when authenticating. The IBM i implementation is based on RFC 6238 -TOTP: Time-Based One-Time Password Algorithm

The IBM i implementation follows RFC 6238, so any compatible client application such as a PC application, smart phone application, smart watch application, or physical token that is standards compliant can be used to generate a TOTP value. The user profile and compatible client application must have the same TOTP key or shared secret. The client application, after it is configured with the TOTP key, generates TOTP values based on the TOTP key and the current time on the device. The user enters the TOTP value as an additional sign-on factor when authenticating to the system. The operating system validates the user ID, password and TOTP value at the same time making it a multi-factor authentication.

Enabling MFA

The IBM i operating system integrated MFA solution requires the system be at a security level (QSECURITY system value) 40 or greater and a password level (QPWDLVL system value) 4 or greater.

MFA is enabled on your system when the Additional sign-on factor security attribute is set to enabled. When the additional sign-on factor is enabled, some interfaces will show an Additional factor field on the sign-on prompt along with the User and Password fields. This does not mean users will be required to enter an additional factor. The additional factor is only required if the user's profile is changed to require it, otherwise the additional factor will be ignored. Enabling the additional factor for a user profile requires actions from both the user and the administrator. The frequency with which a user has to enter a TOTP value is configurable.

Interfaces that do not have an additional factor field require the additional factor value be appended to the password using a colon as the separator (password:additional_factor). The system administrator must educate users on how to use the password field on interfaces that do not provide an additional factor field.

For more information, refer to “Additional sign-on factor security attribute” on page 4.

When a user is required to enter a TOTP value, it requires the system time and client authenticator application time to be synchronized within a few seconds of each other. The Network Time Protocol (NTP) client can be used to keep the system time in sync with other devices in the network. For more information, refer to “Network Time Protocol (NTP) time synchronization” on page 21.

Security administrators must consider client application password usage when enabling MFA requirements for each user. The most challenging password usage examples are:

- Cached password
  - The client application stores a user’s password and authenticates to the server multiple times, over multiple connections, during a variable time period. The time-sensitive TOTP requirement breaks authentication for these applications. Applications that ask permission to store the password can be identified while those doing it implicitly need to be discovered through testing.
  - Applications can be redesigned to prompt for credentials on each authentication or to eliminate additional connections/authentications.
  - Security administrators can allow password caching applications to work for individual user profiles by configuring the frequency that a TOTP value is required.
- Password circumvention
  - An application’s server implementation bypasses the need for the user profile’s password. This happens when the application profile has authority to the user profile used on an interface that allows a special value for the password. An application may perform authentication independent of the user profile and/or password (such as Kerberos). Associating a user profile with this type of authentication that didn’t require a password, conflicts with MFA requirements.
  - Security administrators can use the QIBM_RUN_UNDER_USER_NO_AUTH function ID to control if this circumvention is permitted.

Host Connection Server

The Host connection server (HCS) allows a client to establish authenticated sessions with various host servers. HCS allows a client to authenticate one time and then use that authenticated session to transfer new connections to other host servers without having to re-authenticate. A user configured to always require a TOTP value only has to provide it one time eliminating the need to prompt for credentials multiple times. IBM i Access Client Solutions (ACS), IBM Navigator for i, and Digital Certificate Manager (DCM) have changed to use HCS. For more information, refer to Host connection server.

QIBM_RUN_UNDER_USER_NO_AUTH function ID

The ability to run actions as another user profile based only on having authority to that user profile should be considered. To achieve a complete MFA solution, it is recommended that user profiles require a TOTP value and also have their access to this function ID restricted. The IBM i integrated MFA TOTP implementation permits this password circumvention due to pervasive existing use. However, the Run under a user without authentication (QIBM_RUN_UNDER_USER_NO_AUTH) function ID should be used to block applications from bypassing the need to supply the user profile credentials. Security auditing can be used to assist with determining whether actions would fail if a user is denied access to the function ID. For more information, refer to “QIBM_RUN_UNDER_USER_NO_AUTH function usage ID” on page 7.

Note: The QIBM_RUN_UNDER_USER_NO_AUTH function ID does not require that MFA be enabled or used on the system.

IBM-supplied user profiles

There are IBM®-supplied user profiles with names that end in _NC, for “not changeable”. These user profiles are the same as the corresponding user profiles with names that don’t end in _NC, however they cannot be changed and do not have a password. These user profiles also cannot be denied access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID. They are used in places where the non _NC user

profiles were previously used, such as when submitting jobs, getting profile handles, or as the user profile a server runs under. They should also be used by applications in case the non _NC user profile is denied access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID.

- QPGMR_NC
- QSECOFR_NC
- QSYSOPR_NC
- QUSER_NC

Enhanced profile tokens

Enhanced security protection is available with profile tokens. When a profile token is generated, you can specify a verification ID and/or remote IP address by changing the application to specify these parameters. The matching verification ID and/or remote port must also be specified on the set request for it to be successful. This ensures the profile token is not being used by a bad actor. For more information, refer to “Enhanced profile token security protection” on page 18.

Note: The enhanced profile token does not require that MFA be enabled or used on the system.

Single authentication exit point QIBM_QSY_AUTH

Independent Software Vendor (ISV) security solutions often depend on IBM exit points to implement security protections in addition to what is provided by the operating system. The QIBM_QSY_AUTH exit point provides a way for an exit program to be called during authentication processing for all applications performing an applicable operation. The exit program registered in the registration facility, under the QIBM_QSY_AUTH exit point, is called when a user profile is changed to require calling the exit program. The exit program is passed information to use to perform additional verification and can return success or failure indicators. Some information passed to the exit program will be blank if the application does not provide it on calls to the authentication interfaces. A high privilege user could be required to provide a password and TOTP value, and have the exit program called. The exit program could generate an out-of-band push notification to a phone that requires a fingerprint to continue. For more information, refer to “*REGFAC authentication method” on page 6.

Note: The authentication exit point QIBM_QSY_AUTH does not require that MFA be enabled or used on the system.

Application developer considerations

Some system authentication interfaces with a user password parameter have a separate additional authentication factor parameter. The user experience can be improved when applications expose an additional authentication prompt to their users. This can be accomplished if the application determines the Additional sign-on factor security attribute is enabled then uses the additional authentication factor parameter on authentication interfaces. The IBM i authentication interfaces also include parameters to provide the additional information required to be passed to the QIBM_QSY_AUTH exit program or to create an enhanced profile token. The QIBM_QSY_AUTH exit program can analyze more information when applications consistently provide the additional information on applicable interface calls. However, the IBM i integrated MFA solution is functional without application changes to use these parameters. For more information on the interfaces with the relevant parameters, refer to “*REGFAC authentication method” on page 6 and “Enhanced profile token security protection” on page 18.

Service Tools support

System service tools (SST) and dedicated service tools (DST) support a separate MFA TOTP key implementation not connected to the operating system MFA support. The TOTP keys set for SST users have no relationship to the TOTP keys set for IBM i user profiles, specifically an SST user with a linked profile does not share a TOTP key with the linked profile. Another difference is that SST does not allow setting a frequency for providing the TOTP value, it is required every time a password is required. An SST

administrator can enable MFA for SST without enabling it on the operating system. For more information, refer to Service tools Multi-factor authentication (MFA).

Additional sign-on factor security attribute

The Additional sign-on factor security attribute indicates if MFA is enabled on your system.

The Additional sign-on factor security attribute has multiple purposes:

1. Indicates if sign-on prompts should add an **Additional factor** field.
2. Enables password:additional_factor parsing for user profiles that have an authentication method other than *NONE.
3. Enables the verification of the TOTP value for user profiles with an authentication method of *TOTP.
4. Enables passing the additional factor to the QIBM_QSY_AUTH exit program for user profiles with an authentication method of only *REGFAC.

When the additional sign-on factor is enabled, some interfaces will show an **Additional factor** field on the sign-on prompt along with the **User** and **Password** fields. The IBM i default sign-on panel will have an **Additional factor** field added. If you have a customized sign-on panel defined, you must change the definition to support the QDSIGNON3 format to add the additional factor field to your sign-on panel.

A user profile's authentication methods determine what is required in the additional factor field. When the authentication methods are:

***TOTP**
A TOTP value is required in the additional factor field.

***TOTP and *REGFAC**
A TOTP value is required in the additional factor field. The additional factor sent to the QIBM_QSY_AUTH exit program will be blank.

***REGFAC**
The QIBM_QSY_AUTH exit program can require an application defined additional factor in the additional factor field. The additional factor sent to the exit program will be what is entered in the additional factor field.

***NONE**
The additional factor field is ignored.

If an interface does not have an additional factor field, but an additional factor is required, the additional factor can be entered in the password field as password:additional_factor. For more information, refer to "Password with appended additional factor" on page 5.

If the Additional sign-on factor security attribute is disabled, user profiles with an authentication method of *TOTP are not required to enter a TOTP value to authenticate.

The Change SST Security Attributes (CHGSSTSECA) command, Change additional sign-on factor (CHGADLSGN) parameter, controls whether the Change Security Attributes (CHGSECA) command or IBM Navigator for i can be used to enable or disable the additional sign-on factor. When the SST attribute indicates the additional sign-on factor can be changed, the CHGSECA command or IBM Navigator for i can be used to enable or disable the additional sign-on factor.

For more information, refer to "Enabling MFA on your system" on page 10 and "Enabling MFA for a user" on page 12.

There is also a system service tools (SST) Additional sign-on factor security attribute that is used by SST/DST. For more information, refer to Service tools Multi-factor authentication (MFA).

Authentication methods

Authentication methods cause additional verification during authentication processing. A user can have a list of authentication methods that include *TOTP and *REGFAC.

*TOTP authenticate method

*TOTP authentication method requires that an additional factor be entered along with the password.

The additional factor is a time-based one-time password (TOTP) value that is generated from a TOTP client authenticator application. This authentication method is only enforced when the Additional sign-on factor security attribute is enabled. If the Additional sign-on factor security attribute is disabled, the user profiles with an authentication method of *TOTP are not required to enter a TOTP value.

TOTP key

A TOTP key is the secret key that is stored in your user profile and used as input into the client authenticator application that will generate your TOTP value.

This secret key allows an application to generate a TOTP value that can then be verified when you authenticate since both the user profile and the application that generates your TOTP value have the same secret key. A user must have a TOTP key before their user profile authentication method can be set to *TOTP.

The user's TOTP key is encrypted using AES with a 32-byte derived key before being stored in an internal control block. The control block is protected with the strongest mechanism available to the IBM i operating system running on the Power® hardware. A capability that is called Hardware Storage Protection (HSP) is used to protect the control block. The HSP capability is protection that is built into the Power hardware and enforced by the hardware itself. The HSP value that is used is called "no access from user state" and "protect at all security levels". This HSP protection value keeps all user level code out of the control block (no read or write access) but allows the operating system to read/write the control block. This protection is always activated as the control block is protected at all security levels. If user level code tries to access the control block, the hardware would send an exception and the Licensed Internal Code would send an error to the user level code (and access would be denied).

Recovery key

When authenticating, your recovery key can be used instead of a generated TOTP value when you cannot generate a TOTP value. The recovery key is available to save when you set your TOTP key.

The recovery key can be used for authentication for 10 minutes before it is no longer valid. This allows you to change your TOTP key. You must change your TOTP key within 10 minutes of initially using the recovery key.

If the recovery key is used more than 10 minutes after the initial use, your TOTP key will be removed and you will not be able to authenticate again. You will then need to contact your system administrator to remove your *TOTP authentication method so you can sign on to change your TOTP key. After changing your TOTP key, the administrator can change your authentication method to include *TOTP again.

TOTP optional interval

The TOTP optional interval is the amount of time, in minutes, that a TOTP value is not needed after an initial successful authentication using a password and TOTP value.

This allows interfaces that do not support MFA to be used after a successful authentication with a TOTP value. For more information, refer to "IBM i software and client application considerations" on page 19.

The TOTP optional interval can be set to *NONE which will require the user to enter a TOTP value on every authentication that requires a password, or it can be set to a number of minutes, 1-720. When the specified optional interval expires, the user is required to successfully authenticate using a password and TOTP value again before the interval will restart.

Password with appended additional factor

There are interfaces that require a password but do not have an additional factor field.

When a user is required to enter an additional factor into this type of interface, they must specify the password and additional factor separated by a colon (:) into the password field. The format of

the value entered into the password field must be password:additional_factor (example: myAmazingPa$$w0rd:358538).

This password format is only supported if the Additional sign-on factor security attribute is enabled and the user has an authentication method other than *NONE, otherwise the authentication will fail. If the interface has an additional factor field, use the additional factor field and do not append the additional factor to the password.

A colon is allowed as part of the password. If an additional authentication factor is supported, the search for the colon separating the password and the additional factor starts at the end of the string and looks backward until the colon is found.

The combined length of the password, colon, and additional factor cannot exceed 128 bytes.

- If using an authentication method of *TOTP, the user's password length should not exceed 121 bytes to take into consideration the password plus 1 (for the colon) plus 6 (for the TOTP value).
- If only using an authentication method of *REGFAC, the additional factor gets passed to the exit program registered under the QIBM_QSY_AUTH exit point. A user's password length should not exceed 128 bytes minus 1 (for the colon) minus n. Where n is the length of the additional factor the exit program expects (1-64).

Appending the TOTP value to the password does not work when the client application uses password substitution that is based on a one-way hash. Some IBM clients use this encapsulation to protect passwords in transit. Examples of client applications that would not support appending the TOTP value to the password are IBM i Access Client Solutions (ACS), IBM Navigator for i, and Digital Certificate Manager (DCM). The additional factor needs to be entered in the additional factor field for these interfaces.

*REGFAC authentication method

The primary purpose of the *REGFAC authentication method is to facilitate additional authentication requirements.

*REGFAC authentication method will call the exit program registered under exit point QIBM_QSY_AUTH during authentication processing. Refer to Additional Authentication Exit Program. The exit program is called after a successful authentication. It is not called if the authentication fails.

The exit program has sole responsibility for doing the additional authentication. If authentication is not performed by the exit program and *REGFAC is the only authentication method, this does not result in MFA protection. The administrator should take great care in monitoring the validity of the registered exit program.

Traditionally authentication is thought of as verifying a password. This exit program will be called for more cases. For instance, when the password is a special value.

Authentications using Kerberos and SSH, which do not require a password or TOTP value, will indirectly call the exit program via the interface used to associate a user profile with the Kerberos or SSH authentication.

The operating system gives the exit program information associated with the authentication. The exit program then has the ability to verify the information and return a value to the operating system that causes the authentication to pass or fail.

The *REGFAC authentication method can be used along with the *TOTP authentication method or it can be used independently. If used independently, the value entered into the additional factor field will be passed to the exit program. It can be used by the exit program to perform additional verification. If used along with the *TOTP authentication method, the additional factor field passed to the exit program will be blank.

The exit program is called for these actions:

- Sign-on
- Get Profile Handle API calls

  - The Set Profile Handle API calls use the profile handle. However, the authentication only happens on the get call. If the exit program allows the handle to be created, then the set using it will be allowed.
- Generate Profile Token API calls
  - The Set to Profile Token API calls use the profile token. However, the authentication happens on the generate call. If the exit program allows the token to be created, then the set using the token is allowed provided the enhanced profile token information matches on the generate and set.
- NetServer remote file access

Table 1. Interfaces with additional information parameters

Original API	API with additional information parameters
QSYGETPH	QSYGETPH, with all optional parameters
QsyGetProfileHandle	QsyGetProfileHandle2
QsyGetProfileHandleNoPwd	QsyGetProfileHandleNoPwd2
QSYGENPT	QSYGENPT, with all optional parameters
QsyGenPrfTkn	QsyGenPrfTkn2
QsyGenPrfTknE	QsyGenPrfTknE2

QIBM_RUN_UNDER_USER_NO_AUTH function usage ID

The Run under a user without authentication (QIBM_RUN_UNDER_USER_NO_AUTH) function usage ID prevents a user profile from being the target of an operation initiated by another user profile which did not have to authenticate as the target user.

The default access for the function usage ID is *ALLOWED for all users and that cannot be changed to *DENIED. When a user profile is added to the list as *DENIED, operations with that user profile as the target will fail. This function ID is unique in that it is not the user profile on the list as *DENIED whose actions are restricted, it is other user profiles that are restricted from using that user profile as a target. This protects the integrity of actions performed by the user on the list by preventing another user with *ALLOBJ special authority from running as them.

The protections provided by QIBM_RUN_UNDER_USER_NO_AUTH are intended for interactive user profiles that require credentials for authentication. Administrators should not restrict batch only user profiles from having access to the function ID.

The interfaces that do not work when denied access to the QIBM_RUN_UNDER_USER_NO_AUTH function id, can be found here: IBM-supplied function IDs. Search for QIBM_RUN_UNDER_USER_NO_AUTH.

Operations that check that the target user profile has access to the function ID:

- Get Profile Handle with a special value for the password
- Generate Profile Token with a special value for the password
- Set User ID APIs when the target user is a different user than the current user:
  - Set Effective User ID (qsyseteuid()) API
  - Set Real and Effective User IDs (qsysetreuid()) API
  - Set User ID (qsysetuid()) API
- Submitting a job when the job is being submitted under a different user than the current user
  - User is not *CURRENT or the same as the current user
  - Job description user is not the same as the current user
- Kerberos enabled applications require getting a profile handle with a special value for the password after verifying the Kerberos token. This operation fails if the associated user profile is protected by the function ID.

- SSH, when using public key authentication requires getting a profile handle with a special value for the password. This operation fails if the user profile is protected by the function ID. Password authentication is not affected.

To deny users access to the QIBM_RUN_UNDER_USER_NO_AUTH function usage ID, use one of the following interfaces:

- Change Function Usage (CHGFCNUSG) command.
- In IBM Navigator for i, expand **Security** > **MFA Configuration**, click **Users**.
  - Clear the filter value from the **MFA Key Exists** filter and select **Apply**.
  - Users that have already been denied access to the function ID will have **DENIED** in the **Impersonation** column. Users that are using the default access will have **ALLOWED** in the column.
  - To change the access for a user, right click on the user and select **Properties**.
  - Check the box for **Restrict the ability to impersonate this user profile without first doing authentication by setting the function usage ID QIBM_RUN_UNDER_USER_NO_AUTH to DENIED for this profile**.
  - Click **OK**.

Note: The QIBM_RUN_UNDER_USER_NO_AUTH function ID does not require that MFA be enabled or used on the system. It is recommended to be used in conjunction with user profiles that have an authentication method of *TOTP, however any interactive user profile can be protected.

Example 1

User profile JILL is on the QIBM_RUN_UNDER_USER_NO_AUTH function usage list with a value of *DENIED.

User SAM has *ALLOBJ special authority and is trying to get a profile handle for JILL using the QSYGETPH API specifying *NOPWD for the password parameter. Since a special value is used for the password, no authentication for the target user profile, JILL, is performed. Therefore, JILL, having a value of *DENIED on the QIBM_RUN_UNDER_USER_NO_AUTH function usage list, causes the operation to fail with error message CPF4AF1 – Operation not allowed for user profile JILL.

Example 2

User profile MIKE is on the QIBM_RUN_UNDER_USER_NO_AUTH function usage list with a value of *DENIED.

User SAM is trying to submit a job to run as user MIKE by specifying USER(MIKE) on the SBMJOB command. There is no authentication performed for user MIKE since a password is not needed. MIKE has a value of *DENIED on the QIBM_RUN_UNDER_USER_NO_AUTH function usage list so the operation will fail with error message CPF4AF1 – Operation not allowed for user profile MIKE.

Warning security audit records

You can use security auditing to monitor operations performed by users to assist with determining if the user profile can be denied access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID.

Audit records of type GR, subtype F, and *USAGEWARN in Field 1 are sent when the target user profile is allowed access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID and one of the interfaces is used that would not be allowed if the target user was denied access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID.

Follow these steps to set up the warning audit records.

1. Set up auditing for the system. The QAUDCTL system value must contain *AUDLVL. You can use either commands or IBM Navigator for i to do this.
   - To use commands, refer to Using CHGSECAUD to set up auditing.
   - To use IBM Navigator for i, expand **Security** > **Audit journal**. Click **Audit journal configuration**.

- In the Auditing Configuration panel, click the box to put a check mark next to **Enable action auditing (*AUDLVL)**.
- Click **OK**.

2. The user profiles you want to analyze for adding to the QIBM_RUN_UNDER_USER_NO_AUTH function usage list as *DENIED must have the user action auditing value set to *AUTWARN. You can use either commands or IBM Navigator for i to do this.
   - To use commands, use the Change User Auditing (CHGUSRAUD) command to set the User action auditing value (AUDLVL) to *AUTWARN.
   - To use IBM Navigator for i,expand **Users and Groups** > **Users**.
     - Right click the user profile you want to change and click **Properties**.
     - At the bottom of the Properties panel, click **Capabilities**.
     - On the Capabilities panel click the **Auditing** tab, then click the box to put a check mark next to **Authorization failure warnings**.
     - Click **OK**.
3. Monitor the security audit journal for GR-F *USAGEWARN audit records. The operation that fails when the user is denied access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID will be in Field 3 in the GR-F audit entry. The operations are:
   - SBMJOB - A job is submitted and the specified user that the submitted job runs under is not the same as the user that is submitting the job.
   - GETPH - A special value is specified for the password of the user on one of the get profile handle APIs.
   - GENPT - A special value is specified for the password of the user on one of the generate profile handle APIs.
   - SETUID - The specified user is the target profile on one of the set user ID APIs.
   - NFS - The Network File System server received credentials that map to the user.

Setting up MFA on your system

To setup multi-factor authentication (MFA) on your system, you must enable the Additional sign-on factor security attribute. When enabled, you can change specific user profiles to require them to enter an additional factor when authenticating.

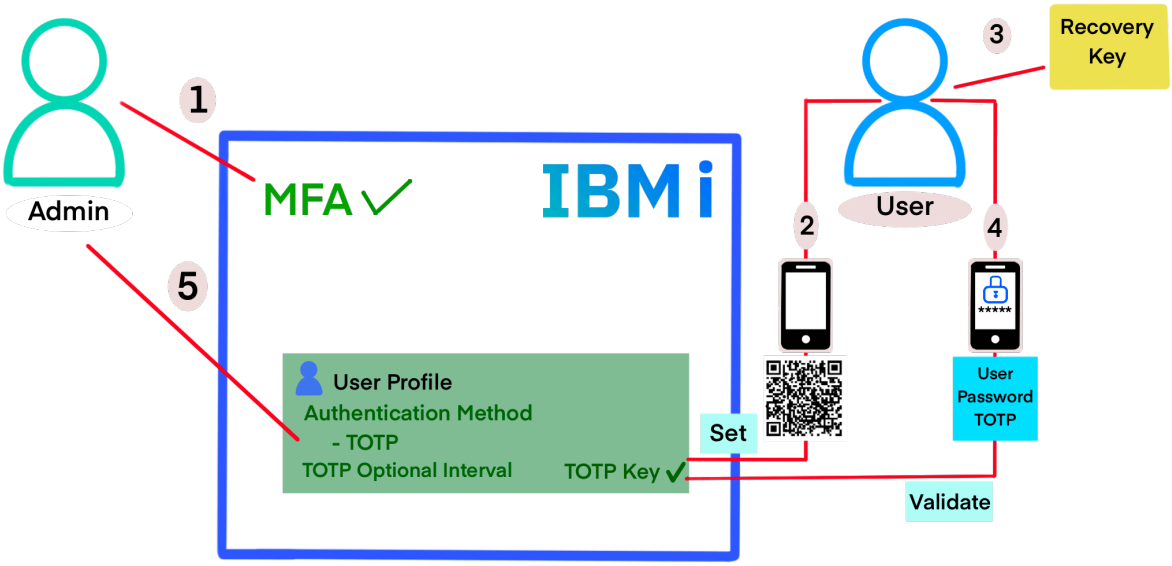

Figure 1. Flow of setting up MFA on your system

Administrator actions:

For more information, refer to "Enabling MFA on your system" on page 10.

Step 1

- The Additional sign-on factor security attribute must be enabled to enforce the *TOTP authentication method. If only using *REGFAC authentication method, you do not need to enable the Additional sign-on factor security attribute unless your exit program requires the additional factor to be passed to it in the Additional authentication exit information parameter. To enable:
  - Make sure system requirements are met.
  - If you have a customized sign-on screen, make the necessary changes.
  - Turn on MFA by enabling the Additional sign-on factor security attribute and IPL.
- To enable *TOTP authentication method:
  - Notify identified users that they need to set their TOTP key. The administrator cannot set the TOTP key for a user profile, each user must set their own TOTP key
- To enable *REGFAC authentication method:
  - Register the QIBM_QSY_AUTH exit program in the registration facility.

User actions:

Only required if setting authentication method to *TOTP. For more information, refer to "Enabling MFA for a user" on page 12.

Step 2

- Set their TOTP key. This saves the TOTP key in their user profile.

Step 3

- Save the recovery key in a safe place. The recovery key was generated when they set their TOTP key.

Step 4

- Enter their TOTP key into their client application.
- Validate the TOTP value generated by the client application.
- Notify the administrator that their TOTP key has been set.

Administrator actions for users:

Step 5

- To enable *TOTP authentication method:
  - If not notified, check if the user has set their TOTP key.
  - If the user's TOTP key has been set, change the user profile to set the authentication method to include *TOTP and to set the desired TOTP optional interval.
- To enable *REGFAC authentication method:
  - Change the user profile to set the authentication method to include *REGFAC.

Enabling MFA on your system

To enable multi-factor authentication (MFA) on your system, the administrator must enable the Additional sign-on factor security attribute.

The Additional sign-on factor security attribute is required to use *TOTP authentication method. The additional factor must be a TOTP value.

If only using *REGFAC authentication method, the exit program may require an additional factor, so the Additional sign-on factor security attribute must be enabled. If the exit program does not require an additional factor, the Additional sign-on factor security attribute does not need to be enabled. The type of additional factor is defined by the exit program.

To enable the Additional sign-on factor security attribute:

1. The security level must be 40 or greater and the password level must be 4 or greater.

   Interfaces that show the current security level and current password level:

   - Display Security Attributes (DSPSECA) command
   - In IBM Navigator for i, expand **Security** > **MFA Configuration**. Click **Security Configuration Information**

   If the security level needs to be changed, refer to Using System Security (QSECURITY) system value to understand the impacts of making a change.

   If the password level needs to be changed, refer to Planning password level changes to understand the impacts of making a change.
2. Change the Additional sign-on factor security attribute, if it is not already *ENABLED.

   Interfaces that show the current additional sign-on factor value:

   - Display Security Attributes (DSPSECA) command
   - In IBM Navigator for i, expand **Security** > **MFA Configuration**. Click **Security Configuration Information**.

   Interfaces that change the additional sign-on factor value:

   - Change Security Attributes (CHGSECA) command, Additional sign-on factor (ADLSGNFAC) parameter.
   - In IBM Navigator for i, expand **Security** > **MFA Configuration**.
     - Click **Security Configuration Information**.
     - Right click **Additional Signon Factor** and select **Change**.
     - In the Change Additional Signon Factor panel, select **Enabled** from the Additional Signon Factor pull-down.
     - Click **Save**

   If the SST security attribute does not allow this attribute to be changed, use the Change SST Security Attributes (CHGSSTSECA) command to set the Change additional sign-on factor (CHGADLSGN) parameter to *YES. Then start again at step “2” on page 11.

   To prohibit the changing of the Additional sign-on factor security attribute after you have set it to the desired value, use the Change SST Security Attributes (CHGSSTSECA) command to set the Change additional sign-on factor (CHGADLSGN) parameter to *NO.

   If you have a customized sign-on screen, you must create a new one based on QDSIGNON3 before you IPL. For more information, refer to Signon screen display file and Creating a sign-on display file.

   If the additional sign-on factor is being changed from *DISABLED to *ENABLED, IPL the system for the pending value to take effect.
3. Optionally set up the Network Time Protocol (NTP) client to synchronize the time on devices. For more information, refer to “Network Time Protocol (NTP) time synchronization” on page 21.

To enable *REGFAC authentication method:

Register the QIBM_QSY_AUTH exit program in the registration facility, use one of the following interfaces:

- Add Exit Program (ADDEXITPGM) command. The default wait time for the exit program to complete processing is 10 seconds. To change the wait time, use the Program Data (PGMDTA) parameter. For example, this will change the wait time to 20 seconds:

```
ADDEXITPGM EXITPNT(QIBM_QSY_AUTH) FORMAT(AUTH0100) PGMNBR(1) PGM(your_library/your_exit_pgm)
REPLACE(*YES) CRTEXITPNT(*NO) PGMDTA(*JOB *CALC 20)
```

- In IBM Navigator for i, expand **Security** > **MFA Configuration**.
  - Click **Authentication Exit Point.**.
  - Right click **QIBM_QSY_AUTH** exit point name and select **Add Exit Program**.
  - In the Add Exit Program panel, enter the exit program name in the **Program** field and the library name in the **Library** field.
  - Click **OK**

Enabling MFA for a user

When multi-factor authentication (MFA) is enabled on the system and a user profile has an authentication method of *TOTP, they will be required to enter a TOTP value as the additional factor when authenticating.

To enable TOTP for a user profile, the user must have a TOTP key and the user profile's authentication method must be set to *TOTP. Setting a user's authentication method to *TOTP involves actions by both the user and the administrator.

Setting up *REGFAC authentication method requires the administrator to register the authentication exit program and set the user profile's authentication method to *REGFAC.

User sets TOTP key

The administrator informs the user they must set their TOTP key. A user must set their own TOTP key, it cannot be set by the administrator.

Commands or IBM Navigator for i can be used to set your TOTP key.

Using commands:

1. Use the Change TOTP key (CHGTOTPKEY) command. This stores the TOTP key in your user profile. A key can be generated or a key can be specified. The key is saved in your user profile and displayed on the screen.
2. The recovery key, generated by the CHGTOTPKEY command, is displayed on the screen and must be copied and stored in a safe place.
3. Enter the TOTP key into a client authenticator application.
4. Check that the TOTP value generated by the client authenticator application verifies successfully by using the Check TOTP (CHKTOTP) command. Pressing **F9=Check TOTP** on the CHGTOTPKEY display prompts for the CHKTOTP command.

Using IBM Navigator for i:

- In IBM Navigator for i:
  - If you do not have access to **QIBM_NAV_ALL_FUNCTION** function ID, the **Manage My MFA Key** panel is displayed after signing on.
  - If you do have access to QIBM_NAV_ALL_FUNCTION function ID, expand **My Work** > **My Additional Authentication Factor** > **Manage My MFA Key**.
- On the **Manage my MFA Key** panel, select **Generate and save a MFA key and recovery key for this user profile**. Click **Next**.
- On the **Validate MFA Key and Save Recovery Key** panel, using your client authenticator application, scan the QR code. Or you can manually enter the value in the **Saved MFA key** field (this is the TOTP key) into your client authenticator application.

- Validate the MFA key by entering your password and the MFA Code (TOTP value) the client application generates. Click **Validate**.
- Save the recovery key in a safe place.

Inform the administrator your TOTP key is set.

Administrator sets authentication methods

The administrator must set the authentication methods for a user to enable them for MFA. The list of authentication methods includes *TOTP and *REGFAC.

To set a user's authentication method to *TOTP, the user must have a TOTP key. To determine if a user has a TOTP key, use one of the following interfaces:

- Display Authorized Users (DSPAUTUSR) command, Additional Authentication Info view, to see if a TOTP key exists for a user.
- In IBM Navigator for i, expand **Security** > **MFA Configuration**, click **Users**. The list defaults to filter on users whose MFA key is set.

To change a user's authentication method, use one of the following interfaces:

- Change User Profile (CHGUSRPRF) command, Authentication Methods (AUTHMTH) parameter.
- In IBM Navigator for i, expand **Security** > **MFA Configuration**.
  - Click **Users**.
  - Set the desired authentication methods:
    - To set *TOTP, right click on the user and select **Enable Users for MFA authentication**.
    - To set *REGFAC, right click on the user again and select **Enable Users for Exit Program Authentication**.

If *TOTP authentication method was set for a user, a TOTP optional interval can be set. To change a user's TOTP optional interval, use one of the following interfaces:

- Change User Profile (CHGUSRPRF) command, TOTP optional interval (TOTPOPTITV) parameter.
- In IBM Navigator for i, expand **Security** > **MFA Configuration**.
  - Click **Users**.
  - Right click on the user profile and select **Properties**.
  - In the **Additional Authentication Options** section, enter the number of minutes in the **Optional Interval** field.
  - Click **OK**.

The remaining minutes in a user's TOTP optional interval can be displayed along with the other MFA attributes. The remaining minutes are only shown if the user has a TOTP optional interval.

To display the MFA attributes for a user, use one of the following interfaces:

- Display Authorized Users (DSPAUTUSR) command, Additional Authentication Info view.
- Display User Profile (DSPUSRPRF) command.
- In IBM Navigator for i, expand **Security** > **MFA Configuration**, click **Users**. To show the remaining minutes, right click on a user profile and select **Properties**.

Authentication method combinations

Each user profile can have unique authentication requirements and user experience.

There are six common user experiences possible with the IBM i integrated MFA solution reflected by the user profiles in Table 2 on page 14 and Table 3 on page 15.

Table 2. Assumes the users have access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID. Attempts to run under these user profiles using an interface that does not require a password or allows a special value for the password are successful (default setting).

User profile	Authentication method	TOTP optional interval	Description
Allen	*NONE	*NONE	No TOTP value required. This is the default setting for all user profiles migrated from prior releases or newly created.
Barb	*TOTP	*NONE	TOTP value required on all password authentications
Carol	*TOTP	10 minutes (1-720)	TOTP value required on initial password authentication. Additional password authentications during the 10-minute optional interval do not require a TOTP value. If a valid TOTP value is provided during an active optional interval, the active option interval resets to 10 minutes.
Denise	*REGFAC	N/A	No TOTP value required. The QIBM_QSY_AUTH exit program is called on every successful authentication. The exit program determines the additional authentication required, if any.
Edward	*TOTP *REGFAC	*NONE	TOTP value required on all password authentications. The QIBM_QSY_AUTH exit program is called on every successful authentication. The exit program determines the additional authentication required, if any.

Table 2. Assumes the users have access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID. Attempts to run under these user profiles using an interface that does not require a password or allows a special value for the password are successful (default setting). (continued)

User profile	Authentication method	TOTP optional interval	Description
Frank	*TOTP *REGFAC	20 minutes	TOTP value required on initial password authentication. Additional password authentications during the 20-minute optional interval do not require a TOTP value. If a valid TOTP value is provided during an active optional interval, the active option interval resets to 20 minutes. The QIBM_QSY_AUTH exit program is called on every successful authentication. The exit program determines the additional authentication required, if any.

Table 3. Assumes the users are denied access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID. Attempts to run under these user profiles using an interface that does not require a password or allows a special value for the password will fail.

User profile	Authentication method	TOTP optional interval	Description
Gene	*NONE	*NONE	No TOTP value required. Kerberos and SSH key only authentication will fail. Other attempts to run under this user profile without providing a password will fail.
Heather	*TOTP	*NONE	TOTP value required on all password authentications. Kerberos and SSH key only authentication will fail. Other attempts to run under this user profile without providing a password will fail.

Table 3. Assumes the users are denied access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID. Attempts to run under these user profiles using an interface that does not require a password or allows a special value for the password will fail. (continued)

User profile	Authentication method	TOTP optional interval	Description
Irwin	*TOTP	10 minutes	TOTP value required on initial password authentication. Additional password authentications during the 10-minute optional interval do not require TOTP value. If a valid TOTP value is provided during an active optional interval, the active option interval resets to 10 minutes. Kerberos and SSH key only authentication will fail. Other attempts to run under this user profile without providing a password will fail.
Jill	*REGFAC	N/A	No TOTP value required. The QIBM_QSY_AUTH exit program is called on every successful authentication. The exit program determines the additional authentication required, if any. Kerberos and SSH key only authentication will fail. Other attempts to run under this user profile without providing a password will fail.

Table 3. Assumes the users are denied access to the QIBM_RUN_UNDER_USER_NO_AUTH function ID. Attempts to run under these user profiles using an interface that does not require a password or allows a special value for the password will fail. (continued)

User profile	Authentication method	TOTP optional interval	Description
Kevin[1]	*TOTP *REGFAC	*NONE	TOTP value required on all password authentications. The QIBM_QSY_AUTH exit program is called on every successful authentication. The exit program determines the additional authentication required, if any. Kerberos and SSH key only authentication will fail. Other attempts to run under this user profile without providing a password will fail.
Lisa	*TOTP *REGFAC	5 minutes	TOTP value required on initial password authentication. Additional password authentications during the 5-minute optional interval do not require TOTP value. If a valid TOTP value is provided during an active optional interval, the active option interval resets to 5 minutes. The QIBM_QSY_AUTH exit program is called on every successful authentication. The exit program determines the additional authentication required, if any. Kerberos and SSH key only authentication will fail. Other attempts to run under this user profile without providing a password will fail.

1 User profile Kevin reflects the most secured user profile possible provided the exit program requires an out-of-band authentication.

Enhanced profile token security protection

A profile token can be passed to one or more additional processes which can then use it to perform tasks on behalf of the authenticated user.

Enhanced profile token security protection is associated with a profile token when restrictions are added during generation. Providing values for the Verification ID and/or Remote IP parameters produces an enhanced profile token. The returned profile token does not have an indication that it is an enhanced token. However, to successfully use the enhanced token, the set to profile token or generate profile token from profile token call must provide the same values used on the generate.

The verification ID is an application defined value that identifies the specific application, service, or action associated with the profile token. The application uses the value to protect the token from being used for an unintended purpose. This is enforced by requiring the matching value be specified on the set or generate profile token from profile token request.

The remote IP address identifies the network connection associated with the profile token. The application uses this value to protect the token from being used from an unintended network client. This is enforced by requiring the matching value be specified on the set generate profile token from profile token request. Profile token generation/verification does not validate the caller provided IP address is from an active network connection.

The verification ID value and remote IP address value cannot be retrieved from a profile token however they are passed to the QIBM_QSY_AUTH exit point prior to generation when the user profile has an authentication method of *REGFAC. The enhanced profile token helps to protect against replay and pre-play token attacks however, applications should consider additional protection of profile tokens used from network clients.

Generation of the Multiple-use profile token type requires enhanced profile token values to be provided in some situations. See Generate Profile Token (QSYGENPT) API under the Profile Token Type description for details.

Note: The Enhanced profile token does not require that MFA be enabled or used on the system.

Application code changes are required to take advantage of enhanced profile token protections. It is recommended that all applications be updated to use enhanced profile tokens.

Table 4. Interfaces for enhanced profile tokens

Original API	**API with enhanced parameters**
QSYGENPT	QSYGENPT, with all optional parameters
QsyGenPrfTkn	QsyGenPrfTkn2
QsyGenPrfTknE	QsyGenPrfTknE2
QSYGENFT	QSYGENFT, with same parameter values used to generate original profile token
QsyGenPrfTknFromPrfTkn	QsyGenPrfTknFromPrfTkn2, with same parameter values used to generate original profile token
QSYSETPT	QSYSETPT, with same parameters values used to generate profile token
QsySetToPrfTkn	QsySetToPrfTkn2, with same parameter values used to generate profile token

IBM i software and client application considerations

Some applications and software interfaces may fail or require client application changes when multi-factor authentication (MFA) related properties are enabled on the IBM i.

Client applications that cache or store a user's password to authenticate to the server later do not work well with MFA. The time-sensitive TOTP requirement breaks authentication for this type of application. Many applications in this category fail completely while others experience unpredictable short-term success before failing on subsequent authentications.

Incompatible examples:

- Stored password with no opportunity to prompt user for TOTP Value.
  - Current user's Encrypted password used by application to authenticate to second system that requires same user profile and password. No way to provide TOTP value to second system.
- Stored password is in password:totp format however the TOTP value has expired.

Applications that ask permission to store the password can be identified while those doing it implicitly need to be discovered through testing.

If a user has an authentication method of *TOTP and they must use an application that is not compatible with MFA, the administrator must set the user's TOTP optional interval parameter to a value other than *NONE. The optional interval should be set to as few minutes as possible to allow the password only authentication necessary to use the applications. Once the user successfully authenticates with a password and TOTP value using any interface, they will be able to authenticate using only the cached password for the duration of their active interval.

Interfaces and applications that support MFA that require explicit changes

- **IBM Toolbox for Java™**
  - If connecting to an IBM i server using user ID and password authentication, and the user profile corresponding to the user ID is using an authentication method of *TOTP, you must specify the additional authentication factor on the Java class used before connecting to the server. The AS400 class has constructors that accept an additional authentication factor.
  - IBM Toolbox for Java applications running on the IBM i that do not specify the user ID and password and expect to use the credentials of the current job may experience authentication errors if the user ID of the current job has an authentication method of *TOTP. The application will need to be modified to obtain and set the TOTP value on the AS400 object.
  - By default, enhanced profile tokens are created when an attempt is made to create a profile token and the IBM i server has support for enhanced profile tokens. You can disable the creation of enhanced profile tokens by setting the JVM option com.ibm.as400.access.AS400.useEnhancedProfileTokens to false.
  - If you have a need to create multiple AS400 objects using the same user ID, password, and TOTP value that has no optional interval, then you will need to first create an AS400 object and use the AS400 object as a parameter to the AS400 constructor that accepts an AS400 object. Otherwise, you will always need to prompt for a TOTP value.
- **IBM i Access Client Solutions (ACS)**
  - When running ACS commands directly on the IBM i (interactively or in batch) and the current job has an authentication method of *TOTP, an authentication failure will occur and ACS will prompt for a current *TOTP under either of the following conditions:
    - The optional interval is set to *NONE.
    - The optional interval is set to a positive value, but the interval is not active or has expired.

    The reason the authentication failure occurs is because the job's credentials are automatically used to authenticate without prompting. When a TOTP value is required, the job's credentials are not enough. So, the user must be prompted to provide new credentials along with a TOTP value. If this

occurs in an interactive job, the user can enter the new credentials and TOTP value. If this occurs in a batch job, the job will hang indefinitely.

- **IBM applications that do not work if the user's active interval has expired**
  - QFileSrv.400
  - NetServer
  - DRDA/DDM (Connect (SQL) does support passing password:totp)
  - Passthrough
  - QNTC
  - IBM i Access ODBC Driver
  - IBM.Data.DB2.iSeries data provider
  - IBMDA400, IDMDASQL, IBMDARLA ADO and OLE DB interfaces
  - Programmer's Toolkit, for more information, refer to API groups, header files, import libraries, and DLLs.
  - Using one of the following APIs from within an application to generate a multiple-use, regenerable profile token, or generate a multiple-use profile token without providing the verification ID and remote IP address, is not allowed:
    - Generate Profile Token (QSYGENPT) API
    - Generate Profile Token Extended (QsyGenPrfTknE) API
    - Generate Profile Token Extended (QsyGenPrfTknE2) API
    - Generate Profile Token From Profile Token (QSYGENFT) API
    - Generate Profile Token From Profile Token (QsyGenPrfTknFromPrfTkn) API
    - Generate Profile Token From Profile Token (QsyGenPrfTknFromPrfTkn2) API

Interfaces and applications that do not work with MFA

- The cluster administrative domain has been enhanced to allow the synchronization of user profiles that have authentication methods. However, most IBM i cluster operations will fail when invoked by a user with either an authentication method of *TOTP or *REGFAC. In addition, operations performed on resources monitored by the administrative domain may cause the resource to go inconsistent if the operation is invoked by a user with either an authentication method of *TOTP or *REGFAC.
- IBM Toolbox for Java, proxy server support is not supported for user profiles with an authentication method of *TOTP.
- When accessing the Network File System (NFS), if the profile the incoming request UID maps to is enabled for MFA, that access is mapped to the anonymous user for the export. The lack of true authentication through NFS is too weak for any user deemed important enough to require MFA verification.
- HTTP basic authentication employs a user name and password to authenticate a service client to a secure endpoint. In the context of the integrated web services (IWS) server, HTTP basic authentication can be provided either by the IBM HTTP Server for i that is front-ending the IWS server, or by the IWS server itself, or both. However, the IWS server does not support user profiles with an authentication method of *TOTP for web services that are deployed as protected by the IWS server and the server is using a user registry based on user profiles. You can use the HTTP Server to front-end an IWS server and it will handle authenticating passwords that contain a TOTP. If a user tries to directly connect to the IWS server and the user profile has an authentication method of *TOTP, the attempt will fail.

Network Time Protocol (NTP) time synchronization

The IBM i integrated time-based one-time password (TOTP) implementation requires the server time be in synchronization with client authenticator devices.

Minor time-drift is tolerated by the TOTP algorithm. However using the Network Time Protocol (NTP) client is recommended to keep the server and device clocks synchronized. For more information, refer to Simple Network Time Protocol.

Configuring the NTP client

- Check the QTIMADJ system value.
  - If it is set to QIBM_OS400_NTP, then the NTP client is running.
  - If it is set to *NONE, then the NTP client is not running. Start NTP services using command: **STRTCPSVR SERVER(*NTP)**.
  - If it is set to QIBM_OS400_SNTP, then the SNTP client is running instead of NTP. Change the client type by following these steps:
    1. In IBM Navigator for i, select **Network** > **Servers** > **TCP/IP Servers**.
    2. Right click on **SNTP** and select **Stop**.
    3. Right click **SNTP** and select **Properties**.
    4. Set the client to auto-start when TCP/IP is started.
    5. Click on the **Client** tab and specify client type **NTP**.
    6. Add multiple time servers reachable on your network.
    7. Click **OK** to save the changes.
    8. Right click on **SNTP** and select **Start**.
  - For more information about the QTIMADJ system value, refer to Specifying SNTP as your time maintenance application.
- For additional NTP client troubleshooting concepts, refer to Troubleshooting SNTP application.

Alternative IBM i MFA solution

IBM PowerSC provides an alternative IBM i multi-factor authentication (MFA) solution with several types of additional factors. However, it is not integrated into the operating system.

The IBM PowerSC MFA out-of-band authentication requires the user to authenticate to the out-of-band web page with one or more factors to retrieve an authentication code called a cache token credential (CTC). The PowerSC MFA agent running on IBM i changes the user profile password to be the CTC value. The user then enters the CTC value obtained from the web page as their password. IBM PowerSC MFA for IBM i is available for releases prior to IBM i 7.6. For more information, refer to *https://www.ibm.com/docs/en/powersc-mfa*.

Code license and disclaimer information

IBM grants you a nonexclusive copyright license to use all programming code examples from which you can generate similar function tailored to your own specific needs.

SUBJECT TO ANY STATUTORY WARRANTIES WHICH CANNOT BE EXCLUDED, IBM, ITS PROGRAM DEVELOPERS AND SUPPLIERS MAKE NO WARRANTIES OR CONDITIONS EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, REGARDING THE PROGRAM OR TECHNICAL SUPPORT, IF ANY.

UNDER NO CIRCUMSTANCES IS IBM, ITS PROGRAM DEVELOPERS OR SUPPLIERS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1. LOSS OF, OR DAMAGE TO, DATA;
2. DIRECT, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; OR
3. LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, SO SOME OR ALL OF THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Programming interface information

This publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Linux® is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Oracle, Inc. in the United States, other countries, or both.

Other product and service names might be trademarks of IBM or other companies.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Product Number: 5770-SS1