

axians

# Multi Factor Authentication (MFA) on IBM i

---

2026

VINCI  
ENERGIES

# Overview

- ▶ About me and the CEAC
- ▶ Password security
- ▶ New OS USRPRF with R760
- ▶ MFA as an integrated part of the OS R760
- ▶ Prerequisites
- ▶ Implementation native OS or via IBM Navigator for I
- ▶ SST/DST
- ▶ Standards and Links




# About the speaker

Katharina Karner

- ▶ Started 2000 at IBM AS400 Hotline
- ▶ Specialization in software HA solutions (MIMIX, iTERA, Quick-EDD, iCluster, Maxava HA etc.)
- ▶ Member of the CEAC since 2024



CEAC (Common   
Europe Advisory  
Council)  
Member



IBM i

# CEAC (Common Europe Advisory Council)

<https://comeur.org/what-is-ceac/>

- ▶ Mission: dialogue with IBM on strategic and long-term issues
- ▶ Organisation: part of Common Europe, members are IT professionals with extensive IBM I experience
- ▶ Our work:
  - Monthly online meetings to discuss IBM ideas with IBM liaison, give updates about enhancements and roadmap presentations
  - Face to face meetings twice a year, usually follow on from the Common conferences. Key members from IBM also attend this event.
- ▶ Our motivation: dedication to IBM i as the membership is on a voluntary basis only.

# CEAC / IBM i Customer Council Ideas Portal

<https://ibm-power-systems-cc.ideas.ibm.com/ideas/>



IBM Power Systems - Customer Council Ideas Portal

Search all ideas...

+ ADD A NEW IDEA

My ideas	0
My votes	3
My proxy votes	0
My subscriptions	0

FILTER BY CATEGORY

Cloud Management Console	60
HMC	443
IBM i	3252
AI with IBM i	7
Application Development	123
BRMS	74
Core OS	129
Db2 for i	454
Db2 Mirror	3
Db2 Web Query	20
Documentation	11

All ideas

- 3** **Always update current user in PSDS after profile swap.**

**VOTE** Swapping user profiles [1] is a common technique for CGI programs and other service oriented programs to make sure the program runs under the right p  
Guest 2 days ago in IBM i / Application Development 3 **Not under consideration**
- 11** **Adding the option to specify a Sender address to the command SNDSMTPEMM**

**VOTE** For years now IBM i lacking a command to specify the sender mail address in a simple manner. Yes there is an API but this is too complicated for the aver  
Rudi Van Helvoirt 11 days ago in IBM i / Core OS 0 Submitted
- 1** **trim (leading and trailing) blanks from input in HMC search fields**

**VOTE** Currently the 'Partitions' or 'Systems' search field filters for an exact match in the HMC Web GUI.As a consequence leading or trailing blanks do matter, bu  
Guest 2 days ago in HMC 0 Submitted
- 2** **Add a new category under IBM Navigator for i, with the ability to plug in user-defined SQL for result sets and charts, similar to way s**

**VOTE** This idea would allow system admins to build up a list and provide useful site-specific, SQL inquiry/review capability for their users, via custom SQL queri  
Guest 3 days ago in IBM i / Web Serving 0 Submitted
- 29** **add CLI option to GUI-feature : "Schedule-management" jobs**

**VOTE** setting up "Schedule-management" jobs is currently a GUI-only feature. (V11R1M1111) add a CLI functionality to this feature. and a clear logging/messagiri  
Guest about 1 month ago in HMC 1 Submitted
- 95** **Fixcentral Downloads of Machine Code updates are limited to 25 per day, Automate request to download beyond the stated limit**

CONFIDENTIAL USE

# Password security

## 2023 Password Cracking Times with Brute Force Program

Number of characters	Just numbers	Lowercase letters	Uppercase and lowercase letters	Numbers, uppercase and lowercase letters	Numbers, Letters & Symbols
6	Right away	Right away	Right away	Right away	Right away
7	Right away	Right away	1 second	2 seconds	4 seconds
8	Right away	Right away	28 seconds	2 minutes	5 minutes
11	Right away	32 minutes	1 month	10 months	3 years
12	1 second	14 hours	6 years	53 years	226 years
14	52 seconds	1 year	17,000 years	202,000 years	1 million years
18	6 days	481,000 years	126 billion years	2 trillion years	26 trillion years

C1-Internal Source: <https://www.oberlin.edu/cit/bulletins/passwords-matter>

# New user profiles on OS R760

Non-changeable users for OS functions

Mit Benutzerprofilen arbeiten

Auswahl eingeben und Eingabetaste drücken.

1=Erstellen 2=Ändern 3=Kopieren 4=Löschen 5=Anzeigen

12=Mit Objekten eines Eigners arbeiten

Ausw	Benutzerprofil	Text
___	QPGMR_NC	Nicht änderbares QPGMR-Profil
___	QSECOFR_NC	Nicht änderbares QSECOFR-Profil
___	QSYSOPR_NC	Nicht änderbares QSYSOPR-Profil
___	QUSER_NC	Nicht änderbares QUSER-Profil

QSTRUP continues to run under QPGMR

C1-Internal Use

# Benefits of Integrated MFA Implementation on IBM I

- ▶ Multi-factor authentication (MFA) adds an additional authentication factor to password authentication to verify your identity.
- ▶ The IBM i integrated MFA solution includes a time-based one-time password key (TOTP).
- ▶ Integrated with IBM i 7.6 operating system, no additional software required
- ▶ Compatible with many TOTP client authenticators
- ▶ The Service Tools User Profiles for SST and DST are also supported.
- ▶ Universal Authentication Exit Point: (QIBM\_QSY\_AUTH)
- ▶ Third-party MFA solutions can be used to integrate into heterogeneous landscapes

## Prerequisites

- ▶ POWER 10 Hardware and IBM i Release 7.6
- ▶ TLS Transport Layer Security must be configured and enabled
- ▶ Security Level 40 oder 50 - SYSVAL(QSECURITY)
- ▶ The password level must be set to 4 - SYSVAL(QPWDLVL)
  - Do a SAVSECCDTA before changing the values, no undo button.
- ▶ MFA Function Activation - CHGSECA ADLSGNFAC(\*ENABLED)
- ▶ An IPL is required to enable the MFA feature.
- ▶ Since the system requires an accurate time for TOTP, NTP (Network Time Protocol) should be used as the client. CFGTCPAPP (\*NTP)

# Transport Layer Security (TLS) Configuration

IBM Navigator for i

Search ut23p97 timmr

- Dashboard
- Home
- Work Management
- Configuration and Service
- System
- Monitors
- My Work
- Network**
- Security
- Users and Groups
- Performance
- File System
- Content Manager OnDemand for i
- Bookmarks
- Serviceability

### TLS Configuration

Actions

Server Name	Status	TLS Port	TLS Port Active	Unsecure Port	Unsecu
> Central Host Server	Started	9470	Active	8470	Active
> Database Host Server	Started	9471	Active	8471	Active
> Data Queue Host Server	Started	9472	Active	8472	Active
	Started	9473	Active	8473	Active
	Started	9474	Active	8474	Active
	Started	9475	Active	8475	Active
	Started	9476	Active	8476	Active
	Started	9480	Active	0	Inactive

Total Rows: 8 << < 1 > >> 100

**Network**

- > TCP/IP Configuration
- ▼ Servers
  - TCP/IP Servers
  - IBM Host Servers
  - DNS Servers
  - User-Defined Servers
  - Alternative Subsystem Routing
  - TLS Configuration**
- > IP Policies
- > Web Administration

Network Attributes

# QPWDLVL 4

Careful examination required

Berechtigte Benutzer anzeigen

Benutzer- profil	Gruppen- profil	Kennwort zuletzt geändert	Kennwort Stufe 0 oder 1	Kennwort Stufe 2 oder 3	Kennwort Stufe 4	Lok. Knwrt verw.
JOGS		23.06.25	*NO	*NO	*YES	*YES
KKARNER		25.06.25	*NO	*NO	*YES	*YES
QANZAGENT		23.06.25	*NO	*NO	*NO	*YES
QAUTPROF		23.06.25	*NO	*NO	*NO	*YES
QBRMS		23.06.25	*NO	*NO	*NO	*YES
QCLUMGT		23.06.25	*NO	*NO	*NO	*YES
QCLUSTER		23.06.25	*NO	*NO	*NO	*YES
QCOLSRV		23.06.25	*NO	*NO	*NO	*YES
QDBSHR		23.06.25	*NO	*NO	*NO	*YES
QDBSHRDO		23.06.25	*NO	*NO	*NO	*YES

- ▶ In QPWDLVL 4, all passwords of password level 0-1 are deleted, level 2-3 if no implementation is possible.
- ▶ If the user profile does not have a password that can be used at password level 4, the password is \*NONE after the QPWDLVL system value is set to 4.
- ▶ Password level 4 is a one-way password encryption algorithm.
- ▶ Testing with DSPAUTUSR +F11 or PRTUSRPRF TYPE(\*PWDLVL).
- ▶ Recommendation: run **SAVSECDATA** prior to any conversion.

# SIGNON Screen

If the Signon screen is adjusted, the program must be updated

## QSYS/QAWTSSRC

Sources for Signon

```

Mit Teildateien arbeiten (mittels PDM)
Datei . . . . . QAWTSSRC
Bibliothek . . . . . QSYS          Listenanfang bei . . . . .
Auswahl eingeben und Eingabetaste drücken.
2=Editieren   3=Kop.   4=Lösch. 5=Anzeigen   6=Drucken
8=Beschreibung anz.   9=Sich. 13=Text ändern 14=Umwand.

Ausw. Teildatei  Art      Text
--- QDSIGNON    _____
--- QDSIGNON2   _____
--- QDSIGNON3   _____
    
```

## SIGNON SCREEN

Additional Signon Factor \*ENABLED

```

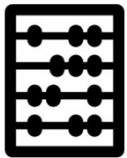
Sign On
System . . . . . : I7075041
Subsystem . . . . : QINTER
Display . . . . . : QPADEV0002

User . . . . . _____
Password . . . . . _____

Program/procedure . . . . . _____
Menu . . . . . _____
Current library . . . . . _____
Additional factor . . . . . _____
    
```

# How a TOTP algorithm works

TOTP generates a one-time password that changes regularly



A key is generated at the host



The generated OPT is entered

The algorithm calculates the validity, based on key and timestamp



The key is imported into the client

A timestamp gives a time value

HMAC calculation of a digit based on the common key and timestamp



# TOTP Clients

Some examples

- SAP Authenticator** (Wirtschaft)
- TOTP Authenticator** (2FA Authentifizierungs App)
- RSA Authenticator (Se...)** (Wirtschaft)
- Authentifizierungs App** (Zwei Faktor Authentifizierung)
- Open Authenticator by...** (An open-source TOTP manager)
- Entrust Identity** (Wirtschaft)
- Microsoft Authenticator** (Schützt Ihre Online-Identität.)
- TOTP Authenticator - O..** (Soziale Netze)
- Authenticator** (Dienstprogramme)
- OpenOTP Token** (Dienstprogramme)
- FortiToken Mobile** (Wirtschaft)
- Google Authenticator** (Dienstprogramme)
- Authentifizierungs App...** (MFA Authenticator - OTP, TOTP)
- OTP Authenticator - TO...** (Dienstprogramme)
- 2FA Authenticator (2FA...** (#1 Rated 2FA Authenticator)
- Duo Mobile** (Sicherheit leicht gemacht)
- OTP Auth** (2-Faktor-Auth für Pros)
- TOTP Authenticator: 2F...** (Authentifizierungs - MFA Auth)
- Authenticator App...** (Dienstprogramme)
- FreeOTP Authenticator** (Dienstprogramme)
- SafeNet MobilePASS+** (Thales Group)
- 2FA Authenticator: TOT...** (Authentifizierungs - MFA Auth)
- easy Login TOTP App** (Dienstprogramme)

C1-Internal Use

# Generating the key

CHGTOTPKEY \*GEN is performed by the user

```
TOTP key . . . . . : FQT4 JVFV IPSL G5F0 43YP EEEF 7LIQ QD6N  
Copy/paste version . . : FQT4JVFVIPSLG5F043YPEEEF7LIQQD6N
```

```
Recovery key . . . . . : CC92F6DDF43AF5D6B95C817547FF39D3  
9F269CE7B88ED580CD496220F6225297
```

The TOTP key has been saved in your profile. It must also be entered into your TOTP generator client application, without the blanks.

Save the recovery key for this TOTP key in a safe place.

# Set up TOTP

## Example Google Authenticator

< Zurück    Kontodaten eingeben

Kontoname

TESTMFA

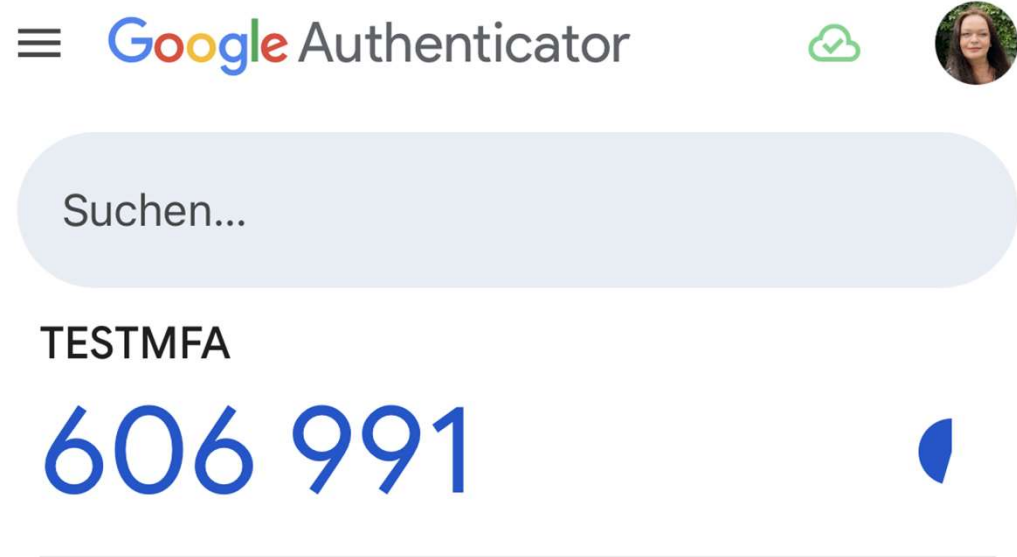
Mein Schlüssel

\*\*\*\*\*

Schlüsseltyp

Zeitbasiert

Hinzufügen



# CHGUSRPRF by sysadmin

Activate TOTP, user by user

## Benutzerprofil ändern (CHGUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Authentifizierungsmethoden . . .	<u>*TOTP</u>	←	*SAME, *NONE, *TOTP, *REGFAC
Optionales TOTP-Intervall . . .	<u>1</u>	←	1-720, *SAME, *NONE
Maximale Anmeldeversuche . . .	<u>*SYSVAL</u>		1-25, *SAME, *SYSVAL
Einheitensitzungen begrenzen . .	<u>*SYSVAL</u>		*SAME, *SYSVAL, *YES, *NO...
Tastaturpufferung . . . . .	<u>*SYSVAL</u>		*SAME, *SYSVAL, *NO...
Max. zulässiger Speicher-groß . .	<u>*NOMAX</u>		
Maximal zulässiger Speicher . .	<u>*SAME</u>		Kilobyte, *SAME, *NOMAX
Höchste Planungspriorität . . .	<u>?</u>		0-9, *SAME

Optional TOTP interval: \*NONE = a token is required every time you log in. Number = minutes until a new token is requested.

# MFA is active

```
                Sign on
                System . . . . . : I7075041
                Subsystem . . . . . : QINTER
                Display . . . . . : QPADEV0003



User . . . . . TESTMFA
Password . . . . .

Program/procedure . . . . . _____
Menu . . . . . _____
Current library . . . . . _____
Additional factor . . . . . 368892
```

# CHGUSRPRF via Navigator for I

## MFA Key Setup by User

IBMI-76.IBM-TCE-CLOUD.COM  test3

 Warnung: This profile has been restricted through function usage ID QIBM\_NAV\_ALL\_FUNCTION and has no further access to Navigator. Login with a user that has the required authority or contact your administrator for more access. 

### Eigenen MFA-Schlüssel

Verwalten Sie den Mehrfaktorauthentifizierungsschlüssel (MFA) für den Benutzer, der momentan bei der GUI angemeldet ist. Der MFA-Schlüssel kann nur vom angemeldeten Benutzer generiert, angegeben, entfernt oder validiert werden. Dieser MFA-Schlüssel ist ein TOTP-Schlüssel (Time-Based One-Time Password), der mit einer Clientanwendung verwendet wird, um einen MFA-Code zu generieren. Der MFA wird dann mit dem Benutzer und dem Kennwort paarweise verbunden, wenn die Authentifizierung bei einem System erfolgt, das MFA nutzt.

#### Für dieses Benutzerprofil ist kein MFA-Schlüssel vorhanden

- MFA-Schlüssel und Wiederherstellungsschlüssel für dieses Benutzerprofil generieren und speichern
- Geben Sie einen MFA-Schlüssel aus Ihrer Clientgeneratoranwendung ein.
- MFA-Schlüssel für dieses Benutzerprofil entfernen
- Überprüfen Sie, ob der MFA-Code und das Kennwort für dieses Benutzerprofil ordnungsgemäß funktionieren.

[Weiter](#)

# QIBM\_NAV\_ALL\_FUNCTION

Adjusting the Permission When the Functional Error Is Reported

**Warnung:** This profile has been restricted through function usage ID QIBM\_NAV\_ALL\_FUNCTION and has no further access to Navigator. Login with a user that has the required authority or contact your administrator for more access.

IBM Navigator for i Suchen

- Dashboard
- Startseite
- Arbeitsmanagement
- Konfiguration und Service
- System
- Überwachungen
- Meine Arbeit
- Netzwerk
- Sicherheit

### Funktionsnutzung

Aktionen

Funktions-ID <span style="float: right;">⌵ ⌶</span>	Funktionsname <span style="float: right;">⌵ ⌶</span>	Standardnutzung <span style="float: right;">⌵ ⌶</span>	Anzeiger für alle Objekte <span style="float: right;">⌵</span> ⌵ ⌶	Zugelassene/Abgele <span style="float: right;">⌵ ⌶</span>
QIBM_NAV_AJS	ADVANCED JOB SCHEDULER	ALLOWED	USED	NO
QIBM_NAV_ALL_FUNCTION	USE OF IBM NAVIGATOR FOR i FUNCTIONS	DENIED	USED	YES
QIBM_ACS_HTTP_PROXY	HTTP PROXY	DENIED	NOT USED	NO
QIBM_ACS_HTTP_PROXY_OSPM	OSPM HTTP PROXY	DENIED	USED	NO
QIBM_QSY_DISPLAY_PWDRULES	Display password rules	ALLOWED	USED	NO
QIBM_LIST_ALL_OBJS	List all objects	DENIED	USED	NO
QIBM_LIST_ALL_OBJS_SQL	List all objects in SQL	DENIED	USED	NO

IBM Tivoli Directory Server Administrat

# QIBM\_NAV\_ALL\_FUNCTION

Adjusting Permission via Navigator or WRKFCNUSG

**Funktionsnutzung ändern** ✕

Funktions-ID	Beschreibung	Standardnutzung	Anzeiger für alle Objekte
QIBM_NAV_ALL_FUNCTION	USE OF IBM NAVIGATOR FOR i FUNCTIONS	DENIED	USED

Nutzungsoptionen für die ausgewählten Funktions-IDs

Standardberechtigung: Abgelehnt ▼

Sonderberechtigung \*ALLOBJ: Verwendet ▼

Verwendungsoptionen für angegebene Benutzer- und Gruppenprofile für die ausgewählte Funktion

Profil(e):  Profile durchsuchen

**Zugriff zulässig**

TEST2

WIGUENTH

**Zugriff verweigert**

Hinzufügen
Entfernen

OK
Abbrechen

```

Mit Funktionsnutzung arbeiten
Auswahl eingeben und Eingabetaste drücken.
2=Nutzung ändern 5=Nutzung anzeigen

Auswahl Funktions-ID Funktionsname
- QIBM_SERVICE_DUMP Service-Speicherauszug
- QIBM_SERVICE_JOB_WATCHER JOB WATCHER
- QIBM_SERVICE_THREAD Threadsteuerung
- QIBM_SERVICE_TRACE Service-Trace
- QIBM_SERVICE_WATCH Serviceüberwachung
- QIBM_NAV_AJS ADVANCED JOB SCHEDULER
2 QIBM_NAV_ALL_FUNCTION USE OF IBM NAVIGATOR FOR i FUNCTIONS
- QIBM_NAV_CONF_SRV CONFIGURATION AND SERVICE
- QIBM_NAV_CUSTOM_CHARTS CUSTOM CHARTS
- QIBM_NAV_FILE_SYSTEM FILE SYSTEM
- QIBM_NAV_FS_DOWNLD FILE SYSTEM DOWNLOAD

Parameter für Auswahl 2 oder Befehl
===>
F3=Verlassen F4=Bedienerführung F5=Aktualisieren F9=Auffinden
F12=Abbrechen F17=Anfang F18=Ende

Weitere ...
    
```

# Set up MFA keys

## IBM i Navigator, creating the MFA key by users

TESTKTKA - Eigenschaften



**Benutzer:**

Name \*:

Beschreibung:

Klasse:

Benutzer aktivieren

**Kennwort:**

Kennwort:

Benutzer muss Kennwort beim nächsten Anmelden ändern

**Zusätzliche Authentifizierungsoptionen:**

MFA-Authentifizierung mit einem TOTP-Schlüssel

Bevor der zusätzliche Faktor auf \*TOTP gesetzt wird, muss ein MFA-Schlüssel vorhanden sein.

MFA-Schlüssel vorhanden: NO

Zuletzt geändert:

**MFA-Schlüssel für dieses Benutzerprofil ändern**

ein, sich für dieses Benutzerprofil auszugeben, ohne vorher eine zusätzliche Authentifizierung durchzuführen, indem Sie die Funktionsverwendungs-ID QIBM\_RUN\_UNDER\_USER\_NO\_AUTH für dieses Profil auf Verweigert setzen

**MFA-Schlüssel ändern**



**Ablauf des Benutzerprofils:**

Ablaufdatum für Benutzerprofil:

**Zusätzliche Benutzereinstellungen:**

- Gruppen
- Möglichkeiten
- Jobs
- Netzwerke
- Persönlich

OK

Abbrechen

# Set up MFA keys

## IBM i Navigator

IBM Navigator for i



Suchen



I7075041



kkarner



Dashboard



Startseite



Arbeitsmanagement



Konfiguration und Service



System



Überwachungen



### Eigenen MFA-Schlüssel verwalten

Verwalten Sie den Mehrfaktorauthentifizierungsschlüssel (MFA) für den Benutzer, der momentan bei der GUI angemeldet ist. Der MFA-Schlüssel kann nur vom angemeldeten Benutzer generiert, angegeben, entfernt oder validiert werden. Dieser MFA-Schlüssel ist ein TOTP-Schlüssel (Time-Based One-Time Password), der mit einer Clientanwendung verwendet wird, um einen MFA-Code zu generieren. Der MFA-Code wird dann mit dem Benutzer und dem Kennwort paarweise verbunden, wenn die Authentifizierung bei einem System erfolgt, das MFA nutzt.

#### Für dieses Benutzerprofil ist kein MFA-Schlüssel vorhanden

- MFA-Schlüssel und Wiederherstellungsschlüssel für dieses Benutzerprofil generieren und speichern
- Geben Sie einen MFA-Schlüssel aus Ihrer Clientgeneratoranwendung ein.
- MFA-Schlüssel für dieses Benutzerprofil entfernen
- Überprüfen Sie, ob der MFA-Code und das Kennwort für dieses Benutzerprofil ordnungsgemäß funktionieren.

[Weiter](#)

# Set up MFA keys

## IBM i Navigator


**MFA-Schlüssel validieren und Wiederherstellungsschlüssel speichern** ×

Der neue MFA-Schlüssel wurde in Ihrem Benutzerprofil gespeichert. Überprüfen Sie, ob der MFA-Code die Anmeldung dieses Benutzerprofils zulässt, und speichern Sie dann den Wiederherstellungsschlüssel.

**1. Gespeicherter MFA-Schlüssel:**  
 Geben Sie mithilfe Ihrer Clientgeneratoranwendung unten den MFA-Schlüssel ein (ohne Leerzeichen), oder scannen Sie den QR-Code

CAQXGCQE QMJY RGTB TEPZ NT6K XTR7 OEY2 📄

CAQX GCQE QMJY RGTB TEPZ NT6K XTR7 OEY2



**2. MFA-Schlüssel validieren:**  
 Geben Sie Ihr Benutzerprofilkennwort und den MFA-Code aus Ihrer Clientgeneratoranwendung ein, um zu überprüfen, ob sich Ihr Benutzerprofil mit MFA anmelden kann.

Kennwort:

MFA-Code:

Überprüfen

**3. Wiederherstellungsschlüssel:**  
 Speichern Sie den Wiederherstellungsschlüssel an einem sicheren Ort. Er kann anstelle des Benutzerkennworts als Einmalige Wiederherstellung verwendet werden, wenn der MFA-Schlüssel und der Code nicht funktionieren.

F6D3EA8C4ED51ABBD4E7489B8CCAA2E5BBE0D4FC45BDE8F073D2D6E61B8CA87 📄 📄

OK

Google Authenticator 🔄 👤

Suchen...

TESTMFA

905 511 ▶

I7075041.AXIANSTEST.LOCAL, kkarner

374 287 ▶



# Validate MFA key


## IBM i Navigator


**Eigenen MFA-Schlüssel verwalten**


Verwalten Sie den Mehrfaktorauthentifizierungsschlüssel (MFA) für den Benutzer, der momentan bei der GUI angemeldet ist. Der MFA-Schlüssel kann nur vom angemeldeten Benutzer generiert, angegeben, entfernt oder validiert werden. Dieser MFA-Schlüssel ist ein TOTP-Schlüssel (Time-Based One-Time Password), der mit einer Clientanwendung verwendet wird, um einen MFA-Code zu generieren. Der MFA-Code wird dann mit dem Benutzer und dem Kennwort paarweise verbunden, wenn die Authentifizierung bei einem System erfolgt, das MFA nutzt.


**Für dieses Benutzerprofil ist ein MFA-Schlüssel vorhanden. Letzte Änderung am: 2025-08-19 13:23:56**

- MFA-Schlüssel und Wiederherstellungsschlüssel für dieses Benutzerprofil generieren und speichern
- Geben Sie einen MFA-Schlüssel aus Ihrer Clientgeneratoranwendung ein.
- MFA-Schlüssel für dieses Benutzerprofil entfernen
- Überprüfen Sie, ob der MFA-Code und das Kennwort für dieses Benutzerprofil ordnungsgemäß funktionieren.

Kennwort:  

MFA-Code:  





# Enable MFA by SYSADMIN

## IBM i Navigator

The screenshot shows the IBM Navigator for i interface. On the left is a navigation sidebar with icons for Dashboard, Startseite, Arbeitsmanagement, Konfiguration und Service, System, Überwachungen, Meine Arbeit, Netzwerk, Sicherheit, Benutzer und Gruppen, Leistung, Dateisystem, Lesezeichen, and Servicefreundlichkeit. The main area is titled 'Benutzer' and contains a table of users. The table has columns for 'Profilart', 'Name', 'Profilstatus', and 'NetServer'. A row for user 'TESTKTKA' is highlighted in blue, with 'User' in the 'Profilart' column and '\*ENABLED' in the 'Profilstatus' column. A context menu is open over this row, listing various actions. The action 'Benutzer für die MFA-Authentifizierung aktivieren' is highlighted in blue, and a red arrow points to it from the right.

Profilart	Name	Profilstatus	NetServer
User	TESTKTKA	*ENABLED	

- Neuer Benutzer (basierend auf) TESTKTKA
- Löschen
- Auf System kopieren
- Disable on System
- Nachricht senden
- Benutzerobjekte >
- Benutzer für die MFA-Authentifizierung aktivieren**
- Benutzer für die Authentifizierung des Exit-Programms freigeben
- Benutzerfunktion auf Verweigert setzen
- Berechtigungsdatensammlung
- Eigenschaften

# CHGUSRPRF

## Activate TOTP, user by user

Das Intranetportal der Axians | Benutzer

Nicht sicher | i7075041:2002/Navigator/mainframe/user-and-groups/users?sortField=useTotpAuthentication&sortOrder=-1

IBM Navigator for i

Suchen | i7075041 | kkarmer

**Benutzer**

Aktionen

Details: Basic All

Name	MFA-Schlüssel vorhanden	MFA-Authentifizierung	Kennwortstufe_2_3
TESTKTKA	YES	YES	YES
TESTMFA	YES	YES	YES
JOGS	NO	NO	YES
KKARNER	NO	NO	YES
QANZAGENT	NO	NO	
QAUTPROF	NO	NO	
QBRMS	NO	NO	
QCLUMGT	NO	NO	
QCLUSTER	NO	NO	
QCOLSRV	NO	NO	
QDBSHR	NO	NO	
QDBSHRDO	NO	NO	
QDFTOWN	NO	NO	
QDIRSRV	NO	NO	
QDLFM	NO	NO	
QDOC	NO	NO	
QDSNX	NO	NO	
QEJB	NO	NO	
QEBSVR	NO	NO	

# MFA is active

Entering the second factor or recovery key



>Welcome to IBM Navigator for i

User Name:

Password:

Additional Factor:

Log in

A red arrow points from the 'Additional Factor' label to the corresponding input field.

## SST/DST MFA

Regardless of the implementation MFA on IBM i

- ▶ System values QDATE, QTIME and QTIMZON must be correct
- ▶ Use of NTP (Network Time Protocol) recommended
- ▶ No period for the validity of the TOTP value, so a token is required every time you log in
- ▶ Function also available in a restricted state

# SST/DST MFA

## Setup

```

Work with Service Tools Security Options
System: I7075041

Console control options
  Display console status screen . . . . . 0 0=No,1=Yes
  Allow console device F18 take over . . . . 1 0=No,1=Yes
Sign-on control and options
  Additional sign-on factor enabled . . . . . 1 0=No,1=Yes ←
  Password expiration interval in days . . . 180 0-366
  Maximum sign-on attempts allowed . . . . . 3 2-15
  Duplicate password control . . . . . 18 0-31
  Block password change . . . . . 0 0-99 hours
  Maximum password length . . . . . 128 1-128
  Minimum password length . . . . . 6 1-128
Password rules
  Limit adjacent character . . . . . 0 0=No,1=Yes
  Limit repeating characters . . . . . 0 0=No,1=Yes
  Limit same password character positions . . 0 0=No,1=Yes
  Limit profile name . . . . . 0 0=No,1=Yes

Enter changes and press Enter or
Press F10 to work with additional password rules.
Press F3 to exit or F12 to return.
    
```

### SST

Option 8 = Service Tools Server Security and Devices

Option 5 = Security options of the service tools

### DST

Option 5 = Work with DST

Option 4 = Safety data

Option 7 = Utilities security options

DSPSSTSECA for testing

# SST/DST MFA

## User Setup

```

Work with Service Tools User IDs                               System:  I7075041
Type option, press Enter.
 1=Create           2=Change password           3=Delete
 4=Display          6=Change profile attributes
 7=Change privileges 8=Change TOTP key ←
Opt User ID      Description                      Status
--
  KKARMERMFA      Enabled
 8 KKARNER        Enabled
  QSECOFR         QSECOFR      Enabled
  QSRV            QSRV         Disabled

F3=Exit  F5=Refresh  F12=Cancel
    
```

### SST

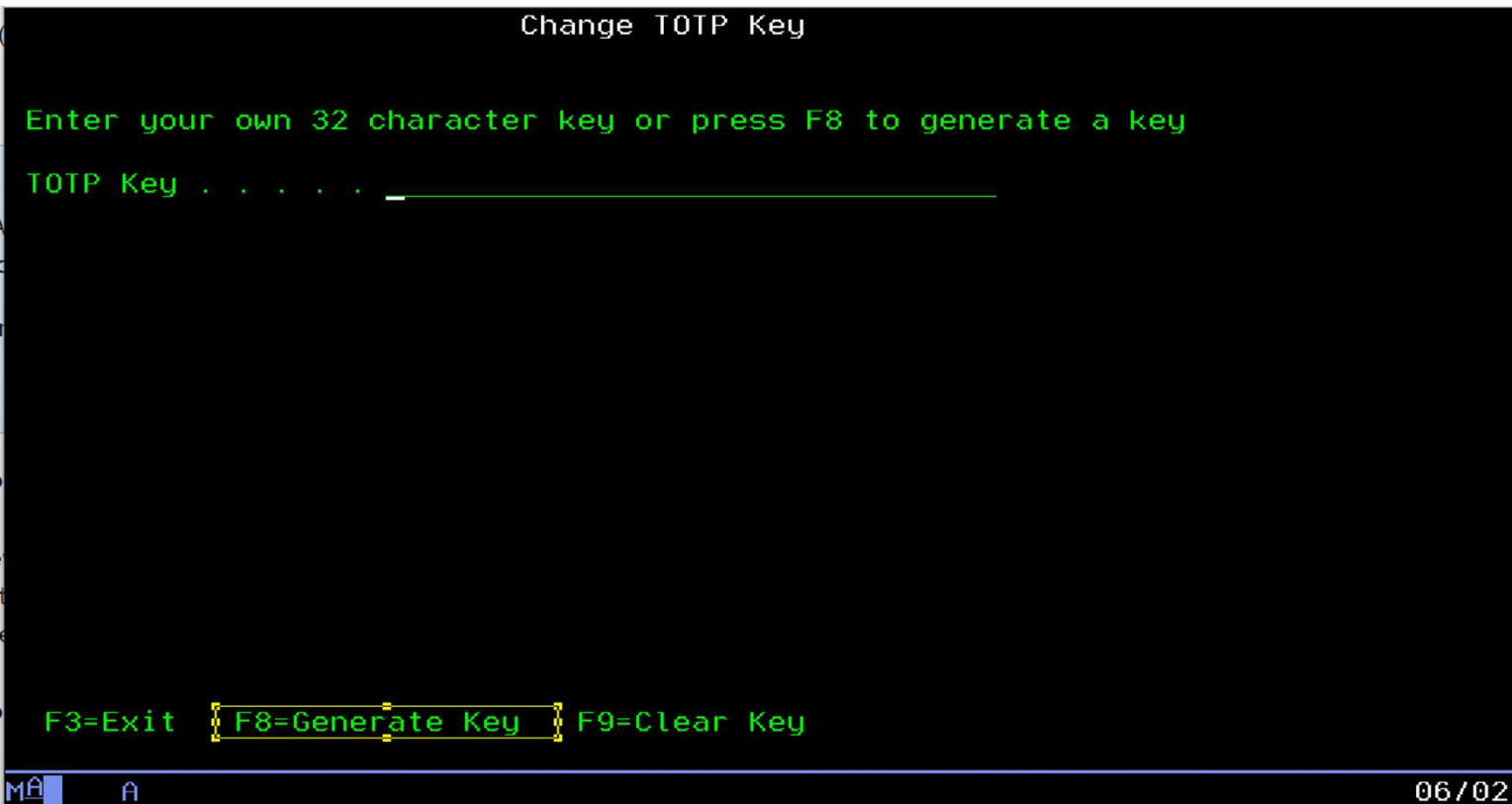
Option 8 = Service Tools Server Security and Devices

Option 1 = Service Tools User IDs

Option 8 = Change TOTP key

# SST/DST MFA

## User Setup



SST

F8 = Generate Key

# SST/DST MFA

## User Setup

```
TOTP Key

TOTP key:
KXP3 KN77 QNLX UZST NSKE SJ44 2RZS 3UTY
Copy and paste version:
KXP3KN77QNLXUZSTNSKESJ442RZS3UTY
Recovery key:
BBDH6HF2A736GCAA6F76ACA42262B7D7E9776A96B2289C6EB4HC332B52HAEE2B

This key must be entered into your TOTP generator client
application, without the blanks.

Save the recovery key for this TOTP key in a safe place.

Press ENTER to verify the key and accept.

F3=Exit
```

Add to Authenticator as usual

< Zurück Kontodaten eingeben

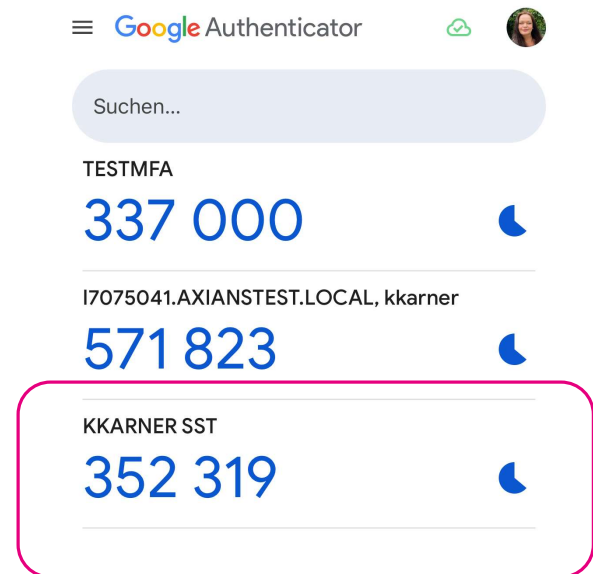
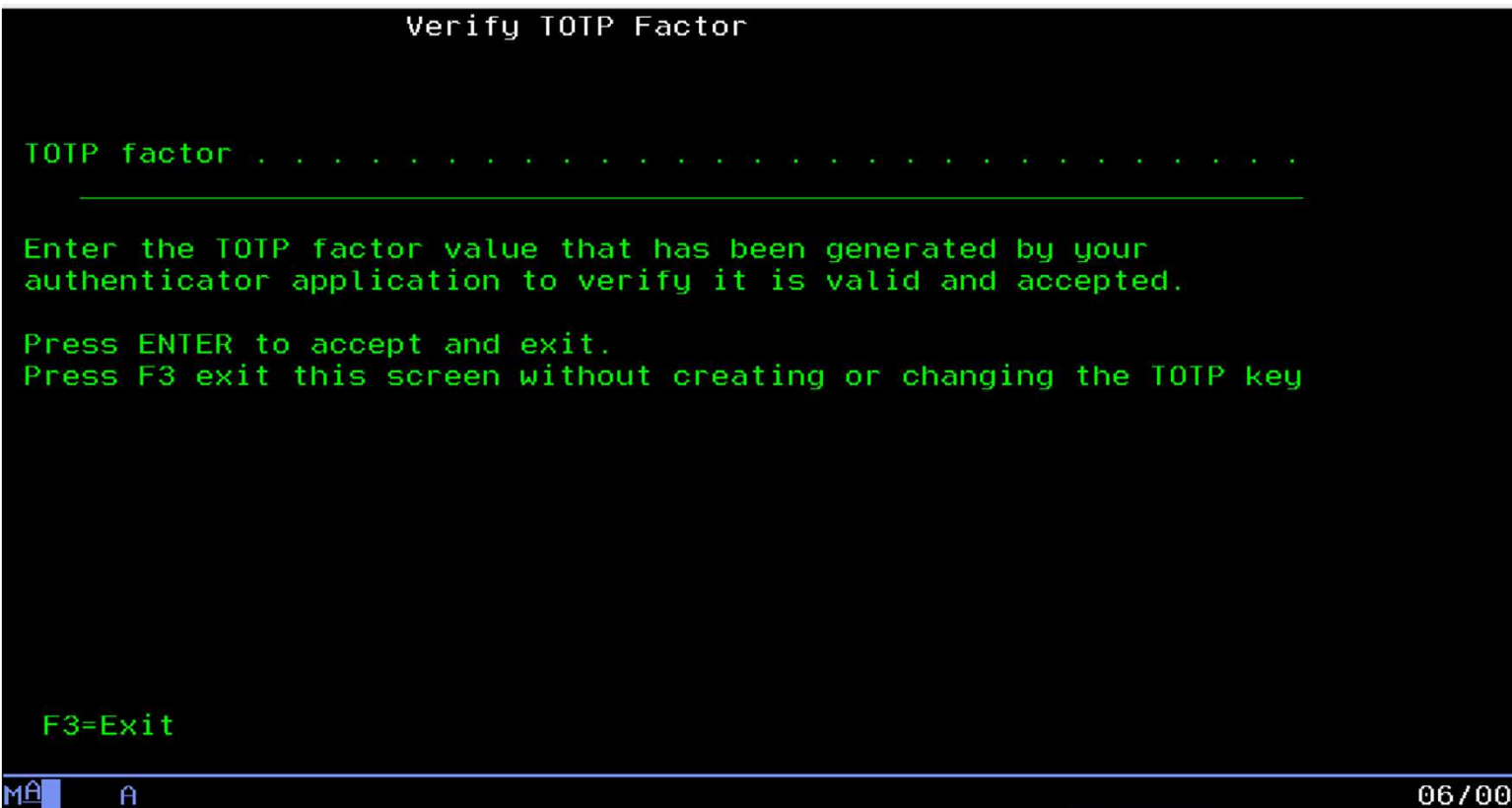
Kontoname

Mein Schlüssel

Schlüsseltyp

# SST/DST MFA

## User Setup



# SST/DST MFA

## User Setup

Display Service Tools User ID

System: I7075041

```
Service tools user ID name . . . . . : KKARNERMFA
Previous sign-on . . . . . : 04.09.25 13:46:30
Password verification not valid . . . . . : 0
Status . . . . . : Enabled
Date password last changed . . . . . : 04.09.25
System date password expires . . . . . : 03.03.26
User date password expires . . . . . : None
Password is set expired . . . . . : No
TOTP key exists . . . . . : Yes
Authentication method . . . . . : TOTP

Linked user profile . . . . . : TESTMFA
Description . . . . . : MFA TEST
```



Anmelden mit STRSST (Start Service Tools)

SYSTEM: I7075041

Benutzer-ID f. Service-Tool. \_\_\_\_\_  
Kennwort f. Service-Tools . \_\_\_\_\_

Zusätzlicher Faktor. . . . . \_\_\_\_\_

Hinweis: Groß-/Kleinschreibung von Kennwort muss beachtet werden.

F3=Beenden F9=Kennwort ändern F12=Abbrechen

# Interfaces without a second factor

## Solutions

- ▶ Password with attached MFA key
- ▶ A colon serves as a separation between password (:) and MFA value
- ▶ Example: `ssh testusr@ibmiktkka my$ecretPassw0rd:123456`
- ▶ ODBC or JDBC interfaces:  
If passwords are stored in configuration files or used in automated jobs, an administrator must review these settings and update them if necessary, see Redbook [IBM i 7.6 Features and Functions](#)

## Host Connection Servers

- ▶ Problem: ACS/Navigator can establish a large number of individual host-server connections
  - Depending on whether a stored PWD is used in the client
  - User with Saved Interval Required (TOTPOPTITV)
- ▶ Solution: New Host Connection Server
  - As a front-end for existing host servers
  - Requires TLS, uses port 9480
  - Persistent TOTP/MFA authenticated connection, all subsequent host-server connections are established through this connection
- ▶ ACS 1.1.9.7, Navigator, DCM and other tools use HCS, also works without an optional interval.

# QIBM\_RUN\_UNDER\_USER\_NO\_AUTH

## Function Usage ID (CHGFCNUSG)

### ► Problem

- The ability to perform actions as a different user profile based only on the permission for that user profile is contrary to MFA principles.
- IBM i's built-in MFA TOTP implementation enables this password bypass due to widespread usage

### ► IBM i Solution

- Optional blocking of applications that bypass the entry of credentials for a user
- A user's entry in (QIBM\_RUN\_UNDER\_USER\_NO\_AUTH) prevents that user profile from being the target of a "Run Under" operation.
- Use is recommended with an MFA/TOTP user profile  
QIBM\_RUN\_UNDER\_USER\_NO\_AUTH does not require a TOTP/MFA configuration for the user or the system

# QIBM\_QSY\_AUTH (\*REGFAC)

## Single authentication exit point (WRKREGINF)

### ► Problem

- The MFA-TOTP implementation built into IBM i may not work with existing enterprise-level MFA solutions used by the customer

### ► IBM i Solution

- The new authentication exit QIBM\_QSY\_AUTH provides the ability to invoke an exit program during authentication processing for all applications that perform a corresponding operation.
- The exit program is given information that can be used to perform additional checks, and it can return a success or failure indicator.
- A deployed exit program could generate an **out-of-band push notification** to a phone that requires a fingerprint to continue.
- For more information, see the \*REGFAC authentication method section in the [IBM documentation](#)

# Regulations and standards

Requiring the implementation of MFA (EU and International)

- ▶ GDPR (General Data Protection Regulation) (EU)
- ▶ PSD2 (Revises Payment Services Directive) (EU)
- ▶ ISO/IEC 27001 (Global Information Security Standard) (EU)
- ▶ NIST 800-171 & NIST 800-53 (Government & Contractors) (US)
- ▶ CMMC (Cybersecurity Maturity Model Certification) (Defense Contractors) (US)
- ▶ GLBA (Gramm-Leach-Bliley Act) (Financial Institutions) (US)
- ▶ PCI DSS (Payment Card Industry Data Security Standard) (Payment Processing) (US)
- ▶ HIPAA (Health Insurance Portability and Accountability Act) (Healthcare) (US)

## Links

- ▶ Password level  
<https://www.ibm.com/docs/en/i/7.5.0?topic=changes-considerations-changing-qpwdlvl-from-2-3-4>
- ▶ MFA on IBM i  
<https://www.ibm.com/docs/en/i/7.6.0?topic=security-multi-factor-authentication-mfa>
- ▶ TLS Configuration  
<https://www.ibm.com/docs/en/i/7.6.0?topic=security-system-tls>
- ▶ IBM 7.6 Features and Functions  
<https://www.redbooks.ibm.com/abstracts/sg248588.html>
- ▶ Using IBM Navigator for I to manage MFA  
<https://www.ibm.com/support/pages/using-ibm-navigator-i-manage-mfa>
- ▶ QIBM\_RUN\_UNDER\_USER\_NO\_AUTH Function Usage ID  
<https://www.ibm.com/docs/en/i/7.6.0?topic=mfam-qibm-run-under-user-no-auth-function-usage-id>
- ▶ SST/DST MFA  
<https://www.ibm.com/docs/en/i/7.6.0?topic=concepts-service-tools-multi-factor-authentication-mfa>

axians

Your contact

Katharina Karner

katharina.karner@axians.at

+43(0)664 / 851 3875

www.axians.at



The best of  
ICT with a  
human  
touch

