Power Week 2025

#pw2025

18 - 19 - 20 novembre 2025
IBM Innovation Studio Paris

S24 – MFA 7.6 avec démonstration

18 novembre 14:45 - 15:45

Ludovic MENARD
IBM France
ludovic_menard@fr.ibm.com

IBM

common FRANCE

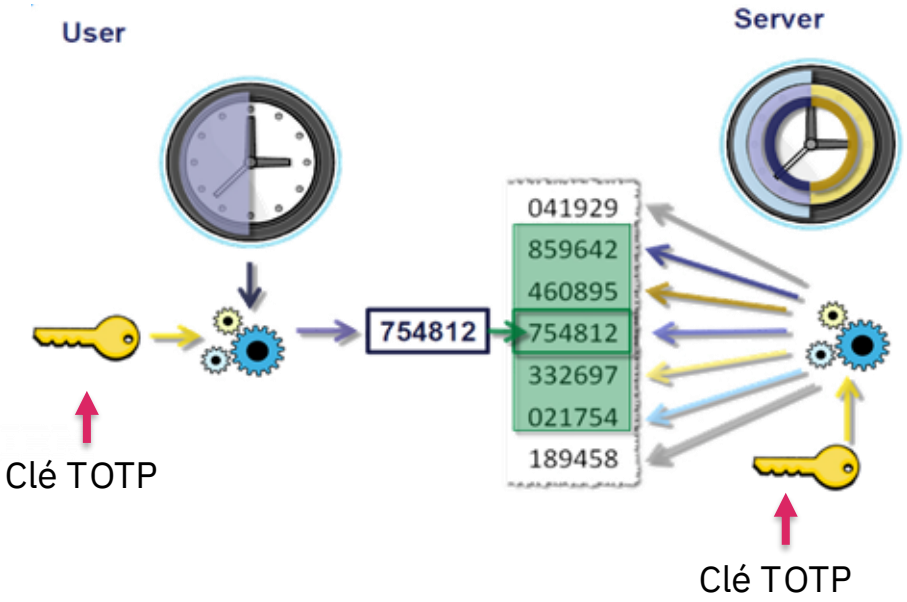
MFA intégré à l'IBM i

- Nouveaux attributs de profil utilisateur pour l'implémentation du mot de passe à usage unique basé sur le temps (TOTP)
  - ✓ Clé secrète partagée, protégée de la même manière qu'un mot de passe
- Fonctionne immédiatement
  - ✓ Fonctionne en état restreint
  - ✓ Aucun impact sur le pare-feu (aucune connexion réseau utilisée)
  - ✓ Aucun programme d'agent ni serveur externe
- Aucun écart entre le traitement du mot de passe et celui de l'authentification par facteur supplémentaire
- Plusieurs options de protection configurables au niveau du profil utilisateur
- Les principaux outils d'administration et de gestion du système IBM i fonctionnent avec la configuration la plus restrictive
  - ✓ Access Client Solutions (ACS)
  - ✓ Navigator for i
- Compatible avec des dizaines d'authentificateurs clients TOTP du secteur
- Implémentation autonome du profil utilisateur des outils de service système (SST/DST)

Présentation de MFA dans la documentation IBM

Mot de passe à usage unique basé sur le temps (TOTP)

- Intégré aux objets de profil utilisateur (*USRPRF)
- Intégré aux profils utilisateur DST/SST
  - Mise en œuvre indépendante

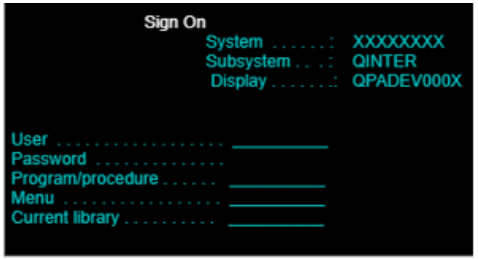


Exemples d'authentificateurs de clients RFC 6238

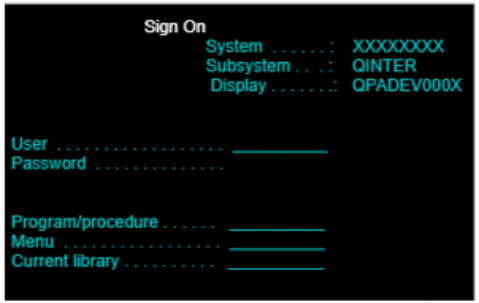
Facteur de connexion supplémentaire activé

- Spécifie si un facteur de connexion supplémentaire peut être utilisé avec un identifiant utilisateur et un mot de passe.

QPWDLVL
0 or 1



- Si cette valeur est activée, le champ de facteur supplémentaire sera affiché sur le panneau de connexion.



- Un utilisateur devra spécifier la valeur du facteur supplémentaire si le profil utilisateur a *TOTP comme méthode d'authentification

QPWDLVL
2, 3, or 4 and
Additional Sign-on
Factor *DISABLED

Exigences
Niveau de sécurité **40** ou **50**
Mot de passe niveau **4**

Si vous utilisez un panneau de connexion personnalisé, créez-en un nouveau basé sur la nouvelle version par défaut

Additional Sign-on
Factor *ENABLED

Intervalle facultatif TOTP

Énoncé du problème

- Certaines applications dépendent de l'utilisation de mots de passe mis en cache en arrière-plan, ce qui ne fonctionnera pas avec la courte durée de vie d'un jeton TOTP.

Solution IBM i 7.6

- Conception d'un intervalle de temps optionnel configurable lorsque la fourniture du jeton TOTP est requise

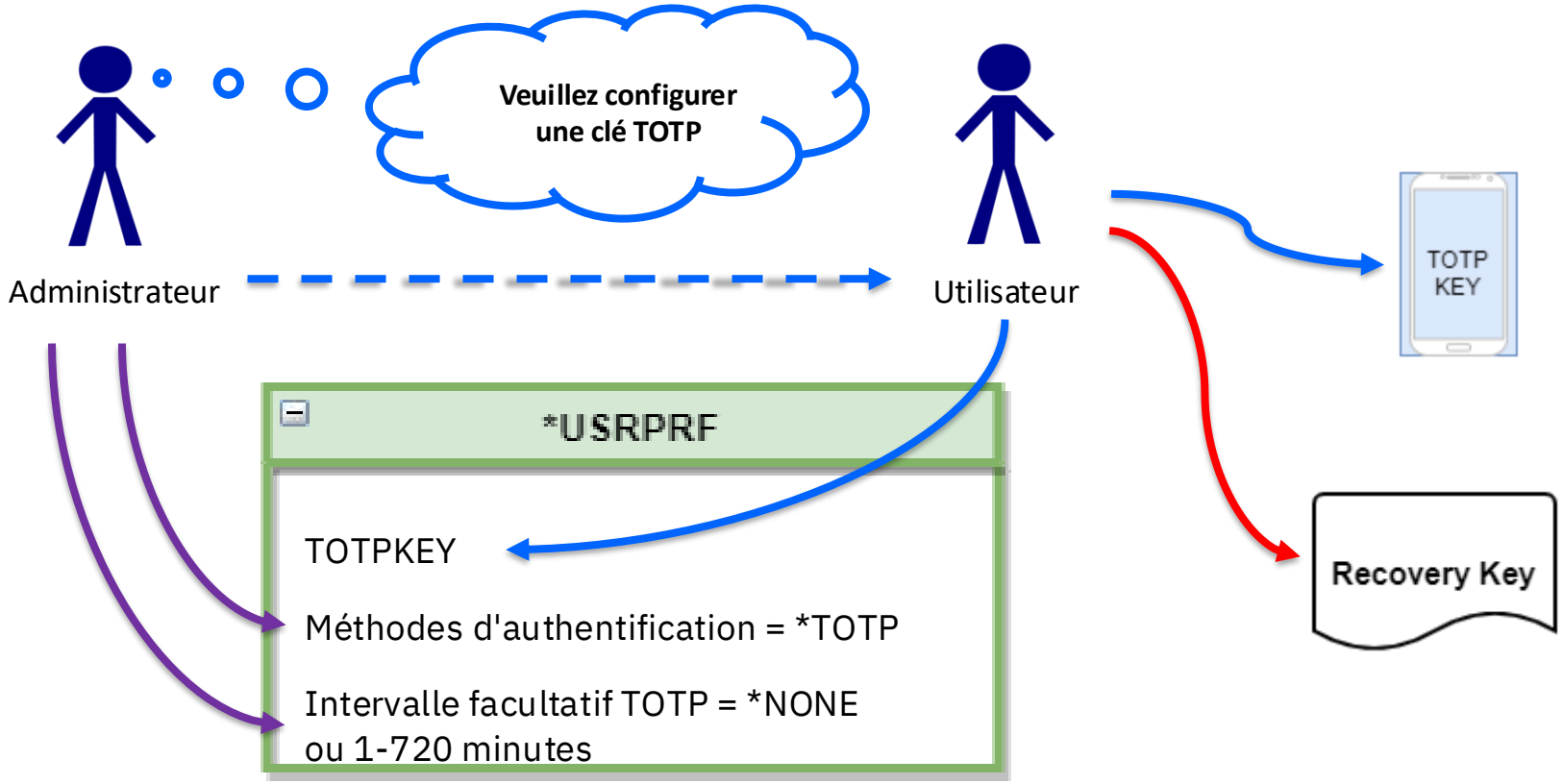
Intervalle facultatif TOTP == ***NONE** *« Mode absolu »*

- Chaque authentification par mot de passe nécessite un jeton TOTP valide
  - ✓ Les clients utilisant des mots de passe mis en cache en secret échoueront
  - ✓ Certains clients pourraient demander chaque connexion unique au système

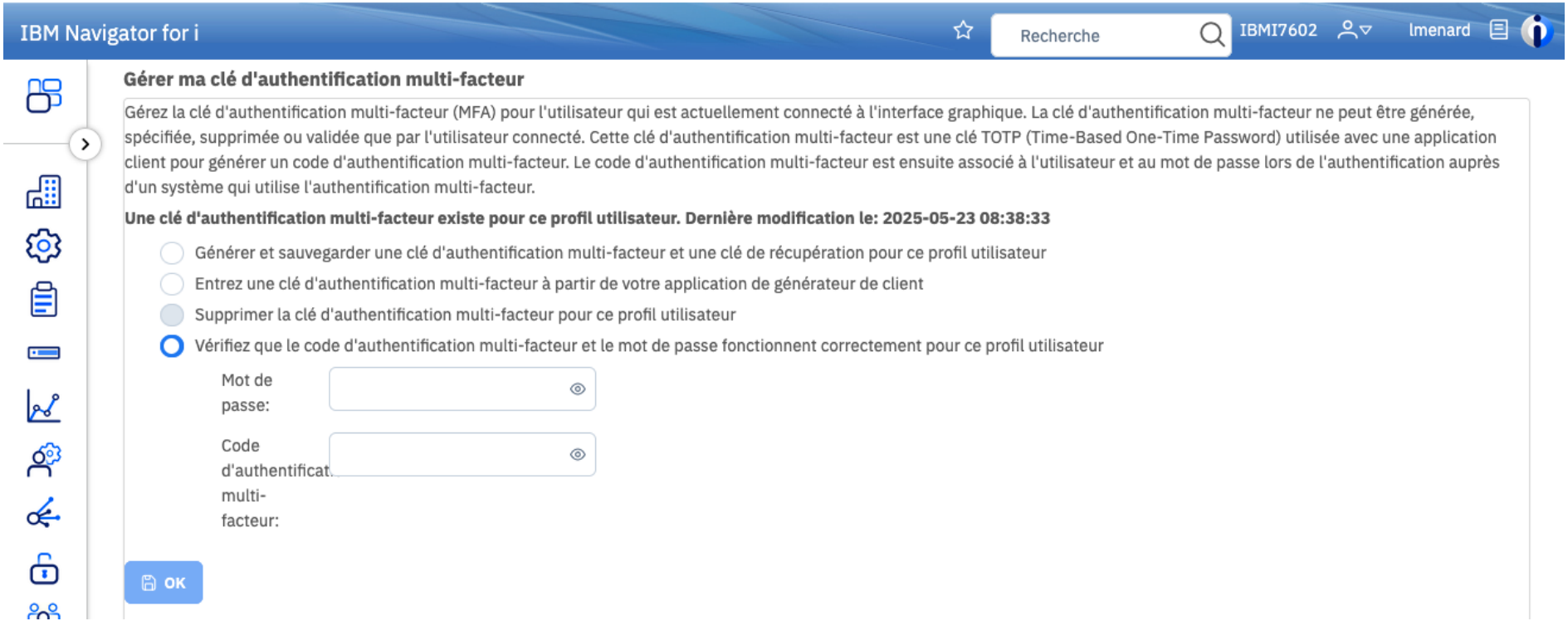
Intervalle facultatif TOTP > 0 [1-720 minutes]

- L'utilisateur effectue une authentification initiale basée sur un mot de passe avec un jeton TOTP
  - ✓ L'intervalle de temporisation démarre
  - ✓ Les demandes d'authentification par mot de passe ultérieures ne nécessitent un mot de passe que jusqu'à l'expiration de l'intervalle.

Expérience de configuration MFA intégrée *TOTP



Gérer ma clé MFA (TOTP)



Configuration de la clé TOTP

Validation de la clé d'authentification multi-facteur et de la clé de récupération de sauvegarde

La nouvelle clé d'authentification multi-facteur a été sauvegardée dans votre profil utilisateur. Vérifiez que le code d'authentification multi-facteur permet à ce profil utilisateur de se connecter, puis sauvegardez la clé de récupération.

1. Clé d'authentification multi-facteur sauvegardée:

A l'aide de votre application de générateur de client, entrez la clé d'authentification multi-facteur ci-dessous (sans espaces) ou numérisez le code QR

RFA7FV5SR7H73VJPYYBRCJXWGGFHAN45

RFA7 FV5S R7H7 3VJP YYBR CJXW GGFH AN45

2. Validation de la clé d'authentification multi-facteur:

Entrez votre mot de passe de profil utilisateur et le code d'authentification multi-facteur de votre application de générateur de client pour confirmer que votre profil utilisateur peut se connecter avec l'authentification multi-facteur

Mot de passe:

Code d'authentification multi-facteur:

Valider

3. Clé de récupération:

Sauvegardez la clé de récupération dans un endroit sûr, elle peut être utilisée à la place du mot de passe de l'utilisateur comme une récupération unique si la clé et le code d'authentification multi-facteur ne fonctionnent pas

B7A0AD7E07F5EAC50D9865730581EB443612CCB7D054FFD5EBEA8A5C6B9DACB9

OK

Notez que vous devez vous connecter avec le profil utilisateur qui configure sa clé TOTP.

CHGTOTPKEY TOTPKEY(*GEN)

```
TOTP key  . . . . . :   JKLW 2ZRK FGEK 5WNZ LD6R HF5J RZIS 4505
Copy/paste version  . . :   JKLW2ZRKFGEK5WNZLD6RHF5JRZIS4505


Recovery key  . . . . . :   E44FFDF4A042F800BF47A88632867AD4
                            48F25AAFFF0F7277A93277EC9AC45597

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.
```

Interfaces supplémentaires non compatibles avec les facteurs

Énoncé du problème

- Aucune possibilité de modifier des centaines d'interfaces client d'application comme Filezilla

Solution IBM i 7.6

- Mot de passe avec facteur supplémentaire ajouté
- deux points (:) interprété comme un séparateur dans le champ du mot de passe
- Permet à presque toutes les applications existantes de fonctionner avec TOTP MFA sans aucune modification !

Exemple : myAmazingPa$$w0rd**:**358538

L'administrateur système informe les utilisateurs qu'ils doivent ajouter la valeur TOTP au mot de passe sur les interfaces sans invite de facteur supplémentaire

Mot de passe avec facteur supplémentaire dans la documentation IBM

ID d'utilisation de la fonction QIBM_RUN_UNDER_USER_NO_AUTH

Énoncé du problème

- La possibilité d'exécuter des actions sous un autre profil utilisateur en se basant uniquement sur l'autorité sur ce profil utilisateur est en conflit avec les principes MFA
- L'implémentation TOTP MFA intégrée d'IBM i permet ce contournement du mot de passe en raison de son utilisation omniprésente

Solution IBM i 7.6

- Empêchez éventuellement les applications de contourner la nécessité de fournir les informations d'identification du profil utilisateur
- L'identifiant de fonction QIBM_RUN_UNDER_USER_NO_AUTH) permet de bloquer certains profils utilisateur pour qu'ils ne puissent pas être utilisés comme cible d'une exécution sous un autre profil.
- Recommandé pour être utilisé en conjonction avec le profil utilisateur MFA/TOTP
- Enregistrements d'audit d'avertissement - Générés lorsque le profil utilisateur est la cible d'une exécution en cours qui échouerait sans accès : CHGUSRAUD USRPRF(AUSER) AUDLVL(*AUTWARN)

- **QIBM_RUN_UNDER_USER_NO_AUTH ne nécessite pas de configuration TOTP/MFA pour l'utilisateur ou le système**

ID d'utilisation de la fonction QIBM_RUN_UNDER_USER_NO_AUTH dans la documentation IBM

Point d'exit d'authentification unique QIBM_QSY_AUTH (*REGFAC)

Énoncé du problème

- L'implémentation TOTP MFA intégrée IBM i peut ne pas fonctionner avec les solutions MFA d'entreprise existantes utilisées par les clients

Solution IBM 7.6

- Le nouveau point de sortie d'authentification unique QIBM_QSY_AUTH permet d'appeler un programme de sortie pendant le traitement d'authentification pour toutes les applications exécutant une opération applicable.
- Le programme de sortie reçoit des informations à utiliser pour effectuer une vérification supplémentaire et peut renvoyer des indicateurs de réussite ou d'échec.
- Un utilisateur disposant de privilèges élevés pourrait être amené à fournir un mot de passe et une valeur TOTP, ainsi qu'à appeler le programme de sortie.
- Un programme de sortie fourni par un administrateur pourrait générer une notification push hors bande sur un téléphone qui nécessite une empreinte digitale pour continuer. Pour plus d'informations, consultez la rubrique relative à la méthode d'authentification *REGFAC dans la documentation IBM.

Méthode d'authentification *REGFAC dans la documentation IBM.

Combinaisons MFA intégrées IBM i une solution pour tous les goûts

Profil utilisateur Laurent

Méthodes d'authentification = *NONE

Profil utilisateur Ludo

Méthodes d'authentification = *TOTP
Intervalle facultative du TOTP = NONE

Profil utilisateur Catherine

Méthodes d'authentification = *REGFAC

Profil utilisateur Béatrice

Méthodes d'authentification = *TOTP *REGFAC
Intervalle facultative du TOTP = NONE

Profil utilisateur Roger

Méthodes d'authentification = *TOTP *REGFAC
Intervalle facultative du TOTP = 10

Profil utilisateur Mathieu

Méthodes d'authentification = *TOTP
Intervalle facultative du TOTP = 10

Profil utilisateur Alain

Méthodes d'authentification = *TOTP
Intervalle facultative du TOTP = NONE

Utilisation de fonction

QIBM_RUN_UNDER_NO_AUTH
Alain = Denied

Outils de service système (SST/DST) MFA

Énoncé du problème

- L'environnement SST/DST limité ne fonctionne pas avec les solutions MFA tierces traditionnelles en raison de l'absence de prise en charge des points de sortie et les méthodes d'authentification telles que Kerberos ne fonctionnent pas dans l'environnement.
- Les utilisateurs SST/DST privilégiés devraient être tenus de fournir plusieurs facteurs d'authentification

7.6 Solution

- Les outils de service système (SST) et les outils de service dédiés (DST) prennent en charge une implémentation de clé TOTP MFA non connectée au système d'exploitation Prise en charge MFA
- Un administrateur SST peut activer MFA pour SST sans l'activer sur le système d'exploitation
- L'apparence est similaire à celle du système d'exploitation , mais SST ne permet pas de définir une fréquence pour fournir la valeur TOTP ; elle est requise chaque fois qu'un mot de passe est requis

Outils de service Authentification multifacteur (MFA) dans la documentation IBM

Power Week

18 -19 - 20 novembre 2025

IBM

common FRANCE

IBM

DEMO
MFA


MERCI