precisely

Assure Multi-Factor Authentication

Guy MARMORAT

iBelieve 2022
Présent et Futur de l'IBM i
Evènement on-line
17 Nov. 22

Gestion des mots de passe IBM i

Bases	Bénéfices
Valeur Système pour le niveau de sécurité QSECURITY (~~10,20~~ & plus)	Mots de passe requis
Valeurs Système pour les tentatives de connexion QMAXSGNACN & QMAXSIGN	Protège contre les mots de passe devinés et les attaques par force brute
Valeur Système pour le niveau du mot de passe QPWDLVL (0,1,2,3,4)	Renforce les mots de passe
Valeurs Système pour la gestion des mots de passe QPWD*	Renforce les mots de passe
Single Sign On & EIM	Simplifie la gestion des mots de passe
SSL, TLS	Encrypte les mots de passe

Ces mesures fournissent une *sécurité de mot de passe de base.*

Comment passer à l'étape suivante?

Les mots de passe, seuls, sont faibles.

La fréquence des violations dues aux mots de passe volés ou devinés et aux attaques par force brute nécessite une couche supplémentaire de sécurité d'authentification des utilisateurs.

Problèmes des mots de passe complexes

- Doit-on encore complexifier les mots de passe ? Pas vraiment
- Pourquoi pas ? Parce que nous devons les écrire !
- Les mots de passe complexes augmentent les coûts et introduisent des faiblesses :
  - Leur gestion est complexe
  - Leur gestion est coûteuse
  - Cela impacte la productivité (réactivation des utilisateurs, changement des mots de passe, etc.)
- Se fier uniquement aux mots de passe c'est mettre tous vos œufs dans le même panier !

NIST's latest Digital Identity Guidelines at https://pages.nist.gov/800-63-3/ (recommandations concernant les mots de passe complexes)

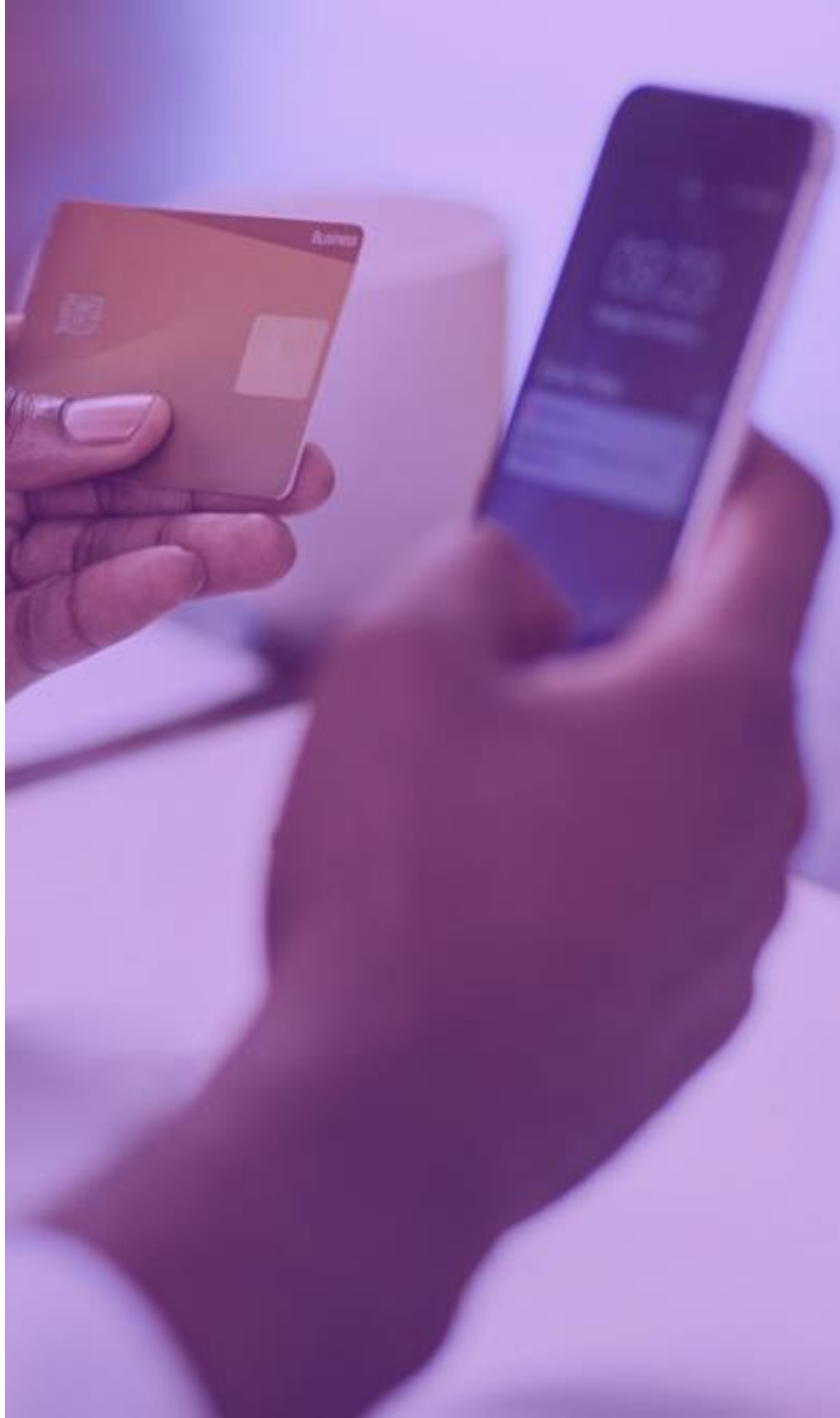
L’Authentification Multifacteur ajoute une couche de sécurité à la connexion

Multi-Factor Authentication (MFA) requiert des réponses aux questions sur 2 ou plusieurs facteurs :

- “Facteur de connaissance”: Quelque chose que l’utilisateur connaît
  - E.g. user ID, mot de passe, PIN, question secrète
- “Facteur de possession”: Quelque chose que l’utilisateur possède
  - E.g. smartphone, smartcard, token
- “Facteur d’inhérence”: Un attribut biologique de l’utilisateur
  - E.g. empreinte, iris, reconnaissance vocale (Biometrics)

L’ Authentification classique sur IBM i utilise 2 éléments du même type de facteur – User ID et Mot de passe.

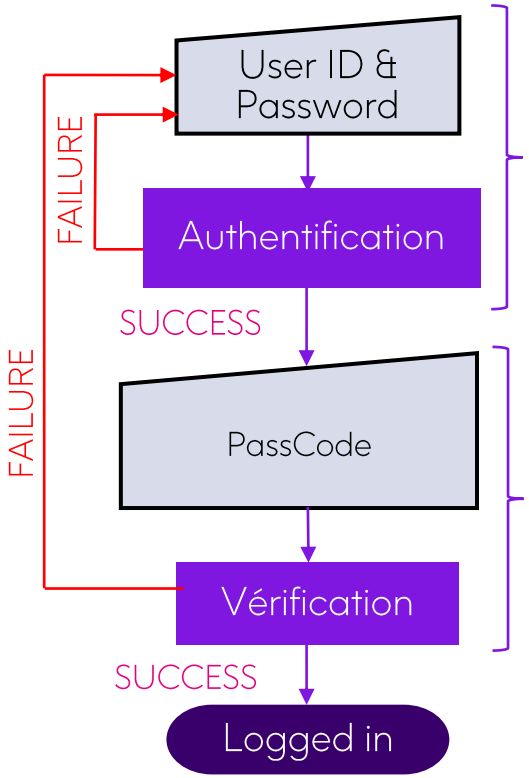
Ceci n'est PAS une Authentification Multifacteur



Authentication multi-étapes vs Multi-Facteurs

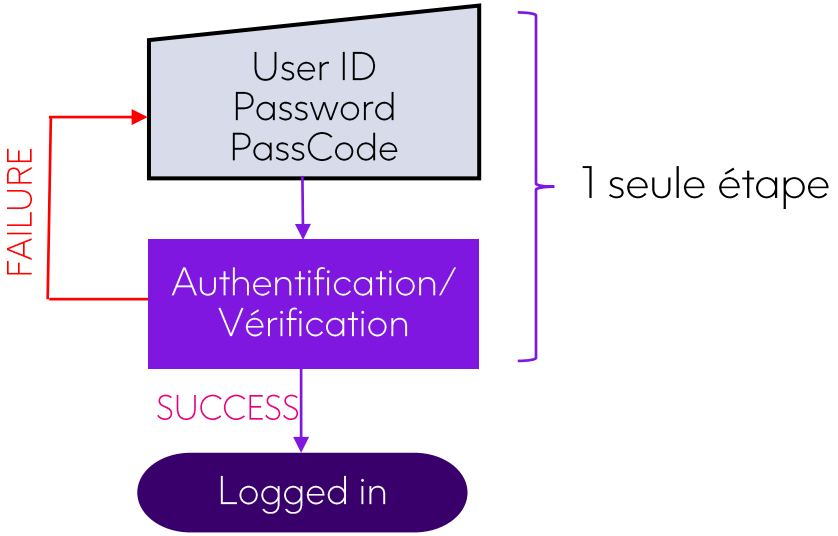
Authentification en plusieurs étapes

- 2 facteurs d'authentification sont présentés séparément, séquentiellement et via des process séparés
- Si l'authentification échoue, l'utilisateur connaît l'étape qui a échoué



Authentification en 1 étape

- Plusieurs facteurs d'authentification présentés en même temps
- Tous les facteurs doivent être validés avant d'accepter l'accès
- Si l'authentification échoue, l'utilisateur ne saura pas quel facteur a échoué



Ne pas savoir quel facteur d'authentification a échoué est frustrant pour les utilisateurs, mais cela est requis par des réglementations telles que PCI.

Pourquoi l'Authentification Multifacteur est incontournable ?

L'Authentification Multifacteur répond aux diverses règlementations pour les banques et prestataires de services de paiement :

- PCI-DSS 3.2 et +
- Directive DSP2
- 23 NYCRR 500
- GLBA / FFIEC

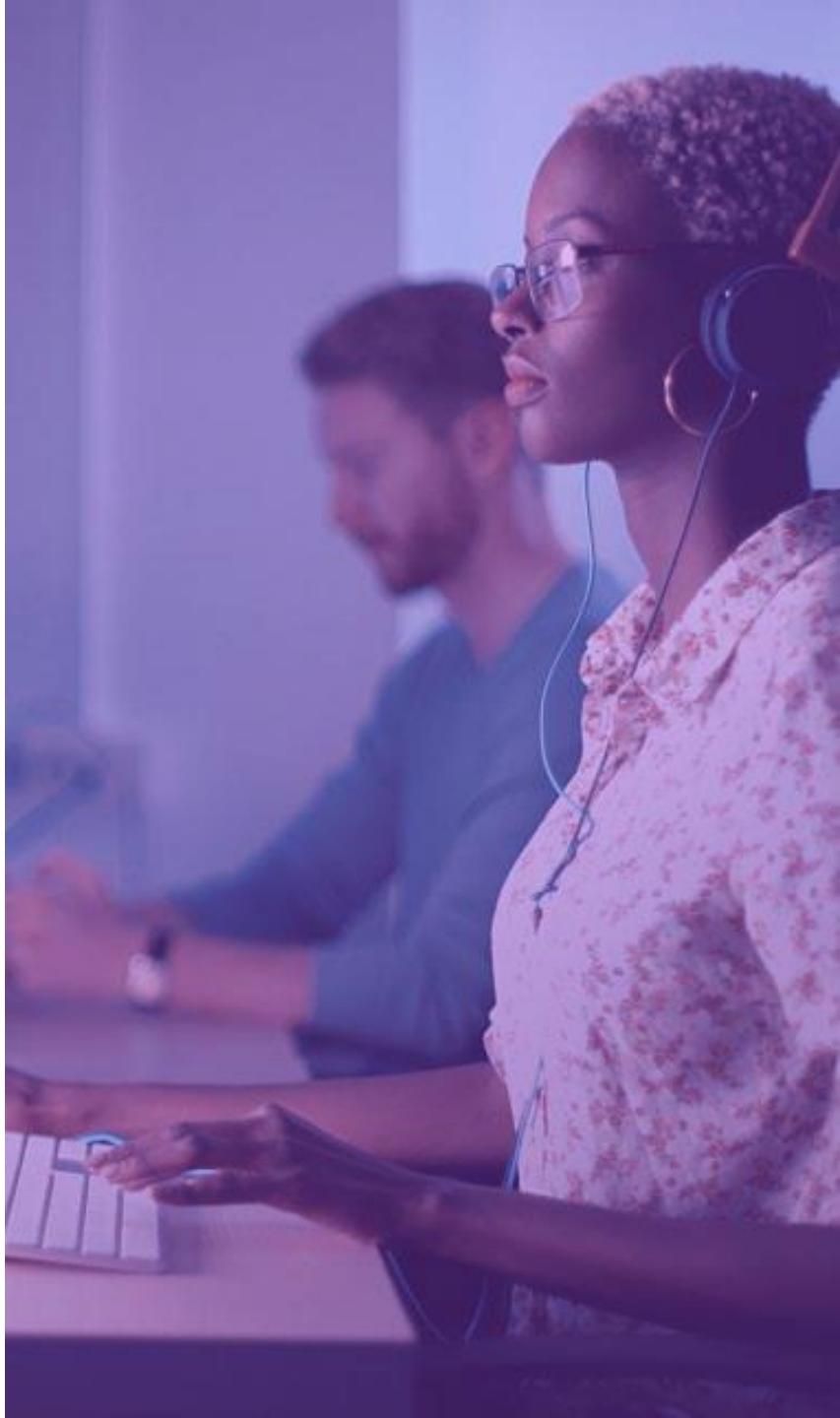
MFA est aussi mentionné pour :

- GDPR
- HIPAA
- Swift Alliance Access
- SOX
- Etc.

L'utilisation sélective de MFA est une bonne pratique de sécurité :

- Évite les problèmes avec des mots de passe faibles
- Évite les problèmes avec des mots de passe complexes

Vous devrez peut-être utiliser l'authentification multifacteur demain, si vous ne l'utilisez pas déjà aujourd'hui



Technologie de l'Authentification

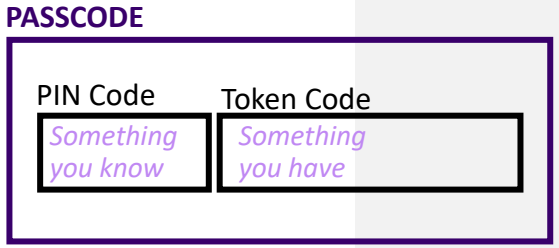
Des facteurs supplémentaires, au-delà du facteur de la connaissance, peuvent être fournis par :

- Smartphone app
- Email
- Appel téléphonique
- SMS/text message (*voir ci-contre*)
- Périphérique matériel tel que des porte-clés ou des jetons
- Appareil biométrique

Services d'authentification génère des codes pour l'utilisateur

Exemple :

- RADIUS compatible (RSA SecurID, Entrust, Duo, Vasco, Gemalto, et plus)
- RFC 6238 (Microsoft Authenticator, Google Authenticator, Authy, Yubico, ...)
- Autres... (TeleSign, et plus)



Combination entre ce que vous connaissez et possédez

MFA ok !

Utilisation de SMS pour l'authentification

PCI DSS s'appuie sur les normes de l'industrie, telles que, NIST, ISO et ANSI, qui couvrent toutes les industries, pas seulement l'industrie du paiement.
Bien que le NIST autorise actuellement l'utilisation de l'authentification par SMS pour MFA, ils conseillent de limiter l'authentification par SMS ou voix car elle présente un risque de sécurité.

Principales caractéristiques à rechercher dans une Solution MFA pour l'IBM i

- Option d'intégration avec l'écran de connexion IBM i
- Capacité à intégrer MFA avec d'autres applications et process IBM i
- Plusieurs options d'authentification adaptées à votre budget et aux authentificateurs existants
- Certification par un organisme reconnu (ex: RSA, NIST)

Principales caractéristiques à rechercher dans une Solution MFA pour l'IBM i

- Règles permettant de déclencher MFA pour des situations spécifiques ou des critères d'utilisation tels que :
  - Profils de groupes, Droits spéciaux
  - IP addresses, Device types, Dates & Heures
  - Et plus…
- Intégration avec d'autres fonctionnalités de sécurité, pour une véritable authentification basée sur les risques
  - Contrôle d'Accès
  - Elevation des Droits
  - SIEM

Autres astuces et éléments à considérer

- Communiquer avec plusieurs serveurs d'authentification
- Que faire en cas d'impossibilité de contacter au moins un des serveurs ?

- Réflexions sur les situations suivantes :
  - Doit-on demander une authentification renforcée pour QSECOFR ?
  - Doit-on demander une authentification renforcée depuis la console ? Le sous-système QCTL ?
  - Comment ajuster les valeurs système QMAXSIGN & QMAXSGNACN ?
- Le code doit être hyper robuste et les process doivent laisser le moins de trace possible
- Le process doit être ultra-sécurisé, auditable, avec même une protection spéciale de points exit

- Nec-plus-ultra : Intégration complète avec de l'élévation de droit, des systèmes de ticket, de la géolocalisation, …

  Pas de "compétition" avec Single Sign-On. SSO simplifie, MFA protège !

Comment Precisely peut vous aider ?

Assure Security: Domaines d'intervention stratégiques

Contrôle d'Accès

Protection des systèmes et des données contre les attaques et les utilisateurs non autorisés

- Empêcher les connexions non autorisées
- Gérer les privilèges des utilisateurs
- Contrôler et restreindre les accès aux données, paramètres systèmes et commandes

Compliance Monitoring

Répondre aux exigences réglementaires avec une visibilité complète sur les problèmes de sécurité

- Automatiser les alertes, les rapports de sécurité et de conformité
- Surveiller et bloquer la consultation des données sensibles
- Envoyer les données de sécurité IBM i dans une solution SIEM

Confidentialité des données

Mise en œuvre intégrale des puissantes fonctionnalités IBM i de protection des données

- Encrypter les données IBM i
- Sécuriser les clés d'encryption
- Tokenisation et Anonymisation
- Sécuriser les transferts de fichiers

Défense contre les malware

Mise en place d'une protection multicouche complète contre les menaces sophistiquées

- Renforcer tous les systèmes et données contre les attaques
- Automatiser et intégrer les technologies et la gestion de la sécurité
- Concevoir une protection résiliente en cas de franchissement d'une ligne de défense

Assure Multi-Factor Authentication

Contrôle d'Accès

Protection des systèmes et des données contre les attaques et les utilisateurs non autorisés

- Empêcher les connexions non autorisées
- Gérer les privilèges des utilisateurs
- Contrôler et restreindre les accès aux données, paramètres systèmes et commandes

Compliance Monitoring

Répondre aux exigences réglementaires avec une visibilité complète sur les problèmes de sécurité

- Automatiser les alertes, les rapports de sécurité et de conformité
- Surveiller et bloquer la consultation des données sensibles
- Envoyer les données de sécurité IBM i dans une solution SIEM

Confidentialité des données

Mise en œuvre intégrale des puissantes fonctionnalités IBM i de protection des données

- Encrypter les données IBM i
- Sécuriser les clés d'encryption
- Tokenisation et Anonymisation
- Sécuriser les transferts de fichiers

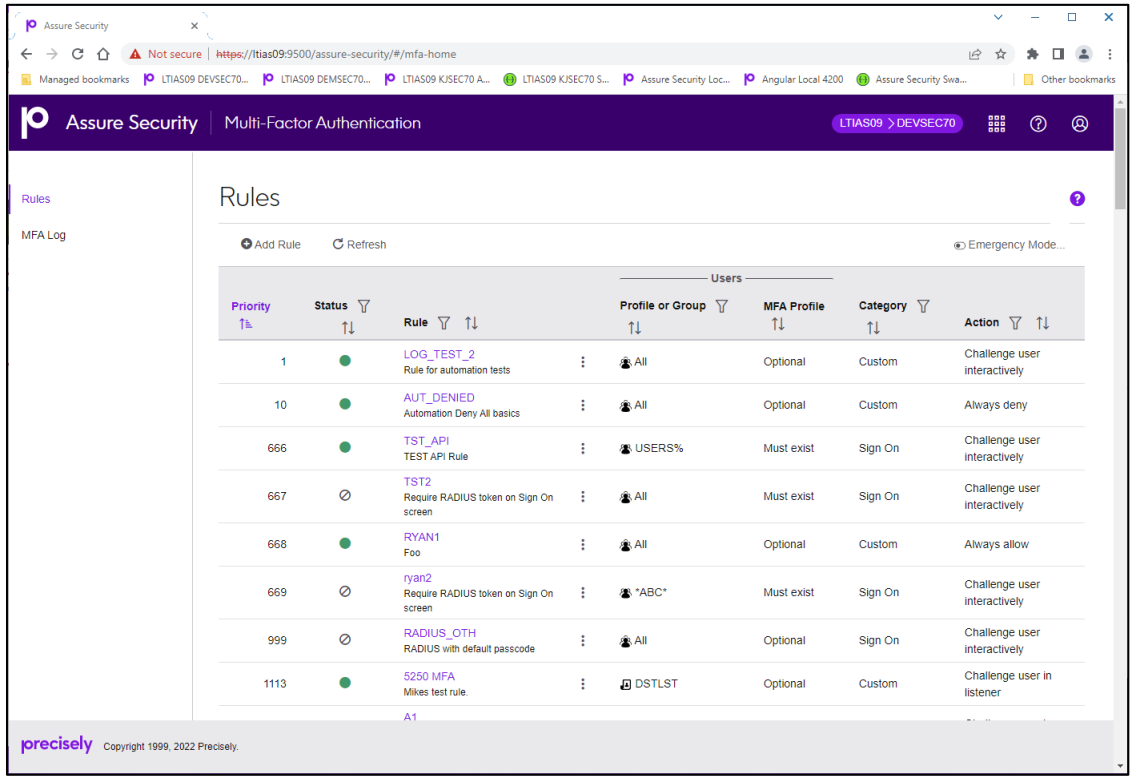
Défense contre les Malware

Mise en place d'une protection multicouche complète contre les menaces sophistiquées

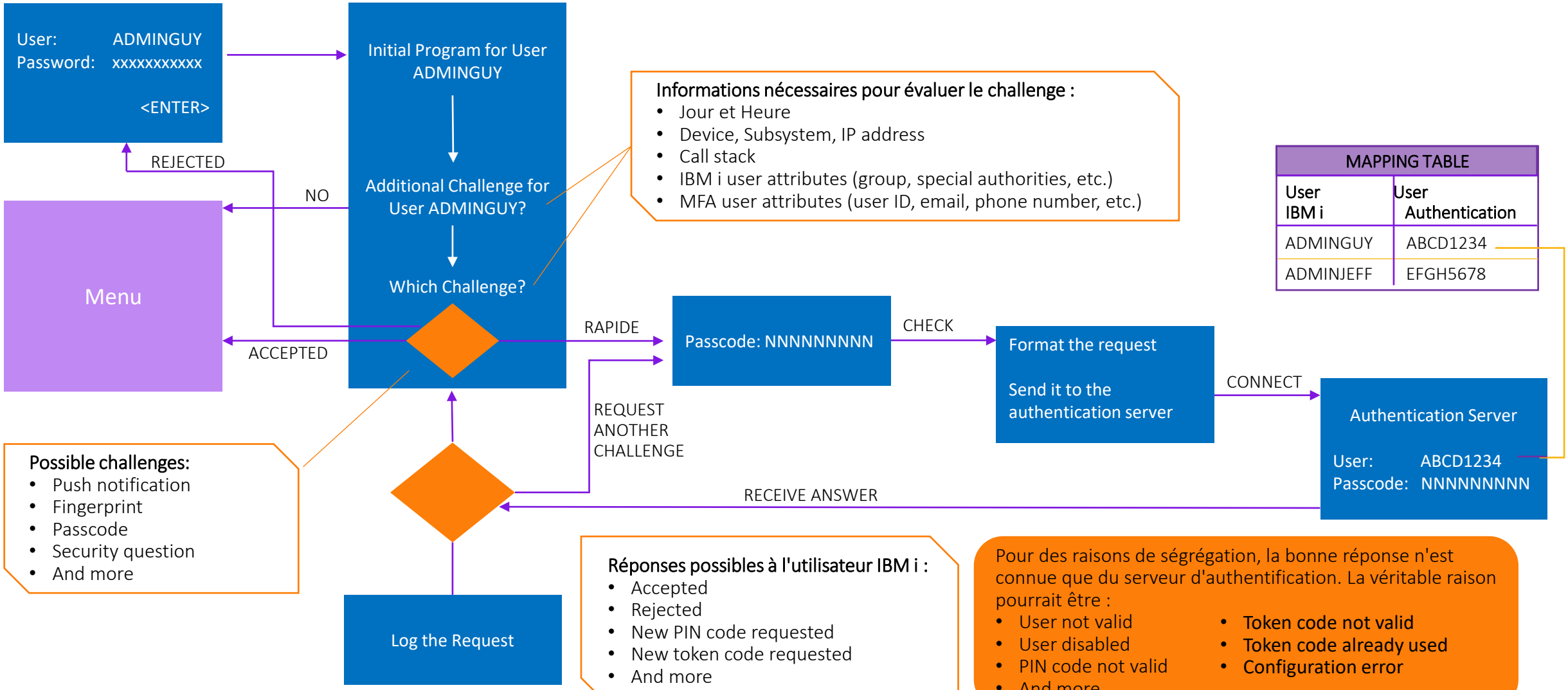
- Renforcer tous les systèmes et données contre les attaques
- Automatiser et intégrer les technologies et la gestion de la sécurité
- Concevoir une protection résiliente en cas de franchissement d'une ligne de défense

Assure Multi-Factor Authentication

- Puissant et flexible
- Options pour initier à partir du 5250 signon ou à la demande
- Options d'authentification en 1 ou 2 étapes
- Prise en charge de plusieurs méthodes d'authentification
- Permet la réactivation de profil et le changement de mot de passe en libre-service
- Prend en charge le principe des « quatre yeux » pour les changements supervisés
- Certifié RSA

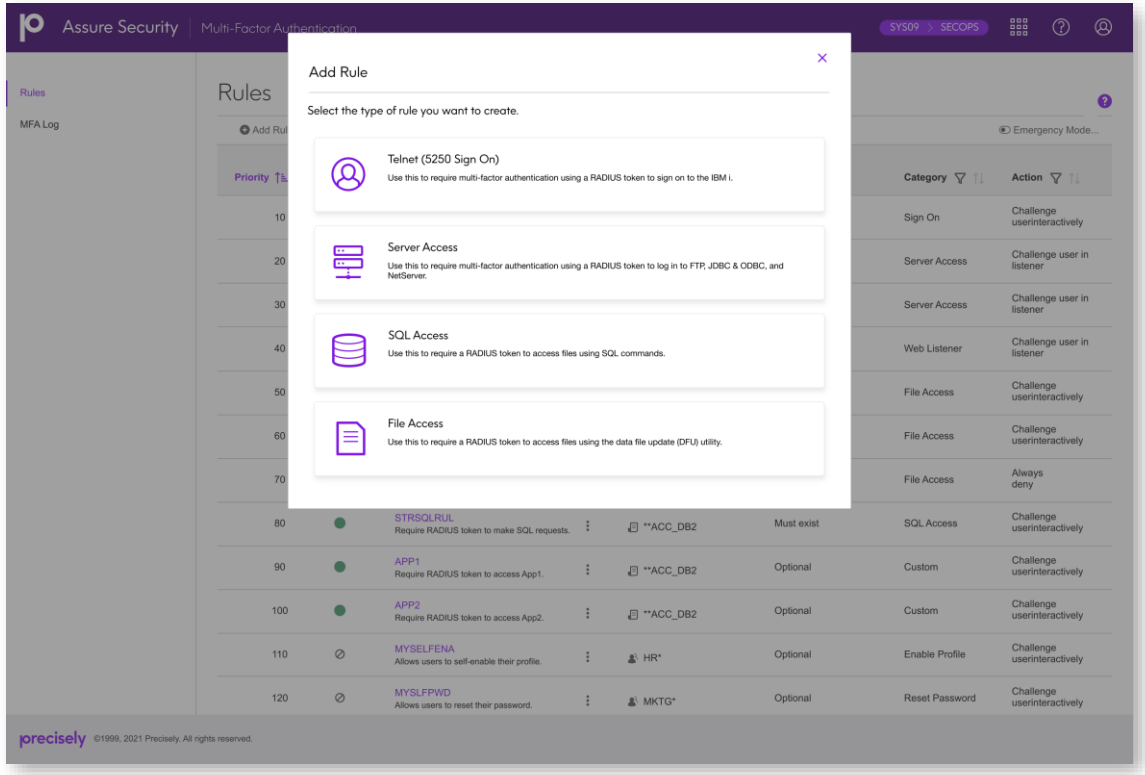


Multi-Factor Authentication Process Flow

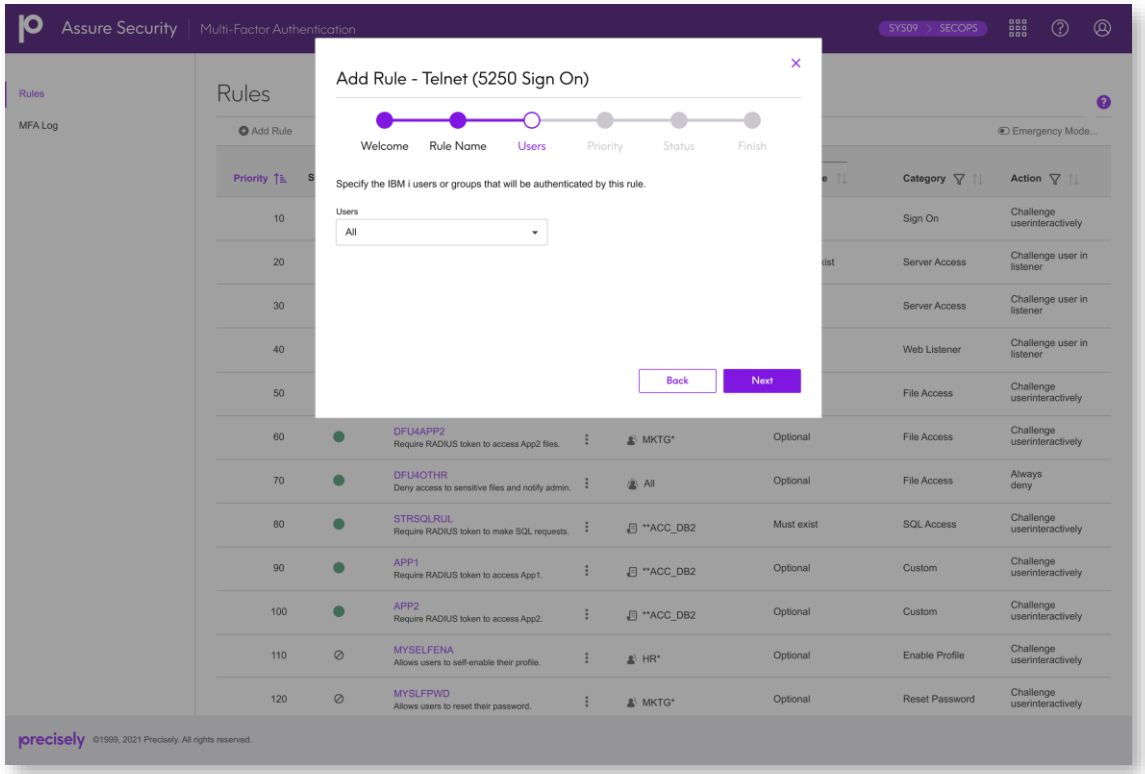


Votre Solution MFA devrait...

... activer une protection pour bien plus que la simple connexion Telnet

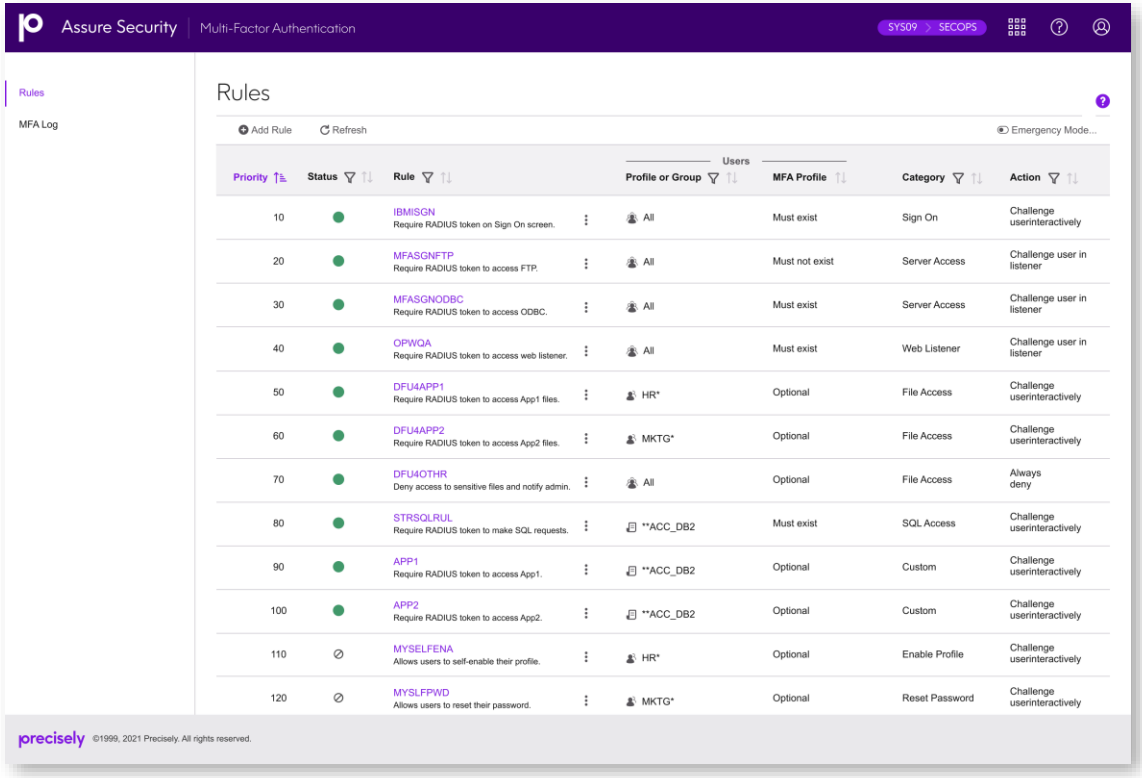


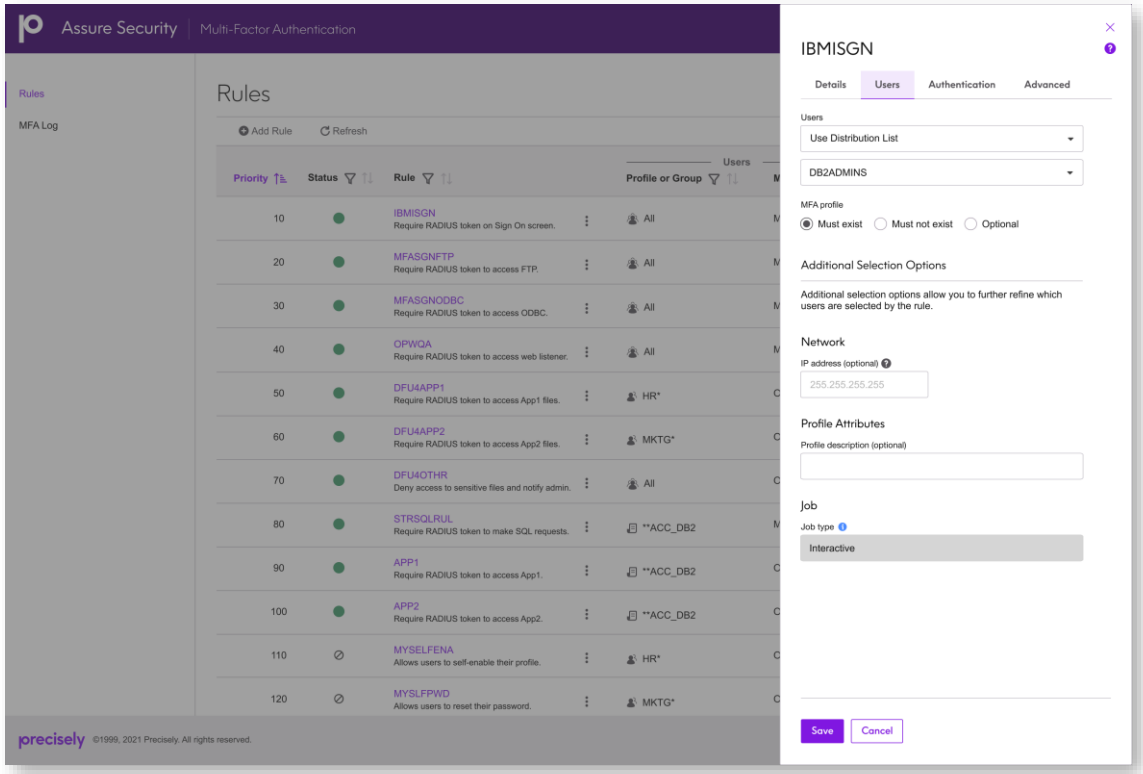
... faciliter l'ajout d'une nouvelle règle



Votre Solution MFA devrait...

... afficher l'état de toutes les règles en un coup d'œil



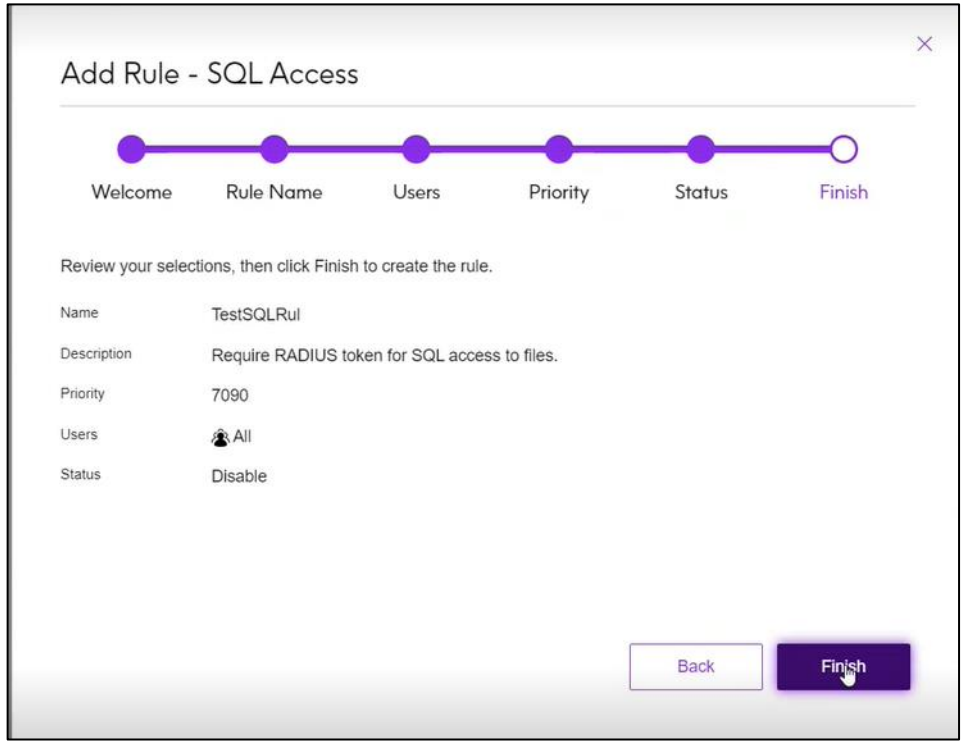


... accéder aux détails de chaque règle

Règles puissantes

Le moteur des règles de Assure MFA facilite la configuration des utilisateurs ou des situations nécessitant une authentification multifacteur

- Les critères des règles incluent, si l'utilisateur est/fait :
  - Enregistré individuellement ou non
  - Un utilisateur ayant des droits limités
  - Un membre d'un profil de groupe
  - En possession de droits spéciaux
  - Un utilisateur d'un poste spécifique
  - Une authentification provenant d'un sous-système ou iASP
  - Un utilisateur d'une adresse IP particulière
  - Une authentification à une certaine date ou heure
- S'il est appelé à la demande, le programme appelant peut aussi être un critère
- Des règles prédéfinies sont fournies pour une mise en œuvre rapide



Prise en charge de multiple méthodes d'Authentification

Authentificateur intégré

Assure MFA a un Authentificateur intégré

- Le Token est transmis par Email et/ou Popup
- Idéal pour les environnements moins exigeants où le coût est un souci

Authentification RADIUS

- Le client RADIUS est porté nativement sur IBM i
- Pour les organisations qui utilisent leur propre RADIUS server ou une Solution tierce telle que :
  - DUO Authenticator
  - Microsoft Azure Authenticator
  - Okta
  - Et d'autres

RSA SecurID authentication

- Assure MFA est certifié RSA SecurID
- Sur site et dans le cloud, software tokens, hardware tokens, push, et options biométriques
- Peut fournir un SID différent du nom de l'utilisateur

RSA READY

Réactivation de profil et changement de mot de passe en libre-service

- Assure Multi-Factor Authentication peut également donner aux utilisateurs la possibilité de :
  - Réactiver leurs profils
  - Changer leur mot de passe

- Les utilisateurs peuvent répondre à des questions de sécurité préconfigurées et/ou recevoir un token via une fenêtre contextuelle, un e-mail ou un dispositif RSA SecurID

- Après avoir fourni toutes les informations demandées, l'utilisateur peut changer son propre mot de passe ou se réactiver

Le « Principe des 4 yeux" pour les changements supervisés

Certaines actions requièrent une supervision :

- Des opérations qui peuvent avoir un impact significatif sur le serveur
- Des changements sur les données extrêmement sensibles

Assure MFA prend en charge le “Principe des 4 Yeux”

- A la demande de l’utilisateur un vérificateur reçoit :
  - Un token à usage unique
  - L’identité de l’utilisateur
  - Le numéro du job
- Le vérificateur saisit le token à usage unique sur l’écran de l’utilisateur et peut ainsi garder un oeil sur les changements effectués

Assure MFA Fonctionnalités avancées

- Ajout d'un gestionnaire d'accès au système
  - Démarrage d'imprimantes de chèques
  - Accés et mis à jour des données
  - Plages IP
  - Heure de la journée/semaine
  - Partages de fichiers
- Protection contre les menaces
  - Identifiants
  - Postes de travail
  - Sessions

5250

- Authentification
  - Programme initial
  - Ecran de sign-on spécifique
- Fonction avancée
  - System Access Manager

FTP

- Authentification
- Fonction avancée
  - System Access Manager

ODBC

- Authentification
- Fonction avancée
  - System Access Manager

NetServer

- Fonctions avancées
  - System Access Manager
    - Partage de fichiers
    - Répertoire de partage de fichiers

Advanced MFA protège contre le vol d'identifiants

Un vol d'identifiant peut arriver de différentes façons :

- Un intrus se trouve sur le réseau et « sniffe » les identifiants et mots de passe des utilisateurs en clair sur le réseau
- Un intrus connaît une application qui stocke des mots de passe en clair et les vole
- Credential stuffing…
  - Un intrus découvre que des identifiants d'utilisateur et des mots de passe ont été volés ailleurs, vendus sur le dark web et tente de les utiliser dans une autre organisation
  - Cela réussit souvent car de nombreuses personnes réutilisent le même mot de passe à plusieurs endroits - banques, amazon et autres prestataires en ligne, puis au travail

Multi-factor Authentication peut prévenir de tout cela !

Pourquoi Assure Multi-Factor Authentication ?

- ✓ Ajoute une couche d'authentification au-delà des mots de passe mémorisés ou écrits
- ✓ Permet de répondre aux exigences des règlementations : PCI DSS 3.2, HIPAA, NYDFS Cybersecurity Regulation, Swift Alliance Access, ...
- ✓ Participe aux mesures de protection contre les Malware et autres attaques
- ✓ Réduit le risque d'accès non autorisés aux systèmes, applications et données
- ✓ Réduit les risques liés aux vols de données
- ✓ Déclenche l'authentification multifacteur basée sur des règles uniquement pour les utilisateurs ou les situations spécifiques qui l'exigent

Exemples d’utilisation dans le monde réel...

Entreprise financière à l’international

Une société mondiale de services financiers massive et complexe soumise à de nombreuses réglementations, notamment PCI DSS et 23 NYCRR 500, souhaitait mettre en œuvre l'authentification multifacteur sur IBM i pour ses utilisateurs distants/privilégiés.

L'entreprise souhaitait utiliser des tokens RSA car ils étaient largement utilisés dans d'autres parties de l'entreprise.

En collaboration avec l'équipe Precisely, elle a mis en œuvre Assure MFA.

En conclusion, cette entreprise a atteint ses objectifs de sécurité et de conformité réglementaire.

Compagnie d'assurance-vie

En tant que fournisseur d'assurance-vie et d'autres produits financiers dans l'État de New York, cette compagnie doit se conformer au règlement sur la cybersécurité du Ministère des Finances (23 NYCRR 500).

Suite à un audit de conformité, l'entreprise a donné une deadline pour implémenter MFA sur ses systèmes IBMi et applications.

Elle utilisait déjà les tokens RSA sur d'autres plateformes.

Choisir Assure MFA était une évidence !

L'implémentation IBM i comprenait une combinaison d'authentification RSA pour les utilisateurs distants et de tokens à usage unique par e-mail pour les autres.

En conclusion, la compagnie a atteint la conformité de manière rentable !

precisely

MERCI DE VOTRE ATTENTION

Pour plus d'informations rendez-vous sur notre site

www.precisely.com/fr

iBelieve 2022
Présent et Futur de l'IBM i

Evènement
on-line
17 Nov. 22

precisely