

RAZ-LEE

Multi **F**actor **A**uthentication ^{iSecurity}



iSecurity Multi Factor Authentication

Our MFA works based on Persons

“One simple action you can take to prevent 99.9% of attacks on your accounts”

Melanie Maynes, Director of Product Marketing Manager
Microsoft Security



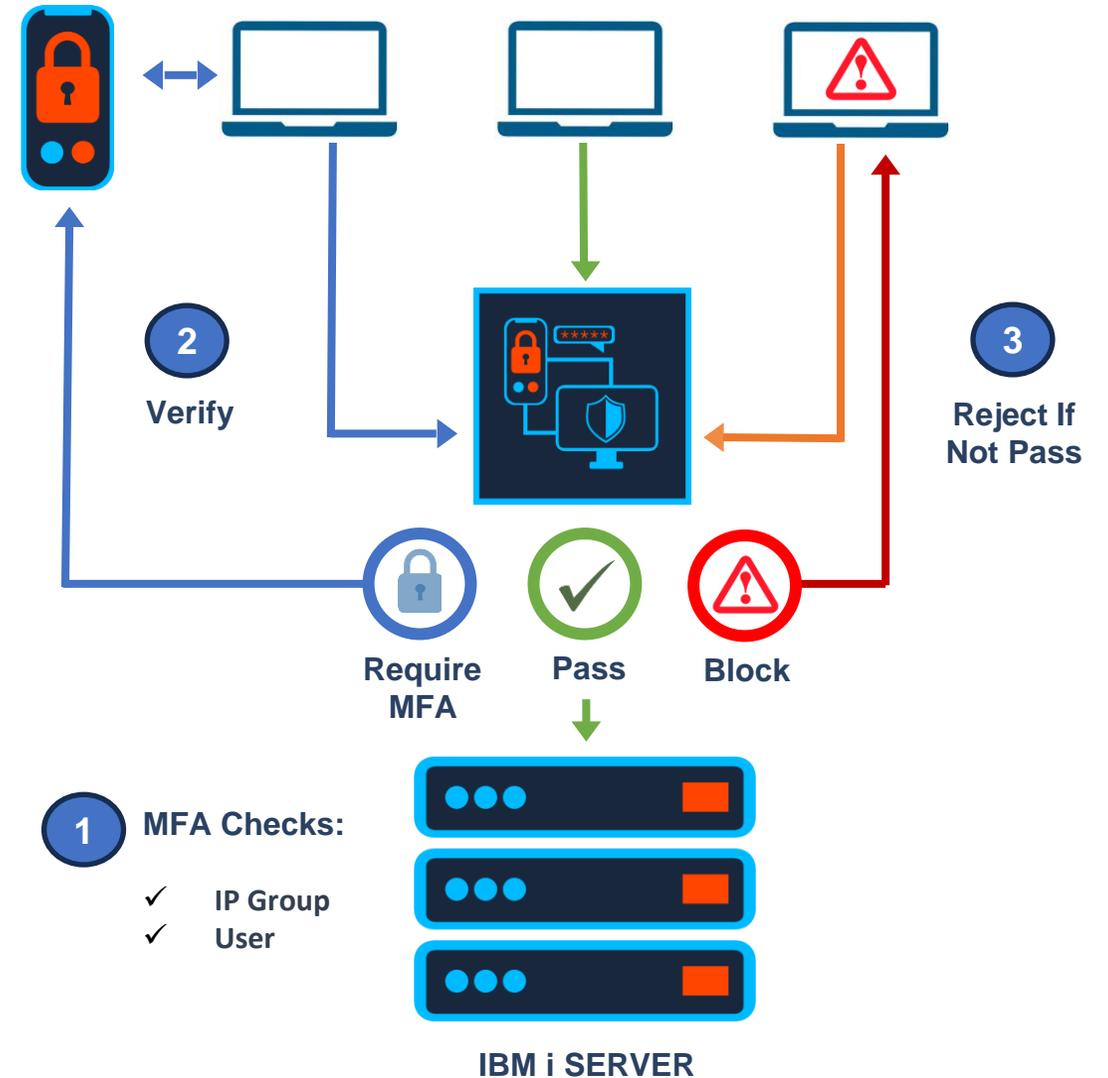
Do I need Multi-Factor Authentication?

iSecurity Multi-Factor Authentication helps your organization meet compliance standards like **PCI-DSS**, **NIS2**, **DORA**, etc. and improve the existing security environment on IBM i.

It requires the user, before gaining access to sensitive systems and data, to verify his or her identity with an additional credential.

Such additional credential is usually based on something he has (cell phone, email...) or something he is (fingerprint, face recognition...).

Lately **MFA** has also become a necessity to qualify for cyber insurance.



Zero Trust Approach

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction.

Rooted in the principle of “never trust, always verify,” Zero Trust protect modern environments and enable digital transformation by using strong authentication methods, leveraging network segmentation, preventing lateral movement and simplifying granular, “least access” policies.

Traditional Security

Where are you coming from?



Zero Trust

Who are you?



iSecurity MFA Insights

MFA works based on Persons, who are the owner of one or more users and at the same time they are inside an IP-Group so we can control every movement for every user within the system.

Our Solution:

- ✓ Enable Secure Sign On.
- ✓ Used to achieve and maintain compliance with leading industry regulations such as PCI-DSS, NIS2, DORA.
- ✓ MFA significantly reduces the risk of system penetration, up to 99%.



MFA in iSecurity Implementation

MFA requires beside the standard User/Password, an additional credential:

- ✓ One-Time Password.
- ✓ TOTP tokens - Time Based One-Time Password - RFC 6238.
- ✓ Using iSecurity APP for Apple or Android mobile phones.
- ✓ If the organization has an existing MFA system, it can be used as the additional credential.

Some additional information:

- ✓ TOTP tokens can be generated by the free Google/Microsoft/... Authenticator, or hardware generators.
- ✓ The APP can use: Fingerprint, Face recognition, Pattern, Pin etc.
- ✓ **MFA** of PingID, Duo, Okta are accessed directly to their APP. Other MFAs are connected by a link.



Token Generators

We can use ANY token generator that complies with RFC 6238, such as Google Authenticator, Microsoft Authenticator, and others. Usually, they are all free. All you need is a Smartphone.

For those who do not have a smart phone - then can use a hardware devices.

- ✓ Token generators create a six-digit codes.
- ✓ The generated codes changes every 30 seconds.
- ✓ It is known only to your call phone and your IBM i.
- ✓ This knowledge is based on a random 26-characters password.
- ✓ This password is entered once only in both sides.
- ✓ It is usually passed as a QR code, but can also be passed as a Character String.

Optionally, the organization may provide some **Emergency tokens**.

iSecurity Multi Factor Authentication

Let's see our Product in Action!

The best way to see how it works is a demo with **iSecurity MFA** running on a real environment.



RAZ-LEE

Selecting Authentication Methods

Person Classes

RLDEV/iSecurity [1]/MFA/Definitions/Person Classes

Class	Verify	Questions	Send By	Valid for (Min.)
*DFT	Email	2	Screen	999
PEPE	None	3	Email	120
QQ	Email	1	Email	10
QQ2	Email	0	Email	10
SASHA	None	2	Screen	999
TOTP	Email	3	Email	120
VCLAS	Email	3	Email	120

Person Class - Edit

Class: *DFT

Verification method: Once

Use Email Use Cell phone

Restrict Emails to domain(s):

Add't Authentication Factor

	OTP	TOTP	Questions	OAuth2	RSA/Radius	OpenID
For MFA	1	2	3	4	5	6
For AOD	1					
For P-R			1			

Use 1-9 to specify Priority (1=Highest) Blank=Do not use

Number of private questions: 2 0-10

Private questions retries: 3 0=*NOMAX

Wait before next attempt: 3 1-999 minutes (999=No retry)

Password-Reset

Perform: Select

Send password by: Screen

Password is valid for: 999 1-999 minutes (999=*NOMAX)

Cancel

iSecurity Navigator

- MFA
 - Persons
 - IP-Group Definitions
 - Local Users Not in Persons
 - MFA Setting for Persons
 - Persons By Users
 - Persons Information
 - Definitions
 - Person Classes
 - External Authentication Providers**
 - MFA Settings
 - Self-Enrollment Control
 - Multi-System
 - Password
 - PGP Encryption
 - Queries and Reports
 - Screen
 - System Information
 - User Management
 - Delete Unused Disabled Users

External Authentication Providers

RLDEV/iSecurity [1]/MFA/Definitions/External Authentication Providers

External Authentication Providers

Oauth2 (Google, Facebook...)

- GOOGLE - OAuth2 for limited device input Copy Delete
- Add OAuth2 provider

RADIUS (Duo, RSA...)

- DUO - Duo Security Copy Delete
- RSA - SecurID Copy Delete
- Add Radius provider

OpenID Connect (PingID...)

- PINGID - Ping Identity Copy Delete
- Add OpenID Connect provider

Sign On Process

1

Anmelden

System RLG
Subsystem QINTER
Bildschirm QPADEV0016

Benutzer RAZADM
Kennwort
Programm/Prozedur
Menü
Aktuelle Bibliothek



2

Anmeldeinformationen System: RLG

Vorherig

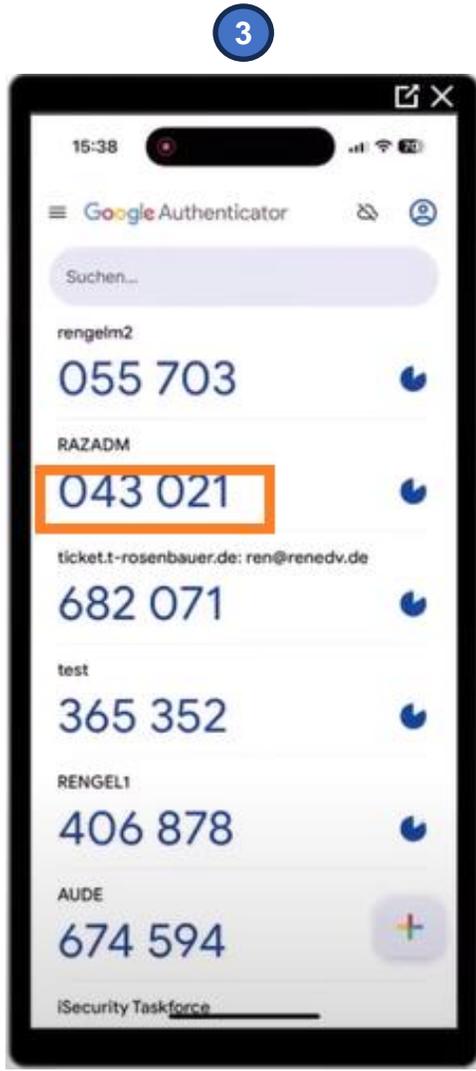
Enter MFA Token RLG

Person RAZADM

Enter TOTP, or press F7 to request a one time password.

MFA Token

F3=Exit F7=Request a one time password



4

Anmeldeinformationen System: RLG

Vorherig

Enter MFA Token RLG

Person RAZADM

Enter TOTP, or press F7 to request a one time password.

MFA Token 043021

F3=Exit F7=Request a one time password



5

MAIN IBM i-Hauptmenü System: RLG

Auswahlmöglichkeiten:

1. Benutzeraufgaben
2. Büroaufgaben
4. Dateien, Bibliotheken und Ordner
6. Datenfernverarbeitung
8. Problembehandlung
9. Menü anzeigen
10. Unterstützende Informationen - Auswahlmöglichkeiten
11. IBM i Access-Aufgaben
90. Abmelden

Auswahl oder Befehl
==> sign

F3=Verlassen F4=Bedienerführung F9=Auffinden F12=Abbrechen
F13=Unterstützende Informationen F23=Anfangsmenü festlegen

(C) COPYRIGHT IBM CORP. 1980, 2018.

MF B 20/011

FTP Sign On Process

1

```
Eingabeaufforderung - ftp 1.1.1.95

C:\Users\Robert>ftp 1.1.1.95
Verbindung mit 1.1.1.95 wurde hergestellt.
220-QTCP at RLG.RAZLEE.CO.IL.
220 Connection will close if idle more than 5 minutes.
501 OPTS unsuccessful; specified subcommand not recognized.
Benutzer (1.1.1.95:(none)): razadm
331 Enter password.
Kennwort:
_
```



2

Ungelesen/Gelesen Personen suchen

Alle Ungelesen Nach Datum

Heute

iSecurity_RLG
*FTPLOG *FYI* MFA confirm... 15:39
<http://1.1.1.95:10000/pr/MfaF>

iSecurity_RLG
RLG - QPRINT/ERROR OUT... 15:05
Systemname: RLG

iSecurity_RLG
RLG - QPRINT/ERROR OUT... 15:02
Systemname: RLG

iSecurity_RLG
RLG - QPRINT/ERROR OUT... 14:59
Systemname: RLG

*FTPLOG *FYI* MFA confirmation

iSecurity_RLG <SMTP@RAZ-LEE.DE>
An robert.engel@razlee.gmbh 15:39

[http://1.1.1.95:10000/pr/MfaRouter.html?
key=509000834751RLG_01240328153911_CET_*FTPLOG_DEURAZADM_RLG_3509312680T](http://1.1.1.95:10000/pr/MfaRouter.html?key=509000834751RLG_01240328153911_CET_*FTPLOG_DEURAZADM_RLG_3509312680T)



3

Google Authenticator

Suchen...

rengelm2
172 137

RAZADM
176 345

ticket.1-rosenbauer.de: ren@renedv.de
344 464

test
592 747

RENGEL1
889 526

AUDE
430 799

iSecurity Taskforce

RAZ-LEE
iSecurity MFA

Benutzer: RAZADM
System: RLG
Server: *FTPLOG
Datum: 2024-03-28 15:39

To confirm that this activity was started by you, please enter the MFA token.

MFA token:
176345

Send



4

```
Eingabeaufforderung - ftp 1.1.1.95

C:\Users\Robert>ftp 1.1.1.95
Verbindung mit 1.1.1.95 wurde hergestellt.
220-QTCP at RLG.RAZLEE.CO.IL.
220 Connection will close if idle more than 5 minutes.
501 OPTS unsuccessful; specified subcommand not recognized.
Benutzer (1.1.1.95:(none)): razadm
331 Enter password.
Kennwort:
230 RAZADM logged on.
ftp> _
```

iSecurity Multi Factor Authentication

| Advantages on our Solution

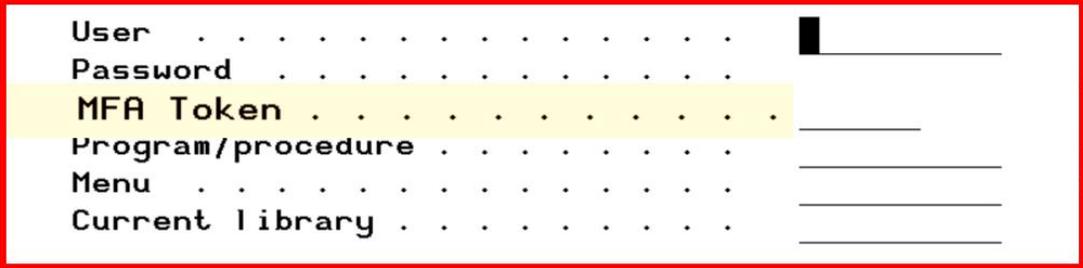
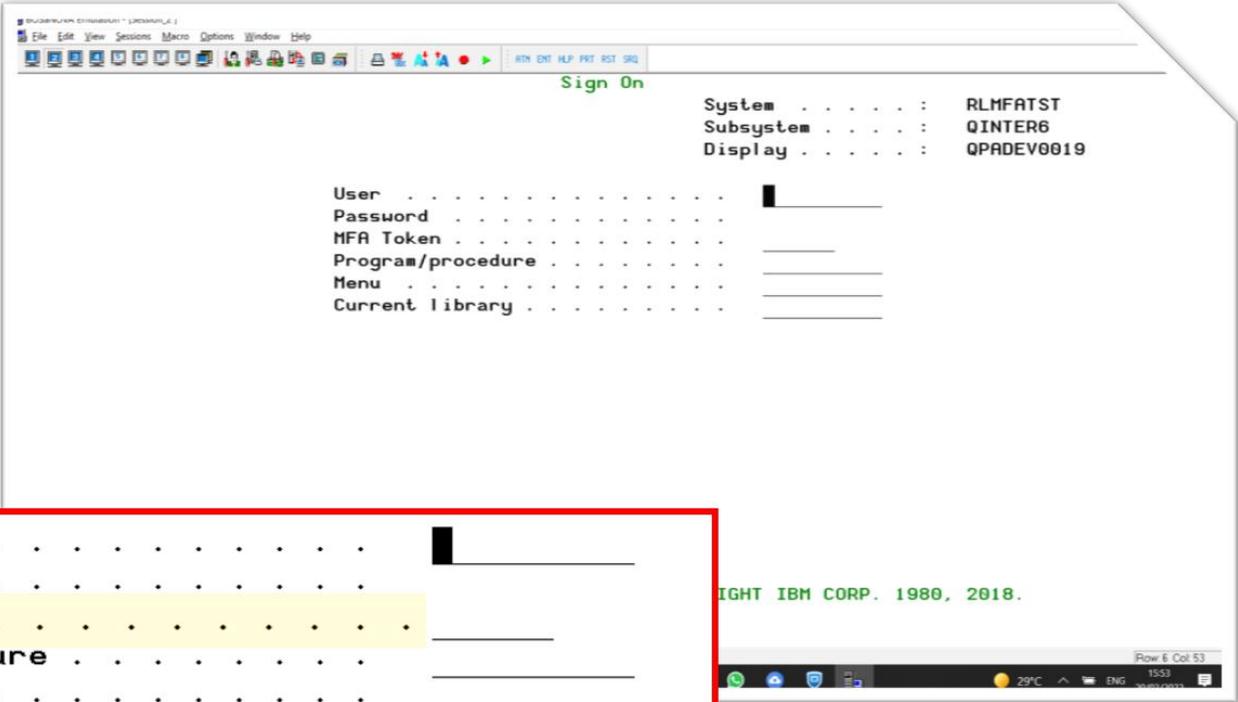
iSecurity MFA can control every movement for every user withing the system.



One Step Authentication

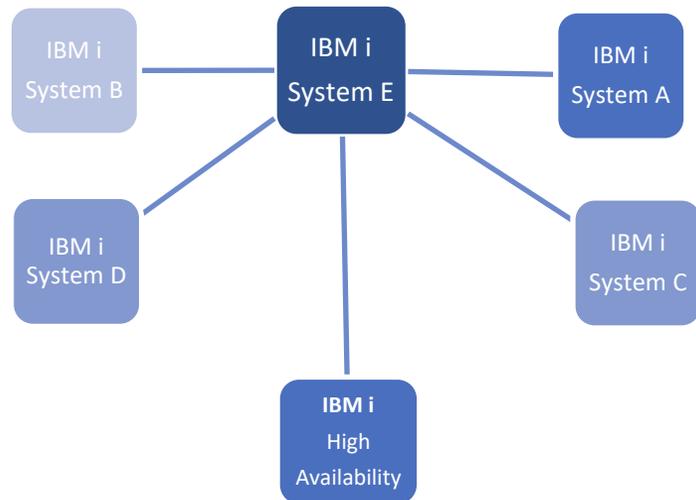
Single Step

Single Step Authentication is considered safer. **iSecurity MFA** enables you to modify the IBM i standard Sign On screen by adding the MFA Token entry field, following the regular password



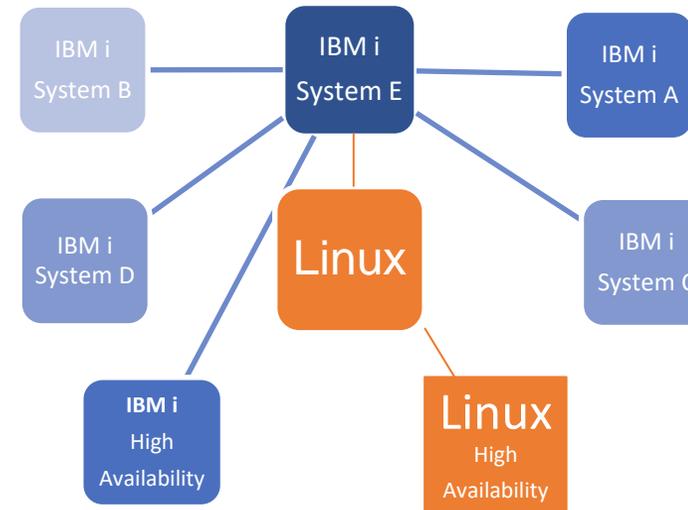
Simplicity

iSecurity MFA/Password-Reset/Authority On Demand



- ✓ Completely Native to the IBM I
- ✓ It installs and activates in minutes
- ✓ No need of additional hardware server
- ✓ No special Smartphone application is needed
- ✓ No special PC application is needed
- ✓ No knowledge of other OS is needed

Others' approach



- × Additional Hardware
- × Additional Software
- × Second Operating System
- × High Complexity

MFA Building Blocks – Person

Person

We are all human beings. We do not wish to get verified again and again. This is why we use the term, Person. This is why we verify Person and not User Profile.

Each Person may have multiple user profiles on multiple systems. Once a Person signs by one of his user profiles, and has been verified by **MFA** as working from a certain IP, he is not bothered again when he signs from the same IP to another session on this or other systems with a user profile that belongs to him.

This verification may be limited by time and includes Regular Sign On, as well as TCP services such as FTP, ODBC, REXEC, IFS share, etc.



MFA Building Blocks - IP Group

IP Group

The regular IP Addresses from which a Person signs on can be grouped in an IP Group, e.g. one or more offices and home addresses.

With **MFA**, you can decide what the system should do when a person signs on from within or from outside of the IP Group. You can decide to use **MFA** only when signing on from the outside, or request **MFA** when signing on from within, and reject other attempts.

This behavior can be set differently for regular Sign On, FTP, ODBC, REXEC, IFS share etc.



Persons and Locations

Now we talk about the combination of Person + IP group, this is extremely important because we can block or allow a person to enter the system depending on his location, so we totally ensure not only that the person is who she says she is, also we know where that person is logging in from.



John

- New York
- Atlanta (2 User Profiles)
- Tel Aviv
- Home

MFA Required Inside
Otherwise Rejected



Nataly

- New York (3 User Profiles)
- Atlanta

MFA Not Required Inside
MFA Required Outside



Matthew

- Tel Aviv
- Home

MFA Not Required Inside
Otherwise Rejected

iSecurity Multi-Factor Authentication Advantages

- ✓ **TCP/IP exit points support:** Our solution provides authentication not only to the standard login, also to TCP/IP servers (exit points).
- ✓ **Additional flexibility:** Based on the IP address from which a user accesses the IBM i. Based on predefined IP Groups (Location. Ranges) users can be rejected / require or not require authentication within the IP group.
- ✓ **iSecurity MFA is native to the IBM i:** Only uses standard applications on it and on smart phones. No need for additional hardware server, no special apps on phones and PCs.
- ✓ **Simplicity for 'Persons':** Users may have multiple profiles to access different systems. **iSecurity MFA** introduces the concept of a person rather than based on profiles. When a person is authenticated once (including the IP group), users can access using any of their user profiles.
- ✓ **Freedom of Authentication Method:** Users of Radius, Qauth2, OpenID (PingID) can get authenticated by one of these apps, **MFA** will continue having these apps in control of the users, eliminating the need for additional authentication.



RAZ-LEE

Contact us About our Products

Sales Representatives

sales@razlee.com

Visit Our Website

www.razlee.com

Multi **F**actor **A**uthentication ^{iSecurity}

