MFA

DATASHEET (iSecurity Suite Authentication & Authorization)

Multi Factor in One Single Step

Multi Factor Authentication (MFA) helps organizations meet compliance standards and improve the existing security environment on IBM i. It requires a user to verify his or her identity with two or more credentials before gaining access to sensitive systems and data. Used for achieving and maintaining compliance with the leading industry regulations, such as PCI-DSS. Lately it has also become a necessity to qualify for cyber insurance.

MFA significantly reduces the risk of system penetration, up to a remarkable 99%

iSecurity Multi Factor Authentication does it simple inside the IBM I, and as a part of the initial program, prompting for MFA at sign-on. We do not need to use multiple login stages, one step is enough.

iSecurity Multi Factor Authentication is a powerful solution to enable Secure Sign On.

Flexibility

iSecurity Multi Factor Authentication is based on Ip Ranges and Person one MFA is good enough for all of a Person's activity from the same IP for a specified time!

Which Person	Person 01	Person 02	Person 03
From Where they Work	Work From Points A,B,C,D	Work From Points A,B	Work From Points C,D
Inside MFA required?	MFA required from Inside	No MFA From Inside	MFA required from Inside
Outside MFA Reject User	Cannot sign on from Outside	MFA required from Outside	MFA required from Outside

Authentication Freedom

MFA works with every Authenticator App available in the Market. We use ANY Token generator, such as Google Authenticator on a mobile phone or by any hardware device. Freedom is part of our Multi Factor Authentication.

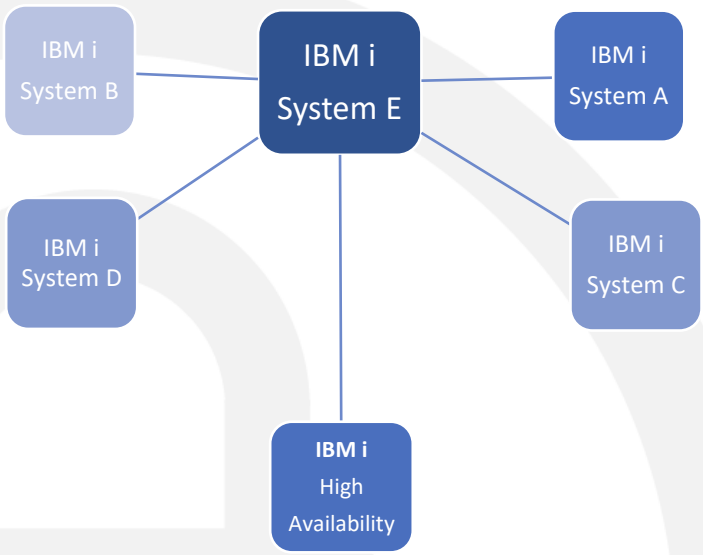
Key Features

- Integrated at Initial Screen
- We look at Person and IP-Group
- One MFA is good enough for all of a Person's activities, from the same IP, for a specified time.
- TCP/IP exit points support MFA provides authentication not only to the standard login, also to TCP/IP servers (exit points). Including:
  - FTP Server
  - REXEC
  - FTP Client
  - ODBC
  - File Server
  - Remote PGM/CMD
  - DDM/DRDA
- 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.
- 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.

Our Solution Approach

We love to keep things as simple as possible, also the iSecurity Multi Factor Authentication follows this directive, only needing to be installed at the IBM i System.

iSecurity MFA/PR/AOD



Implementation Requirements

MFA Servers

- Linux Server – IBM Does it All
- Linux installation – Don't Need it
- Linux HA for the above – Don't Need it
- Unique Server Software – Don't Need it

Dedicate Mobile and Desktop Apps

- Smartphone App – Any Authenticator
- Special PC Application – Don't Need it
- Other S.O. Knowledge – Don't Need it
- Special Hardware Keys – Don't Need it

Let's Get Started

Schedule your Demo and protect Authentication & Authorization on your Systems with iSecurity Multi Factor Authentication.

RAZ-LEE iSecurity