



# Assure Multi-Factor Authentication

## Strengthen password security with Multi-Factor Authentication

As stories of data breaches caused by exploited credentials continue to make headlines, it is clear that basic password protection mechanisms are no longer good enough. Organizations require an additional layer of protection that is also easy to use and doesn't impose an additional burden on administrators.

Multi-factor authentication, also referred to as two-factor authentication, has become a popular method for strengthening security since it requires a user to provide more than one identifying factor prior to accessing a system, an application or its data. These factors can include something they know (user id, password, PIN), something they have (email account, smart phone, token device) or something they are (finger print, iris scan).

Assure Multi-Factor Authentication, a feature of Assure Security, improves the security of your IBM i system and core business applications. With Assure Multi-Factor Authentication you can:

- Add an authentication layer beyond memorized or written passwords
- Meet regulatory requirements and recommendations in PCI DSS 3.2, HIPAA, 23 NYCRR 500, Swift Alliance Access and others
- Invoke rules-based multi-factor authentication only for users or specific situations that require it
- Lower the risk of unauthorized access to systems, applications and data
- Reduce the risk of data theft and its costs and consequences
- Maintain an audit trail of multi-factor authentication failures for alerts, reports or integration with a SIEM solution
- The use of Assure Multi-Factor Authentication can be expanded to support password self-service and the "four eyes principle" of supervised changes to sensitive data.

Passwords alone are weak. The frequency of breaches due to stolen or guessed passwords and brute-force attacks requires an additional layer of user authentication security.

Time	Rule	Profile	User	RADIUS Profile	Decision	Reason	Authenticating User
2021-09-08 12:36:12	*DEFAULT	HASKLE	-	-	Deny	MFA007-Action is "REJECT"	-
2021-09-08 12:35:45	MFA0NF1P	MILLERT	tommler	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:34:43	MFA0ND0BC	MILLERT	tommler	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:33:21	CPWGA	MILLERT	tommler	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:32:12	DFUAPP1	SMITH	branseth	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:31:18	DFUAPP2	SMITH	branseth	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:30:39	DFUOTHR	JONES	craigones	-	Deny	MFA007-Action is "REJECT"	-
2021-09-08 12:29:56	SQLRL	SMITH	branseth	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:28:11	APP1	JONES	craigones	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:27:12	APP1	JONES	craigones	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:26:16	APP1	JONES	craigones	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:25:36	MYSLFPWD	OLSCH	duddson	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:24:42	APP1	JONES	craigones	-	Allow	MFA007-Authenticated by RSA	-
2021-09-08 12:23:57	*DEFAULT	HASKLE	-	-	Deny	MFA007-Action is "REJECT"	-
2021-09-08 12:22:29	SQLRL	SMITH	branseth	-	Allow	MFA007-Authenticated by RSA	-



## Powerful, flexible Multi-Factor Authentication

Assure Multi-Factor Authentication provides peace of mind by ensuring only authorized individuals obtain access to your systems and sensitive data, and delivers the flexibility to meet the needs of your environment and business. Multifactor authentication can be integrated into the IBM i 5250 signon screen or invoked on demand.

When integrated with the signon screen, you can choose between single-step or two-step authentication. Singlestep authentication requires both the user's password and a token for authentication. The user is not told which one failed if either is incorrect, delivering true multi-factor authentication. With the two-step process, a token screen is presented after the IBM i signon.

Assure Multi-Factor Authentication's rules engine makes it easy to configure the solution to invoke multi-factor authentication screens only for the users or specific situations that require it. Rules criteria are available to specify which users should authenticate through Assure Multi-Factor Authentication based on whether they:

- are registered or unregistered
- are limited capability users
- are a member of specific group profiles
- possess special authorities
- are using a specific device
- are authenticating from a specific subsystem or iASP
- have a particular IP address
- are authenticating at a certain date or time.

If Assure Multi-Factor Authentication is invoked on demand, either manually or in a program, the calling program can also be specified as a criterion. Predefined rules are provided to help you get started quickly. With Assure Multi-Factor Authentication you also have a choice of authentication methods:

- **Built-In Authenticator** - Assure Multi-Factor Authentication has a built-in authentication service that transmits a token by email and/or popup. This method is recommended for cost-sensitive environments.
- **RADIUS-Compatible Authenticators** - Assure Multi-Factor Authentication contains a RADIUS client that runs natively on IBM i for organizations that wish to use an existing RADIUS-based authenticator or build their own RADIUS server. This includes authenticators such as the DUO Authenticator and the Microsoft Azure Authenticator.
- **RSA SecurID®** - Assure Multi-Factor Authentication is certified by RSA as compliant with SecureID to serve the most demanding environments through integration with RSA RADIUS servers and RSA RADIUS cloud services. RSA cloud services support biometrics, such as a finger print or facial image from a mobile phone, in addition to traditional voice mail token, SMS token, and push approval methods.

Authentication failures can be logged by Assure Multi-Factor Authentication for monitoring and optional forwarding to a SIEM server.

## Self-Service user re-enablement and password changes

Assure Multi-Factor Authentication's on-demand authentication capabilities can also be used to grant users the ability to re-enable their profiles or change their passwords if forgotten. If configured, users can answer pre-configured security questions and/or receive a single-use token via popup, email or RSA SecurID device before performing changes to their profiles.

## Four eyes principle for supervised changes to sensitive data

For operations that could have significant impact on the server, or for data changes that are so sensitive they must be supervised by a second pair of eyes, Assure Multi-Factor Authentication can be used to enforce a four eyes policy. When a user wishes to perform such a change or operation, a designated administrator receives an email with a single-use token along with information on the identity of the user making the request and the job number. The administrator can then enter the single-use token into the user's screen and observe the change while it is made.

## RSA certification

Visit <https://community.rsa.com/docs/DOC-92160> to view the RSA SecurID Access Implementation Guide for Assure Multi-Factor Authentication.

Priority	Status	Rule	Profile or Group	Users	MFA Profile	Category	Action
10	On	MFA5250 Require RADIUS token on Sign-On screen.	All	All	Must exist	Sign On	Challenge user interactively
20	On	MFA5250FP Require RADIUS token to access FTP.	All	All	Must not exist	Server Access	Challenge user in listener
30	On	MFA5250DBS Require RADIUS token to access DDS.	All	All	Must exist	Server Access	Challenge user in listener
40	On	CPV5250 Require RADIUS token to access web browser.	All	All	Must exist	Web Listener	Challenge user in listener
50	On	DFUAAPP1 Require RADIUS token to access Applet files.	All	HR*	Optional	File Access	Challenge user interactively
60	On	DFUAAPP2 Require RADIUS token to access Applet files.	All	MKTG*	Optional	File Access	Challenge user interactively
70	On	DFUACTHR Open access to transfer files and notify admin.	All	All	Optional	File Access	Always deny
80	On	STRSQLRUL Require RADIUS token to make SQL requests.	All	**ACC_DB2	Must exist	SQL Access	Challenge user interactively
90	On	APP1 Require RADIUS token to access Applet.	All	**ACC_DB2	Optional	Custom	Challenge user interactively
100	On	APP2 Require RADIUS token to access Applet.	All	**ACC_DB2	Optional	Custom	Challenge user interactively
110	Off	MYSELFNA Allow users to self-enable their profile.	All	HR*	Optional	Enable Profile	Challenge user interactively
120	Off	MYSELFPWD Allow users to reset their password.	All	MKTG*	Optional	Reset Password	Challenge user interactively