Power Week 2025

#pw2025

18 - 19 - 20 novembre 2025
IBM Innovation Studio Paris

Multi-Level Control Strategies for securing IBM I Access

20 novembre 11:15 - 12:15

Stephan Leisse
Principal Sales Engineer
PRECISELY
stephan.leisse@precisely.com

precisely

IBM

common
FRANCE

Power Week

18 -19 - 20 novembre 2025

Multi-Level Control Strategies for securing IBM I Access

IBM

common

FRANCE

IBM

precisely

CO
Kitchen
Office
Bathroom
TTRWIN
1 2 3
4 5 6
7 8 9
* 0 #
renkforce

IBM i System-Access Security

Keep unauthorized users out of your IBM i; maintain tight control over what authorized users can do once logged in monitor their activities

Consider these 4 questions

1. "How do you ensure that the User logging in is the actual person?“

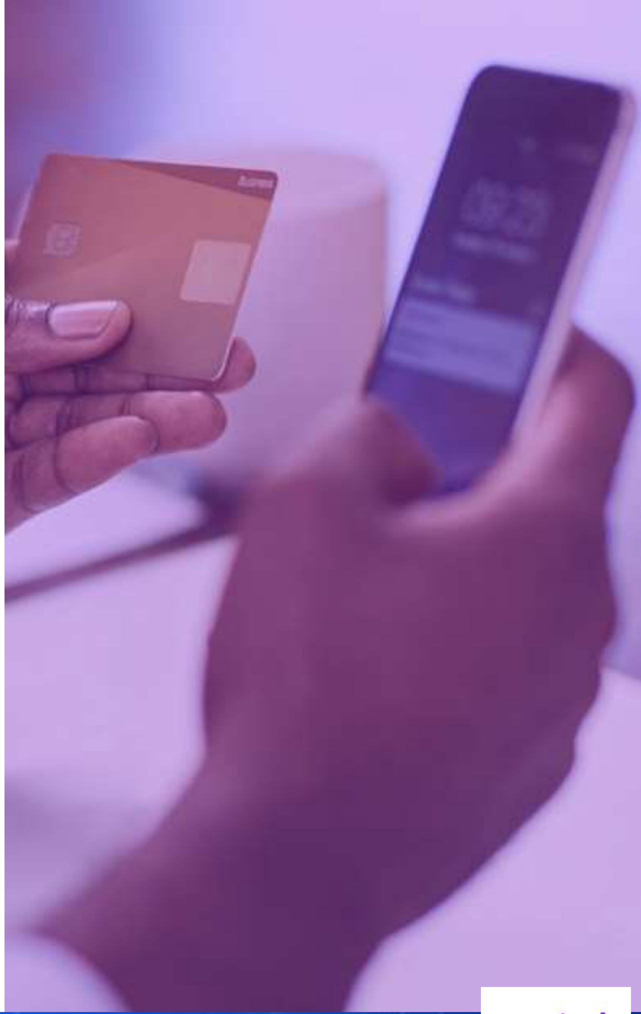
Multi-Factor Authentication Adds a Layer of Login Security

Multi-Factor Authentication (MFA), requires responses to challenge questions based upon two or more of the following factors:

- A "Knowledge Factor": Something the user knows
  - E.g. user ID, password, PIN, security question
- A "Possession factor": Something the user physically has
  - E.g. smartphone, smartcard, token device
- An "Inherence Factor": Something biologically unique to the user
  - E.g. fingerprint, iris scan, voice recognition (Biometrics)

Typical authentication on IBM i uses 2 items of **the same class or type factor** – such as User ID and Password.

This is ***NOT*** multi-factor authentication.



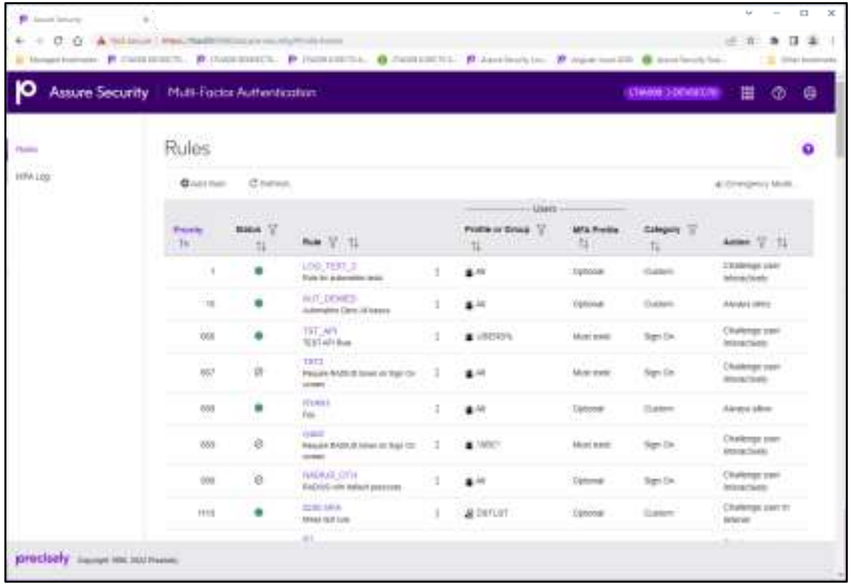
Why Multi-Factor Authentication?

- ✓ Adds an authentication layer above and beyond memorized or written passwords
- ✓ Enables your organization to meet audit and regulatory requirements and recommendations in PCI DSS 4.0, HIPAA, NYDFS Cybersecurity Regulation, Swift Alliance Access and more
- ✓ Lowers the risk of unauthorized access to systems, applications and data
- ✓ Reduces the risk of password theft and its costs and consequences
- ✓ Invokes rules-based multi-factor authentication only for users or specific situations that require it

How Precisely Can Help

Assure Multi-Factor Authentication

- Powerful, flexible multi-factor authentication for IBM i
- Options to initiate from the 5250 signon or on-demand
- Options for one-step or two-step authentication
- Options for authentication on FTP-ODBC/JDBC-SSH-Netserver (IFS) etc.
- Enables self-service profile re-enablement and self-service password changes
- Supports the Four Eyes Principle for supervised changes



Rules

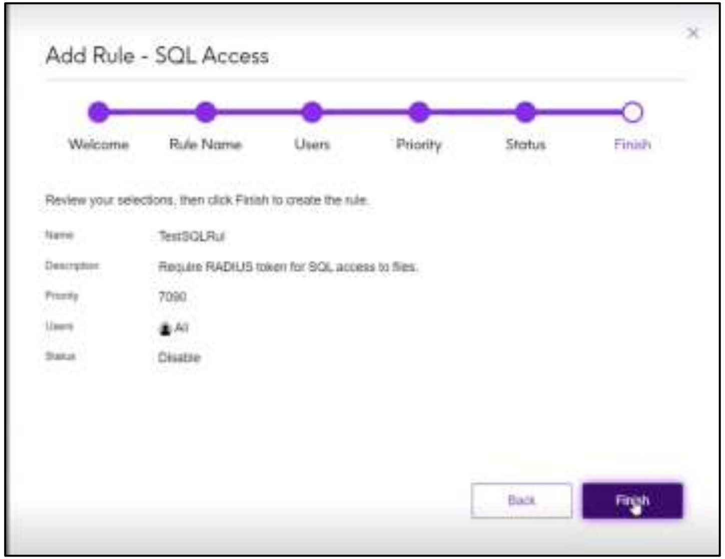
Priority	Status	Rule		Profile or Group	MFA Profile	Category	Action
1	●	LOG_TEST_2 [illegible]	1	All	Optional	Custom	Challenge user interactively
10	●	AUT_DENIED [illegible]	1	All	Optional	Custom	Always deny
666	●	TST_API TEST API Rule	1	USER45%	Must exist	Sign On	Challenge user interactively
667		TEST Require RADIUS token on Sign On screen	1	All	Must exist	Sign On	Challenge user interactively
668	●	[illegible]	1	All	Optional	Custom	Always allow
669		[illegible] Require RADIUS token on Sign On screen	1	[illegible]	Must exist	Sign On	Challenge user interactively
699		RADIUS_OTH RADIUS with default password	1	All	Optional	Sign On	Challenge user interactively
1110	●	5250 MFA [illegible]	1	DEFLIST	Optional	Custom	Challenge user in [illegible]

precisely Copyright [illegible] Precisely

Powerful Rules

Assure Multi-Factor Authentication's rules engine makes it easy to configure users or situations requiring multi-factor authentication

- Rules criteria include whether the user is:
  - Registered or unregistered
  - A limited-authority user
  - A member of specific group profiles
  - In possession of special authorities
  - Using a specific device
  - Authenticating from a specific subsystem or iASP
  - Using a particular IP address
  - Authenticating at a certain date or time



Review your selections, then click Finish to create the rule.

Name: TestSQLRul
Description: Require RADIUS token for SQL access to files.
Priority: 7090
Users: All
Status: Disable

- If invoked on demand, the calling program can also be a criterion
- Pre-defined rules are provided for quick implementation

Multiple Authentication Methods

Security challenge questions

- Assure Multi-Factor Authentication asking multiple security questions and validate with user pre-entered answers
  - Pre-Defined questions delivered
  - Supports different languages
  - Simply & easy additional authentication

Built-in authenticator

- Assure Multi-Factor Authentication has a built-in authenticator
  - Token is transmitted by email and/or popup
  - Best for less demanding environments where cost is an issue

TOTP authentication (coming soon)

- TOTP associated to each Assure Security MFA User
- Web based user management
- 'Self-Service' Registration process
- Support any industry standard TOTP generation application such as
  - Google Authenticator
  - Okta Verify
  - Microsoft Authenticator, etc.

RSA & RADIUS authentication

- Assure MFA is certified with RSA SecurID
- On-premise and cloud, software tokens, hardware tokens, push, and biometric options for any RADIUS compatible Server like
  - Okta, Duo
  - Microsoft Entra (Azure) thru NPS
  - Other RFC protocol-based RADIUS

RSA READY

IBM’s New MFA Offering for IBM i

IBM i v7.6 includes MFA capabilities

- Highlights growing industry adoption
- Timely move as corporations seek robust security solutions

We have been focused on MFA for years

- We have deep expertise
- Track record of continues innovation
- We’ve helped many customers implement an MFA solution

Assure MFA offers a more comprehensive solution

- IBM's MFA solution has potential notable limitations
- Assure MFA can address these gaps

Choosing an MFA Solution for IBM i

Every company needs MFA on their IBM i systems. IBM's latest MFA offering is evidence of this importance, but Assure MFA is a more robust, full-featured solution. Here's why…

User-Friendly Authentication

IBM's solution is limited to TOTP only. Assure MFA supports multiple authentication methods, including push notifications and On-Demand Authentication, which are more user-friendly.

+

Centralized Management

Assure MFA utilizes centralized Radius servers, making it easier to manage. IBM's implementation requires users to create and configure keys for each system, adding complexity.

+

Integration with IAM Platforms

Assure MFA supports integration with various Identity and Access Management (IAM) platforms such as Okta, DUO, Microsoft Entra ID and others, providing flexibility and ease of use.

+

Incremental MFA Definitions

Assure MFA offers a phased approach to defining users and applications. This allows for better productivity and gradual testing. IBM's MFA requires all applications to be MFA-protected at once for selected users.

Ransomware Protection

Our MFA integration with SAM offers enhanced ransomware protection, taking MFA to the next level and contributing to your Zero Trust strategy.

+

Flexible Control

Assure MFA provide the ability to define controls at the individual user or group level, offering more flexibility in implementation

+

Support for Older OS Versions:

Assure MFA supports OS levels below v7.6, ensuring that customers with older systems are not left behind

=

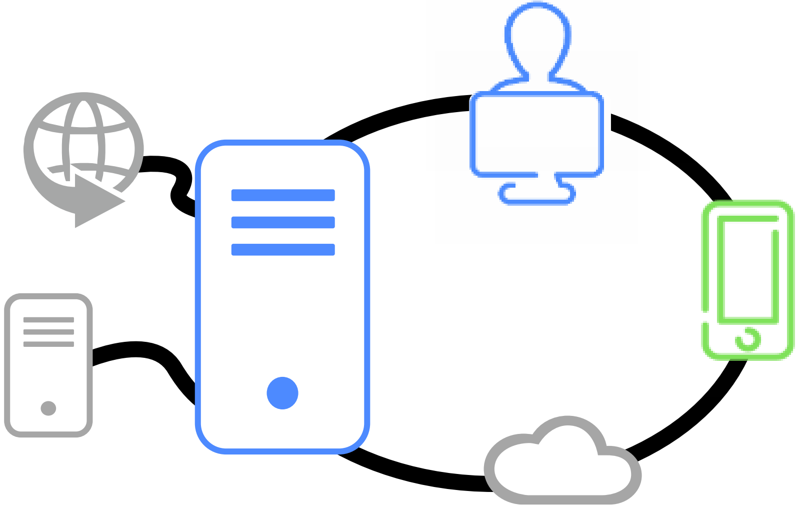
Assure MFA offers a more complete solution!

Consider these 4 questions

1. "How do you ensure that the User logging in is the actual person?"
2. "Should the user have permission to access the resource?

Network interfaces, the often-overlooked risk

- Network Servers are likely to be your single biggest threat
- Activities that come through the network servers are ubiquitous – you may not be able to tell who is downloading (or uploading), running SQL statements, or even executing remote commands
- Some servers allow command functions and IGNORE a profile's 5250 command line restriction



Securing Access to IBM i

IBM i is increasingly connected and integrated

- Legacy, proprietary protocols are interconnected with open-source protocols – creating access point security headaches
- The worldwide hacker community now recognizes the IBM i as a high-value target

Four critically important routes of access must be secured

- Networks and Endpoints
- Communication ports
- Databases
- System Commands

Exit Point Programs are key to securing routes of access

- Exit Points are essentially security checkpoints
- Exit Programs are the guards

Exit Points and Exit Programs

How do exit points and exit programs work?

- Exit points provide “hooks” to invoke one or more user-written exit programs for a variety of OS-related operations
- Exit programs allow or deny access based on parameters such as permissions, date/time, user profile settings, IP addresses, etc.

How are exit programs used for access control?

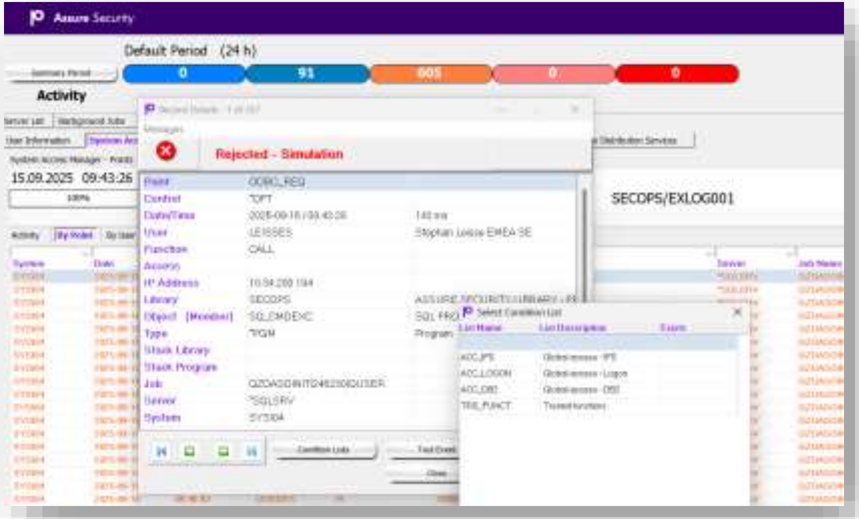
- Exit point programs are registered to particular exit points
- Command exit points can allow or deny command execution based on context and parameters
- Exit programs can also trigger actions such as logging access attempts, disabling user profiles, sending an alert, etc.

How Precisely Can Help

Assure System Access Manager

Comprehensive control of external and internal access

- **Network access**
  - (FTP, ODBC, JDBC, OLE DB, DDM, DRDA, NetServer, etc.)
- **Communication port access**
  - (using ports, IP addresses, sockets - covers SSH, SFTP, SMTP, etc.)
- **Database access**
  - (open-source protocols - JSON, Node.js, Python, Ruby, etc.)
- **Command access**



15.09.2025 09:43:26

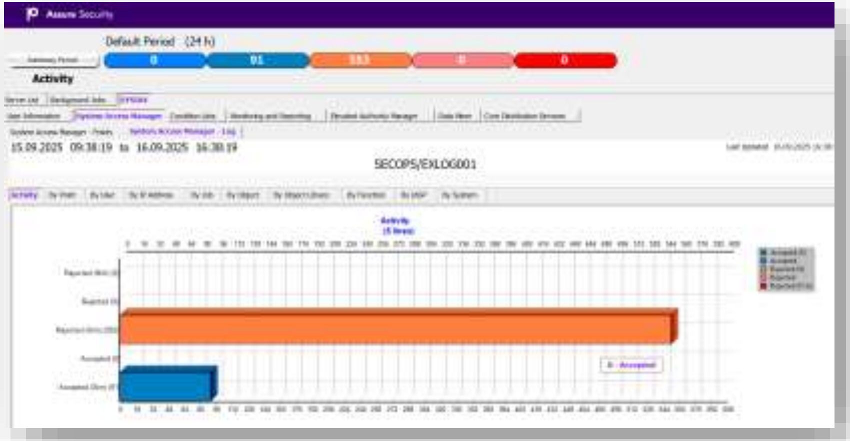
Point	ODBC_REQ	
Control	*OPT	
Date/Time	2025-09-15 / 09:43:26	140 ms
User	LEISSES	Stephan Leisse EMEA SE
Function	CALL	
Access		
IP Address	10.94.200.194	
Library	SECOPS	ASSURE_SECURITY_LIBRARY
Object (Member)	SQL_CMDEXC	SQL PRO
Type	*PGM	Program
Stack Library		
Stack Program		
Job	QZDASOINIT/QUSER	
Server	*SQLSRV	
System	SYS304	

List Name	List Description	Exists
ACC_IPS	Global access - IPS	
ACC_LOGON	Global access - Logon	
ACC_DB	Global access - DB	
TRS_FUNCT	Trusted functions	

Assure System Access Manager

Powerful, flexible and easy to manage

- Easy to use graphical interface
- Standard configuration easy deployment
- Powerful, flexible rules for controlling access based on conditions such as date/time, user profile settings, IP addresses, etc.
- Simulation mode for rules testing
- Provides alerts and produces reports
- Logs access data for SIEM integration



Consider these 4 questions

1. "How do you ensure that the User logging in is the actual person?“
2. “Should the user have permission to access the resource?
3. “Is the current (high) privilege needed all the time?”

What Is Elevated Authority?

- Granting elevated authority gives a user more powerful IBM i system privileges
  - Also referred to as "Special Authorities" or "Privileged Access"
- Enables more advanced data, object, and field access and control, beyond standard System Defined Authorities
- To perform certain parts of their jobs, many users need to have elevated authority, at least temporarily
- Key word is "Temporary"
- To prevent cascading and catastrophic security breakdowns, the processes for granting and revoking elevated authority must itself be very carefully managed and controlled

Challenges of Managing Elevated Authority

- Users naturally feel that they can be trusted and should have more authority to do their job more efficiently. Administrators can be pressured to agree.
- Manually granting and revoking elevated authority is risky:
  - Elevating Authority is easy, and can be done with a few keystrokes in a rushed moment, without proper oversight or logging
  - Revocation steps may be postponed, deprioritized by the tyranny of the urgent, or may simply be forgotten
- Activities of users with elevated authorities must be logged, to comply with regulations
- Activities of administrators with elevated authority also need to be monitored and logged, under “2-Key” principles

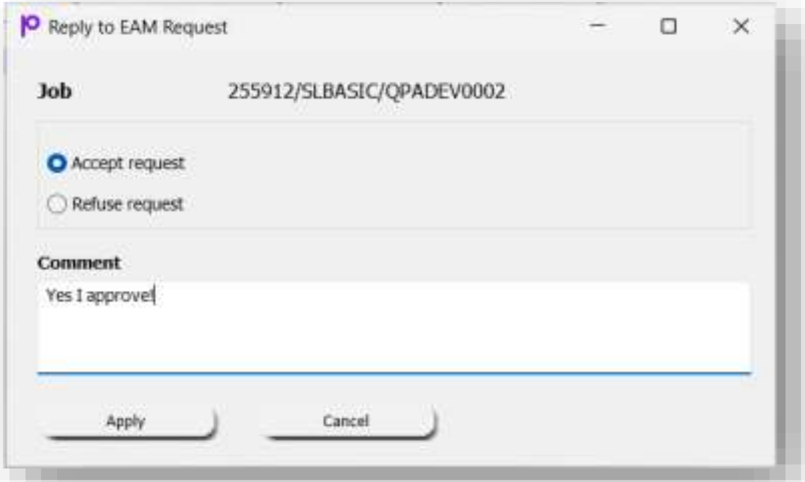
I need to be *SYSOPR for this assignment!
I need *ALLOBJ to do my job!
Can I have *SPLCTL for my project?

How Precisely Can Help

Assure Elevated Authority Manager

Allows easy elevation of authority as-needed basis

- Users request elevated authorities for a specific action
- Administrators can manually grant requests or rules can be configured to automatically grant requests
- Rules can be defined for source and target profiles based on group profiles, supplemental groups, lists of users and more
- Rules can also determine the context in which authority can be granted, such as time of date, job name, IP address and more


Reply to EAM Request

Job 255912/SLBASIC/QPADEV0002

● Accept request

○ Refuse request

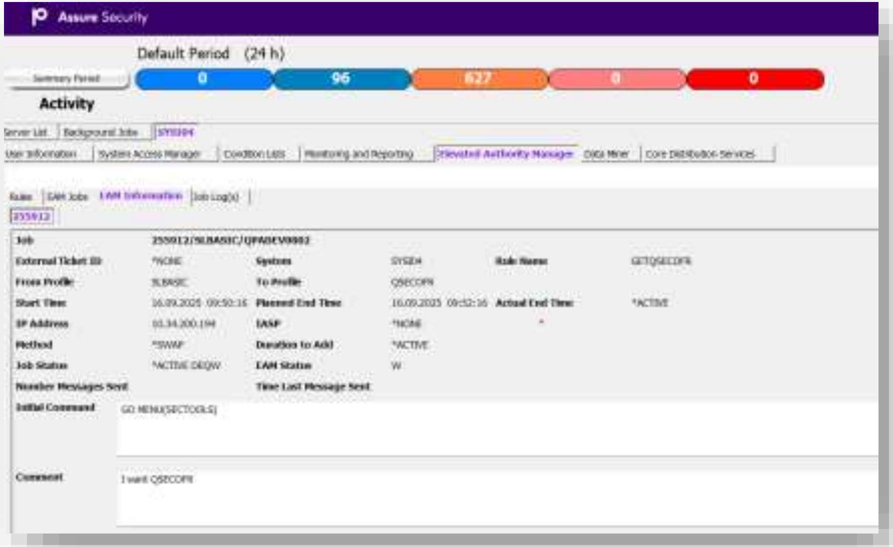
Comment

Yes I approve

Assure Elevated Authority Manager

Provides flexibility and control

- *SWAP or *ADOPT methods can be used to elevate authority
- An option is available to log (*LOG) user activity without changing authorities
- Handles processes connecting via ODBC, JDBC, DRDA and FTP

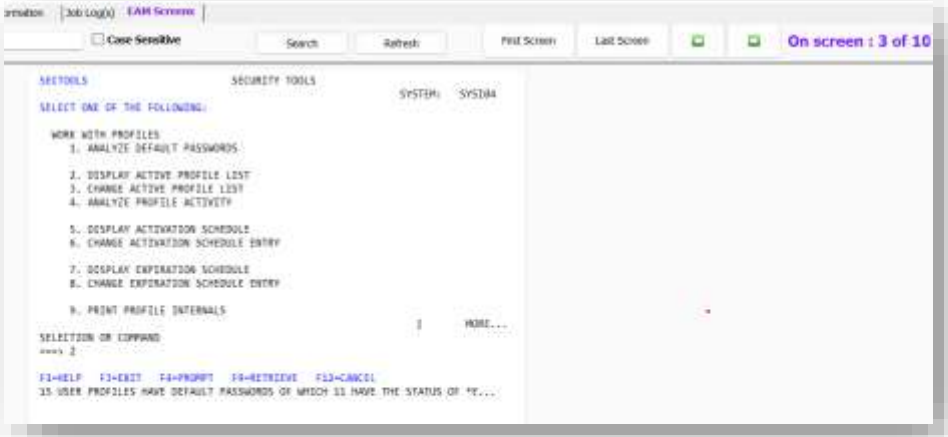


Job	255912/SLBASIC/QPADEV0002				
External Ticket ID	*NONE	System	SYSDE4	Rule Name	GETQSECOFR
From Profile	SLBASIC	To Profile	QSECOFR		
Start Time	16.09.2025 09:50:16	Planned End Time	16.09.2025 09:52:16	Actual End Time	*ACTIVE
IP Address	10.34.200.194	IASP	*NONE	*	
Method	*SWAP	Duration to Add	*ACTIVE		
Job Status	*ACTIVE DEQW	EAM Status	W		
Number Messages Sent		Time Last Message Sent			
Initial Command	GO MENU(SECTOOLS)				
Comment	I want QSECOFR				

Assure Elevated Authority Manager

Enables comprehensive monitoring of elevated profiles

- Monitors elevated users and duration of elevation from GUI or 5250 displays
- Maintains an audit trail of elevated activity using job logs, screen captures and journals
- Produces alerts on events such as exceeding authorized time
- Generates reports in a variety of formats
- Allows integration with ticketing systems



```
SECTOOLS                    SECURITY TOOLS
                                                  SYSTEM:   SYSTD4
SELECT ONE OF THE FOLLOWING:

  WORK WITH PROFILES
     1. ANALYZE DEFAULT PASSWORDS

     2. DISPLAY ACTIVE PROFILE LIST
     3. CHANGE ACTIVE PROFILE LIST
     4. ANALYZE PROFILE ACTIVITY

     5. DISPLAY ACTIVATION SCHEDULE
     6. CHANGE ACTIVATION SCHEDULE ENTRY

     7. DISPLAY EXPIRATION SCHEDULE
     8. CHANGE EXPIRATION SCHEDULE ENTRY

     9. PRINT PROFILE INTERNALS
                                                  1      MORE...
SELECTION OR COMMAND
===> 2

F1=HELP   F3=EXIT   F4=PROMPT   F9=RETRIEVE   F12=CANCEL
15 USER PROFILES HAVE DEFAULT PASSWORDS OF WHICH 11 HAVE THE STATUS OF *E...
```

Consider these 4 questions

1. "How do you ensure that the User logging in is the actual person?“
2. “Should the user have permission to access the resource?
3. “Is the current (high) privilege needed all the time?”
4. “Do I need **to monitor** the user's activity?”

Monitoring Security is Essential

Monitoring changes to systems and data is necessary for:

- Rapid response to security and data integrity issues
- Preventing deviations from compliance and security policies
- Ensuring application integrity and performance

Monitoring and logging enables forensics and auditing goals

- Proactively identifying subtle patterns of malware and ransomware
- Supporting discussion of security issues with executive teams
- Establishing and improving Data Governance practices

Regulations require that you track changes to your system and its data

- PCI DSS
- HIPAA
- GDPR
- SOX
- CCPA
- 23 NYCRR 500
- and many more

Monitoring IBM i Security

A strong IBM i security foundation requires solutions that monitor all system and data activity in detail – and capture vital security data in log files

IBM i offers many detailed and secure audit logs

- System Journal – QAUDJRN
- Database (Application) Journals – for Before and After Images
- Other IBM Journals are available
- QHST Log Files – DSPLOG Command
- System Message Queues – QSYSOPR, QSYSMSG

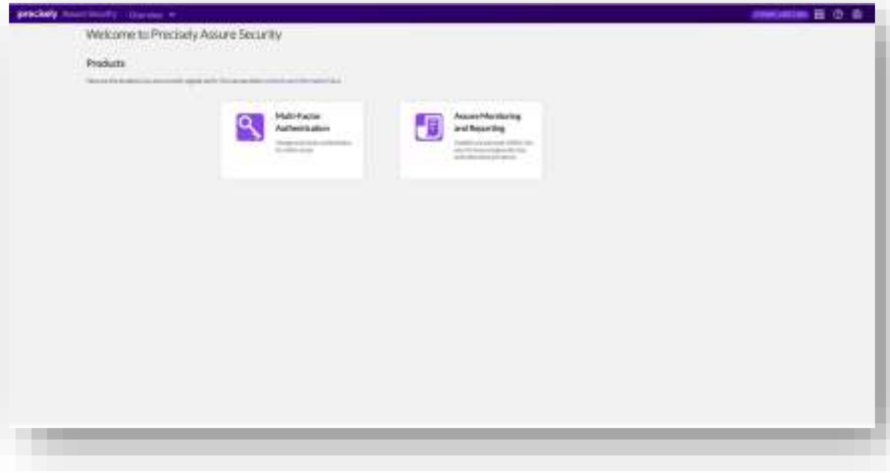
Turn on auditing, save journal receivers, and take advantage of everything the operating system can log for you!

How Precisely Can Help

Assure Monitoring & Reporting

Comprehensive monitoring of system and database activity

- Provides security and compliance event alerts via e-mail popup or syslog
- Includes out-of-the-box, customizable models for ERP applications or GDPR compliance
- Serves as a powerful query engine with extensive filtering
- Produces clear, easy-to-read reports continuously, on a schedule or on-demand
- Supports multiple report formats including PDF, XLS, CSV and PF formats
- Distributes reports via SMTP, FTP or the IFS
- Offers online help guides and tooltips with clear instructions

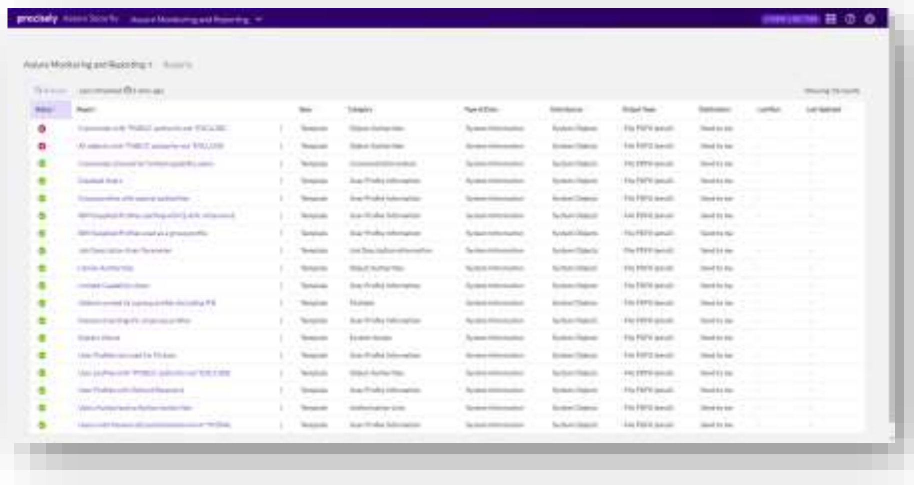

Welcome to Precisely Assure Security

Products

Sample Reports

Here are just a few examples of reports you can create with Assure Monitoring and Reporting

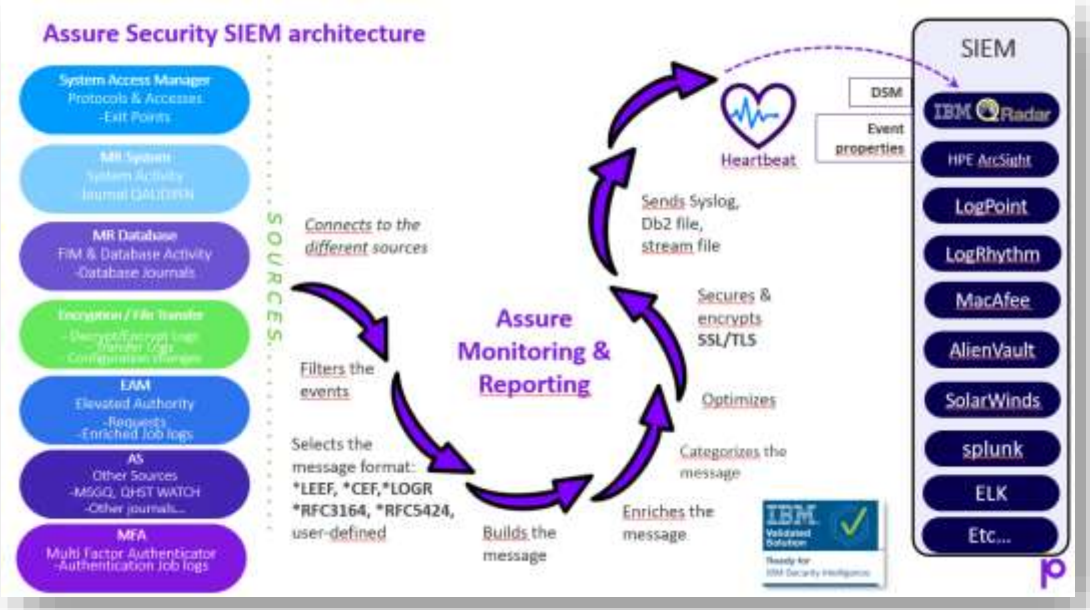
- Unusual number of login attempts, failed or successful
- Any attempts to sign into a specific account
- Unusual number of changes to User Authorities
- User Authority or file accesses events outside normal business hours
- Command line activity for powerful users (*ALLOBJ, *SECADM)
- All attempts to access, modify, overwrite, copy or delete sensitive database fields, spool files, backup data
- Changes to system values, user profiles, and authorization lists



SIEM Integration

Forward IBM i security data to your Security Information and Event Management (SIEM) solution:

- Highly configurable so SIEMs aren't flooded with unnecessary information.
- Works with all popular SIEMs including, QRADAR, etc.
- Competition tends to be much less granular and not as well integrated with specific SIEMs
- Supports multiple protocols like LEEF, CEF, RFC3164 ,RFC5424 etc.



Summary

IBM i System-access Security

1

Multi-factor authentication

2

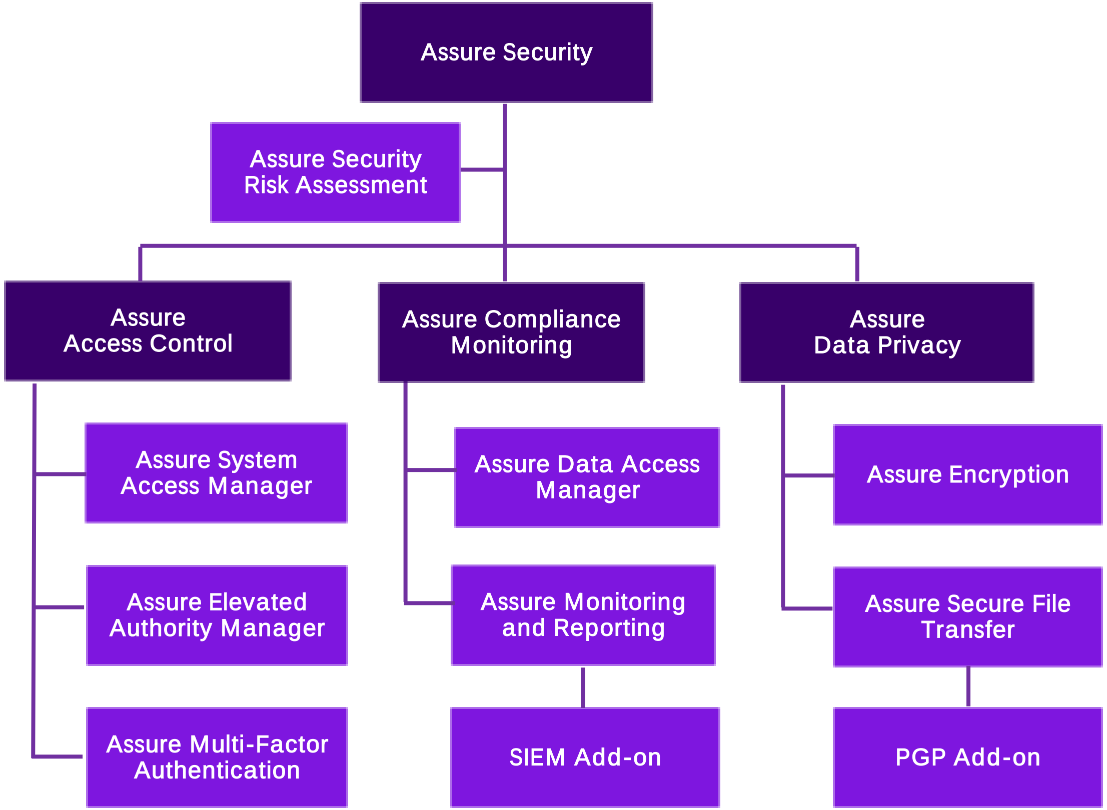
Elevated Authority management

3

System access Management

4

Monitoring & Reporting with SIEM Integration



Assure Security
Assure Security Risk Assessment
Assure Access Control
Assure Compliance Monitoring
Assure Data Privacy
Assure System Access Manager
Assure Elevated Authority Manager
Assure Multi-Factor Authentication
Assure Data Access Manager
Assure Monitoring and Reporting
SIEM Add-on
Assure Encryption
Assure Secure File Transfer
PGP Add-on

Choose the full product

Choose a feature bundle

Or select a specific capability

Thanks !
Questions ? Answers !

www.precisely.com

Demo

White papers

Case studies

Contact

stephan.leisse@precisely.com

MERCI