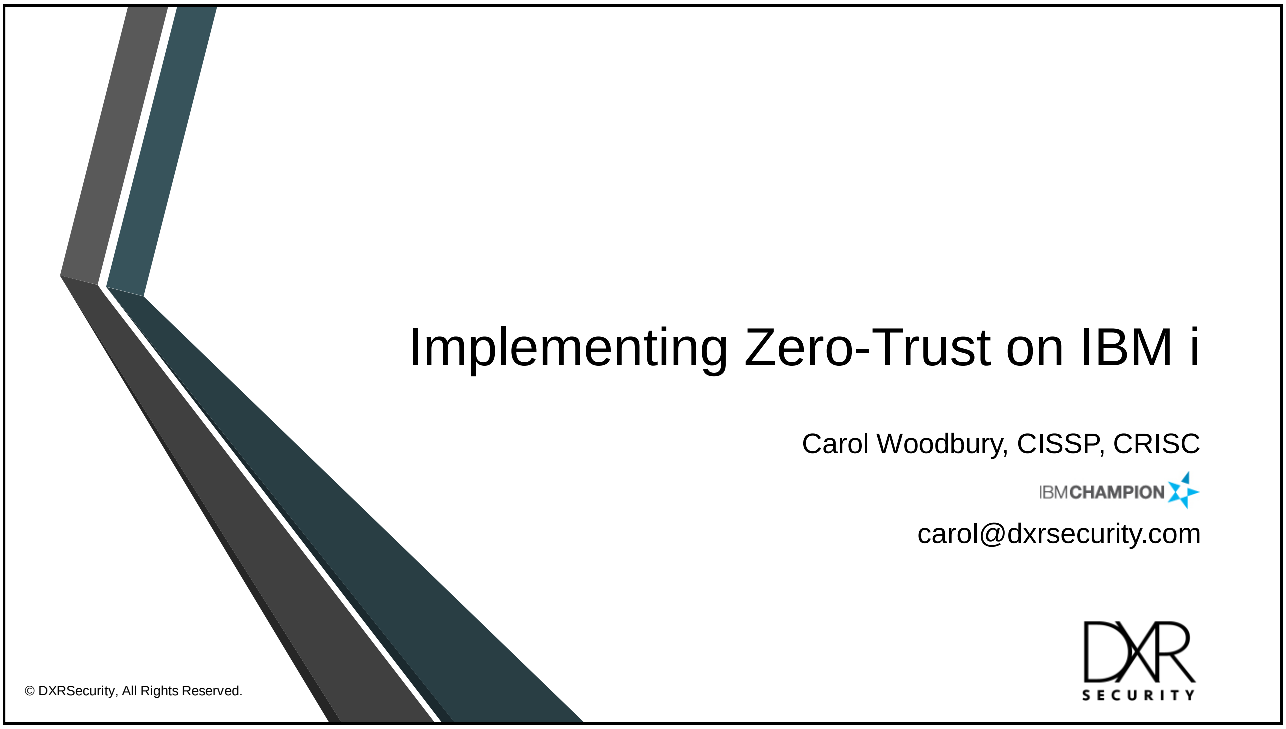
FRESCHE SOLUTIONS

Implementing Zero-Trust on IBM i

Carol Woodbury
CTO, DXR Security

Pauline Brazil Ayala
VP, Compliance & Security Solutions



Implementing Zero-Trust on IBM i

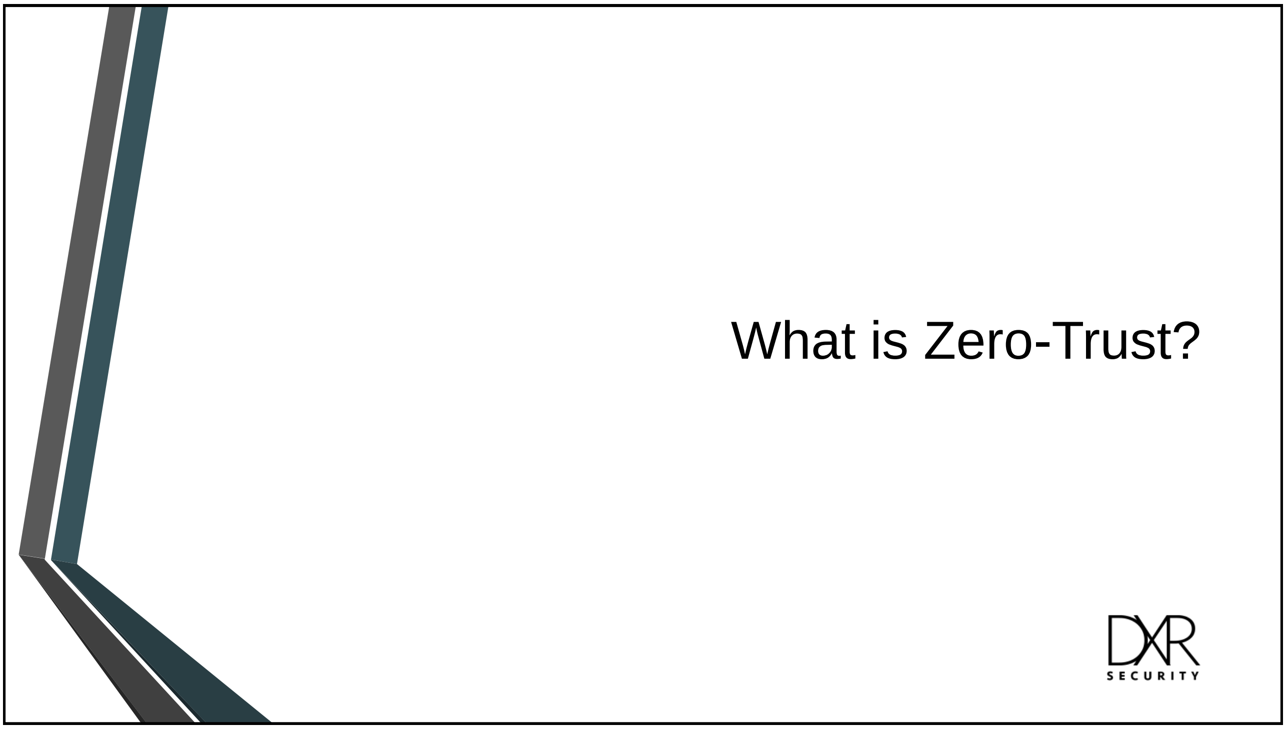
Carol Woodbury, CISSP, CRISC

IBM CHAMPION

carol@dxrsecurity.com

DXR SECURITY

1

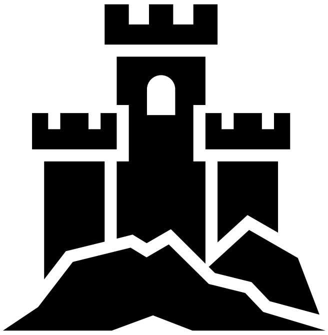


What is Zero-Trust?

DXR SECURITY

2

Perimeter Defense



- Implicit trust
  - Allows unrestricted movement/access after initial access
- Doesn’t take into account:
  - Malicious insiders
  - Accidental errors
  - Stolen credentials

DXR SECURITY

3

Zero-Trust

- First introduced in 2004, then popularized in 2010 by John Kindervag
- Strong identity and access management greatly reduces the risk of malicious attacks and insider threats
- Trust is based on the user and their role/responsibilities rather than where they are (inside or outside of the network).

Resources:

- https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security
- https://techchannel.com/Trends/02/2023/westley-mcduffie-zero-trust-security

iChime hosted by Charlie Guarino

DXR SECURITY

4

Can’t Implement on Just One System or Area

5

Is it …

Least privilege access

Deny by default

Defense in depth

Regular reviews

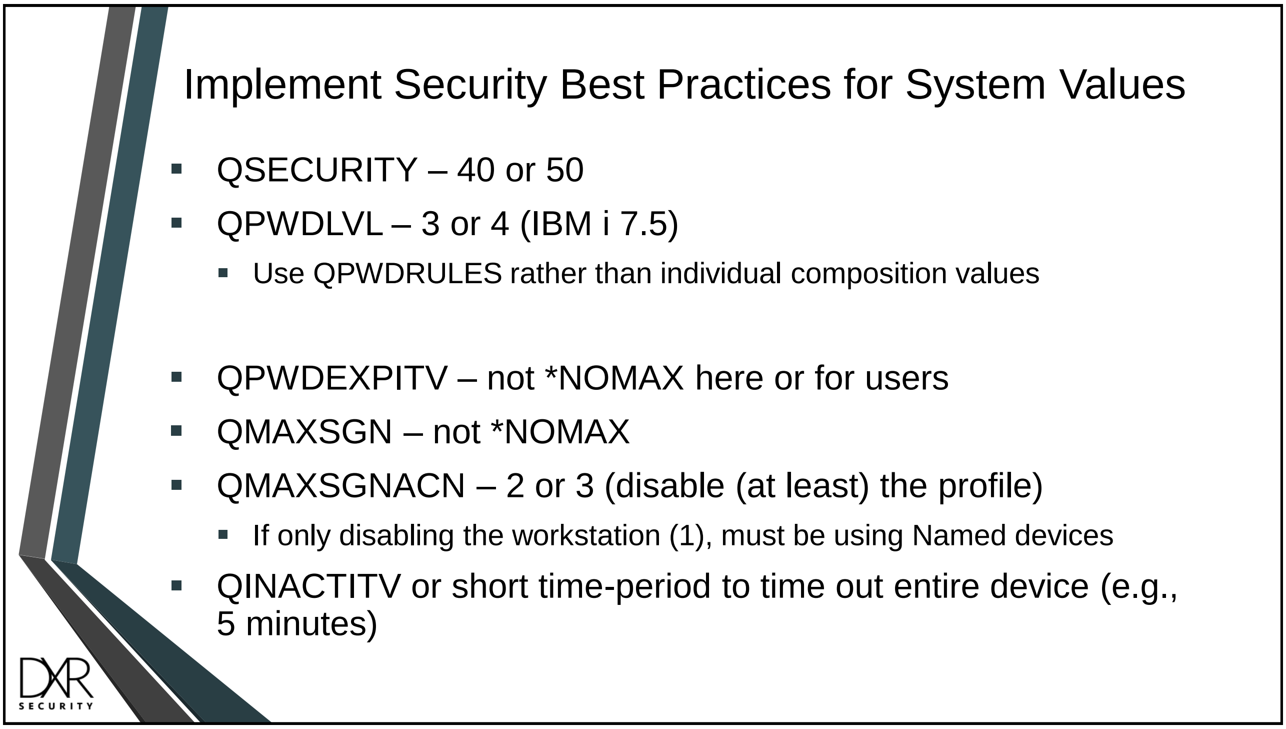
6

Security is Not a One-time Event … it's a Lifestyle!

7

Implementing Zero-Trust on IBM i

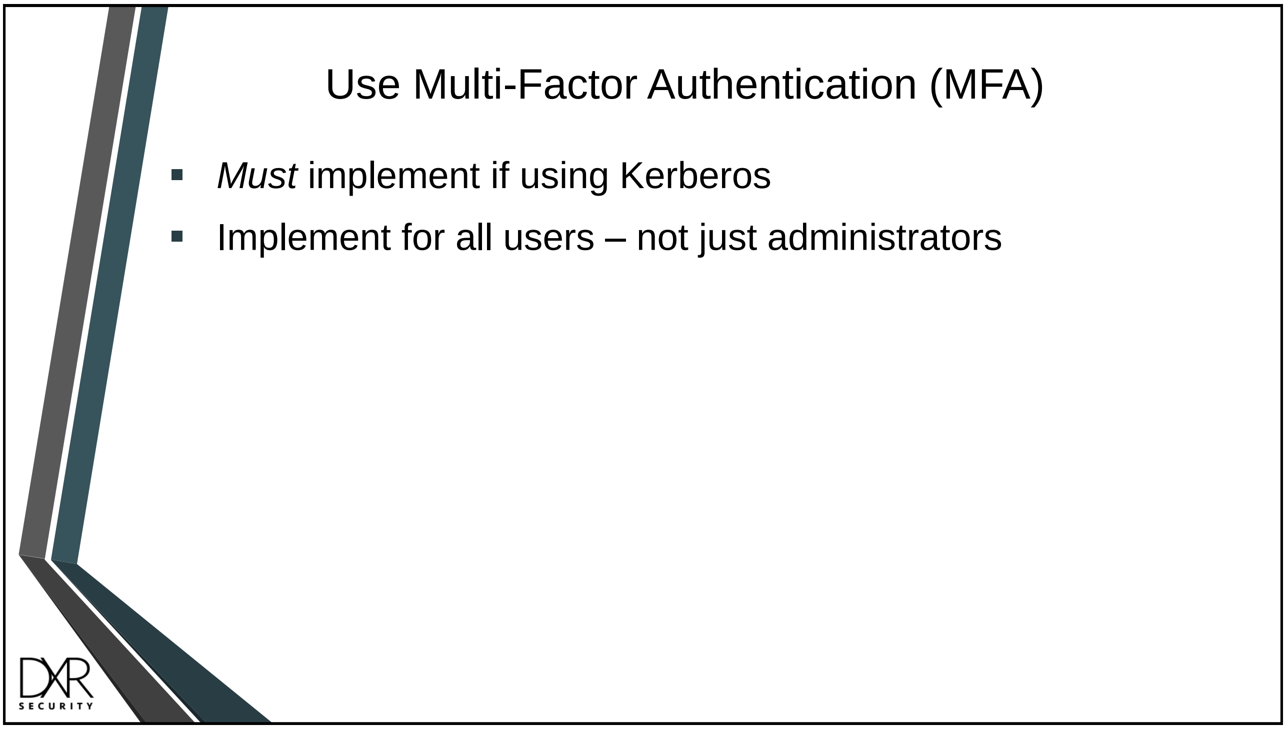
8



Implement Security Best Practices for System Values

- QSECURITY – 40 or 50
- QPWDLVL – 3 or 4 (IBM i 7.5)
  - Use QPWDRULES rather than individual composition values
- QPWDEXPITV – not *NOMAX here or for users
- QMAXSGN – not *NOMAX
- QMAXSGNACN – 2 or 3 (disable (at least) the profile)
  - If only disabling the workstation (1), must be using Named devices
- QINACTITV or short time-period to time out entire device (e.g., 5 minutes)

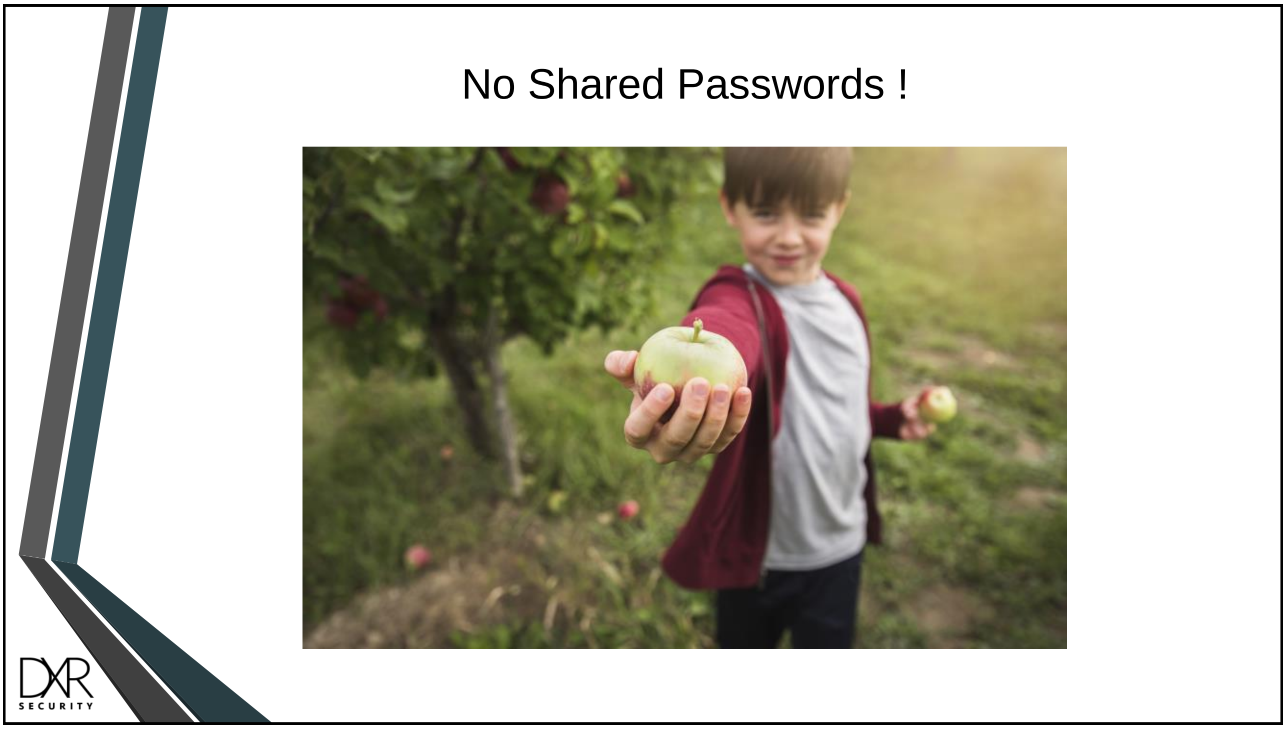
9



Use Multi-Factor Authentication (MFA)

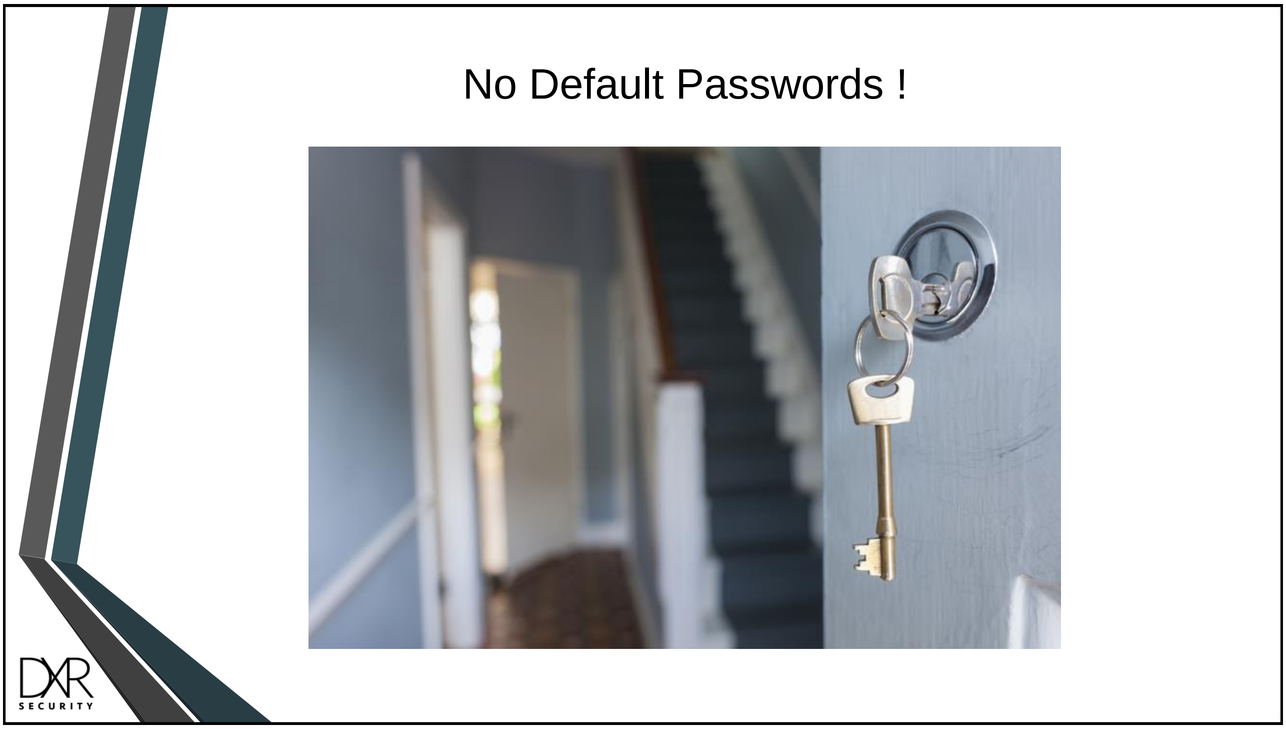
- *Must* implement if using Kerberos
- Implement for all users – not just administrators

10



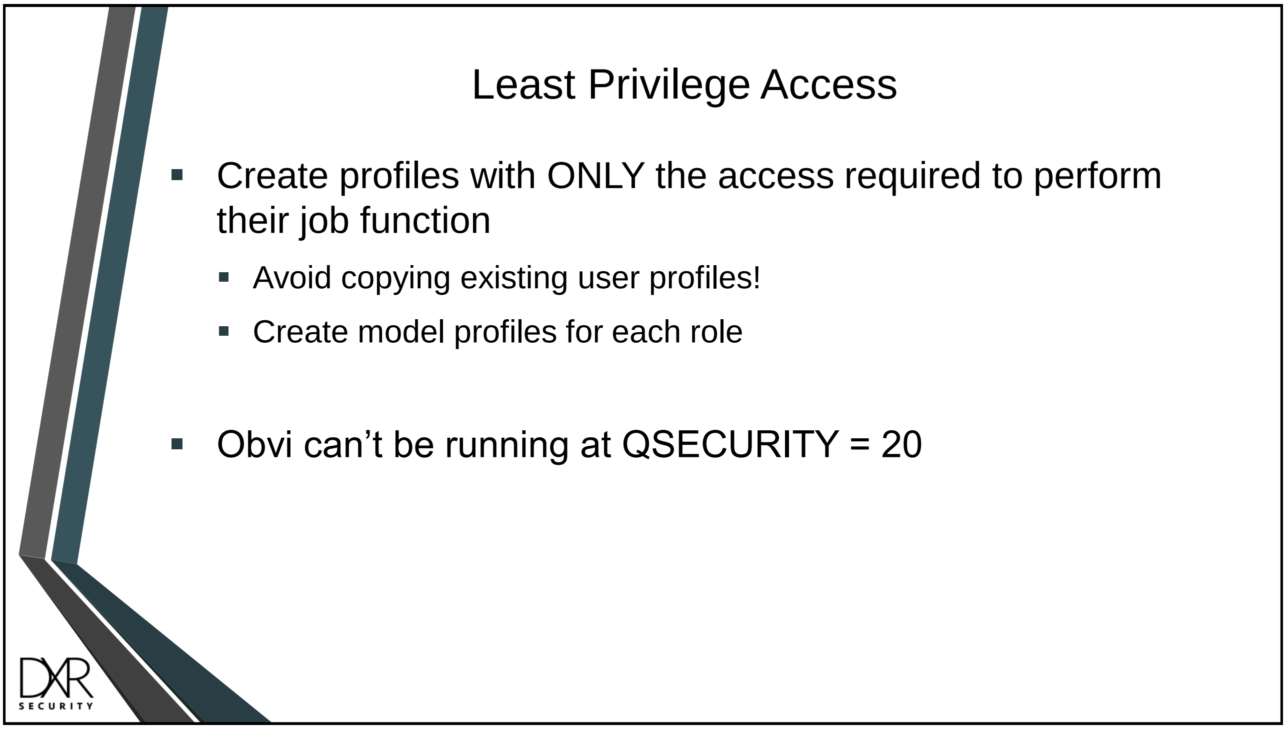
No Shared Passwords !

11



No Default Passwords !

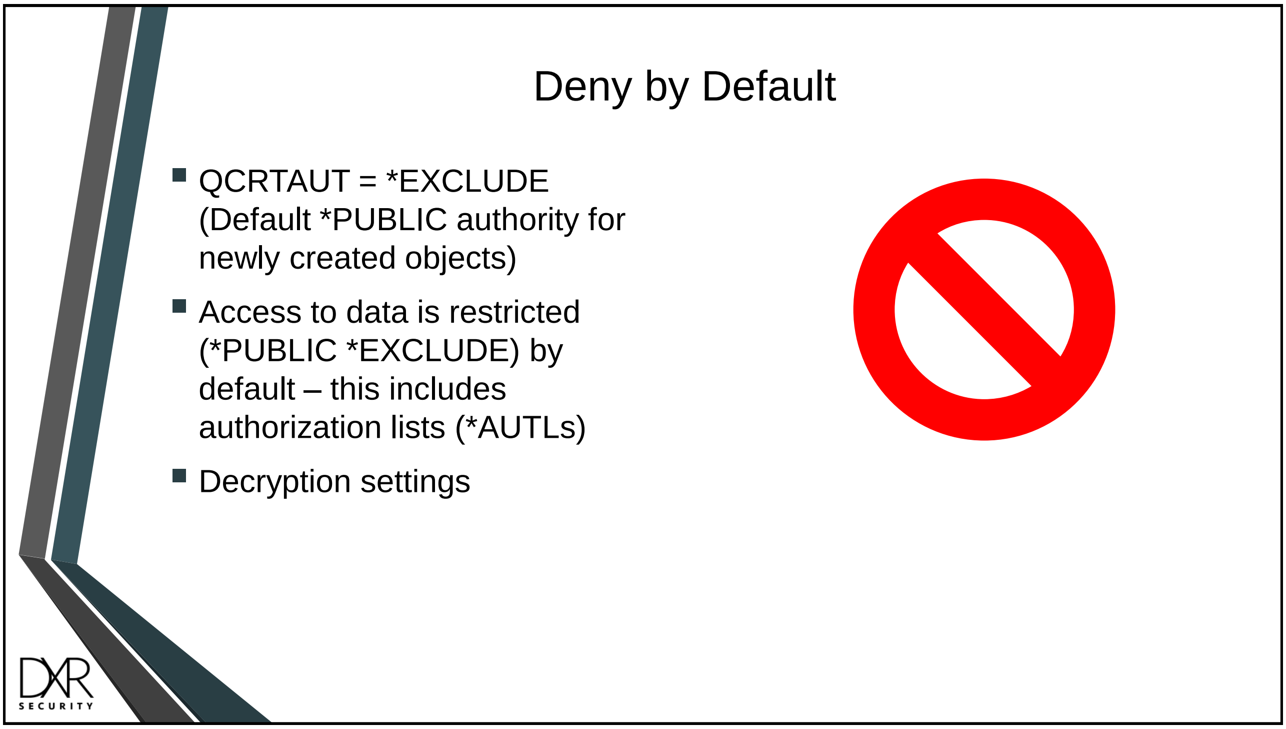
12



Least Privilege Access

- Create profiles with ONLY the access required to perform their job function
  - Avoid copying existing user profiles!
  - Create model profiles for each role
- Obvi can’t be running at QSECURITY = 20

13



Deny by Default

- QCRTAUT = *EXCLUDE (Default *PUBLIC authority for newly created objects)
- Access to data is restricted (*PUBLIC *EXCLUDE) by default – this includes authorization lists (*AUTLs)
- Decryption settings

14

Deny by Default - continued

- Exit point software access
- SSH
- File shares (IBM i 7.5 – limit use via autls)
- Navigator for i
- ACS features
- ACS client deployment

DXR SECURITY

15

Clean up!

- Don't start TCP/IP services you aren't using
- Don't install software you won't use
- Uninstall software no longer in use -- including past versions after software upgrades
- Remove old data

- Stay current!

DXR SECURITY

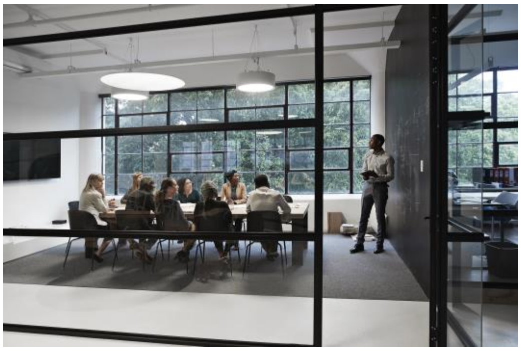
16

Rinse and Repeat: Review these on a Regular Basis!

- System value settings
- User profile settings:
  - Special authorities – from both user and group inheritance
  - Group membership
  - Private authorities
  - Inactive profiles
- Application access
- Object authorities:
  - To key database files and directories
  - Authorization lists
- Exit point access
- Navigator for i access

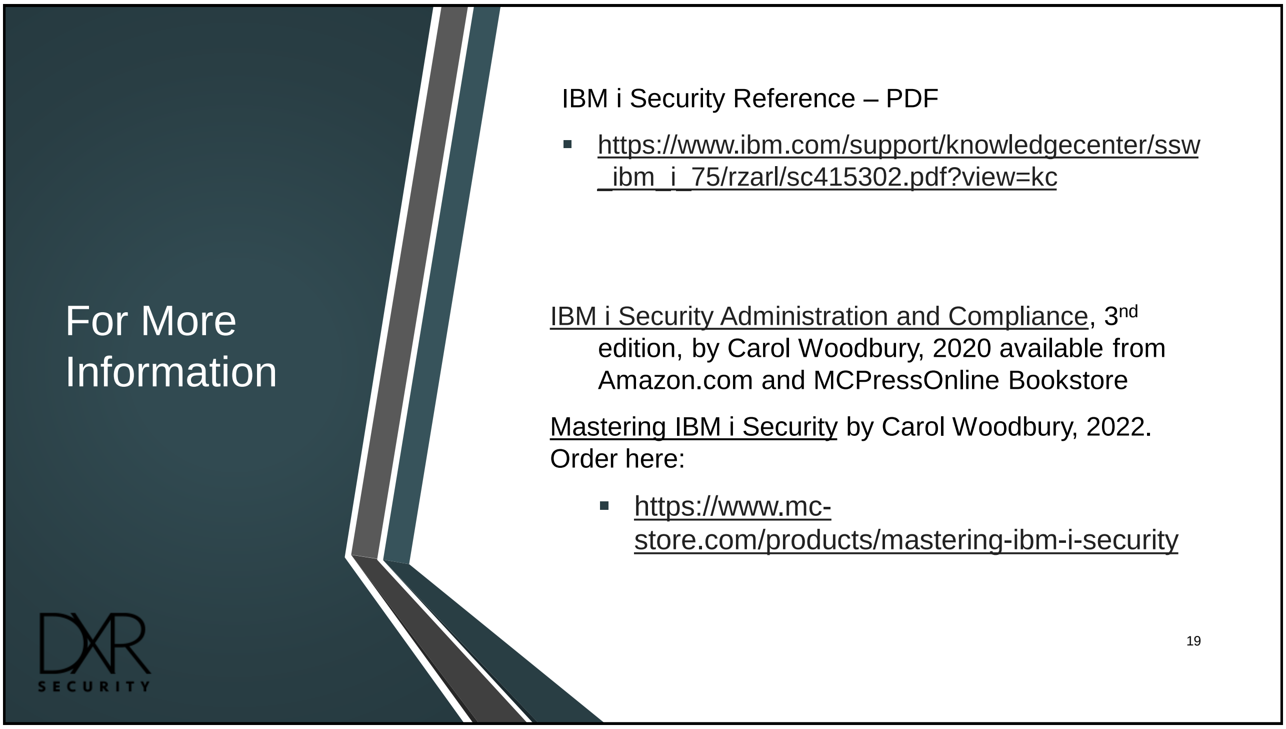
17

Agree as an Organization to …



- Scope
- Priorities
- Timeline to accomplish

18



For More Information

IBM i Security Reference – PDF

- https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_75/rzarl/sc415302.pdf?view=kc

IBM i Security Administration and Compliance, 3nd edition, by Carol Woodbury, 2020 available from Amazon.com and MCPressOnline Bookstore

Mastering IBM i Security by Carol Woodbury, 2022. Order here:

- https://www.mc-store.com/products/mastering-ibm-i-security

POLL: What layers of security are you currently implementing?

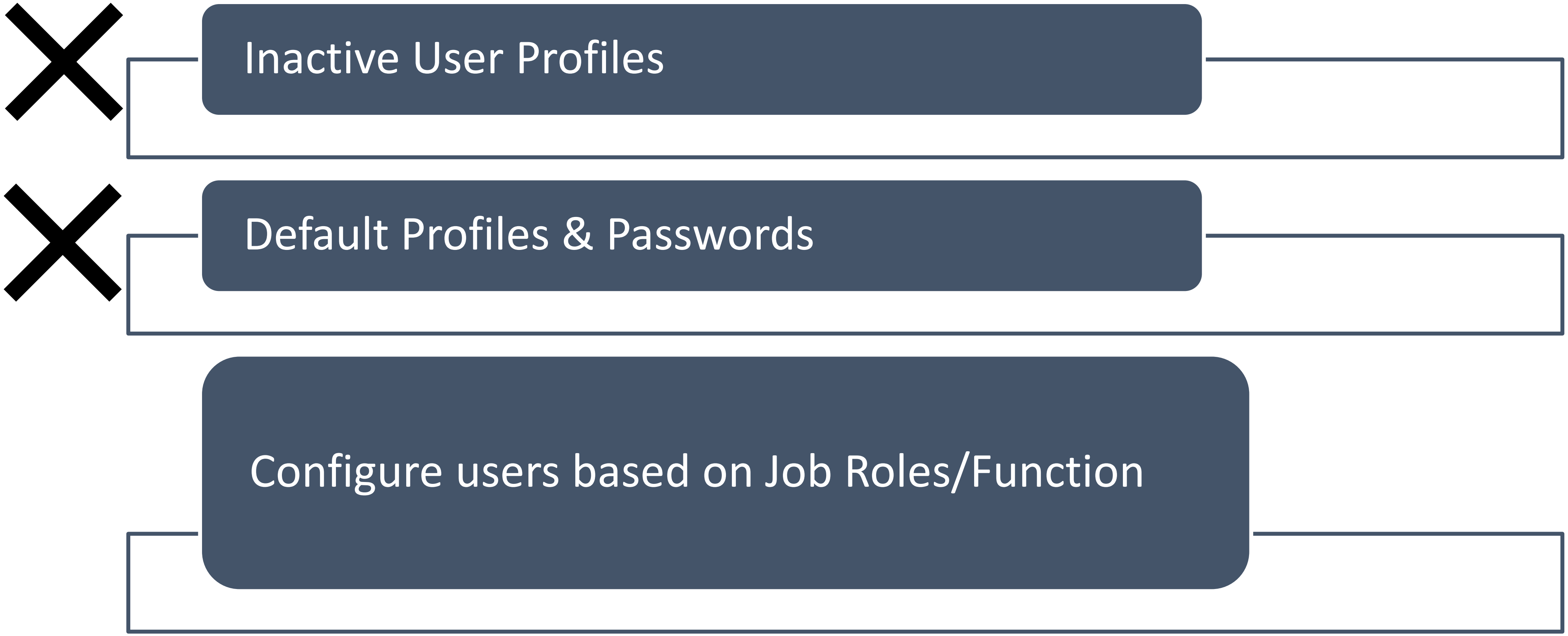
Layers of Penetration

Corporate Network (including Firewalls & MFA)

IBM i Server

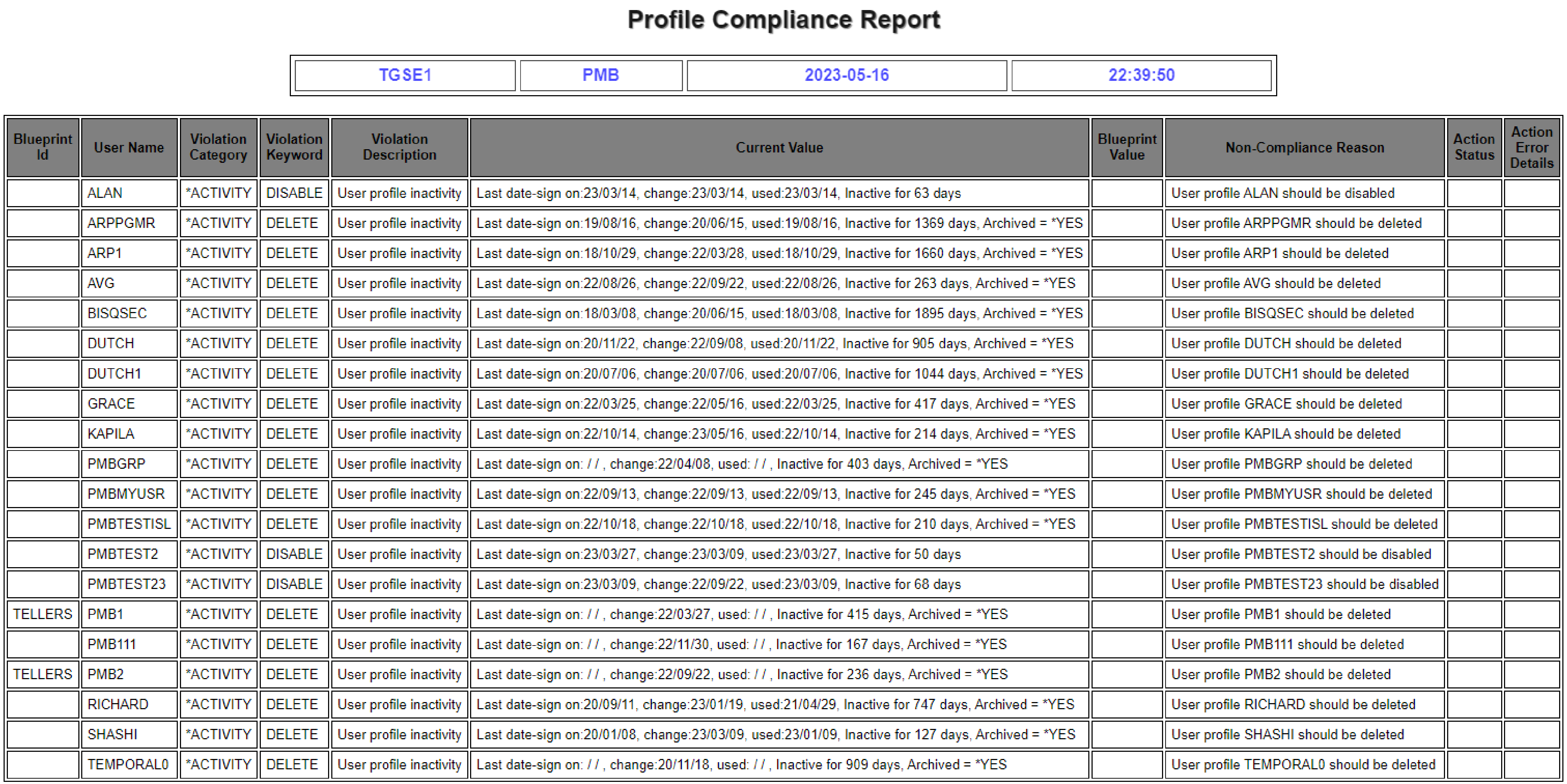
- User Profile Configuration
- Multi-factor Authentication
- IBM i Network Services
  - Remote Servers (FTP, ODBC, Telnet, …)
  - Socket Connections
- Object Authorities / IFS Permissions
- Access Escalation Management
- Command Security
- Encryption

User Profile Blueprints



- ✗ Inactive User Profiles
- ✗ Default Profiles & Passwords
- Configure users based on Job Roles/Function

Profile Blueprints – Auto-disable/delete user profiles

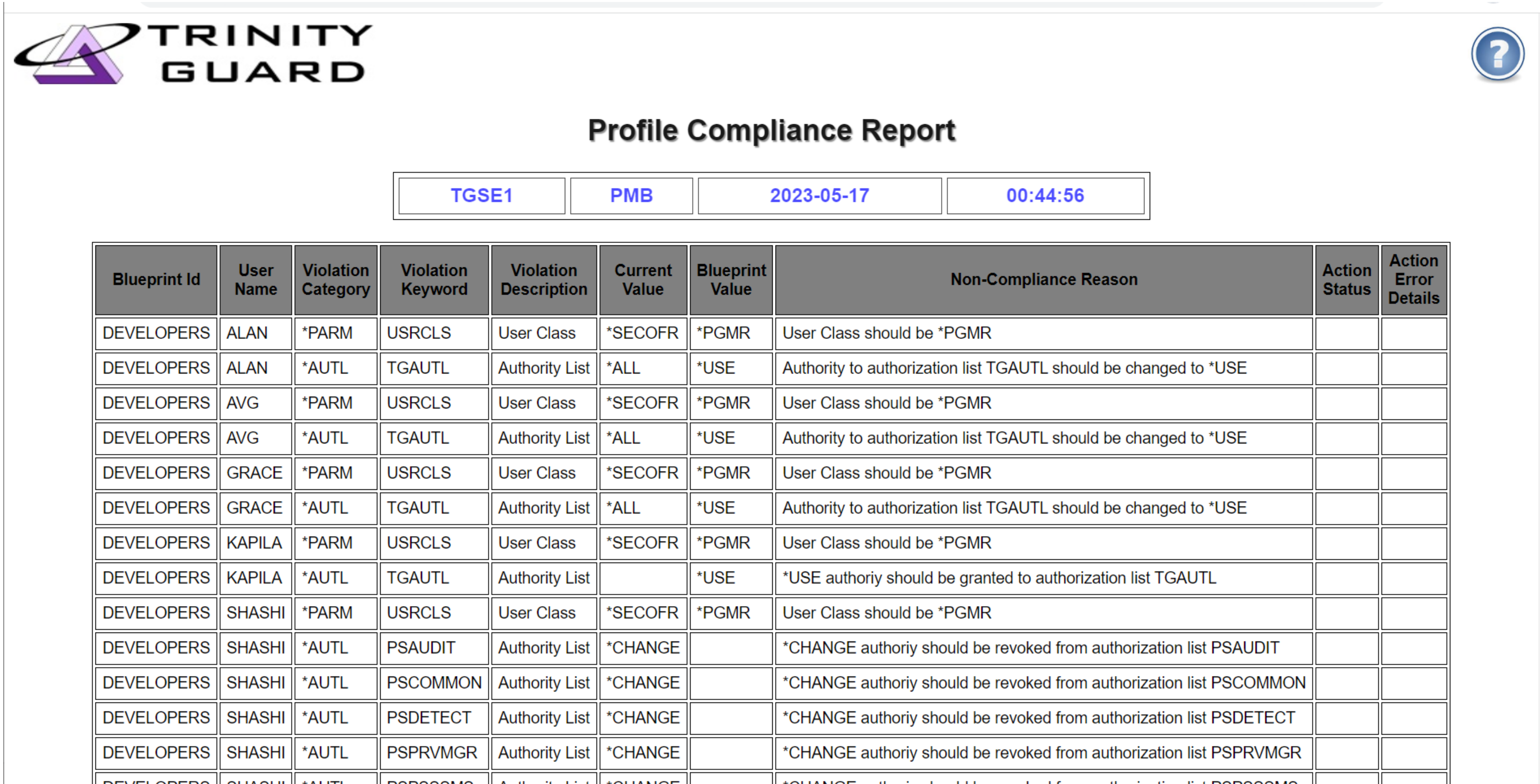


Profile Compliance Report

TGSE1	PMB	2023-05-16	22:39:50

Blueprint Id	User Name	Violation Category	Violation Keyword	Violation Description	Current Value	Blueprint Value	Non-Compliance Reason	Action Status	Action Error Details
	ALAN	*ACTIVITY	DISABLE	User profile inactivity	Last date-sign on:23/03/14, change:23/03/14, used:23/03/14, Inactive for 63 days		User profile ALAN should be disabled		
	ARPPGMR	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:19/08/16, change:20/06/15, used:19/08/16, Inactive for 1369 days, Archived = *YES		User profile ARPPGMR should be deleted		
	ARP1	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:18/10/29, change:22/03/28, used:18/10/29, Inactive for 1660 days, Archived = *YES		User profile ARP1 should be deleted		
	AVG	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:22/08/26, change:22/09/22, used:22/08/26, Inactive for 263 days, Archived = *YES		User profile AVG should be deleted		
	BISQSEC	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:18/03/08, change:20/06/15, used:18/03/08, Inactive for 1895 days, Archived = *YES		User profile BISQSEC should be deleted		
	DUTCH	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:20/11/22, change:22/09/08, used:20/11/22, Inactive for 905 days, Archived = *YES		User profile DUTCH should be deleted		
	DUTCH1	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:20/07/06, change:20/07/06, used:20/07/06, Inactive for 1044 days, Archived = *YES		User profile DUTCH1 should be deleted		
	GRACE	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:22/03/25, change:22/05/16, used:22/03/25, Inactive for 417 days, Archived = *YES		User profile GRACE should be deleted		
	KAPILA	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:22/10/14, change:23/05/16, used:22/10/14, Inactive for 214 days, Archived = *YES		User profile KAPILA should be deleted		
	PMBGRP	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on: / / , change:22/04/08, used: / / , Inactive for 403 days, Archived = *YES		User profile PMBGRP should be deleted		
	PMBMYUSR	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:22/09/13, change:22/09/13, used:22/09/13, Inactive for 245 days, Archived = *YES		User profile PMBMYUSR should be deleted		
	PMBTESTISL	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:22/10/18, change:22/10/18, used:22/10/18, Inactive for 210 days, Archived = *YES		User profile PMBTESTISL should be deleted		
	PMBTEST2	*ACTIVITY	DISABLE	User profile inactivity	Last date-sign on:23/03/27, change:23/03/09, used:23/03/27, Inactive for 50 days		User profile PMBTEST2 should be disabled		
	PMBTEST23	*ACTIVITY	DISABLE	User profile inactivity	Last date-sign on:23/03/09, change:22/09/22, used:23/03/09, Inactive for 68 days		User profile PMBTEST23 should be disabled		
TELLERS	PMB1	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on: / / , change:22/03/27, used: / / , Inactive for 415 days, Archived = *YES		User profile PMB1 should be deleted		
	PMB111	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on: / / , change:22/11/30, used: / / , Inactive for 167 days, Archived = *YES		User profile PMB111 should be deleted		
TELLERS	PMB2	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on: / / , change:22/09/22, used: / / , Inactive for 236 days, Archived = *YES		User profile PMB2 should be deleted		
	RICHARD	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:20/09/11, change:23/01/19, used:21/04/29, Inactive for 747 days, Archived = *YES		User profile RICHARD should be deleted		
	SHASHI	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on:20/01/08, change:23/03/09, used:23/01/09, Inactive for 127 days, Archived = *YES		User profile SHASHI should be deleted		
	TEMPORAL0	*ACTIVITY	DELETE	User profile inactivity	Last date-sign on: / / , change:20/11/18, used: / / , Inactive for 909 days, Archived = *YES		User profile TEMPORAL0 should be deleted		

Profile Blueprints – define templates for users - quickly identify users out of compliance – option to auto enforce compliance



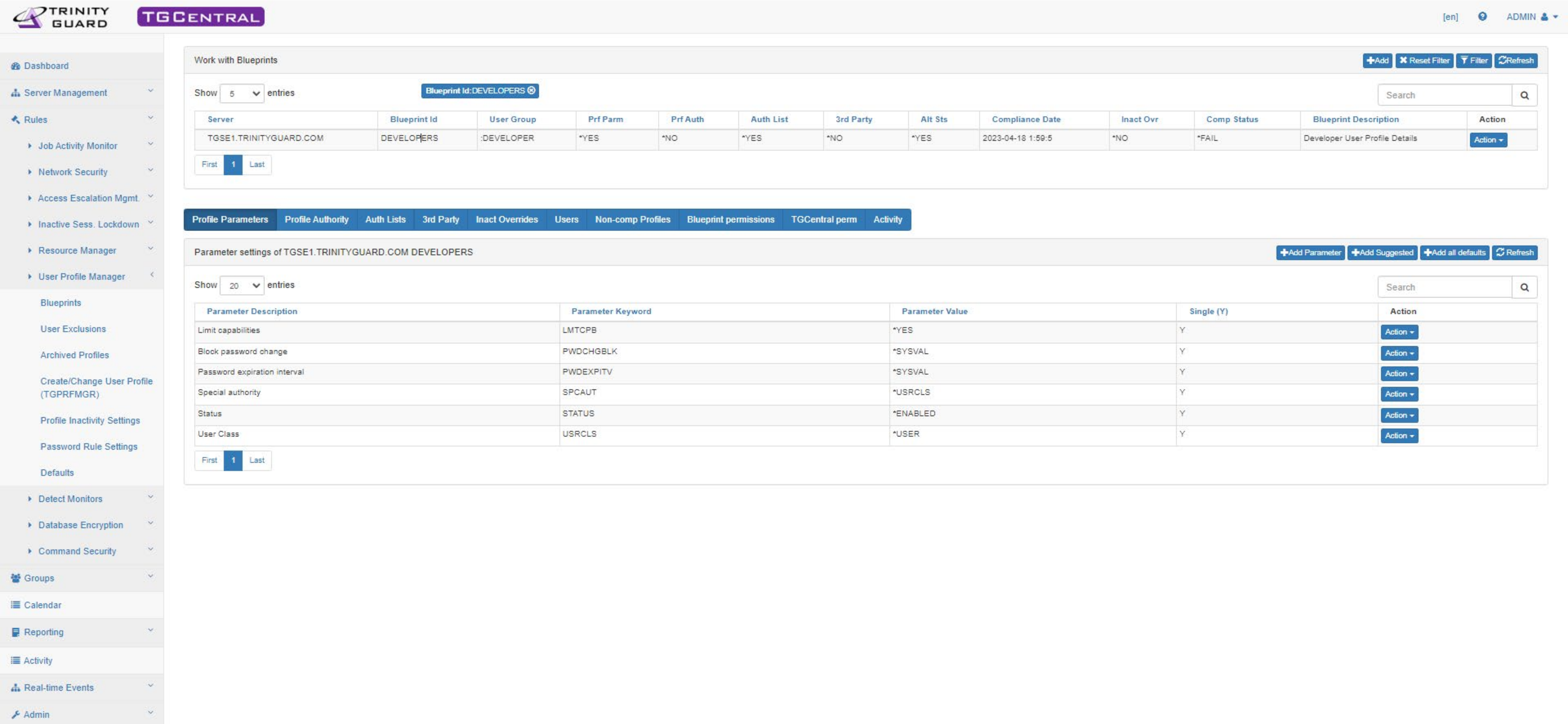
TRINITY GUARD

Profile Compliance Report

TGSE1	PMB	2023-05-17	00:44:56

Blueprint Id	User Name	Violation Category	Violation Keyword	Violation Description	Current Value	Blueprint Value	Non-Compliance Reason	Action Status	Action Error Details
DEVELOPERS	ALAN	*PARM	USRCLS	User Class	*SECOFR	*PGMR	User Class should be *PGMR		
DEVELOPERS	ALAN	*AUTL	TGAUTL	Authority List	*ALL	*USE	Authority to authorization list TGAUTL should be changed to *USE		
DEVELOPERS	AVG	*PARM	USRCLS	User Class	*SECOFR	*PGMR	User Class should be *PGMR		
DEVELOPERS	AVG	*AUTL	TGAUTL	Authority List	*ALL	*USE	Authority to authorization list TGAUTL should be changed to *USE		
DEVELOPERS	GRACE	*PARM	USRCLS	User Class	*SECOFR	*PGMR	User Class should be *PGMR		
DEVELOPERS	GRACE	*AUTL	TGAUTL	Authority List	*ALL	*USE	Authority to authorization list TGAUTL should be changed to *USE		
DEVELOPERS	KAPILA	*PARM	USRCLS	User Class	*SECOFR	*PGMR	User Class should be *PGMR		
DEVELOPERS	KAPILA	*AUTL	TGAUTL	Authority List		*USE	*USE authoriy should be granted to authorization list TGAUTL		
DEVELOPERS	SHASHI	*PARM	USRCLS	User Class	*SECOFR	*PGMR	User Class should be *PGMR		
DEVELOPERS	SHASHI	*AUTL	PSAUDIT	Authority List	*CHANGE		*CHANGE authoriy should be revoked from authorization list PSAUDIT		
DEVELOPERS	SHASHI	*AUTL	PSCOMMON	Authority List	*CHANGE		*CHANGE authoriy should be revoked from authorization list PSCOMMON		
DEVELOPERS	SHASHI	*AUTL	PSDETECT	Authority List	*CHANGE		*CHANGE authoriy should be revoked from authorization list PSDETECT		
DEVELOPERS	SHASHI	*AUTL	PSPRVMGR	Authority List	*CHANGE		*CHANGE authoriy should be revoked from authorization list PSPRVMGR		

Profile Blueprints – configure user profile gold standards for any user profile attribute



Work with Blueprints

Show 5 entries

Blueprint Id:DEVELOPERS ⊗

Server	Blueprint Id	User Group	Prf Parm	Prf Auth	Auth List	3rd Party	Alt Sts	Compliance Date	Inact Ovr	Comp Status	Blueprint Description	Action
TGSE1.TRINITYGUARD.COM	DEVELOPERS	:DEVELOPER	*YES	*NO	*YES	*NO	*YES	2023-04-18 1:59:5	*NO	*FAIL	Developer User Profile Details	Action

First 1 Last

Parameter settings of TGSE1.TRINITYGUARD.COM DEVELOPERS

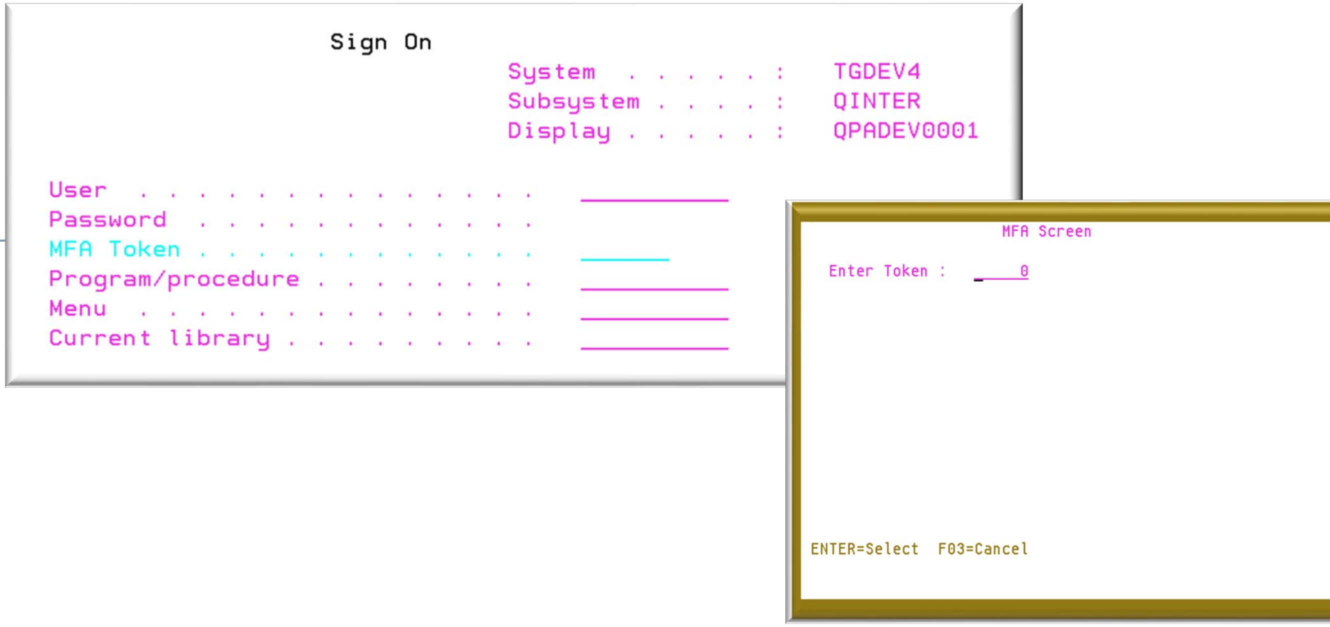
Show 20 entries

Parameter Description	Parameter Keyword	Parameter Value	Single (Y)	Action
Limit capabilities	LMTCPB	*YES	Y	Action
Block password change	PWDCHGBLK	*SYSVAL	Y	Action
Password expiration interval	PWDEXPITV	*SYSVAL	Y	Action
Special authority	SPCAUT	*USRCLS	Y	Action
Status	STATUS	*ENABLED	Y	Action
User Class	USRCLS	*USER	Y	Action

First 1 Last

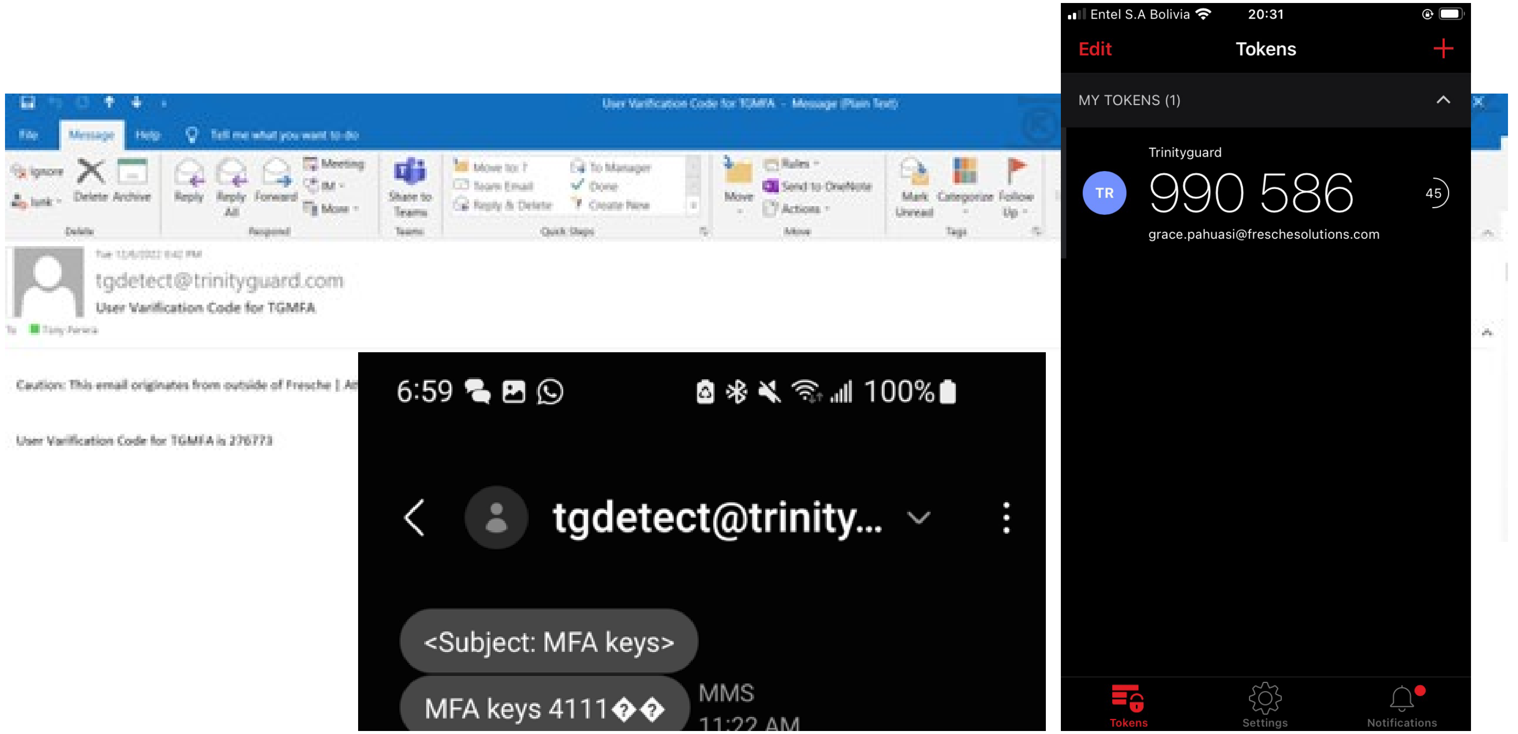
TGMFA

- Multi-Factor Authentication for IBM i TELNET
  - Via modified sign-on screen
  - Via pop-up screen
- Multi-Factor Authentication - Algorithms
  - SHA-1, SHA-256, SHA-512
- Token Lengths Supported
  - 6 and 8
- Authentication via
  - Email
  - Text
  - OTP app (2FA Authenticator or similar App)



```
                              Sign On
                                   System . . . . . :   TGDEV4
                                   Subsystem . . . . :   QINTER
                                   Display . . . . . :   QPADEV0001

 User . . . . . . . . . . . . . .              __________
 Password . . . . . . . . . . . .              __________
 MFA Token . . . . . . . . . . . .             ______
 Program/procedure . . . . . . . .             __________
 Menu . . . . . . . . . . . . . .              __________
 Current library . . . . . . . . .             __________
```

```
                    MFA Screen

  Enter Token :    _     0




 ENTER=Select  F03=Cancel
```



Tue 12/6/2022 8:42 PM

tgdetect@trinityguard.com

User Verification Code for TGMFA

To Tony Ferreira

Caution: This email originates from outside of Fresche | At

User Verification Code for TGMFA is 276773

6:59 100%

tgdetect@trinity...

<Subject: MFA keys>

MFA keys 4111�� MMS 11:22 AM

Entel S.A Bolivia 20:31

Edit Tokens +

MY TOKENS (1)

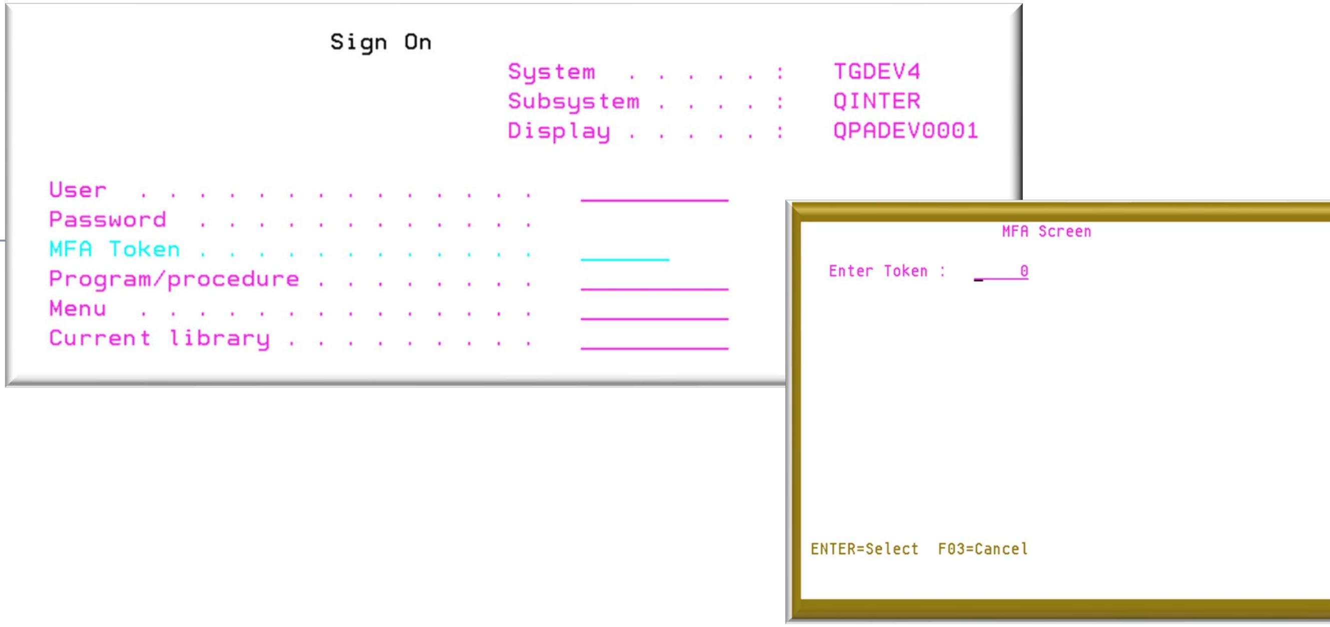
Trinityguard

TR 990 586 45

grace.pahuasi@freschesolutions.com

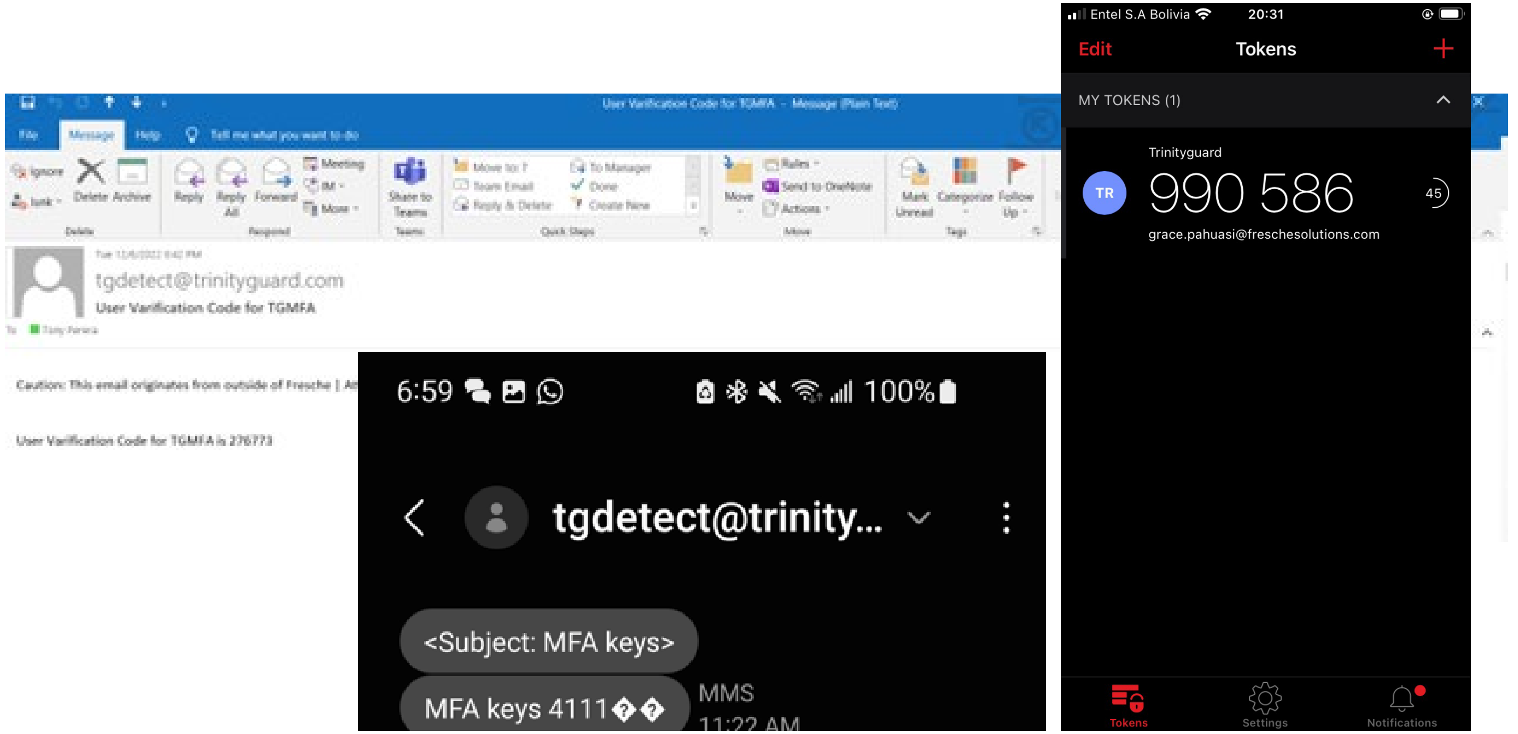
TGMFA

- Multi-Factor Authentication for IBM i TELNET
  - Via modified sign-on screen
  - Via pop-up screen
- Multi-Factor Authentication - Algorithms
  - SHA-1, SHA-256, SHA-512
- Token Lengths Supported
  - 6 and 8
- Authentication via
  - Email
  - Text
  - OTP app (2FA Authenticator or similar App)



```
                              Sign On
                                     System . . . . . :    TGDEV4
                                     Subsystem . . . . :   QINTER
                                     Display . . . . . :   QPADEV0001

User . . . . . . . . . . . . . .          __________
Password . . . . . . . . . . . .          
MFA Token . . . . . . . . . . .           ______
Program/procedure . . . . . . .           __________
Menu . . . . . . . . . . . . . .          __________
Current library . . . . . . . .           __________
```

```
                      MFA Screen

  Enter Token :   _____0





ENTER=Select  F03=Cancel
```



Tue 12/6/2022 9:42 PM

tgdetect@trinityguard.com

User Varification Code for TGMFA

To Tony Ferreira

Caution: This email originates from outside of Fresche | At

User Varification Code for TGMFA is 276773

6:59 100%

tgdetect@trinity...

<Subject: MFA keys>

MFA keys 4111��

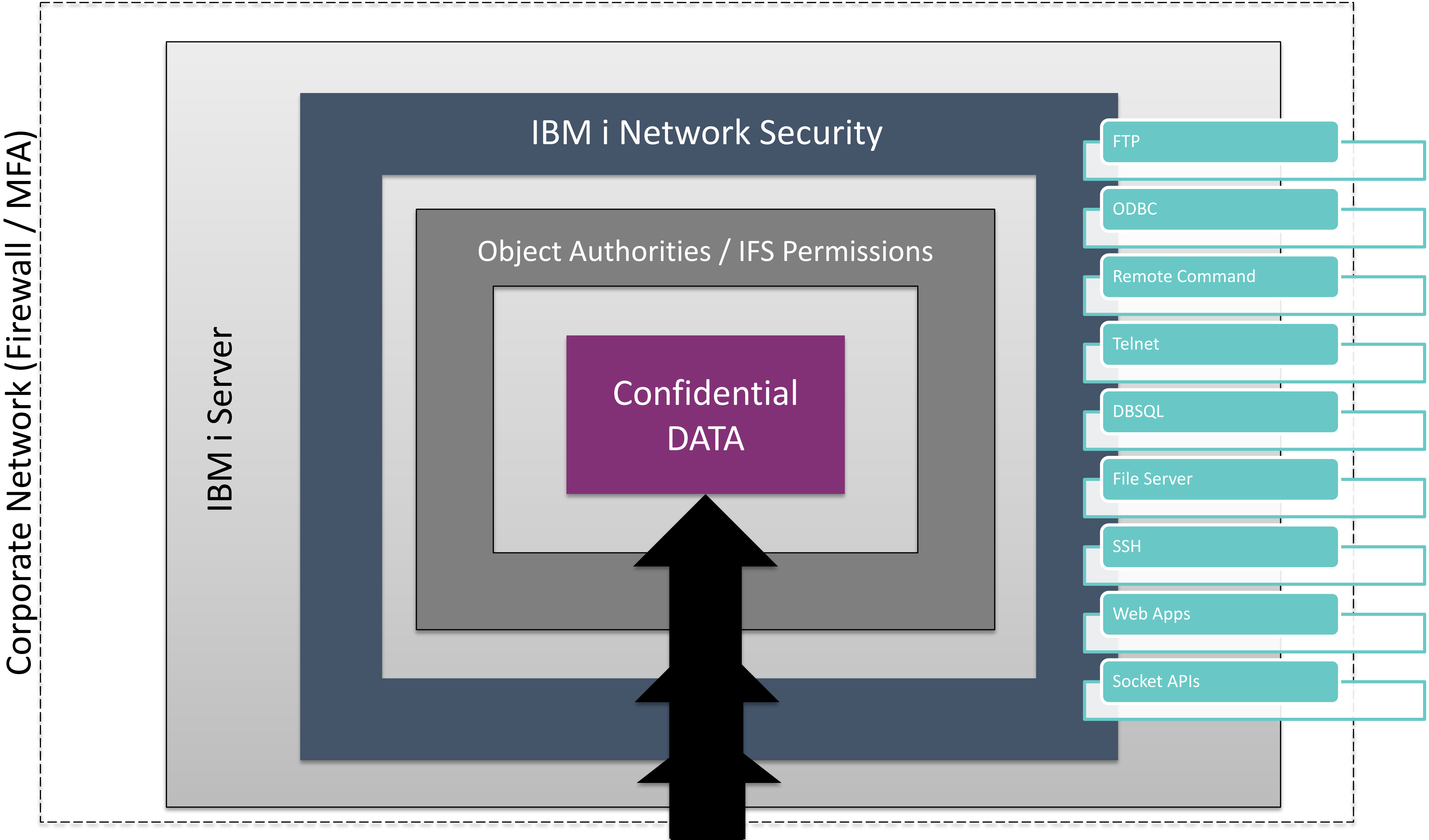
MMS 11:22 AM

Entel S.A Bolivia 20:31

Trinityguard

TR 990 586 45

grace.pahuasi@freschesolutions.com



Corporate Network (Firewall / MFA)

IBM i Server

IBM i Network Security

Object Authorities / IFS Permissions

Confidential DATA

FTP

ODBC

Remote Command

Telnet

DBSQL

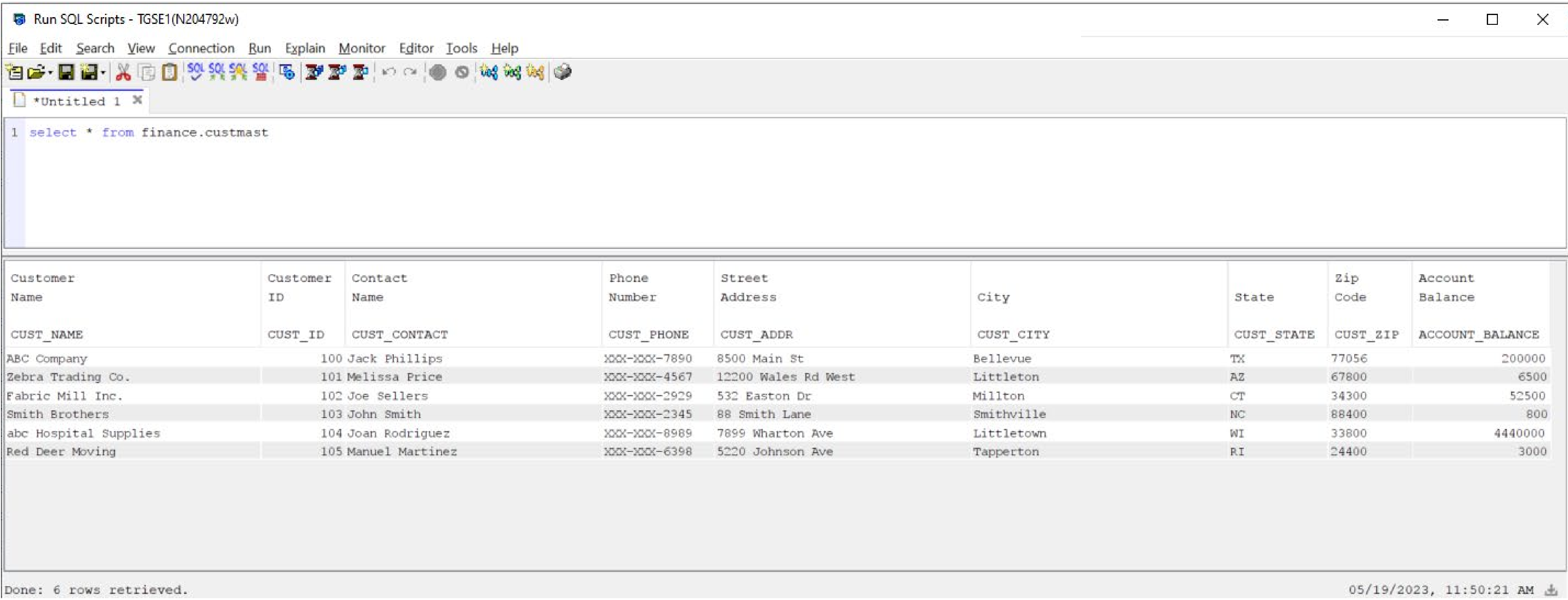
File Server

SSH

Web Apps

Socket APIs

Network Security – See all incoming activity to IBM i


Run SQL Scripts - TGSE1(N204792w)
File Edit Search View Connection Run Explain Monitor Editor Tools Help
*Untitled 1

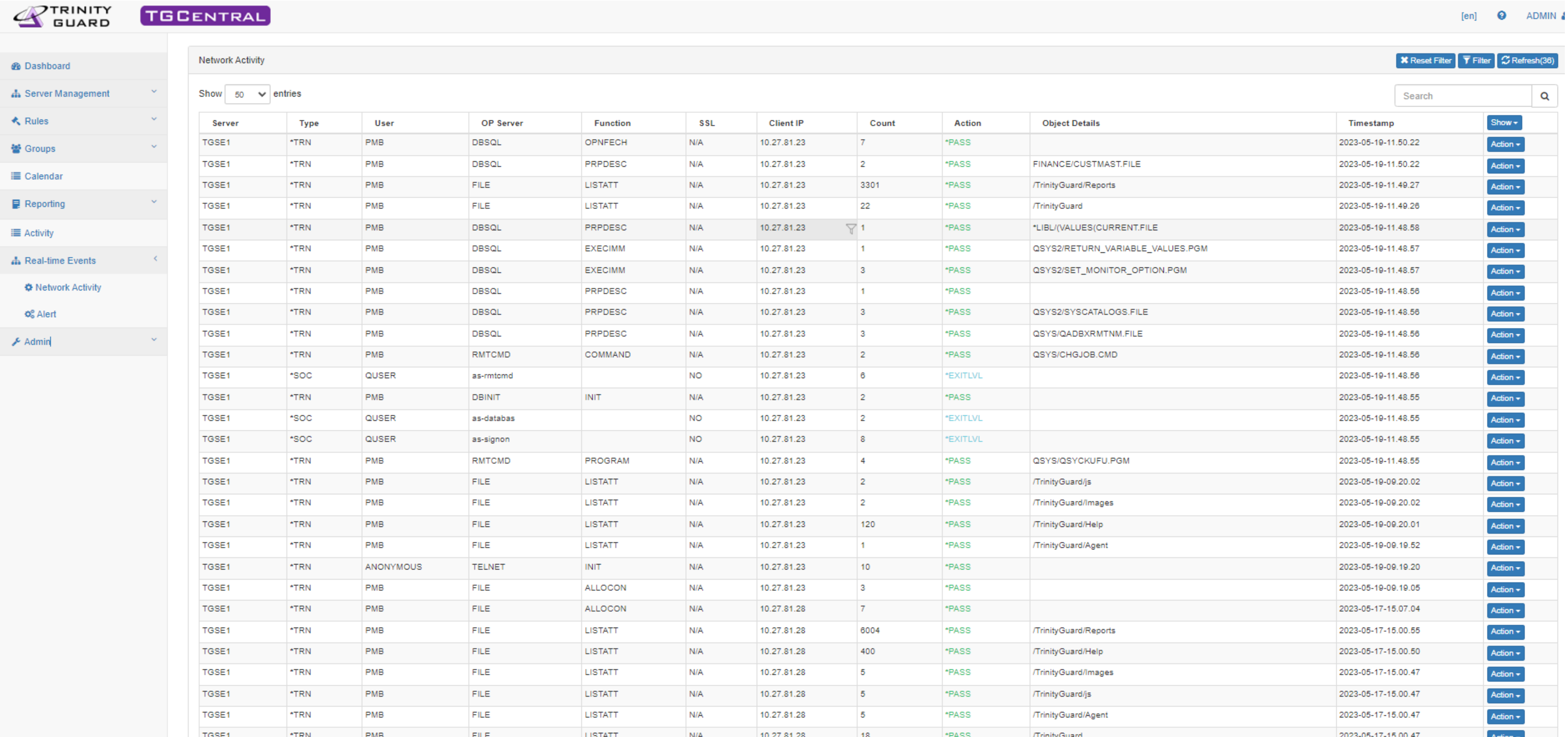
```
select * from finance.custmast
```

Customer Name	Customer ID	Contact Name	Phone Number	Street Address	City	State	Zip Code	Account Balance
CUST_NAME	CUST_ID	CUST_CONTACT	CUST_PHONE	CUST_ADDR	CUST_CITY	CUST_STATE	CUST_ZIP	ACCOUNT_BALANCE
ABC Company	100	Jack Phillips	XXX-XXX-7890	8500 Main St	Bellevue	TX	77056	200000
Zebra Trading Co.	101	Melissa Price	XXX-XXX-4567	12200 Wales Rd West	Littleton	AZ	67800	6500
Fabric Mill Inc.	102	Joe Sellers	XXX-XXX-2929	532 Easton Dr	Millton	CT	34300	52500
Smith Brothers	103	John Smith	XXX-XXX-2345	88 Smith Lane	Smithville	NC	88400	800
abc Hospital Supplies	104	Joan Rodriguez	XXX-XXX-8989	7899 Wharton Ave	Littletown	WI	33800	4440000
Red Deer Moving	105	Manuel Martinez	XXX-XXX-6398	5220 Johnson Ave	Tapperton	RI	24400	3000

Done: 6 rows retrieved.

05/19/2023, 11:50:21 AM

Network Security – See all incoming activity to IBM i

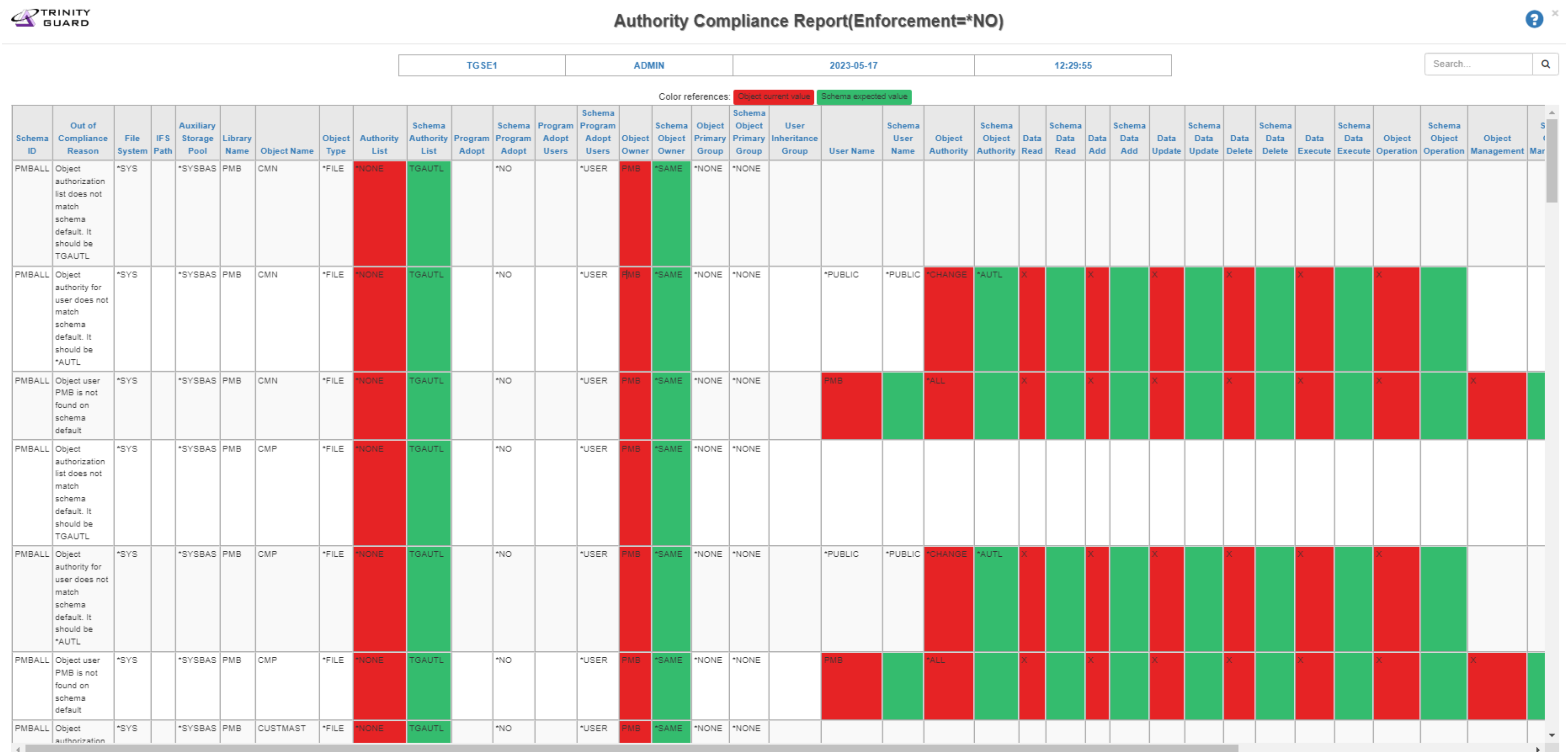


Network Activity

Show 50 entries

Server	Type	User	OP Server	Function	SSL	Client IP	Count	Action	Object Details	Timestamp	Show
TGSE1	*TRN	PMB	DBSQL	OPNFECH	N/A	10.27.81.23	7	*PASS		2023-05-19-11.50.22	Action
TGSE1	*TRN	PMB	DBSQL	PRPDESC	N/A	10.27.81.23	2	*PASS	FINANCE/CUSTMAST.FILE	2023-05-19-11.50.22	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.23	3301	*PASS	/TrinityGuard/Reports	2023-05-19-11.49.27	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.23	22	*PASS	/TrinityGuard	2023-05-19-11.49.26	Action
TGSE1	*TRN	PMB	DBSQL	PRPDESC	N/A	10.27.81.23	1	*PASS	*LIBL/(VALUES(CURRENT.FILE	2023-05-19-11.48.58	Action
TGSE1	*TRN	PMB	DBSQL	EXECIMM	N/A	10.27.81.23	1	*PASS	QSYS2/RETURN_VARIABLE_VALUES.PGM	2023-05-19-11.48.57	Action
TGSE1	*TRN	PMB	DBSQL	EXECIMM	N/A	10.27.81.23	3	*PASS	QSYS2/SET_MONITOR_OPTION.PGM	2023-05-19-11.48.57	Action
TGSE1	*TRN	PMB	DBSQL	PRPDESC	N/A	10.27.81.23	1	*PASS		2023-05-19-11.48.56	Action
TGSE1	*TRN	PMB	DBSQL	PRPDESC	N/A	10.27.81.23	3	*PASS	QSYS2/SYSCATALOGS.FILE	2023-05-19-11.48.56	Action
TGSE1	*TRN	PMB	DBSQL	PRPDESC	N/A	10.27.81.23	3	*PASS	QSYS/QADBXRMTNM.FILE	2023-05-19-11.48.56	Action
TGSE1	*TRN	PMB	RMTCMD	COMMAND	N/A	10.27.81.23	2	*PASS	QSYS/CHGJOB.CMD	2023-05-19-11.48.56	Action
TGSE1	*SOC	QUSER	as-rmtcmd		NO	10.27.81.23	6	*EXITLVL		2023-05-19-11.48.56	Action
TGSE1	*TRN	PMB	DBINIT	INIT	N/A	10.27.81.23	2	*PASS		2023-05-19-11.48.55	Action
TGSE1	*SOC	QUSER	as-databas		NO	10.27.81.23	2	*EXITLVL		2023-05-19-11.48.55	Action
TGSE1	*SOC	QUSER	as-signon		NO	10.27.81.23	8	*EXITLVL		2023-05-19-11.48.55	Action
TGSE1	*TRN	PMB	RMTCMD	PROGRAM	N/A	10.27.81.23	4	*PASS	QSYS/QSYCKUFU.PGM	2023-05-19-11.48.55	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.23	2	*PASS	/TrinityGuard/js	2023-05-19-09.20.02	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.23	2	*PASS	/TrinityGuard/Images	2023-05-19-09.20.02	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.23	120	*PASS	/TrinityGuard/Help	2023-05-19-09.20.01	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.23	1	*PASS	/TrinityGuard/Agent	2023-05-19-09.19.52	Action
TGSE1	*TRN	ANONYMOUS	TELNET	INIT	N/A	10.27.81.23	10	*PASS		2023-05-19-09.19.20	Action
TGSE1	*TRN	PMB	FILE	ALLOCON	N/A	10.27.81.23	3	*PASS		2023-05-19-09.19.05	Action
TGSE1	*TRN	PMB	FILE	ALLOCON	N/A	10.27.81.28	7	*PASS		2023-05-17-15.07.04	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.28	6004	*PASS	/TrinityGuard/Reports	2023-05-17-15.00.55	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.28	400	*PASS	/TrinityGuard/Help	2023-05-17-15.00.50	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.28	5	*PASS	/TrinityGuard/Images	2023-05-17-15.00.47	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.28	5	*PASS	/TrinityGuard/js	2023-05-17-15.00.47	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.28	5	*PASS	/TrinityGuard/Agent	2023-05-17-15.00.47	Action
TGSE1	*TRN	PMB	FILE	LISTATT	N/A	10.27.81.28	18	*PASS	/TrinityGuard	2023-05-17-15.00.47	Action

Object Authorities & IFS Permissions – Define gold standards – quickly uncover anomalies – option to auto enforce compliance



Authority Compliance Report(Enforcement=*NO)

TGSE1	ADMIN	2023-05-17	12:29:55

Color references: Object current value Schema expected value

Schema ID	Out of Compliance Reason	File System	IFS Path	Auxiliary Storage Pool	Library Name	Object Name	Object Type	Authority List	Schema Authority List	Program Adopt	Schema Program Adopt	Program Adopt Users	Schema Program Adopt Users	Object Owner	Schema Object Owner	Object Primary Group	Schema Object Primary Group	User Inheritance Group	User Name	Schema User Name	Object Authority	Schema Object Authority	Data Read	Schema Data Read	Data Add	Schema Data Add	Data Update	Schema Data Update	Data Delete	Schema Data Delete	Data Execute	Schema Data Execute	Object Operation	Schema Object Operation	Object Management	S Mar
PMBALL	Object authorization list does not match schema default. It should be TGAUTL	*SYS		*SYSBAS	PMB	CMN	*FILE	*NONE	TGAUTL		*NO		*USER	PMB	*SAME	*NONE	*NONE																			
PMBALL	Object authority for user does not match schema default. It should be *AUTL	*SYS		*SYSBAS	PMB	CMN	*FILE	*NONE	TGAUTL		*NO		*USER	PMB	*SAME	*NONE	*NONE		*PUBLIC	*PUBLIC	*CHANGE	*AUTL	X		X		X		X		X		X			
PMBALL	Object user PMB is not found on schema default	*SYS		*SYSBAS	PMB	CMN	*FILE	*NONE	TGAUTL		*NO		*USER	PMB	*SAME	*NONE	*NONE		PMB		*ALL		X		X		X		X		X		X		X	
PMBALL	Object authorization list does not match schema default. It should be TGAUTL	*SYS		*SYSBAS	PMB	CMP	*FILE	*NONE	TGAUTL		*NO		*USER	PMB	*SAME	*NONE	*NONE																			
PMBALL	Object authority for user does not match schema default. It should be *AUTL	*SYS		*SYSBAS	PMB	CMP	*FILE	*NONE	TGAUTL		*NO		*USER	PMB	*SAME	*NONE	*NONE		*PUBLIC	*PUBLIC	*CHANGE	*AUTL	X		X		X		X		X		X			
PMBALL	Object user PMB is not found on schema default	*SYS		*SYSBAS	PMB	CMP	*FILE	*NONE	TGAUTL		*NO		*USER	PMB	*SAME	*NONE	*NONE		PMB		*ALL		X		X		X		X		X		X		X	
PMBALL	Object authorization	*SYS		*SYSBAS	PMB	CUSTMAST	*FILE	*NONE	TGAUTL		*NO		*USER	PMB	*SAME	*NONE	*NONE																			

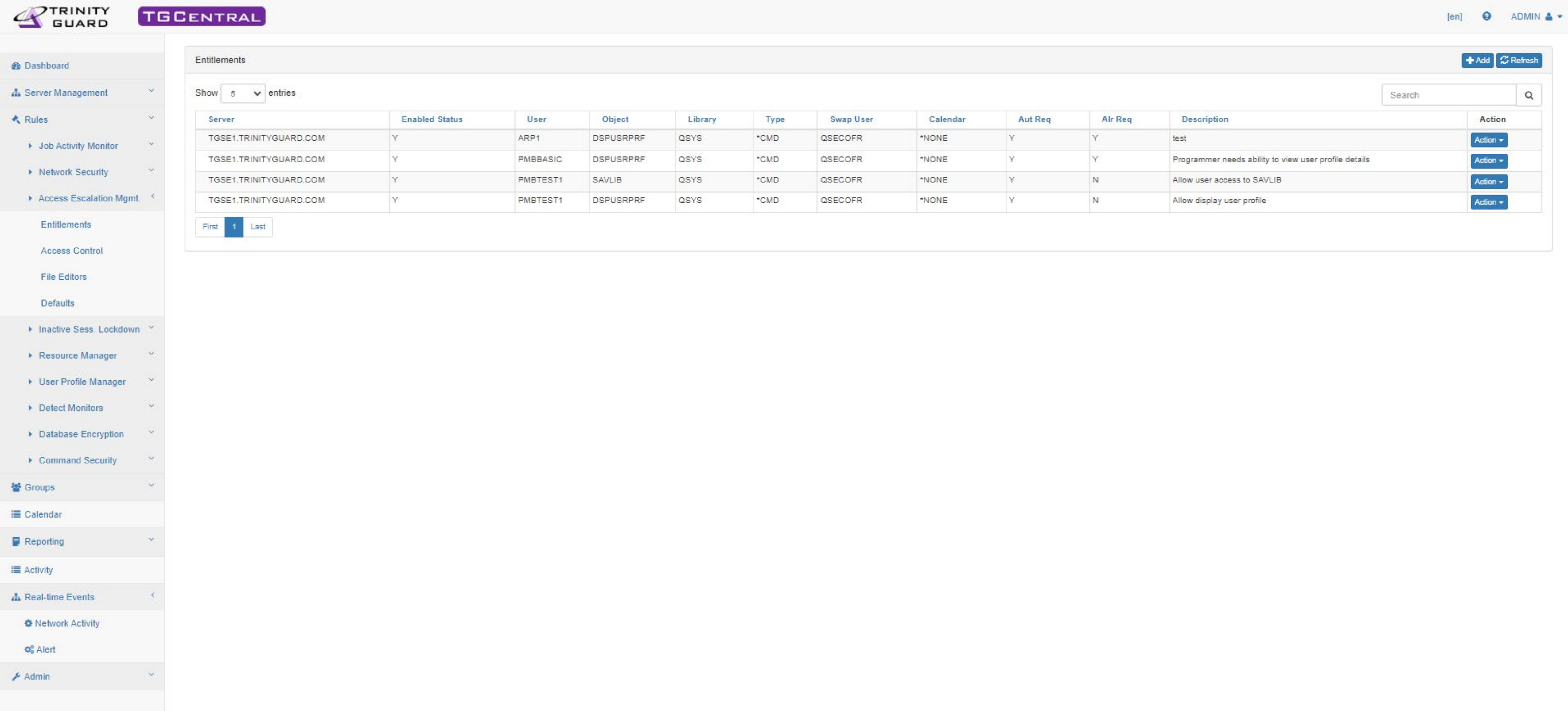
Access Escalation Management

- Leverage least-privilege model
- Privileged activity is permitted intentionally and audited
- Granular rules based on job function

Command Security

- Easily restrict access to sensitive commands
- Granular rules
- Auditing and alerting

Access Escalation – Granular entitlements – can require user authentication and/or alerting when invoked

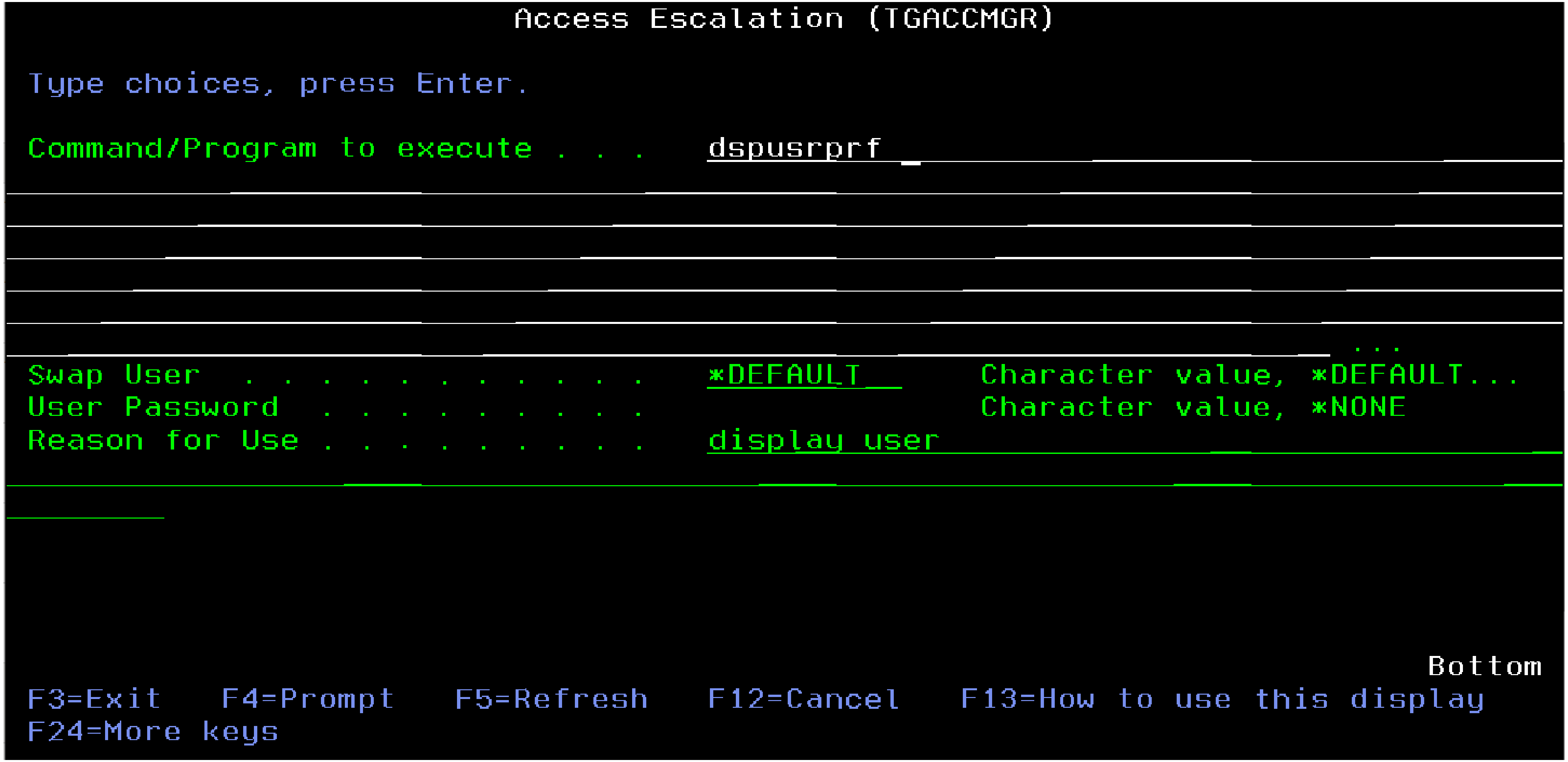


Entitlements

Show 5 entries

Server	Enabled Status	User	Object	Library	Type	Swap User	Calendar	Aut Req	Alr Req	Description	Action
TGSE1.TRINITYGUARD.COM	Y	ARP1	DSPUSRPRF	QSYS	*CMD	QSECOFR	*NONE	Y	Y	test	Action
TGSE1.TRINITYGUARD.COM	Y	PMBBASIC	DSPUSRPRF	QSYS	*CMD	QSECOFR	*NONE	Y	Y	Programmer needs ability to view user profile details	Action
TGSE1.TRINITYGUARD.COM	Y	PMBTEST1	SAVLIB	QSYS	*CMD	QSECOFR	*NONE	Y	N	Allow user access to SAVLIB	Action
TGSE1.TRINITYGUARD.COM	Y	PMBTEST1	DSPUSRPRF	QSYS	*CMD	QSECOFR	*NONE	Y	N	Allow display user profile	Action

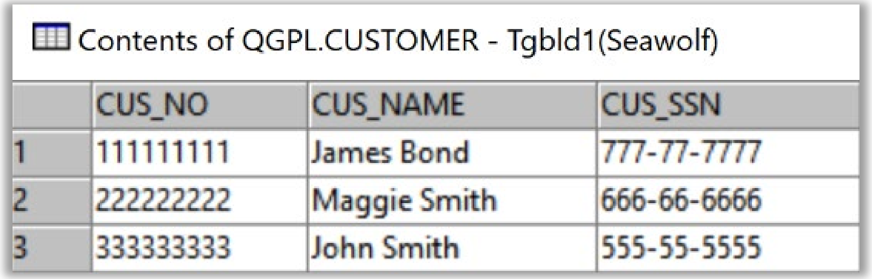
Access Escalation – Entitlement in action



```
                         Access Escalation (TGACCMGR)

 Type choices, press Enter.

 Command/Program to execute . . .    dspusrprf









                                                                        ...
 Swap User  . . . . . . . . . . .    *DEFAULT      Character value, *DEFAULT...
 User Password  . . . . . . . . .                  Character value, *NONE
 Reason for Use . . . . . . . . .    display user





                                                                         Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

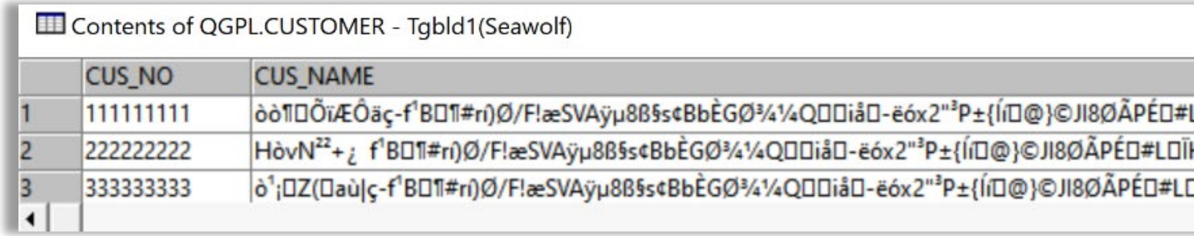
TGEncrypt

- Database Field-level Encryption
  - AES 256-Bit Encryption – standard recommended by NIST
  - Use TG internal keys or use existing keystore data to encrypt data
- Masking Field Data
  - Create your own mask for how end-users see sensitive data
- Scrambling Field Data
  - Scramble data based on internal TG scramble algorithm or customize your own algorithm



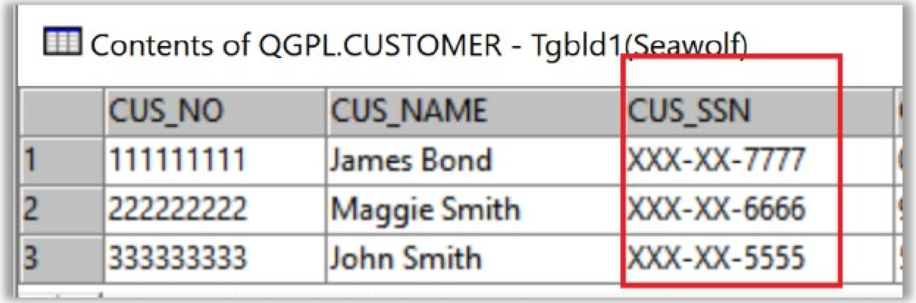
Contents of QGPL.CUSTOMER - Tgbld1(Seawolf)

	CUS_NO	CUS_NAME	CUS_SSN
1	111111111	James Bond	777-77-7777
2	222222222	Maggie Smith	666-66-6666
3	333333333	John Smith	555-55-5555



Contents of QGPL.CUSTOMER - Tgbld1(Seawolf)

	CUS_NO	CUS_NAME
1	111111111	òò¶□ÕïÆÔäç-f¹B□¶#rı)Ø/F!æSVAÿµ8ß§s¢BbÈGØ¾¼Q□□iå□-ëóx2"³P±{Íí□@}©JI8ØÃPÉ□#L
2	222222222	HòvN²²+¿ f¹B□¶#rı)Ø/F!æSVAÿµ8ß§s¢BbÈGØ¾¼Q□□iå□-ëóx2"³P±{Íí□@}©JI8ØÃPÉ□#L□Ïk
3	333333333	ò¹¡□Z(□aù|ç-f¹B□¶#rı)Ø/F!æSVAÿµ8ß§s¢BbÈGØ¾¼Q□□iå□-ëóx2"³P±{Íí□@}©JI8ØÃPÉ□#L□



Contents of QGPL.CUSTOMER - Tgbld1(Seawolf)

	CUS_NO	CUS_NAME	CUS_SSN
1	111111111	James Bond	XXX-XX-7777
2	222222222	Maggie Smith	XXX-XX-6666
3	333333333	John Smith	XXX-XX-5555

Next Steps

- ✓ IBM i Security Assessment
- ✓ IBM i Penetration Test

Have a project in mind? Questions?

Let us know in the exit survey, or get in touch:

pauline.ayala@fleschesolutions.com

info@freschesolutions.com