Key Vulnerabilities & How To Protect Against Them

IBM i Security Workshop

Presenter

Alan Hamm

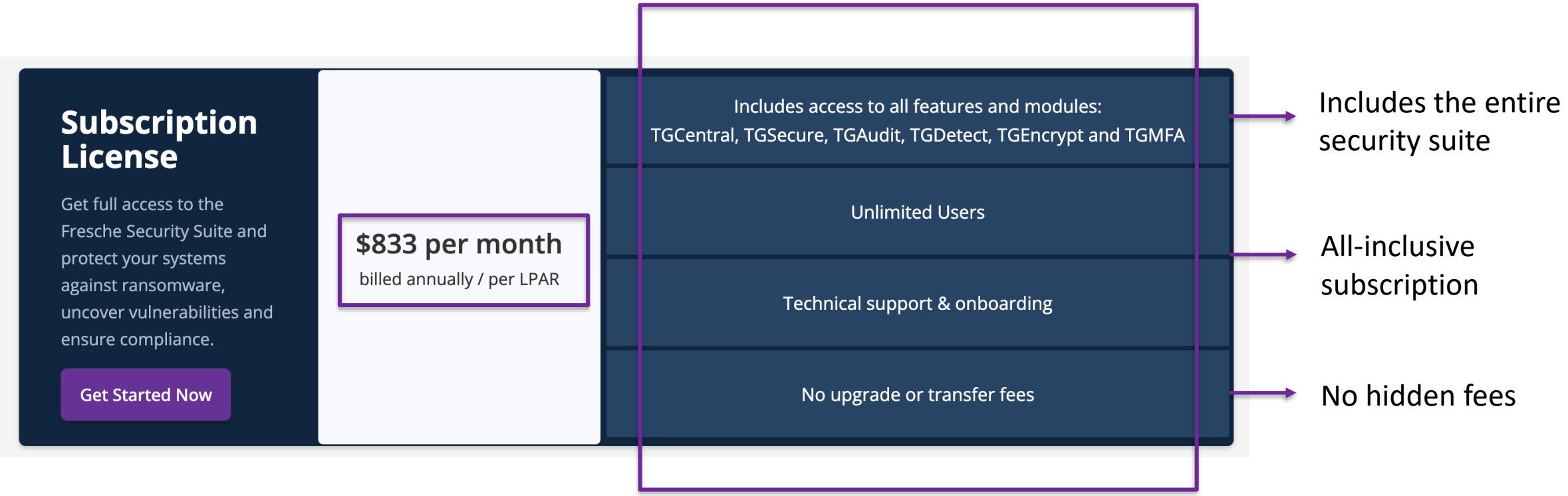
Senior Security Engineer
alan.hamm@freschesolutions.com

- Over 25 years of experience in the IT industry, specializing in IBM i security.
- Leverages development background to solve automation and configuration problems.
- 17 years as an application developer, systems integrator, business analyst, and data center lead.

Agenda

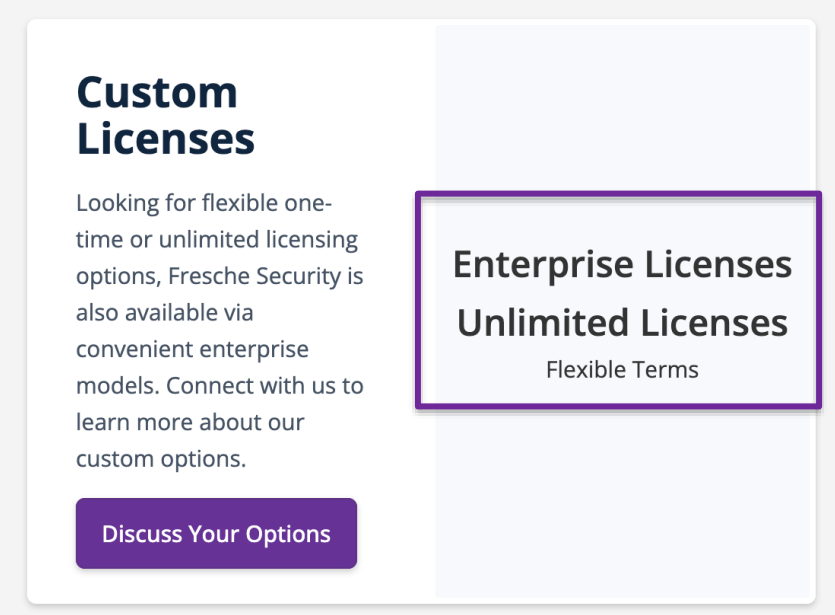
- Introduction
- TGSecurity Suite: Overview
- TGSecurity Suite: Subscription Models
- How to Secure:
  - Network Security & Exit Points >> Network Monitoring
  - IFS & Object Authority >> Zero Trust
  - Access Management >> Privileged Access Management
  - SIEM and Forensic Accounting >> Security Event Notifications
  - Auditing and Compliance >> Security Logging/Auditing
- Assessment Report: Sample

Powerful Security in an Affordable Subscription Model



FRESCHE SOLUTIONS

Security Services & Flexible Subscriptions



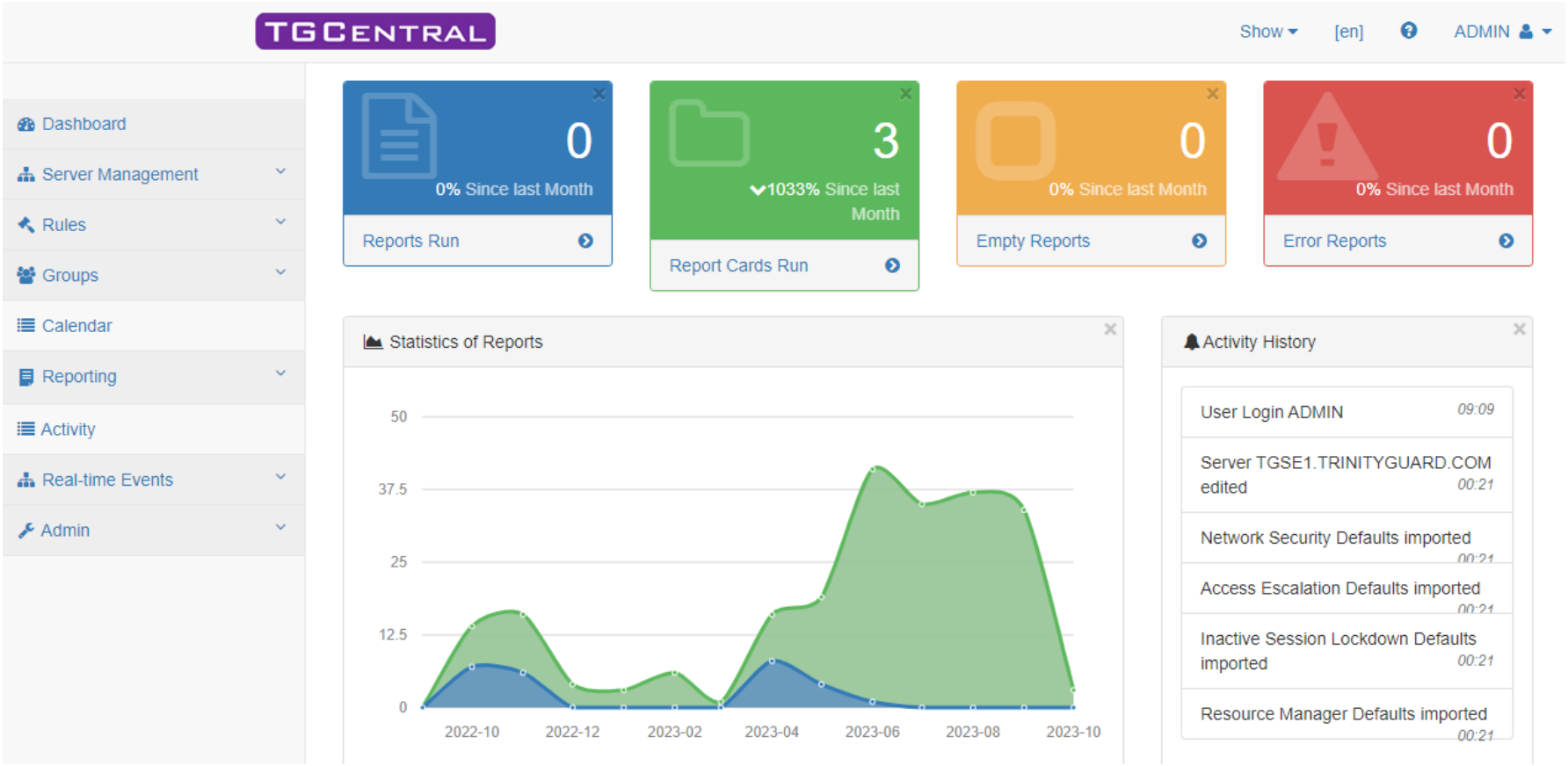
Self assess with free trial

Affordable access to IBM i security experts

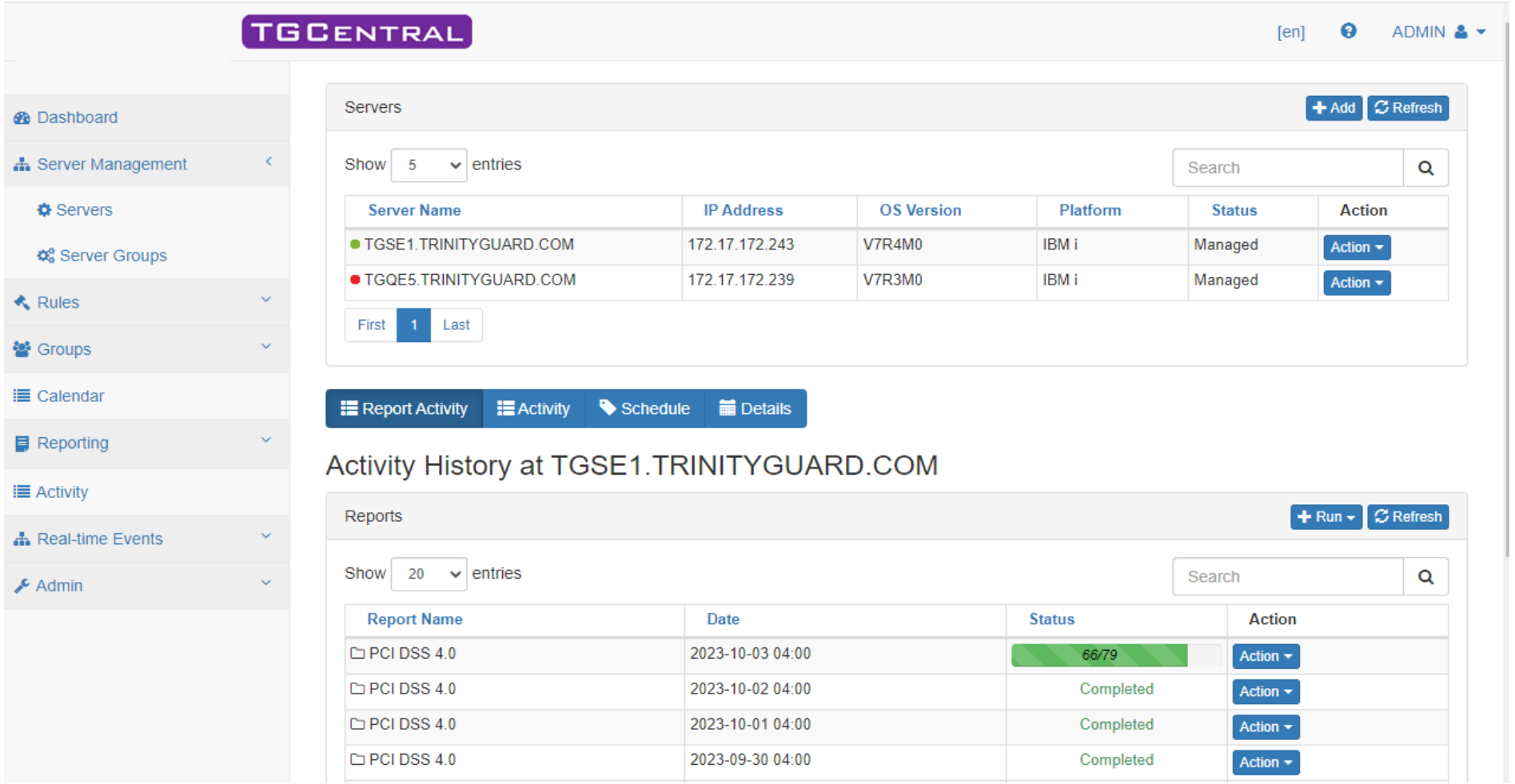
Trusted advisors Fresche & DXR (Carol Woodbury)

FRESCHE SOLUTIONS

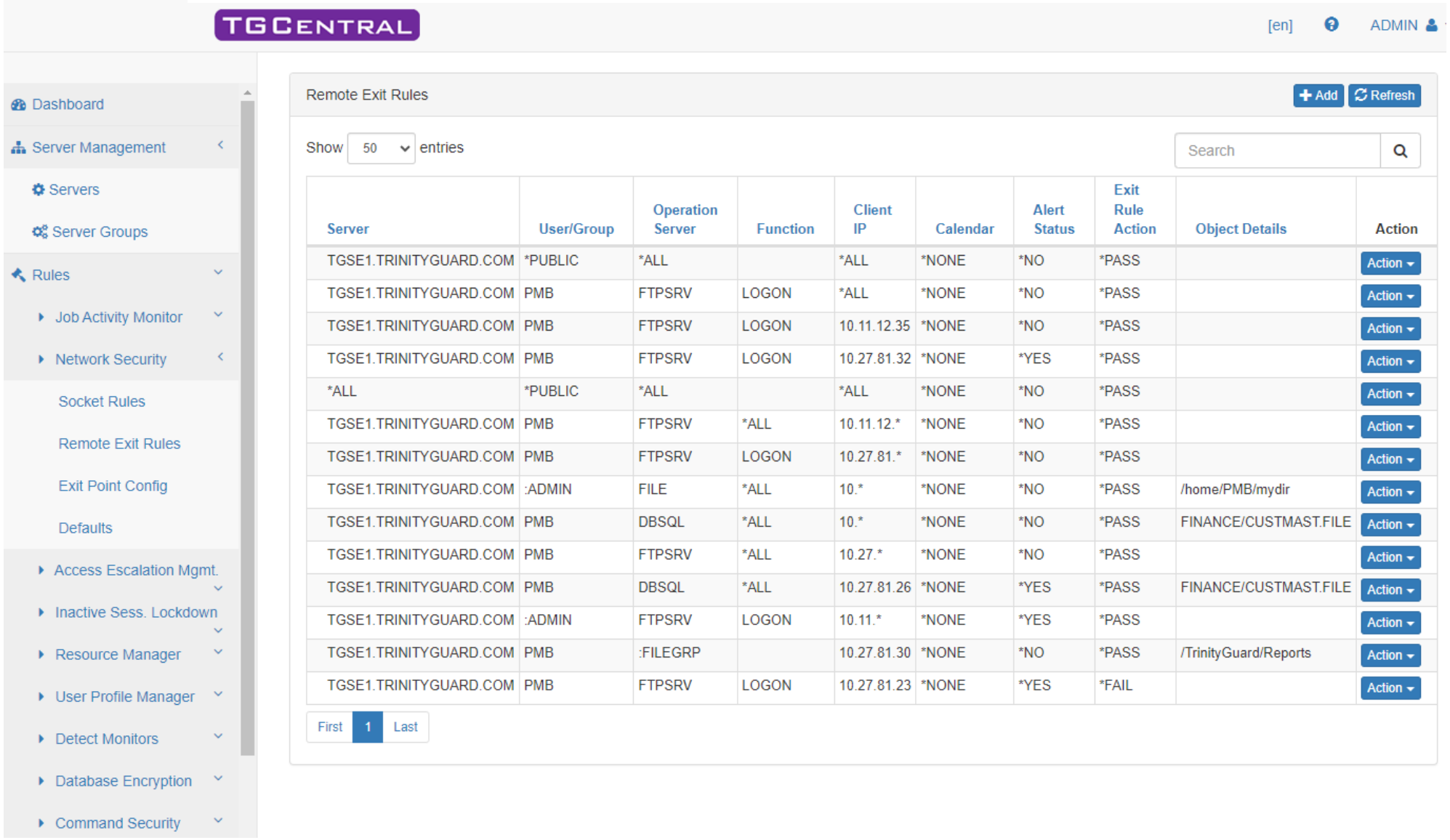
The GUI Interface



The GUI Interface

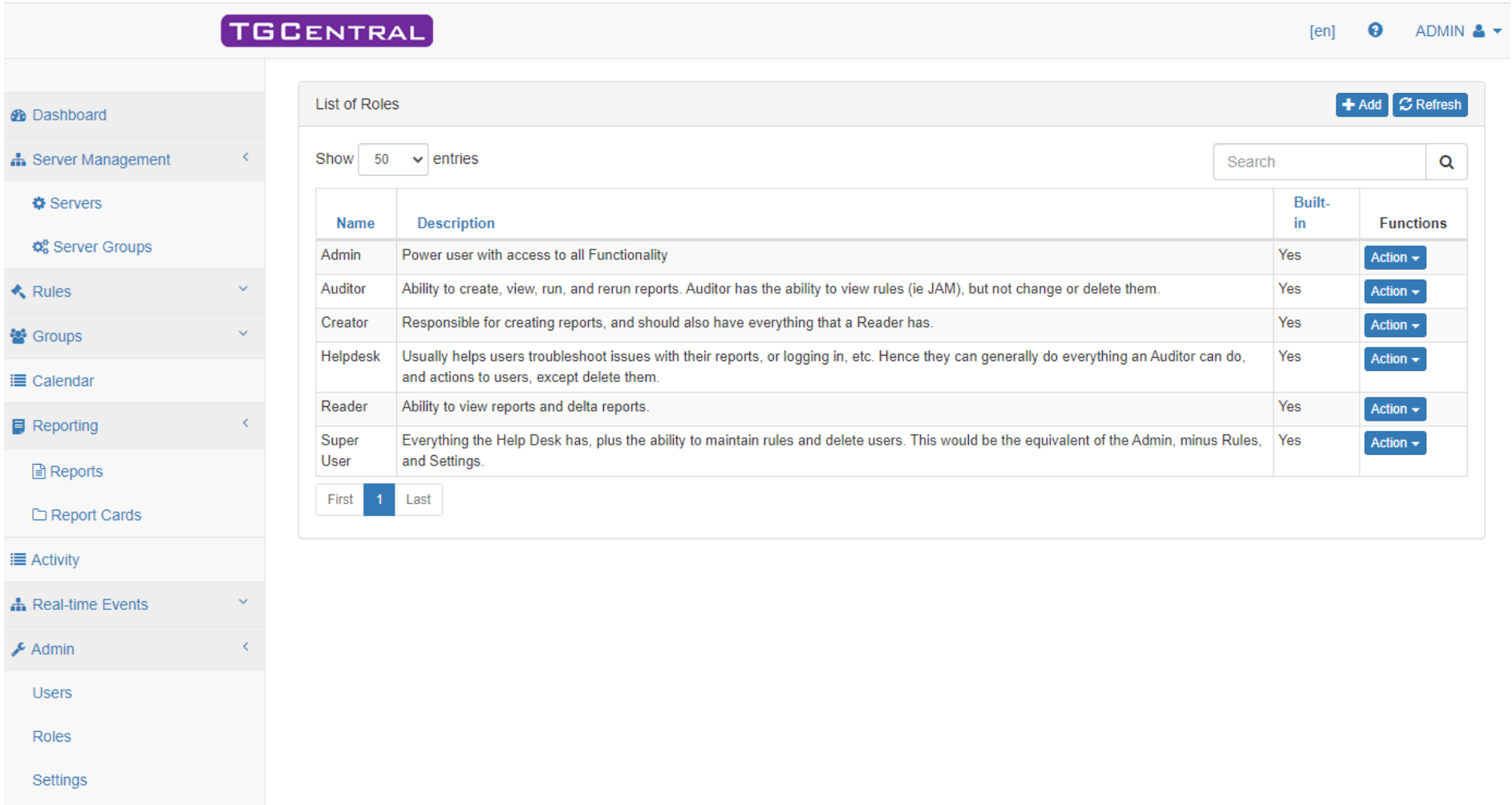


The GUI Interface



FRESCHE SOLUTIONS

The GUI Interface

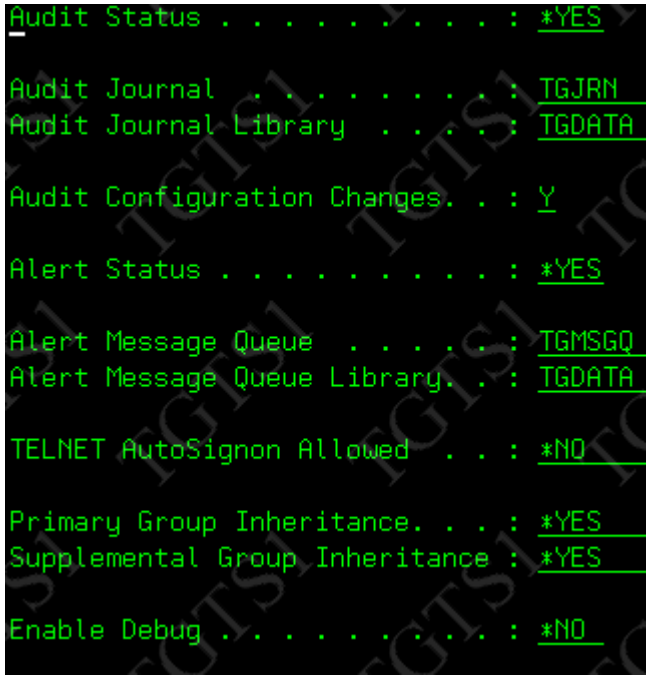


FRESCHE SOLUTIONS

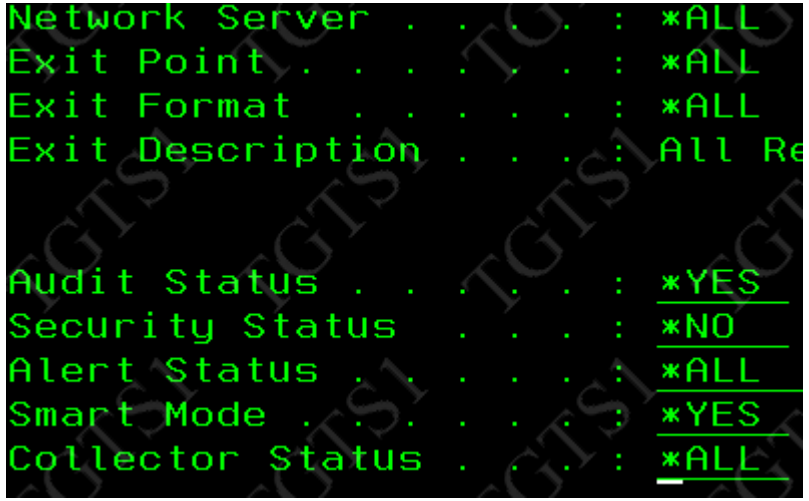

Poll: What layers of your IBM i have you secured?

TG Security Suite: Overview

- Accessing the Suite
- Authorizing users
- Checking product version and license
- Assessing Exit Point defaults



- TGMENU
- 70. Work with TG Product Users or edtautl tgautl
- 80. Licensing Status
- TGSecure->Network Security-> Network Security Defaults
- TGSecure->Network Security-> Exit Point Configuration->F7



FRESCHE SOLUTIONS

Network Security and Exit Points

How to objectives:
Log detailed exit point information
**No exit points by default = No detailed logging/monitoring

To add/remove exit programs:

TGMENU->2. TGSecure->1. Network Security->10. Exit Point Configuration

or

TGNTWCFG

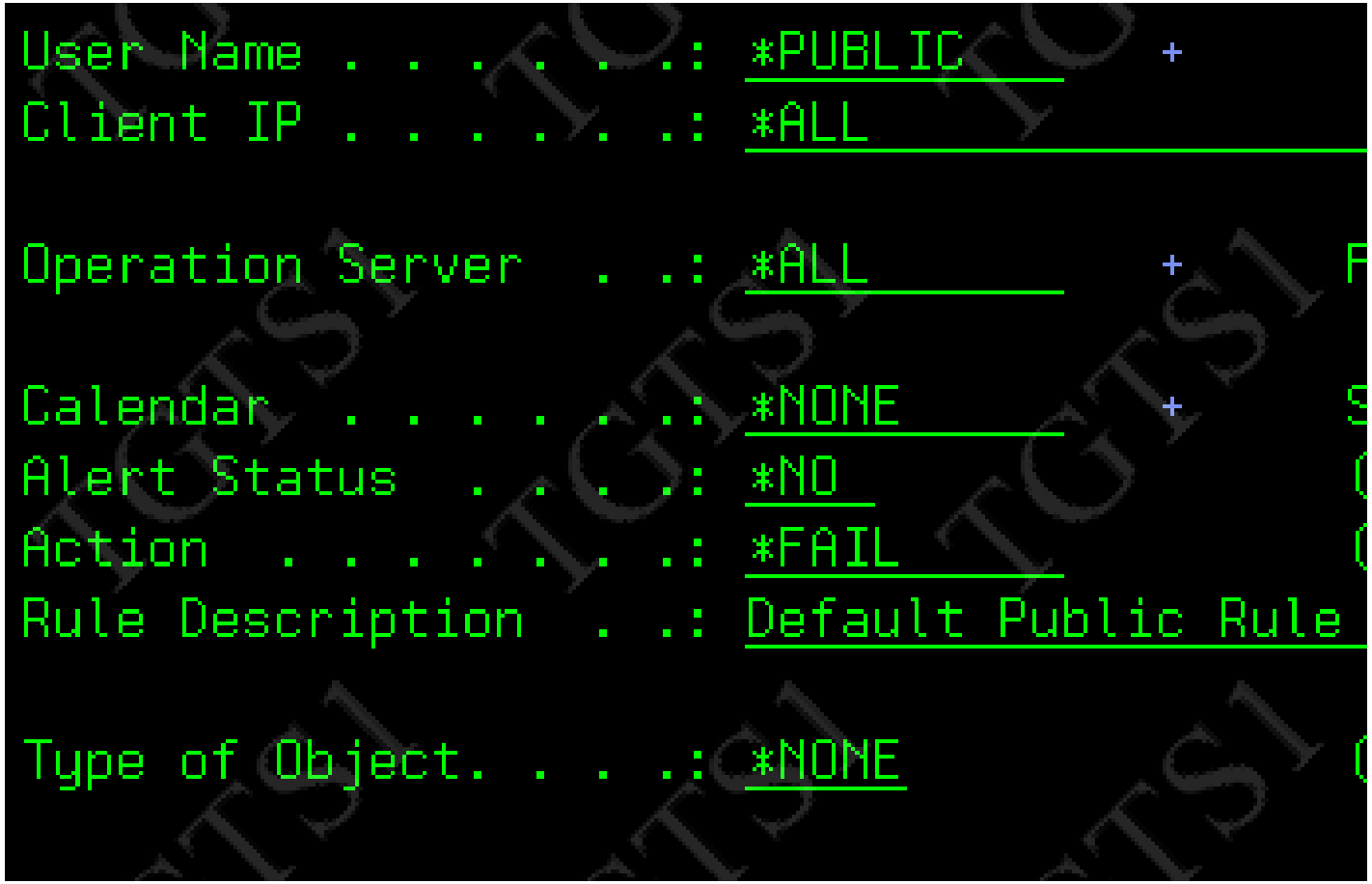
```
TGNTWCFG SERVER(*ALL) ACTION(*ADDCYC) RUNI(*YES)
```

OR

```
TGNTWCFG SERVER(*FTP)          ACTION(*ADDCYC) RUNI(*YES)
TGNTWCFG SERVER(*DATABASE) ACTION(*ADDCYC) RUNI(*YES)
TGNTWCFG SERVER(*FILE)         ACTION(*ADDCYC) RUNI(*YES)
TGNTWCFG SERVER(*DDM)          ACTION(*ADDCYC) RUNI(*YES)
TGNTWCFG SERVER(*SOCKET)    ACTION(*ADDCYC) RUNI(*YES)
```

Network Security and Exit Points

Best practices – deny by default - modify *PUBLIC (default rule)



Network Security and Exit Points

Generate/View FTP transactions:
cmd
ftp 172.17.172.240
cd /demo/public
cd /demo/it
cd /demo/hr

How to *PASS transactions:

Allow individual User - FTPSRV LOGON
Allow using user group :FTPUSERS - FTPSRV LOGON using
Allow QTCP *PRE *AIPPASS - FTPSRV INIT
Allow QTCP *PRE *TRUSTED - FTPSRV INIT

IFS and Object Authority

Best practices – deny by default - *PUBLIC *EXCLUDE

How to secure using QSYS:
Create authority schema APP01_QSYS

Owner = APP01
Authorization list = APP01
*PUBLIC = *AUTL
APP01 = *ALL

*PGM
Owner = APP01
Authorization list = *NONE
*PUBLIC = *USE
APP01 = *ALL
Use adopted authority = *YES
Adopted user profile = *OWNER

*FILE
Owner = APP01
Authorization list = *NONE
*PUBLIC = *EXCLUDE
APP01 = *ALL

*DTAARAFILE
Owner = APP01
Authorization list = *NONE
*PUBLIC = *EXCLUDE
APP01 = *ALL

Object	Type
QSYS/APP01	*USRPRF
QSYS/APP01	*AUTL
QSYS/APP01	*LIB
APP01/FILE01 – FILE04	*FILE
APP01/PGM01 – PGM04	*FILE
APP01/QCLLESRC	*FILE
APP01/QRPGLESRC	*FILE
APP01/VERSION	*DTAARA

IFS and Object Authority

Create Object Group :APP01

TGMENU->2. TGSecure->4. Resource Manager->

3. Work with Groups->1. Work with Object Groups->F6

```
Group Name . . . . : :APP01

Group Description: APP01
```

Add objects

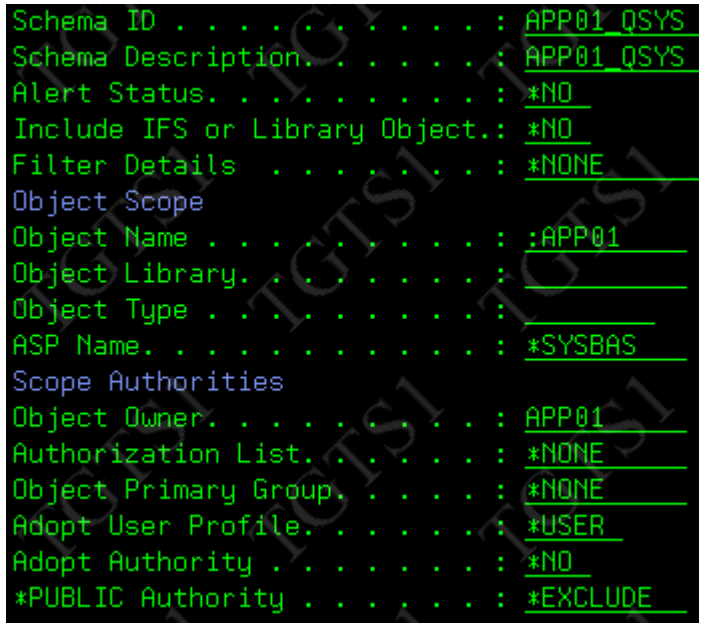
```
Group Name/Desc.: :APP01     APP01

Subset Criteria -  File Sys.: *ALL        Obj.Name: *ALL

2=Edit 4=Delete

Opt  File System   Object  Name

_    *SYS          APP01/*ALL.ALL
_    *SYS          QSYS/APP01.LIB
```

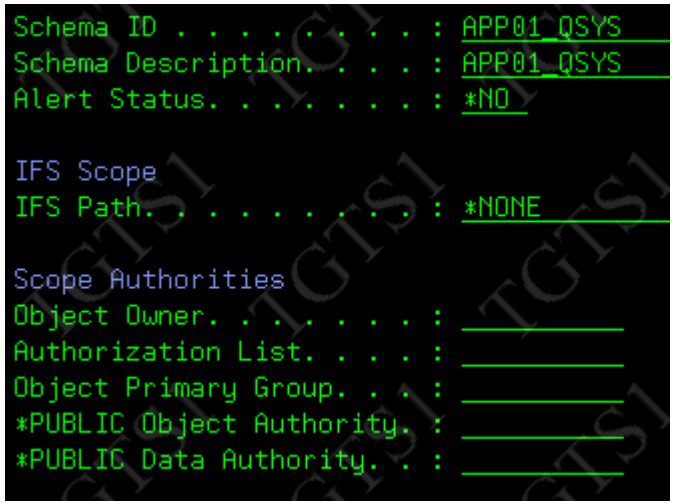
IFS and Object Authority

Authority schema APP01_QSYS

TGMENU->2. TGSecure->4. Resource Manager->

1. Authority Schema Configuration->F6





IFS and Object Authority

Zero Trust

Define schema

```
Schema ID. . : APP01_QSYS
Description. : APP01_QSYS

2=Edit 3=Copy 4=Delete  5=Display


   File Path or                        Library   Object     Object   Object     Auth       User       Auth       Exception
Opt Sys  ASP                                     Name       Type     Owner      List       Object
_   *SYS *SYSBAS                                 :APP01              APP01      *NONE      *PUBLIC    *EXCLUDE   *NO
_   *SYS *SYSBAS                                 :APP01              APP01      *NONE      APP01      *ALL       *NO
```

```
Schema ID  . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : *ALL
Object Library . . . : APP01
Object Type. . . . . : *PGM
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE
Adopt User Profile . : *OWNER
Adopt Authority. . . : *YES
User Authority Settings
User Name. . . . . : *PUBLIC
Object Authority . . : *USE
```

```
Schema ID  . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : *ALL
Object Library . . . : APP01
Object Type. . . . . : *PGM
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE
Adopt User Profile . : *OWNER
Adopt Authority. . . : *YES
User Authority Settings
User Name. . . . . : APP01
Object Authority . . : *ALL
```

```
Schema ID  . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : APP01
Object Library . . . : QSYS
Object Type. . . . . : *LIB
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : APP01
Object Primary Group.: *NONE
Adopt User Profile . : *USER
Adopt Authority. . . : *NO
User Authority Settings
User Name. . . . . : *PUBLIC
Object Authority . . : *AUTL
```

```
Schema ID  . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : APP01
Object Library . . . : QSYS
Object Type. . . . . : *LIB
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : APP01
Object Primary Group.: *NONE
Adopt User Profile . : *USER
Adopt Authority. . . : *NO
User Authority Settings
User Name. . . . . : APP01
Object Authority . . : *ALL
```

IFS and Object Authority

Run Compliance Report

Take option 22

Or

TGAUTCMP SCHID(APP01_QSYS) ARPT(*NO) OUTPUT(*) ENFO(*NO) RUNI(*YES)

IFS and Object Authority

Best practices – deny by default - *PUBLIC *EXCLUDE

How to secure using IFS:

Create authority schema APP01_IFS

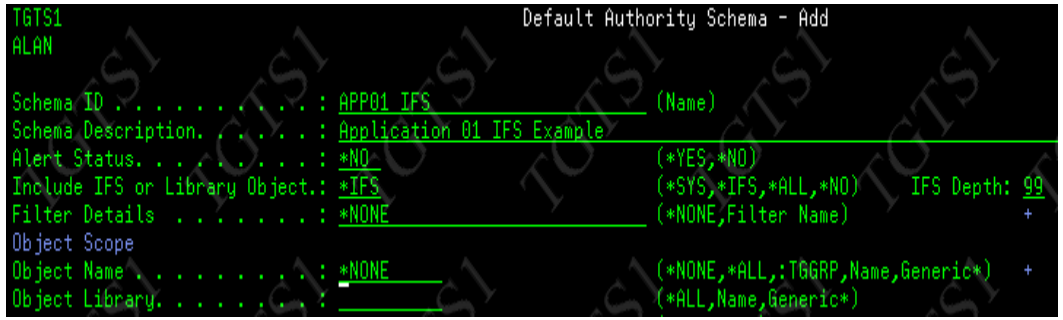
Application location = /demo/App01
Owner = APP01
Authorization list = *NONE
*PUBLIC = *EXCLUDE
APP01 = *ALL

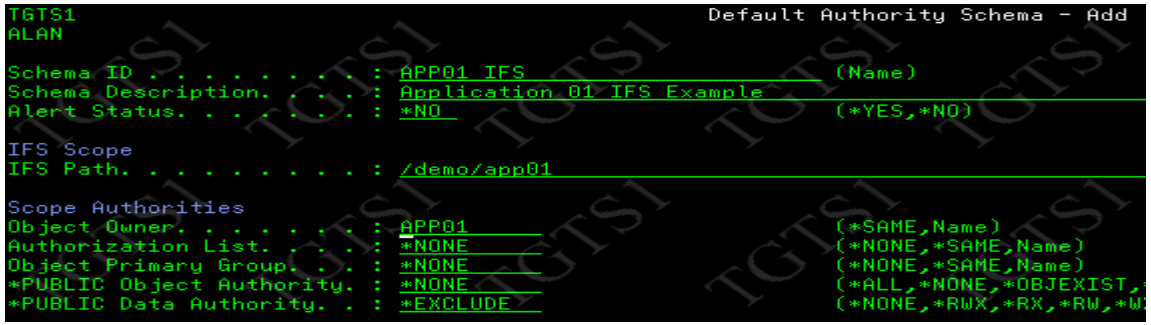
Application support team needs access to logs!
/demo/App01/log
Owner = App01
Authorization list = *NONE
*PUBLIC = *EXCLUDE
APP01 = *ALL
GRPPGMRS = *RX

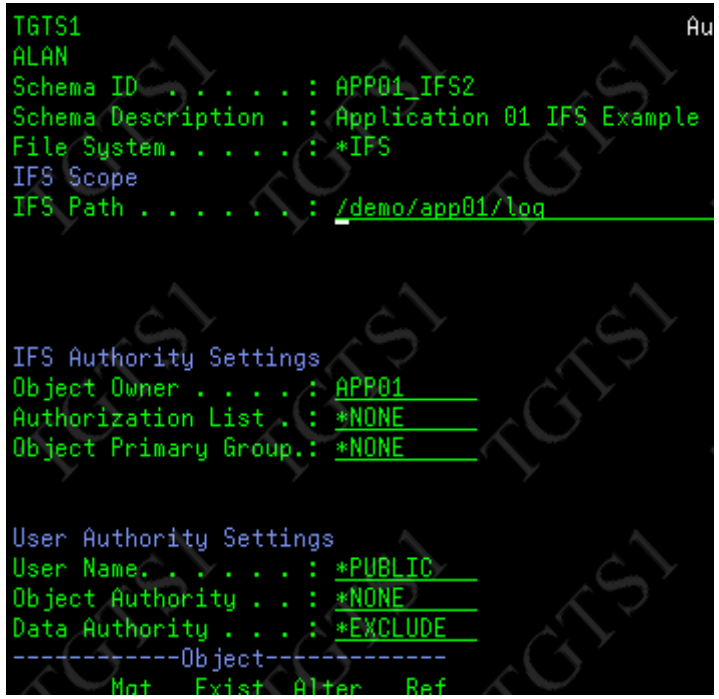
IFS and Object Authority

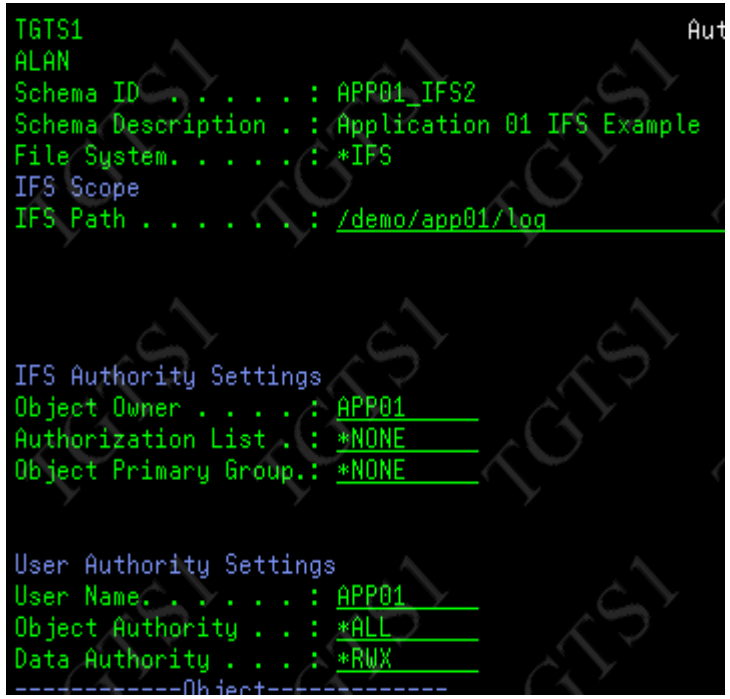
Zero Trust

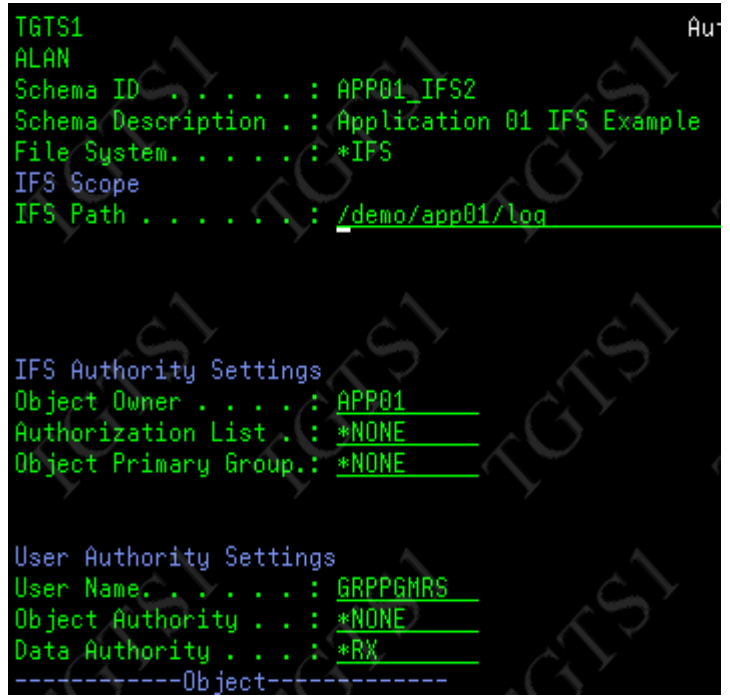
Define schema











IFS and Object Authority

Run Compliance Report

Take option 22

Or

TGAUTCMP SCHID(APP01_IFS) ARPT(*NO) OUTPUT(*) ENFO(*NO) RUNI(*YES)

Access Management

Privileged Access Management

Blueprint

Use Case: Restricted User Provisioning without *SECADM
Allow Development manager (ALANNONSEC) the ability to enable their service account (APP01) when needed.

FRESCHE SOLUTIONS

Access Management

Privileged Access Management

Create Blueprint APP01_STATUS_CHANGE

```
TGTS1                                          Blueprint - Add  (Step 1/6)
ALAN

Blueprint details
Blueprint ID. . . . . . . . . . . . . . . . . . . . : APP01_STATUS_CHANGE
Blueprint Description . . . . . . . . . . . . . . . : APP01 STATUS CHANGE
Alert Status. . . . . . . . . . . . . . . . . . . . : *NO

User Scope. . . . . . . . . . . . . . . . . . . . . : :APP01

Inactivity Overrides
Inactivity until User Profile is disabled (days). . : *DFT
Inactivity until User Profile is deleted  (days). . : *DFT
Object owner for objects owned by deleted profiles. : *DFT
```

```
TGTS1                                                          Bluepri
ALAN                                                           User Pro

Blueprint ID . . . . . . . . . . . . : APP01_STATUS_CHANGE
Description. . . . . . . . . . . . . : APP01 STATUS CHANGE

Set the User Profile Parameter values.

4=Delete 2=Edit

Opt Parameter                          Parameter  Parameter
    Description                        keyword    Value

    Status                             STATUS     *ENABLED
```

FRESCHE SOLUTIONS

Access Management

Privileged Access Management

Create Blueprint APP01_STATUS_CHANGE

```
TGTS1                                          Blueprint - Add  (Step 3/6)
ALAN                                          User Profile Object Authoriti

Blueprint ID. . : APP01_STATUS_CHANGE           Description. . : APP01 STATI

Enter the Object Authority settings.

*USRPRF Object
Object Owner  . . . . . . . . . . :  *DFT_____  (*DFT,Name,*USRPRF)
Owner Authority . . . . . . . . . :  _________  (*CHANGE,*USE,*EXCLUDE,*ALL)
*PUBLIC Authority . . . . . . . . :  _________  (*AUTL,*USE,*CHANGE,*ALL,*EXCI

*MSGQ Object
Object Owner  . . . . . . . . . . :  *DFT_____  (*DFT,Name,*USRPRF)
Owner Authority . . . . . . . . . :  _________  (*CHANGE,*USE,*EXCLUDE,*ALL)
*PUBLIC Authority . . . . . . . . :  _________  (*AUTL,*USE,*CHANGE,*ALL)
```

```
TGTS1                                          Blueprint - Add (Step 4/6)
ALAN                                            Authority List Settings

Blueprint ID . . . . . . . . . . : APP01_STATUS_CHANGE
Description. . . . . . . . . . . : APP01 STATUS CHANGE

Set the Authority Lists.

4=Delete

     Authority   Authority
 Opt List        Value       Description
```

```
TGTS1                                          Blueprint - Add (Step 5/6)
ALAN                                             3rd party Integration

Blueprint ID . . . . . . . . . . : APP01_STATUS_CHANGE
Description. . . . . . . . . . . : APP01 STATUS CHANGE

Set 3rd Party script to  run and Pass  User Profile($USRPRF)  and/or Description ($TEXT)

4=Delete

     Script  Script
 Opt Type    Statement
```

```
TGTS1                                          Blueprint - Add  (Step 6/6)
ALAN                                             Blueprint Permissions

Blueprint ID. . : APP01_STATUS_CHANGE           Description. . : APP01 STATUS CHANGE

Authorize admin/help desk users to use the blueprints.

User/Group. . . . . . . . : ALANNONSEC  (:TGUSGRP)  +
Create Permissions. . . . : *NO         (*YES,*NO)
Change Permissions. . . . : *YES        (*YES,*NO)
```

FRESCHE SOLUTIONS

Access Management

Privileged Access Management

Blueprint APP01_STATUS_CHANGE

ADDAUTLE AUTL(TGAUTL) USER(ALANNONSEC) AUT(*USE)

Check it out, test it!

TGPRFCMP COMPN(APP01_STATUS_CHANGE) OUTPUT(*) ENFO(*NO) RUNI(*YES)

TGPRFCMP COMPN(APP01_STATUS_CHANGE) OUTPUT(*) ENFO(*YES) RUNI(*YES)

SIEM and Forensic Accounting

Security Event Notifications

Detect

SIEM and Forensic Accounting

QHST : QSECOFR logins

TGMENU -> 3. TGDetect -> 1. Work with Monitors -> QHST 10 -> 20

Auditing and Compliance

Security Logging/ Auditing

*NOTE

Not logged/audited by default

System Values

TGMENU -> 2. TGSecure -> 7. System Value Management -> 1. Work with System Values

Profile management:

TGMENU -> 2. TGSecure -> 5. User Profile Management -> 5. Profile Inactivity Settings

Reporting: ☺

TGMENU -> 1. TGAudit

30. Work with Reports (TGWRKRPT)

31. Work with Report Cards (TGWRKCARD)

Assessment Report

Date:11/03/22
Time:07:11:00
System:TGTS1

Category	Description	Number of Violations	Pass/Fail Status	Report Link
Network	Sockets-related exit points not secured	2	FAIL	Detailed Report
Network	Remote server exit points not secured	15	FAIL	Detailed Report
Profiles	System Service Tools users	2	FAIL	Detailed Report
Resources	Integrated File System security	1	FAIL	Detailed Report
Resources	Allow object restore option	1	FAIL	Detailed Report
Resources	Allow user domain objects in libraries	1	FAIL	Detailed Report
Configuration	Auditing control contains AUDLVL and OBJAUD	0	PASS	Detailed Report
Configuration	Attention events are audited	0	PASS	Detailed Report
Configuration	Authorization failures are audited	0	PASS	Detailed Report
Configuration	All object creations are audited	0	PASS	Detailed Report
Configuration	All deletions of external objects on the system are audited	0	PASS	Detailed Report
Configuration	Actions that affect a job are audited	0	PASS	Detailed Report
Configuration	Networking and communications functions are audited	0	PASS	Detailed Report
Configuration	Generic object tasks are audited	0	PASS	Detailed Report
Configuration	OfficeVision are audited	0	PASS	Detailed Report

Next Steps…

- Download a Free Trial
- Subscribe to TGSecurity Suite
- Speak with a security expert
- Conduct a Pen Test

Questions?

alan.hamm@freschesolutions.com

info@freschesolutions.com

FRESCHE SOLUTIONS