

---

# TESTBED AS400

## SekChek for OS/400 Security Report

---

System: S65E570C

9 March 2012

---

## Contents

SekChek Options	3
System Details	4
System Configuration	5
1. Report Summaries	7
1.1 Comparisons Against Industry Average and Leading Practice	8
1.2 Answers to Common Questions	13
1.3 Summary of Changes since the Previous Analysis	16
2. System Values	17
3. User Profiles and Classes	30
4. Profiles with Special Authorities	33
5. Password Change Intervals Greater than 30 Days	39
6. Group Profiles and their Members	42
7. Redundant Groups	43
8. Passwords Equal to Profile Name	44
9. Profiles with Expired Passwords	45
10. Passwords, 30 Days and Older	46
11. Last Logons, 30 Days and Older	48
12. Invalid Signon Attempts Greater than 3	51
13. Profiles Allowed Simultaneous Device Sessions	52
14. Profiles with Limited Capability	55
15. Profiles with Attention-Key Programs	58
16. Profiles without Signon (Display) Information	59
17. Group and IBM-Supplied Profiles	62
18. Initial Programs and Menus	63
19. Disabled Profiles	65
20. Damaged Profiles	67
21. Profiles Created in the Last 90 Days	68
22. Programs with Adopted Authorities	70
23. Object and Data Authorities for Selected Objects	73
24. Network Services	78
25. Other Considerations	80

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

SekChek Options	
Reference Number	1009090006
Requester	Richard Burns
Telephone Number	+44 (881) 846 8971
City	London
Client Country	UK
Charge Code	SekChek100909
Client Code	SEK001
Client Industry Type	Communications
Host Country	South Africa
Security Standards Template	0 - SekChek Default
Evaluate Against Industry Type	Communications
Compare Against Previous Analysis	Not Selected
Report Format	Word 2007
Paper Size	A4 (21 x 29.7 cms)
Spelling	English UK
Large Report Format	MS-Access database
Large Report (Max Lines in Word Tables)	10000
Summary Document Requested	Yes
Scan Software Version Used	Version 5.0.2
Scan Software Release Date	18-Jun-2009

Your *SekChek* report was produced using the above options and parameters.

You can change these settings for all files you send to us for processing via the *Options* menu in the *SekChek* Client software on your PC. You can also tailor them (i.e. temporarily override your default options) for a specific file via the *Enter Client Details* screen. This screen is displayed:

- For *SekChek* for NT and NetWare - during the Scan process on the target Host system;
- For *SekChek* for AS/400 and UNIX - during the file encryption process in the *SekChek* Client software.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

System Details	
System	S65E570C
Scan Time	03-Sep-2010 11:43
OS/400 Version	V6R1M0
System Model	520
System Serial Number	65E570C

*Report Date: 9 March, 2012*

**Declaration.**

*The provided observations and recommendations are in response to a benchmarking analysis that compares the user's information security features against industry. The recommendations are organized to identify possible implications to the company based on the gathered information, to identify a leading practices risk rating of the implications and provide possible recommended actions. The benchmarking analysis and the related observations and recommendations should supplement management's analysis but should not be and cannot be solely relied upon in any instance to identify and/or remediate information security deficiencies. Further, the observations and recommendations herein do not identify the cause of a possible deficiency or the cause of any previously unidentified deficiencies. The causes of the deficiencies must be determined by management for the recommendations selected to be relevant.*

© 1996-2012 SekChek IPS. All rights reserved.

SekChek is a registered trademark of SekChek IPS. All other trademarks are the property of their respective owners.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## System Configuration

### Operating System

OS version	V6R1M0
System model number	520
System serial number	65E570C

### Date / Time Formats

Date format	MDY
Date separator	/
Time separator	:
Sample date	10/03/09
Sample time	11:43:13
Sample date / time	09/25/2009 11:43:13.971612
UTC offset	+0200
Time adjustment	*NONE
Time zone	QP0200SAST

### SSL Specification

Cipher list	*RSA_AES_128_CBC_SHA *RSA_RC4_128_SHA *RSA_RC4_128_MD5 *RSA_AES_256_CBC_SHA *RSA_3DES_EDE_CBC_SHA *RSA_DES_CBC_SHA *RSA_EXPORT_RC4_40_MD5 *RSA_EXPORT_RC2_CBC_40_MD5 *RSA_NULL_SHA *RSA_NULL_MD5
Cipher control	*OPSYS
Protocols	*OPSYS

### Locale, Language

Country identifier	US
Locale path	/QSYS.LIB/EN_US.LOCALE
Language identifier	ENU
Currency symbol	\$
Coded character set identifier	65535
Graphic char set and code page	697 37
Graphic identifier control	*DEV D
Keyboard language character set	USB

### System Limits

Initial number of active jobs	200
Additional number of active jobs	30
Initial total number of jobs	200
Maximum number of jobs	163520
Spooling control block additional storage	2048

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Additional number of total jobs	30
Base storage pool activity level	79
Base storage pool minimum size	96659
Communications recovery limits	0 0
Maximum history log records	5000
Maximum spooled files	9999
Machine storage pool size	270100
Query processing time limit	*NOMAX
UPS supply delay time	200 200
UPS message queue	QSYS/QSYSOPR

### Library List

System part	QSYS QSYS2 QHLPSYS QUSRSYS
User part	QGPL QTEMP

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

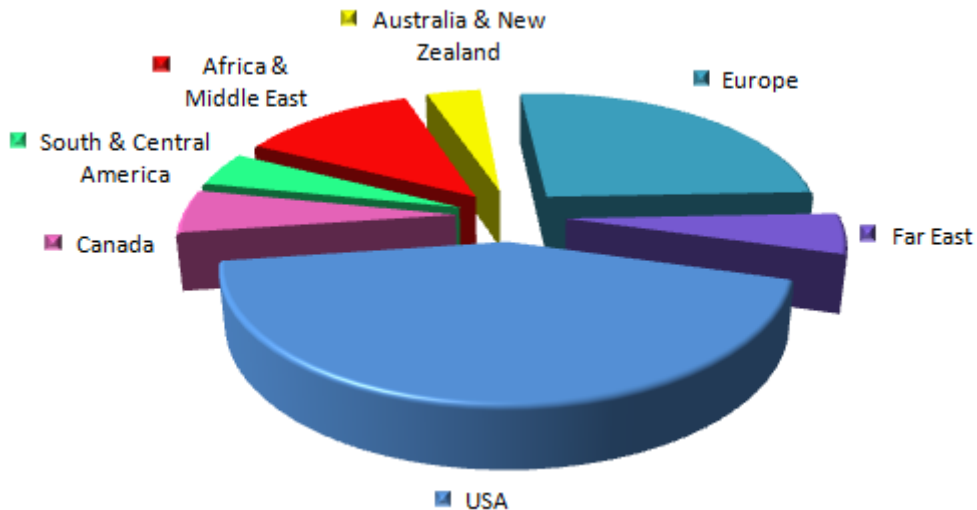
CONFIDENTIAL

## 1. Report Summaries

The following two charts illustrate the diversity of regions and industries that make up the population of AS400 systems in our statistics database. The remaining graphs in the *Report Summary* section evaluate security on your system against this broad base of real-life security averages.

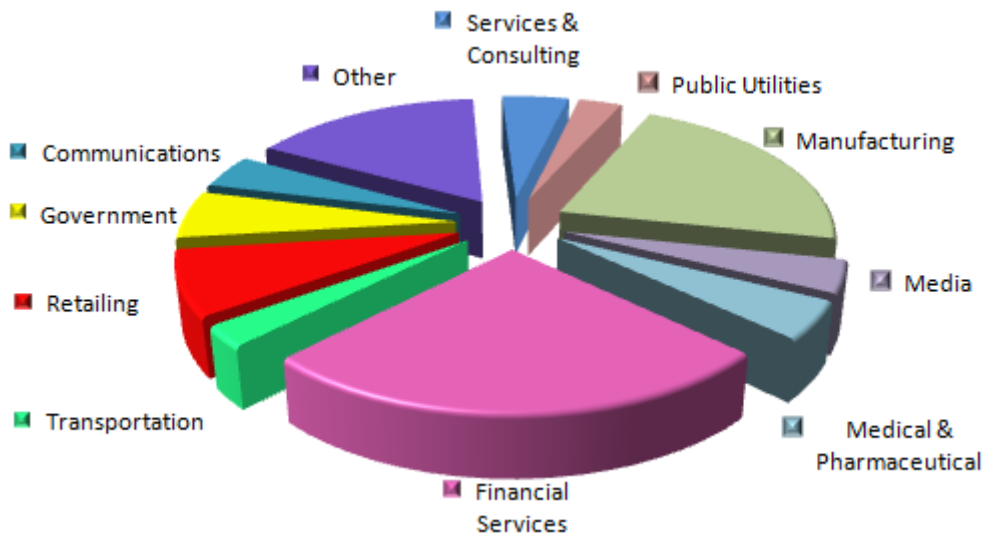
SekChek is used by the Big Four audit firms, IS professionals, internal auditors, security consultants & general management in more than 120 countries.

### Statistics Population by Region



As new reviews are processed, summaries of the results (excluding client identification) are automatically added to a unique statistics database containing more than 60,000 assessments.

### Statistics Population by Industry Type



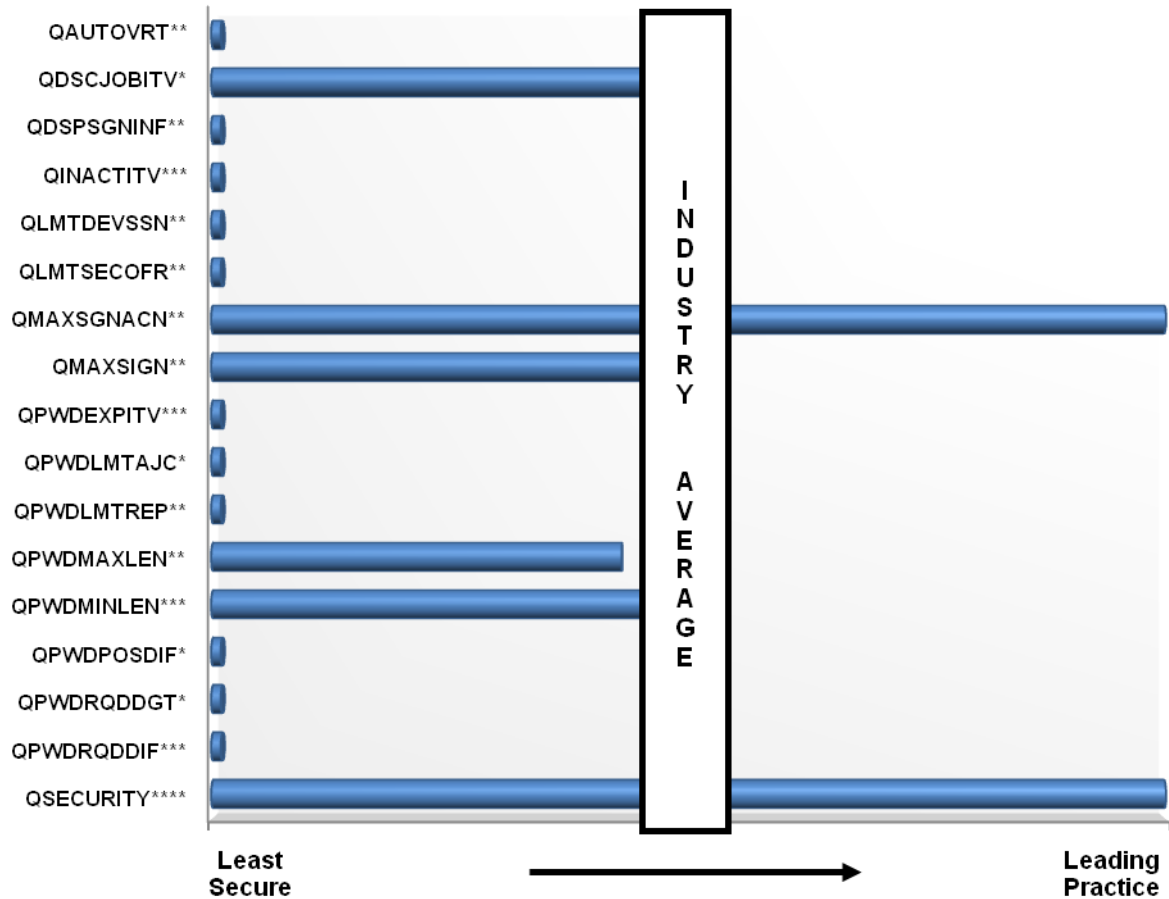
# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 1.1 Comparisons Against Industry Average and Leading Practice

### Summary of System-Wide Security Values



This graph compares your System Values against the industry average using the following criteria:  
Country = <All>; Industry Type = Communications; Machine Size (Nbr of Accounts) = <All>

System Values appear in alphabetical sequence.

This, and the following [summary report](#), are of most value when they are used to compare 'snapshots' of your security measures at different points in time. Used in this way they provide a fairly clear picture of whether your security measures are improving or becoming weaker.

**Industry Average** is a dynamic, calculated average for *all* AS/400 systems processed by *SekChek* for AS/400. It indicates how your security measures compare with those of other organisations using AS/400 systems.

**Leading Practice** is the standard adopted by the top 10 to 20 percent of organisations.

**Asterisks** (\*) after System Values indicate their relative importance and individual contribution towards security of your system. I.e. System Values followed by 3 asterisks (\*\*\*) are considered more important, and to have a greater impact on security than those followed by 1 asterisk (\*). This is an approximation and should be used as a guide only.

A very small bar (equating to roughly 1%) probably indicates that the security feature is not enabled on your system. Many System Values have only 2 possible settings - 'on' or 'off'.

For more information and detail, see the report [System Values](#).

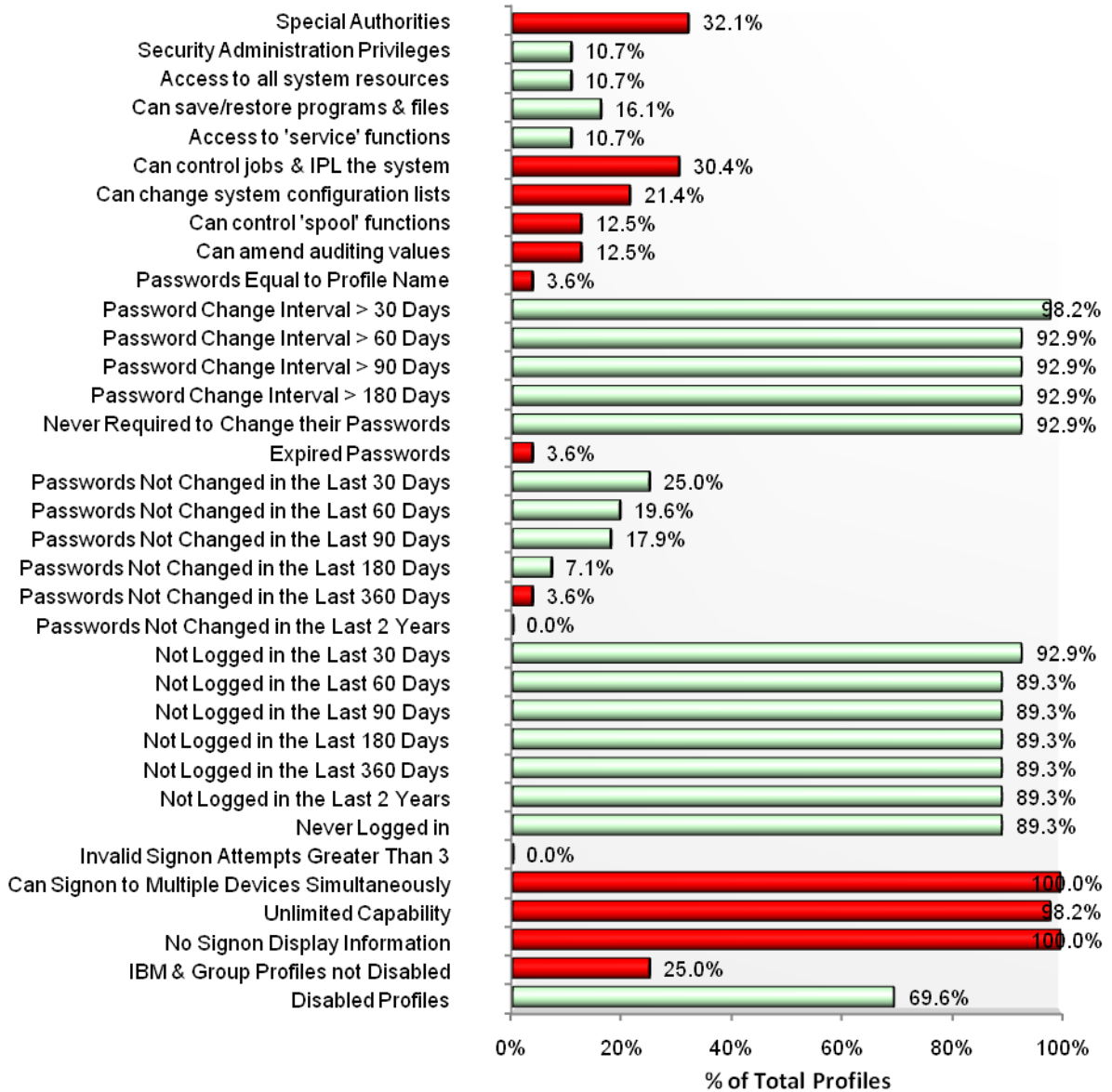
# Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

## Comparisons Against Industry Average and Leading Practice (continued)

### Summary of User Profiles



This graph compares against the industry average using the following criteria:  
 Country = <All>; Industry Type = Communications; Machine Size (Nbr of Accounts) = Very Small  
■ Better than the industry average; ■ Worse than the industry average

Total number of profiles defined to your system: 56.

This summary report presents the number of profiles, with the listed characteristics, as a percentage of the *total* number of profiles defined to your system. In general, longer bars highlight potential weaknesses in your security measures and should be investigated.

For more information and detail, refer to the relevant section in the *main body* of the report.

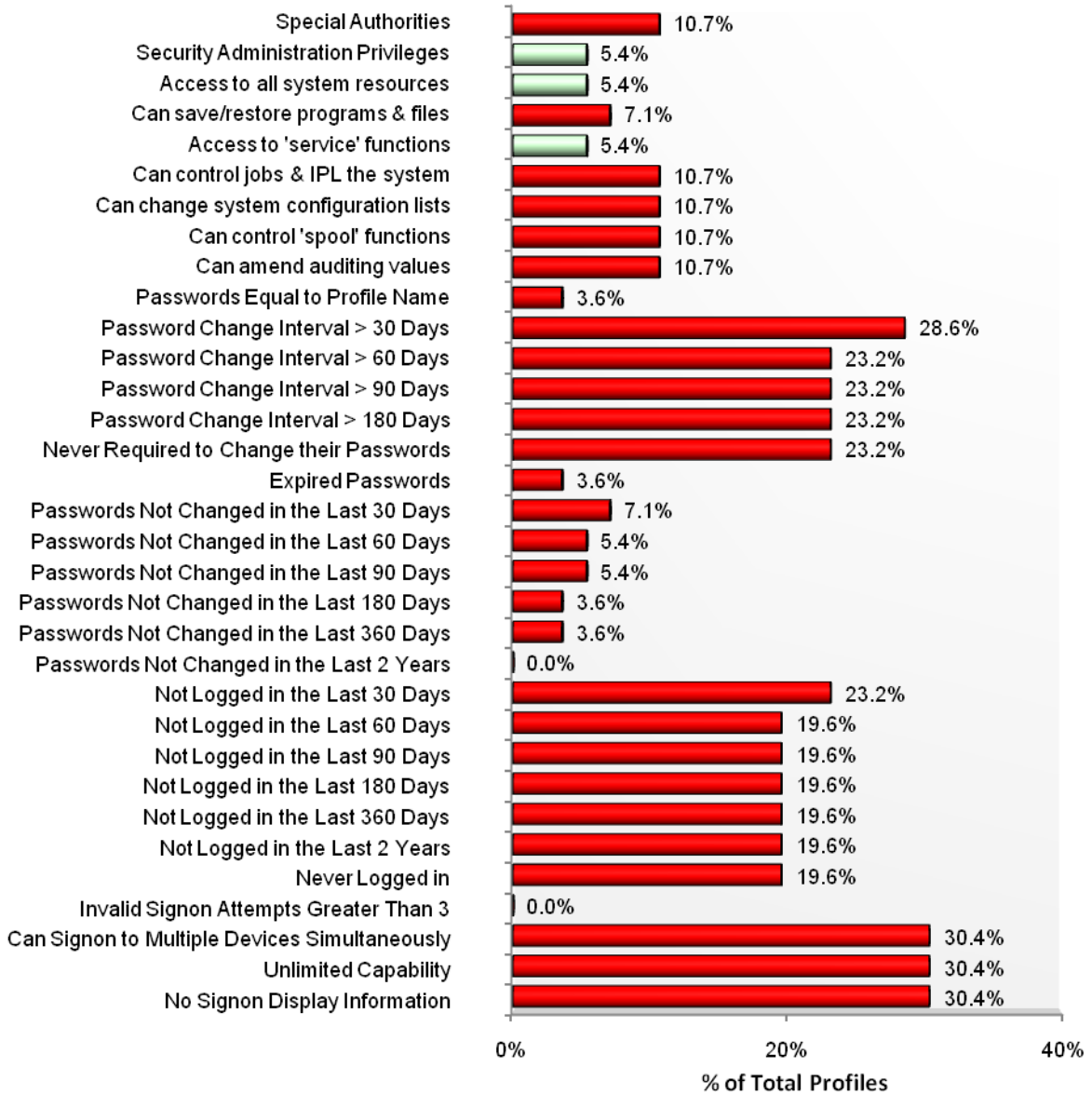
# Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

## Comparisons Against Industry Average and Leading Practice (continued)

### Summary of User Profiles (excluding disabled profiles)



This graph compares against the industry average using the following criteria:  
 Country = <All>; Industry Type = Communications; Machine Size (Nbr of Accounts) = Very Small  
■ Better than the industry average; ■ Worse than the industry average

Total number of profiles defined to your system: 56.

This summary report presents the number of *enabled* profiles (i.e. excluding those with a status of disabled or a password = \*NONE), with the listed characteristics, as a percentage of the *total* number of profiles defined to your system. In general, longer bars highlight potential weaknesses in your security measures.

For more information and detail, refer to the relevant section in the [main body](#) of the report.

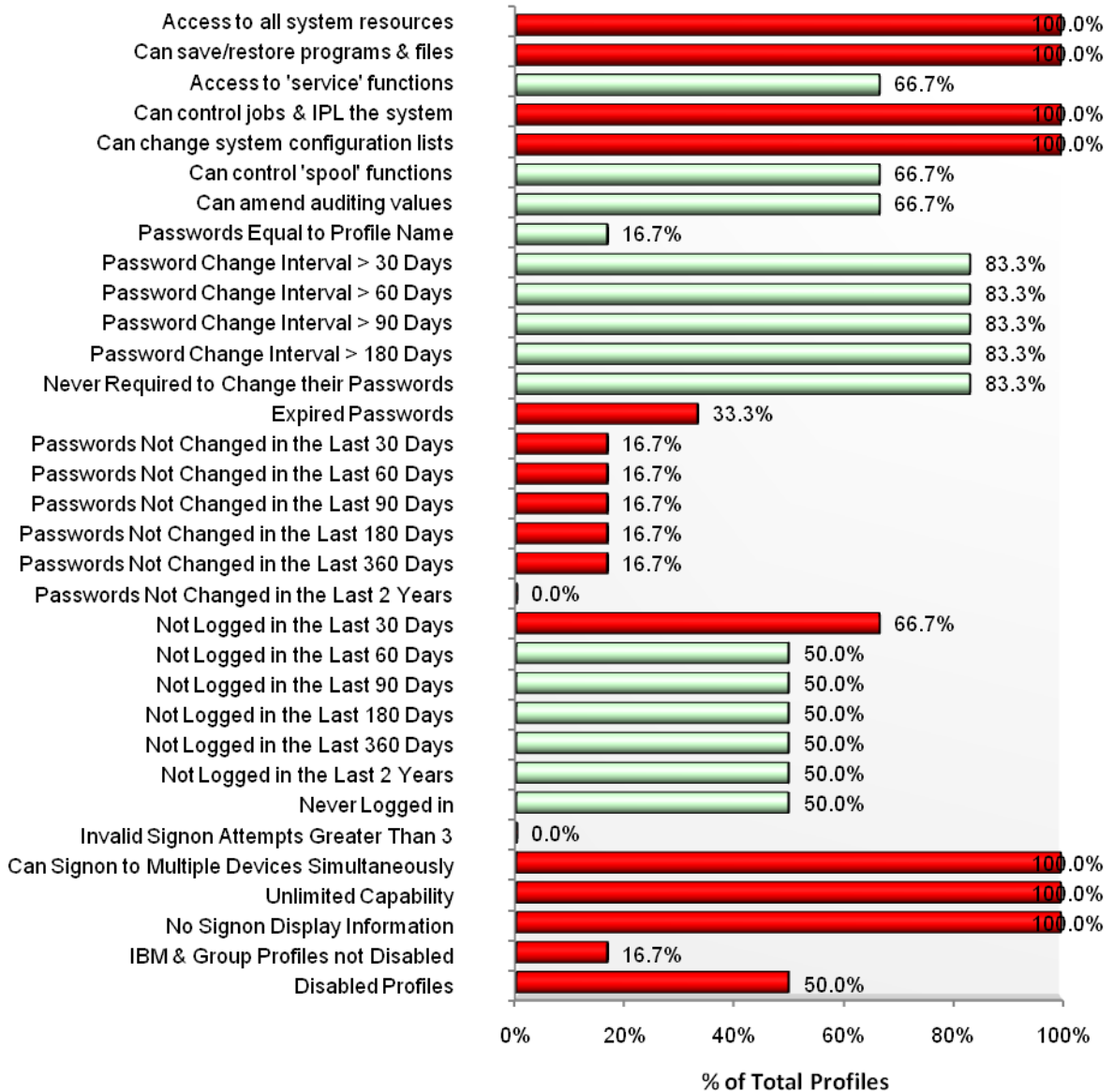
# Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

## Comparisons Against Industry Average and Leading Practice (continued)

### Summary of Administrator Profiles



This graph compares against the industry average using the following criteria:  
 Country = <All>; Industry Type = Communications; Machine Size (Nbr of Accounts) = Very Small  
■ Better than the industry average; ■ Worse than the industry average

Total number of profiles with administrative authorities (\*SECADM) defined to your system: 6.

This summary report presents the number of *administrator* profiles (i.e. profiles that have \*SECADM special authorities), with the listed characteristics, as a percentage of the *total* number of Administrator profiles defined to your system. In general, longer bars highlight potential weaknesses in your security measures and should be investigated.

For more information and detail, refer to the relevant section in the *main body* of the report.

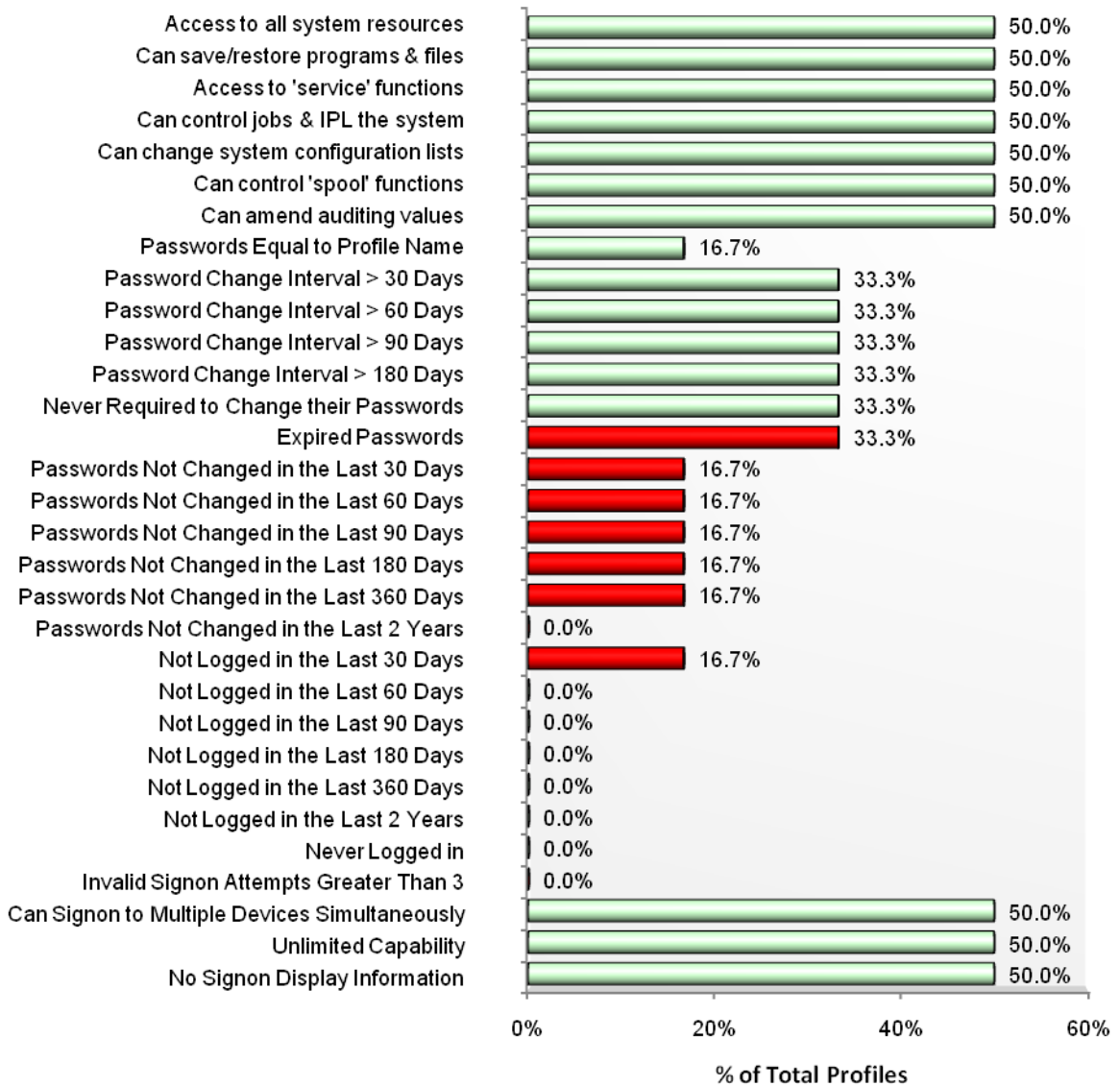
# Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

## Comparisons Against Industry Average and Leading Practice (continued)

### Summary of Administrator Profiles (excluding disabled profiles)



This graph compares against the industry average using the following criteria:  
 Country = <All>; Industry Type = Communications; Machine Size (Nbr of Accounts) = Very Small

█ Better than the industry average; 
 █ Worse than the industry average

Total number of profiles with administrative authorities (\*SECADM) defined to your system: 6.

This summary report presents the number of *enabled administrator* profiles (i.e. profiles that have \*SECADM special authorities, excluding those with a status of disabled or a password = \*NONE), with the listed characteristics, as a percentage of the *total* number of administrator profiles defined to your system. In general, longer bars highlight potential weaknesses in your security measures.

For more information and detail, refer to the relevant section in the [main body](#) of the report.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 1.2 Answers to Common Questions

The following charts are intended to provide quick answers to the most common questions regarding security of a system.

The diagrams highlight the relative numbers of objects with the listed attributes. The total population used to plot each chart is included in brackets ( ) after each chart title. Each section includes a link to more detailed information contained in other sections of this report.

### When were the user accounts created?

The charts show when user accounts were created on your system. Grouped by all accounts and accounts with administrative (\*SECADM) authority. Includes active and disabled accounts.

More information: [User Accounts Created in the Last 90 Days](#)

All Accounts (56)



SECADM Accounts (6)



### When were the user accounts changed?

The charts show when user accounts were last changed. Grouped by all accounts and accounts with administrative (\*SECADM) authority. Includes active and disabled accounts.

All Accounts (56)



SECADM Accounts (6)



## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

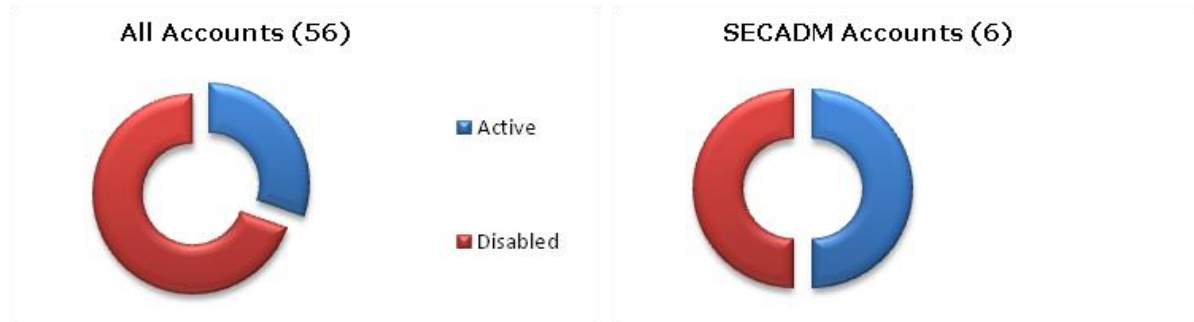
CONFIDENTIAL

### What is the status of the accounts?

The charts analyse user and group accounts by their status: active or disabled. An account may be disabled because its status has been set to disabled and / or its password has been set to \*NONE.

39 out of 56 accounts are disabled on this system.

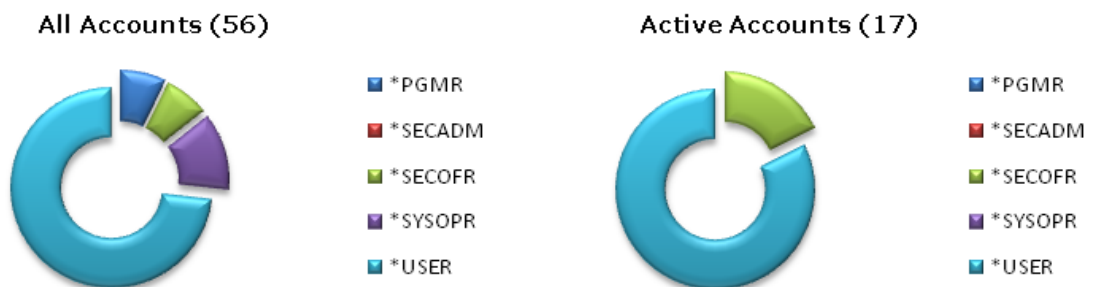
More information: [Disabled Profiles](#)



### What classes are assigned to user accounts?

The charts show which user classes have been assigned to the user / group accounts. Grouped by all accounts (active and disabled) and active (i.e. not disabled) accounts only.

More information: [User Profiles and Classes](#)



### How active are user accounts?

The charts indicate when accounts were last used to logon to the system. Grouped by all accounts and accounts with administrative (\*SECADM) authority. Excludes disabled accounts.

More information: [Last Logons, 30 Days and Older](#)



## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

### How frequently do users change their passwords?

The charts show when user login passwords were last changed. Grouped by all accounts and accounts with administrative (\*SECADM) authority. Excludes disabled accounts.

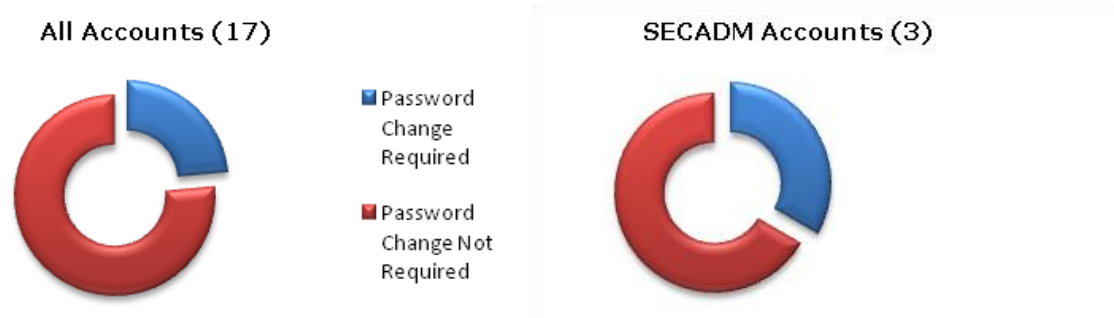
More information: [Passwords, 30 Days and Older](#)



### Are users forced to change their passwords?

The charts show the percentage of accounts with a password that is not required to be changed. Grouped by all accounts and accounts with administrative (\*SECADM) authority. Excludes disabled accounts.

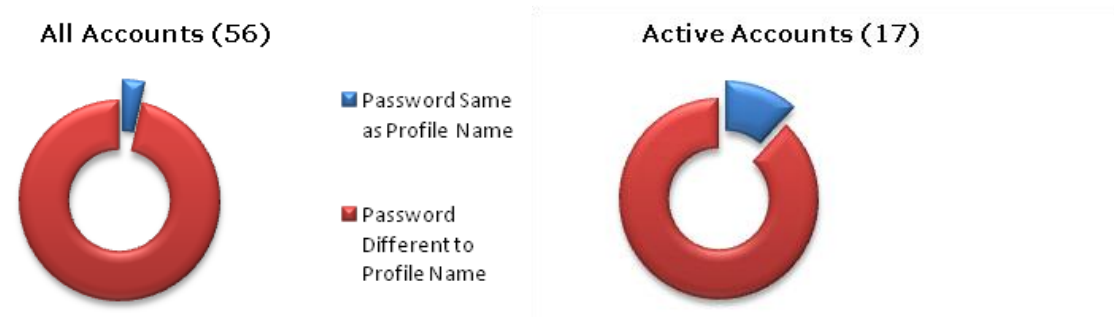
More information: [Password Change Intervals](#)



### Are there any accounts with a password equal to the account name?

The charts show the percentage of accounts with a password equal to the account name. Grouped by all accounts (active and disabled) and active (i.e. not disabled) accounts only.

More information: [Passwords Equal to Profile Name](#)



## Security Analysis: TESTBED AS400

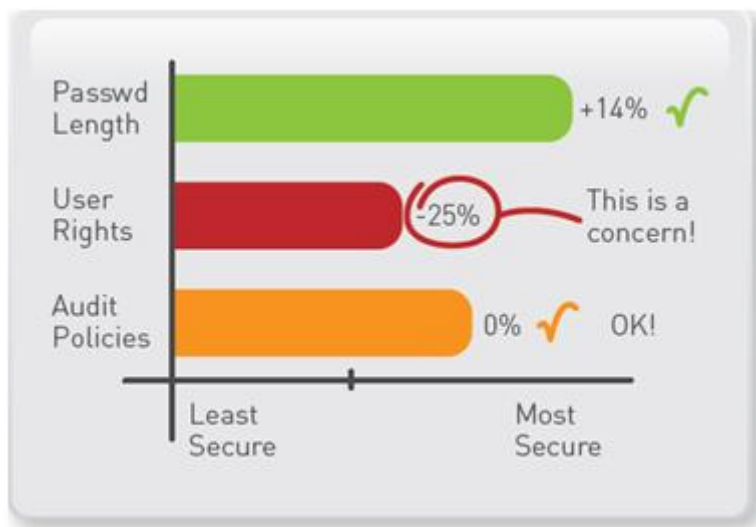
System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

### 1.3 Summary of Changes since the Previous Analysis

Need to quickly highlight changes in security controls since your previous review?

SekChek's latest time-comparison graphs are just the solution!



*Note: The above graph is provided for illustrative purposes only.*

A collection of easy-to-read reports in a very familiar format provides you with visual indicators of:

- Whether security has improved, weakened, or remained about the same since your previous analysis
- The effectiveness of your measures to strengthen controls
- Whether risk is increasing or decreasing
- The degree of change, both positive and negative

The applications are endless. Some of the practical benefits are:

- Time savings. Reduced time spent poring over volumes of unconnected information
- Objectivity. The results are guaranteed to be the same regardless of who performs the review
- Compliance with legislation. Easier monitoring for compliance with statutory requirements imposed by SOX, HIPAA and other legislative changes relating to corporate governance
- More powerful justifications. The ability to present more convincing arguments to senior, non-technical management who do not have the time, or the inclination, to understand masses of technical detail

Interested?

Contact us at [inbox@sekchek.com](mailto:inbox@sekchek.com) to find out how to get started.

## Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

### 2. System Values

This report lists the system-wide security defaults (System Values) defined for your system and compares them with Leading Practice values.

System Value	Current Value	Leading Practice
<a href="#">QALWOBJRST</a>	*ALL	*NONE
<a href="#">QALWUSRDMN</a>	*ALL	*ALL
<a href="#">QATNPGM</a>	*ASSIST	*ASSIST or *NONE
<a href="#">QAUDCTL</a>	*NONE	*AUDLVL
<a href="#">QAUDENDACN</a>	*NOTIFY	*NOTIFY
<a href="#">QAUDFRCLVL</a>	*SYS	*SYS
<a href="#">QAUDLVL</a>	*NONE	*AUTFAIL *CREATE *DELETE *SECURITY *SERVICE *SAVRST
<a href="#">QAUDLVL2</a>	*NONE	see <a href="#">QAUDLVL</a> (refer notes below).
<a href="#">QAUTOVRT</a>	*NOMAX	0
<a href="#">QCRTAUT</a>	*CHANGE	*CHANGE
<a href="#">QCRTOBJAUD</a>	*NONE	*NONE
<a href="#">QDEVRCYACN</a>	*DSCMSG	*DSCMSG
<a href="#">QDSCJOBIV</a>	240	120 or less
<a href="#">QDSPSGNINF</a>	0	1
<a href="#">QINACTIV</a>	*NONE	20 or less.
<a href="#">QINACTMSGQ</a>	*ENDJOB	*DSCJOB or *ENDJOB
<a href="#">QLMTDEVSSN</a>	0	1
<a href="#">QLMTSECOFR</a>	0	1
<a href="#">QMAXSGNACN</a>	3	3
<a href="#">QMAXSIGN</a>	6	3 or less
<a href="#">QPWDCHGBLK</a>	*NONE	V6R1 onwards.
<a href="#">QPWDEXPITV</a>	*NOMAX	30; maximum of 60.
<a href="#">QPWDEXPWRN</a>	7	7 (V6R1 and later)
<a href="#">QPWDLMTAJC</a>	0	1
<a href="#">QPWDLMTCHR</a>	*NONE	*NONE
<a href="#">QPWDLMTREP</a>	0	1; V3R1 and later - '2'.
<a href="#">QPWDLVL</a>	0	3 (refer notes below).
<a href="#">QPWDMAXLEN</a>	8	12 or greater (see QPWDLVL also).
<a href="#">QPWDMINLEN</a>	6	8 or greater.
<a href="#">QPWDPOSDIF</a>	0	1

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

System Value	Current Value	Leading Practice
<i>QPWDRQDDGT</i>	0	1
<i>QPWDRQDDIF</i>	0	Prior to V3R1 - '1' V3R1 and later - less than '5'.
<i>QPWDRULES</i>	*PWDSYSVAL	V6R1 and later
<i>QPWDVLDPGM</i>	*NONE	*NONE
<i>QRETSVRSEC</i>	0	0
<i>QRMTSIGN</i>	*FRCSIGNON	*FRCSIGNON
<i>QSECURITY</i>	40	40 or greater.
<i>QSHRMEMCTL</i>	1	0

### Notes

**Leading Practice** is the standard adopted by the top 10 to 20 percent of organisations.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

### Functions of SYSVALs and Potential Exposures

#### QALWOBJRST

Determines whether you will allow objects to be restored to your system.

- \*ALL = Allow objects to be restored.
- \*ALWPGMADP = Allow applications that adopt the owner's authority to be restored.
- \*NONE = Do not allow objects to be restored to your system.

#### Exposure

If not adequately controlled, objects could be accidentally restored to your system.

#### QALWUSRDMN

Specifies which libraries are allowed to contain user domain objects of type \*USRSPC (user space), \*USRIDX (index) and \*USRQ (queue). The restriction does not apply to user domain objects of type \*PGM, \*SRVPGM and \*SQLPKG.

- \*ALL = User domain object types \*USRSPC, \*USRIDX and \*USRQ are allowed in all libraries.
- Library name list* = List of libraries that can contain these user domain object types.

If your system has high security requirements, consider restricting user domain objects to library QTEMP and a small number of libraries only.

#### Exposure

Not significant unless your security requirements are very high. The system cannot audit the movement of information to and from user domain objects.

#### QATNPGM

This program is called when the user presses the Attention key. *Can be overridden in the User Profile.*

#### Exposure

If this is a user-developed program, it could undermine security in several ways, depending on its function. For example, it could provide access to the command line for users normally limited with "Limited capability = \*YES".

#### QAUDCTL

Determines whether auditing is performed for the [QAUDLVL](#) system value and objects or users (defined with the CHGOBJAUD and CHGUSRAUD commands).

- \*NONE = No auditing is performed.
- \*AUDLVL = Auditing is performed for functions selected on the QAUDLVL system value and on the AUDLVL parameter on specific user profiles.
- \*OBJAUD = Auditing is performed for objects selected via the CHGOBJAUD and CHGDLOAUD commands.
- \*NOQTEMP = Auditing is *not* performed for most actions if the object is in library QTEMP. The QTEMP library is used to store temporary objects for jobs.

#### Exposure

If set to \*NONE, it will not be possible to monitor security violations and detect unauthorised or undesirable activity on the system.

#### QAUDENDACN

Determines the action taken by the system if auditing is active and is unable to write entries to the audit journal.

- \*NOTIFY = Message is sent to the QSYSOPR and QSYSMSG message queues, until auditing is restarted.
- \*PWRDWNSYS = The system powers down immediately.

#### Exposure

Not significant. Use \*PWRDWNSYS only if your environment has very high security needs.

#### QAUDFRCLVL

Determines how often new audit journal entries are forced from memory to auxiliary storage.

- \*SYS = The system decides based on internal performance.
- Number of records = Number of records that can accumulate in memory before being written to storage.

#### Exposure

Not significant. If it is critical that no audit records are lost if the system ends abnormally, specify '1'.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

### QAUDLVL

Determines the events that are logged to the audit trail. Operates in conjunction with the [QAUDCTL](#) system value. QAUDLVL allows up to 16 auditing values to be defined.

*NONE	=	No audit logging
*AUDLVL2	=	See note below
*AUTFAIL	=	Log access failures
*CREATE	=	Log created objects
*DELETE	=	Log deletion of objects
*JOBDATA	=	Log job start, stop data etc.
*NETBAS	=	Log network base functions (V5R3 & later)
*NETCLU	=	Log cluster and cluster resource group operations (V5R3 & later)
*NETCMN	=	Log networking and communications functions (V5R3 & later)
*NETFAIL	=	Log network failures (V5R3 & later)
*NETSCK	=	Log socket tasks (V5R3 & later)
*OBJMGT	=	Log moves & renames
*OFCSRVR	=	Log OfficeVision/400 tasks
*OPTICAL	=	Log all optical functions (V5R3 & later)
*PGMADP	=	Log program adoptions
*PGMFAIL	=	Log integrity violations
*PRTDATA	=	Log printing functions
*SAVRST	=	Log restore operations
*SECCFG	=	Log security configuration (V5R3 & later)
*SECDIRSRV	=	Log changes or updates when doing directory service functions (V5R3 & later)
*SECIPC	=	Log changes to interprocess communications (V5R3 & later)
*SECNAS	=	Log network authentication service actions (V5R3 & later)
*SECURN	=	Log security run time functions (V5R3 & later)
*SECCKD	=	Log socket descriptors (V5R3 & later)
*SECURITY	=	Log changes to security
*SECVFY	=	Log use of verification functions (V5R3 & later)
*SECVLDL	=	Log changes to validation list objects (V5R3 & later)
*SERVICE	=	Log use of system service tools
*SPLFDATA	=	Log spooled file functions
*SYSMGT	=	Log system management tasks

#### Note:

If \*AUDLVL2 is specified in the QAUDLVL system value, the effective auditing values are a combination of the values specified in the QAUDLVL and [QAUDLVL2](#) system values. If the \*AUDLVL2 is not specified in the QAUDLVL system value, any auditing values specified in the [QAUDLVL2](#) system value are ignored by the system.

#### Exposure

If events are not logged, it will not be possible to monitor security violations and undesirable activity on the system.

### QAUDLVL2

An extension to [QAUDLVL](#). If \*AUDLVL2 is specified as one of the values in the [QAUDLVL](#) system value, the system will look for additional auditing values in the QAUDLVL2 system value. QAUDLVL2 allows for an additional 99 auditing values to be selected. This system value was introduced in V5R3M0.

Refer to the table listed in [QAUDLVL](#) for possible audit values for this system value.

#### Exposure

Refer to [QAUDLVL](#).

### QAUTOVRT

Determines the number of virtual device descriptions that the system will automatically create if no device is available for use.

#### Exposure

If set to a value greater than '0', an unsuccessful intruder using TELNET can reconnect, attach to a newly-created virtual device, and continue trying to access the system.

### QCRTAUT

Determines the public authority for a newly created object if the following conditions are met:

- Create authority (CRTAUT) for the new object's library is set to \*SYSVAL

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

- The new object is created with public authority (AUT) of \*LIBCRTAUT.
- \*CHANGE = Anyone can change.  
\*USE = Anyone can view, but not change.  
\*ALL = Anyone can perform any function.  
\*EXCLUDE = Not allowed to use.

### **Exposure**

Not significant. However, if the value is changed from the default of \*CHANGE, this could cause problems on your system because several IBM-supplied libraries, such as QSYS, have a CRTAUT value of \*SYSVAL.

### **QCRTOBJAUT**

Determines the auditing value for a new object, if the auditing default for the new object's library is set to \*SYSVAL.

- \*NONE = No auditing is done for the object.  
\*USRPRF = Auditing is based on the value in the profile accessing the object.  
\*CHANGE = An audit record is written whenever the object is changed.  
\*ALL = An audit record is written for any action that affects the contents of the object.

### **Exposure**

Not significant. The value you select depends on the auditing needs of your organisation.

### **QDEVRCYACN**

System action when an I/O error occurs for an interactive job's workstation.

- \*DSCMSG = Disconnects the job & displays an error message when the users signs on again.  
\*DSCENDRQS = Disconnects the job & performs a cancel request function (to return control of the job back to the last request level) when the user signs on again.  
\*ENDJOB = Ends the job. A job log is produced.  
\*ENDJOBNOLOG = Ends the job. A job log is not produced.  
\*MSG = Displays a message only. The application program performs error recovery.

### **Exposure**

If set to \*MSG, there is a risk of the device disconnecting and another device connecting using the same address. This would present an obvious security exposure.

### **QDSCJOBTV**

Determines how long the system waits (in minutes) before taking action on a disconnected job.

### **Exposure**

If set too high it increases the risk of intruders gaining access to the system via active and disconnected workstations.

### **QDSPSGNINF**

Displays information about previous sign-on activity each time user signs on. *Can be overridden in the User Profile.*

- 0 = Do not display.  
1 = Display.

### **Exposure**

If previous sign-on activity is not displayed, successful intruders could use user profiles without detection by the owners.

### **QINACTIV**

Determines how long the system waits (in minutes) before taking action (defined in QINACTMSGQ) when a job is inactive.

### **Exposure**

If set too high it increases the risk of intruders gaining access to the system via active and unattended workstations.

### **QINACTMSGQ**

What the system does when the QINACTIV value is reached.

- \*NONE = No action.  
\*DSCJOB = Job continues to run, but the display is signed off.  
When the same user signs-on again, the job continues where it left off.  
\*ENDJOB = Job is ended.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

### **Exposure**

If set to \*NONE, it increases the risk of intruders gaining access to the system via active and unattended workstations. Note however, that a value of \*DSCJOB can result in loss of information when certain PC/Support jobs are running.

### **QLMTDEVSSN**

Determines whether a user is allowed to sign-on to more than one workstation at the same time. *Can be overridden in the User Profile.*

0 = Not Limited to a specific number of device sessions.

1 = Limited to a single device session.

2 - 9 = Limited to the specified number of device sessions.

### **Exposure**

If simultaneous sign-ons with the same user profile are allowed, it increases the risk of an intruder:

- Gaining access via active and unattended workstations;
- Using a user profile without the owner's knowledge.

### **QLMTSECOFR**

Determines whether users with \*ALLOBJ or \*SERVICE special authority are allowed to sign-on at any workstation.

0 = Allowed.

1 = Not allowed.

These users must be explicitly allowed to sign-on at specific workstations (by granting \*CHANGE authority to the device).

### **Exposure**

If user profiles with these powerful special authorities are allowed to sign-on from any device, it increases the opportunity for intruders to guess their passwords.

### **QMAXSIGNACN**

What the system does when the QMAXSIGN value is reached.

1 = Device (only) disabled.

2 = User profile (only) disabled

3 = User profile and device disabled

### **Exposure**

If set to '1' or '2', it increases the risk of an intruder being able to guess passwords for user profiles.

### **QMAXSIGN**

Maximum invalid sign-on attempts (wrong password for user profile).

### **Exposure**

If set too high, it increases the risk of an intruder being able to guess passwords for user profiles.

### **QPWDCHGBLK**

The Block Password Change (QPWDCHGBLK) system value specifies the time period during which a password is blocked from being changed after the prior successful password change operation.

\*NONE = The password can be changed at any time.

1 – 99 = A password cannot be changed within the specified number of hours after the prior successful password changed operation.

### **Exposure**

If set, a user cannot change her password *immediately* if she suspects it is known by someone else.

### **QPWDEXPITV**

Password expiry interval in days. *Can be overridden in the User Profile.*

### **Exposure**

If set too high, successful intruders could continue to use a user profile for a long period before its password is next changed by the owner. Also, a long period between password changes increases the risk of passwords becoming common knowledge amongst a group of people.

### **QPWDEXPWRN**

The number of days prior to password expiration when the password expiration warning message is displayed.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

### **Exposure**

None.

### **QPWDLMTAJC**

Determines whether adjacent numbers are allowed in passwords.

0 = Allowed.

1 = Not allowed.

### **Exposure**

If allowed, users could select trivial passwords, such as '123456'. This would make it easier for an intruder to guess a password and gain access to the system.

### **QPWDLMTCHR**

Determines what characters are not allowed in passwords.

Stored in message ID SEC1DAB in message file QSECLIB/QSECMSGF (default is 'AEIOU@ \$#')

### **Exposure**

Dependent on the settings for other password controls, users could select easy-to-guess trivial passwords, such as 'JANUARY' or 'PASSWORD'.

### **QPWDLMTREP**

Determines whether the same character is allowed to appear more than once in a password.

0 = Allowed.

1 = Not allowed.

2 = Not allowed consecutively. (V3R1 onwards)

### **Exposure**

If allowed, users could select easy-to-guess trivial passwords, such as 'AAAAAA'.

### **QPWDLVL**

This System Value was introduced in V5R1M0.

The QPWDLVL System Value allows you to implement stronger controls over user passwords through the use of password levels. Password levels control properties such as, password length and complexity, and whether NetServer passwords are retained or removed from a system.

NetServer passwords enable Windows clients to access shared directory paths and output queues residing on OS/400 systems and allow the AS/400 system to communicate with the AS/400 Client Support for Windows Network Neighborhood.

There are 4 password levels that can be assigned to the QPWDLVL System Value:

#### **Password Level 0 (Short passwords using a limited character set)**

Supports user passwords from 1-10 characters and retains NetServer passwords.

This setting allows your system to communicate with other systems on the network that are running with either an operating system release less than V5R1M0 or a QPWDLVL value of 0 or 1.

This is the default setting.

#### **Password Level 1 (Short passwords using a limited character set. Disable AS/400 NetServer on Windows 95/98/ME)**

Supports user passwords from 1-10 characters, but removes NetServer passwords.

Eliminating NetServer passwords from a system that does not need to communicate with the AS/400 Client Support for Windows Network Neighborhood increases the overall security.

This setting allows your system to communicate with other systems on the network that are running with either an operating system release less than V5R1M0 or a QPWDLVL value of 0 or 1.

#### **Password Level 2 (Long passwords using an unlimited character set)**

Supports user passwords from 1-128 characters and allows you to communicate with AS/400 NetServer as long as your password is 1-14 characters in length.

QPWDLVL 2 cannot be used if your system communicates with other systems that are running with either an operating system release less than V5R1M0 or a QPWDLVL value of 0 or 1.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

QPWDLVL 2 is viewed as a compatibility level that allows you to move back to QPWDLVL 0 or 1 as long as your password meets the requirements of passwords that are valid under these password levels.

## **Password Level 3 (Long passwords using an unlimited character set. Disable AS/400 NetServer on Windows 95/98/ME)**

Supports user passwords from 1-128 characters and removes passwords that are used at QPWDLVL 0 or 1.

QPWDLVL 3 cannot be used if your system communicates with other systems that are running with either an operating system release less than V5R1M0 or a QPWDLVL value of 0 or 1.

QPWDLVL 3 cannot be used if your system communicates with AS/400 NetServer or any other system that limits the length of passwords from 1-10 characters.

Regardless of the password level, the system automatically creates passwords compatible with QPWDLVL 2 and 3 whenever a password is changed or a user logs on to the system.

Passwords for password levels 0 and 1 have the following characteristics:

- Passwords may be from 1-10 characters in length;
- Passwords are not case sensitive;
- Passwords can contain only alpha-numeric characters or the following special characters \$, @, # and *underscore*;
- Passwords may not contain blank characters.

Passwords for password levels 2 and 3 have the following characteristics:

- Passwords may be from 1-128 characters in length;
- Passwords are case sensitive;
- Passwords may contain any character including blank characters;
- Passwords may not start with the '\*' character;
- Trailing blanks are removed from the password;
- Passwords with only blank characters will be rejected by the system.

### **QPWDMAXLEN**

Maximum password length.

#### **Exposure**

If too short, it makes it easier for an intruder to guess passwords and gain access to the system.

### **QPWDMINLEN**

Minimum password length.

#### **Exposure**

If too short, it makes it easier for an intruder to guess passwords and gain access to the system.

### **QPWDPOSDIF**

Determines whether every position in a new password must differ from the same position in the previous password.

0 = Need not differ.

1 = Must differ.

#### **Exposure**

Dependent on the value set for other password controls, if not set it increases the risk of an intruder being able to guess passwords for user profiles.

### **QPWDRQDDGT**

Determines whether passwords must contain at least one number.

0 = Number not required.

1 = Password must contain at least one number.

#### **Exposure**

If numbers are not required in passwords, users can select trivial passwords such as "JANUARY" or "MONDAY". Depending on the value set for other password controls, it increases the risk of an intruder guessing passwords for user profiles.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

### QPWDRQDDIF

Controls duplicate passwords. Determines whether the new password must be different to the previous 32 passwords.

Prior to V3R1:

0 = Can be the same.

1 = Must be different to any of the previous 32 passwords.

V3R1 onwards:

0 = Can be the same as old passwords

5 = Cannot be the same as the last 10 passwords

1 = Cannot be the same as the last 32 passwords

6 = Cannot be the same as the last 8 passwords

2 = Cannot be the same as the last 24 passwords

7 = Cannot be the same as the last 6 passwords

3 = Cannot be the same as the last 18 passwords

8 = Cannot be the same as the last 4 passwords

4 = Cannot be the same as the last 12 passwords

### Exposure

Dependent on the value set for other password controls, if not set it increases the risk of an intruder being able to guess passwords for user profiles.

### QPWDRULES

The Password Rules (QPWDRULES) system value specifies the rules used to check whether a password is formed correctly. You can specify more than one value for the QPWDRULES system value, unless you specify \*PWDSYSVAL.

**\*PWDSYSVAL** = This value specifies that the QPWDRULES system value is ignored and the other password system values are used to check whether a password is formed correctly. These other password system values include QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF, and QPWDQDDGT.

**Note:** If any value other than \*PWDSYSVAL is specified for QPWDRULES, the QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF, and QPWDQDDGT system values are ignored when a new password is checked to see if it is formed correctly. In addition, any attempt to change these system values will be rejected as long as the QPWDRULES system value contains a value other than \*PWDSYSVAL.

**\*CHRLMTAJC** = The value specifies that a password cannot contain 2 or more occurrences of the same character that are positioned adjacent to each other. This value performs the same function as specifying a value of 2 for the QPWDLMTREP system value. If the \*CHRLMTREP value was specified, this value cannot be specified.

**\*CHRLMTREP** = The value specifies that a password cannot contain 2 or more occurrences of the same character. This value performs the same function as specifying a value of 1 for the QPWDLMTREP system value. If the \*CHRLMTAJC value was specified, this value cannot be specified.

**\*DGLMTAJC** = The value specifies that a password cannot contain 2 or more adjacent digit characters.

**\*DGLMTFST** = The value specifies that the first character of a password cannot be a digit character. If \*LTRLMTFST and \*SPCCHRLMTFST values were specified, this value cannot be specified. If the system is operating at password level 0 or 1, the system functions like the \*DGLMTFST value is specified.

**\*DGLMTLST** = The value specifies that the last character of the password cannot be a digit character. If \*LTRLMTLST and \*SPCCHRLMTLST values were specified, this value cannot be specified.

**\*DGTMAXn** = The value specifies the maximum number of digit characters that can occur in the password. The **n** is a number from 0 to 9. Only one \*DGTMAXn value can be specified. If a \*DGTMINn value is also specified, the **n** value specified for \*DGTMAXn must be greater than or equal to the **n** value specified for \*DGTMINn.

**\*DGTMINn** = The value specifies the minimum number of digit characters that must occur in the password. The **n** is a number from 0 to 9.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Only one \*DGTMINn value can be specified. If a \*DGTMAXn value is also specified, the n value specified for \*DGTMAXn must be greater than or equal to the n value specified for \*DGTMINn.

- \*LMPRFNAME** = The uppercase password value cannot contain the complete user profile name in consecutive positions.
- \*LMTSAMPOS** = The same character cannot be used in a position corresponding to the same position in the previous password. This value performs the same function as the QPWDPOSDIF system value.
- When the password is set by the Change User Profile (CHGUSRPRF) or Create User Profile (CRTUSRPRF) command, this password rule cannot be checked because the previous password value is not supplied.
- \*LTRLMTAJC** = The value specifies a password cannot contain 2 or more adjacent letter characters.
- \*LTRLMTFST** = The value specifies the first character of the password cannot be a letter character. If \*DGTLMTFST and \*SPCCHRLMTFST values were specified, this value cannot be specified. If the system is operating with a QPWDVLV value of 0 or 1, \*LTRLMTFST and \*SPCCHRLMTFST cannot both be specified.
- \*LTRLMTLST** = The value specifies the last character of the password cannot be a letter character. If \*DGTLMTLST and \*SPCCHRLMTLST values were specified, this value cannot be specified.
- \*LTRMAXn** = The value specifies the maximum number of letter characters that can occur in the password. The n is a number from 0 to 9.
- Only one \*LTRMAXn value can be specified. If a \*LTRMINn value is also specified, the n value specified for \*LTRMAXn must be greater than or equal to the n value specified for \*LTRMINn.
- If a \*MIXCASEn value is also specified, the n value specified for \*LTRMAXn must be greater than or equal to 2 times the n value specified for \*MIXCASEn.
- \*LTRMINn** = The value specifies the minimum number of letter characters that must occur in the password. The n is a number from 0 to 9.
- Only one \*LTRMINn value can be specified. If a \*LTRMAXn value was specified, the n value specified for \*LTRMAXn must be greater than or equal to the n value specified for \*LTRMINn.
- \*MAXLENnnn** = The value specifies the maximum number of characters in a password. The nnn is a number from 1 to 128 (without leading zeros). This value performs the same function as the QPWDMAXLEN system value.
- If the system is operating at QPWDVLV 0 or 1, the valid range is from 1 to 10. If the system is operating at QPWDVLV 2 or 3, the valid range is from 1 to 128.
- The nnn value specified must be large enough to accommodate all \*MIXCASEn, \*DGTMAXn, \*LTRMAXn, \*SPCCHRMAXn, first and last character restrictions, and non-adjacent character requirements.
- If \*MINLENnnn is also specified, the nnn value specified for \*MAXLENnnn must be greater than or equal to the nnn value specified for \*MINLENnnn.
- If no \*MAXLENnnn value is specified, a value of \*MAXLEN10 is assumed if the system is operating with a QPWDVLV value of 0 or 1 or a value of \*MAXLEN128 is assumed if the system is operating with a QPWDVLV value of 2 or 3.
- \*MINLENnnn** = The value specifies the minimum number of characters in a password. The nnn is a number from 1 to 128 (without leading zeros).
- If the system is operating at QPWDVLV 0 or 1, the valid range is from 1 to 10. If the system is operating at QPWDVLV 2 or 3, the valid range is from 1 to 128.
- If \*MAXLENnnn is also specified, the nnn value specified for \*MAXLENnnn must be greater

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

than or equal to the nnn value specified for \*MINLENnnn.

If no \*MINLENnnn value is specified, a value of \*MINLEN1 is assumed.

**\*MIXCASEn** = The value specifies a password must contain at least n uppercase and n lowercase letters. The n is a number from 0 to 9. This value is rejected if the system is operating with a QPVDLVL value of 0 or 1 because passwords are required to be uppercase.

Only one \*MIXCASEn value can be specified.

If a \*LTRMAXn value was specified, the n value specified for \*LTRMAXn must be greater than or equal to two times the n value specified for \*MIXCASEn.

**\*REQANY3** = The value specifies a password must contain characters from at least three of the following four types of characters.

- Uppercase letters
- Lowercase letters
- Digits
- Special characters

When the system is operating with a QPVDLVL of 0 or 1, \*REQANY3 has the same effect as if \*DGTMIN1, \*LTRMIN1, and \*SPCCHRMIN1 were all specified.

**\*SPCCHRLMTAJC** = The value specifies a password cannot contain 2 or more adjacent (consecutive) special characters. A character is considered as a special character if its equivalent unicode character has the property of not being a letter nor a digit.

**\*SPCCHRLMTFST** = The value specifies the first character of the password cannot be a special character. A character is considered as a special character if its equivalent unicode character has the property of not being a letter nor a digit.

If \*DGTLMTFST and \*LTRLMTFST values were specified, this value cannot be specified. If the system is operating with a QPVDLVL value of 0 or 1, \*LTRLMTFST and \*SPCCHRLMTFST cannot both be specified.

**\*SPCCHRLMTLST** = The value specifies the last character of the password cannot be a special character. A character is considered as a special character if its equivalent unicode character has the property of not being a letter nor a digit.

If \*DGTMLTLST and \*LTRLMLTLST values were specified, this value cannot be specified.

**\*SPCCHRMAXn** = The value specifies the maximum number of special characters that may occur in the password. The n is a number from 0 to 9. A character is considered as a special character if its equivalent unicode character has the property of not being a letter nor a digit.

Only one \*SPCCHRMAXn value can be specified. If a \*SPCCHRMINn value was specified, the n value specified for \*SPCCHRMAXn must be greater than or equal to the n value specified for \*SPCCHRMINn.

**\*SPCCHRMINn** = The value specifies the minimum number of special characters that must occur in the password. The n is a number from 0 to 9. A character is considered as a special character if its equivalent unicode character has the property of not being a letter nor a digit.

Only one \*SPCCHRMINn value can be specified. If a \*SPCCHRMAXn value was specified, the n value specified for \*SPCCHRMAXn must be greater than or equal to the n value specified for \*SPCCHRMINn.

### QPVDVLDPGM

Determines whether a special exit program is called to validate new passwords.

\*NONE = Not used.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## **Exposure**

No significant exposure if not used. However, such an exit could prevent users from selecting trivial passwords, such as months of the year, days of the week etc.

## **QRETSVRSEC**

The Retain Server Security (QRETSVRSEC) system value determines whether decryptable authentication information associated with user profiles or validation list (\*VLDL) entries can be retained on the host system. This does not include the iSeries user profile password.

The encrypted data field of a validation list entry is typically used to store authentication information. Applications specify whether to store the encrypted data in a decryptable or non-decryptable form. If the applications choose a decryptable form and the QRETSVRSEC value is changed from 1 to 0, the encrypted data field information is removed from the entry. If the encrypted data field of a validation list entry is stored in a non-decryptable form, it is not affected by the QRETSVRSEC system value.

0 = Server security data is removed (not retained) on the host system.

1 = Server security data is retained on the host system.

## **Exposure**

If set (Server security data is retained), the risk of unauthorised access to sensitive authentication information is increased.

## **QRMTSIGN**

Determines how the system handles a remote sign-on attempt.

\*FRCSIGNON = Normal sign-on required. System always checks for a valid user profile and password.

\*SAMEPRF = Password is not checked. Source and target user profiles are checked to ensure they are the same.

\*REJECT = Remote sign-on is not allowed.

\*VERIFY = System always checks for a valid user profile and password. Normal sign-on required unless SECURELOC=\*YES (on APPC device description on target system), in which case an interactive job starts with same user profile name as the profile on the source system.

## **Exposure**

If not set to \*FRCSIGNON or \*REJECT, the risk of unauthorised remote sign-ons is increased.

## **QSECURITY**

Determines the overall security mode.

10 = No password or resource security.

20 = Password checking, no resource security.

30 = Password checking and resource security.

40 = Password checking, resource security and integrity protection for the OS.

50 = Password checking, resource security and enhanced integrity protection. (e.g. validates parameters for interfaces to the OS and restricts message handling between system and user state programs)

## **Exposure**

If set to a value of '10' or '20', you have insufficient control over access to system resources and objects and your system is very exposed.

## **QSHRMEMCTL**

The Share Memory Control (QSHRMEMCTL) system value defines which users are allowed to use shared memory or mapped memory that has write capability.

0 = Users cannot use shared memory, or use mapped memory that has write capability.

This value means that users cannot use shared-memory APIs (for example, shmat() — Shared Memory Attach API), and cannot use mapped memory objects that have write capability (for example, mmap() — Memory Map a File API provides this function).

1 = Users can use shared memory or mapped memory that has write capability.

This value means that users can use shared-memory APIs (for example, shmat() — Shared Memory Attach API), and can use mapped memory objects that have write capability (for example, mmap() — Memory Map a File API provides this function).

## **Exposure**

For environments with higher security requirements, a value of 1 (Users can use shared memory or mapped memory that has write capability) might pose a potential risk to your system and assets because different users can add, change and delete entries in the shared memory or stream file.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

### Risk Rating

---

Medium to High. (dependent on the System Value involved)

### Recommended Action

---

Installation standards should be amended to bring them in-line with the recommended values outlined in the table above. System Values should be brought in-line with the installation standards.

Although the combined effect of OS/400's password control features is to make it extremely difficult for potential intruders to guess passwords (even via 'dictionary attacks'), it also has the effect of making it more difficult for users to select acceptable passwords.

As such, you should consider providing users with a list of the criteria, examples of valid and invalid passwords, and suggestions for thinking of a good password.

Some general guidelines for selecting passwords are:

- Don't use your user profile name, first or last name.
- Don't use other information easily obtained about you, such as telephone number, car registration number, date of birth etc.
- Don't use a password less than 5 characters.
- Don't use a word contained in a dictionary.
- Do use a password in mixed-case.
- Do use a password with alpha and numeric or special characters.

Some examples of difficult-to-guess, yet easy-to-remember passwords are:

- dog;Bone
- book+cup
- 5four3
- Threwthru
- card-post
- 1+2=four

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 3. User Profiles and Classes

### Section Summary

There are a total of 56 profiles defined on your system:

- 7.1% (4) are \*PGMR profiles
- 0.0% (0) are \*SECADM profiles
- 7.1% (4) are \*SECOFR profiles
- 12.5% (7) are \*SYSOPR profiles
- 73.2% (41) are \*USER profiles

### Section Detail

User Class	Profile Name	Group Name	Group?	Profile Owner
*PGMR	QPGMR	*NONE	*NO	Programmer and Batch User
	QRJE	*NONE	*NO	IBM-supplied User Profile
	QSRV	*NONE	*NO	Service User Profile
	QSRVBAS	*NONE	*NO	Basic Service User Profile
*SECOFR	QSECOFR	*NONE	*NO	Security Officer
	QSYS	*NONE	*NO	Internal System User Profile
	SMURF	*NONE	*NO	Security Officer
	TERRYJ	GROUP1	*NO	Security Officer
*SYSOPR	QANZAGENT	*NONE	*NO	Trace Analyzer Agent Server
	QIBMHELP	*NONE	*NO	IBM Eclipse Online Help
	QLPAUTO	*NONE	*NO	IBM-supplied User Profile
	QLPINSTALL	*NONE	*NO	IBM-supplied User Profile
	QSRVAGT	*NONE	*NO	IBM-supplied User Profile
	QSYSOPR	*NONE	*NO	System Operator
	QTCP	*NONE	*NO	Internal TCP/IP User Profile
*USER	AUDITOR1	GROUP1	*NO	Auditor
	AUDITOR2	GROUP1	*NO	Auditor
	GROUP1	*NONE	*YES	Test Group
	QAUTPROF	*NONE	*NO	IBM-supplied User Profile
	QBRMS	*NONE	*NO	IBM-supplied User Profile
	QCLUMGT	*NONE	*NO	IBM-supplied User Profile
	QCLUSTER	*NONE	*NO	IBM-supplied User Profile
	QCOLSRV	*NONE	*NO	IBM-supplied User Profile
	QDBSHR	*NONE	*NO	Internal Data Base User Profile
	QDBSHRDO	*NONE	*NO	Internal Data Base User Profile
	QDFTOWN	*NONE	*NO	Default Owner for System Objects
	QDIRSRV	*NONE	*NO	System Directory Services Server User Profile
	QDLFM	*NONE	*NO	IBM-supplied User Profile
	QDOC	*NONE	*NO	Internal Document User Profile
	QDSNX	*NONE	*NO	IBM-supplied User Profile
	QEJB	*NONE	*NO	IBM-supplied User Profile
	QEJBSVR	*NONE	*NO	IBM-supplied User Profile
	QFNC	*NONE	*NO	IBM-supplied User Profile
	QGATE	*NONE	*NO	IBM-supplied User Profile

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

User Class	Profile Name	Group Name	Group?	Profile Owner
	QIPP	*NONE	*NO	IBM-supplied User Profile
	QLWISVR	*NONE	*NO	
	QMGTC	*NONE	*NO	IBM-supplied User Profile
	QMSF	*NONE	*NO	Mail Server Framework Profile
	QNETSPLF	*NONE	*NO	Internal Spool Network Profile
	QNFSANON	*NONE	*NO	IBM-supplied User Profile
	QNTP	*NONE	*NO	IBM-supplied User Profile
	QPEX	*NONE	*NO	IBM-supplied User Profile
	QPM400	*NONE	*NO	IBM-supplied User Profile
	QSNADS	*NONE	*NO	IBM-supplied User Profile
	QSPL	*NONE	*NO	Internal Spool User Profile
	QSPLJOB	*NONE	*NO	Internal Spool User Profile
	QTCM	*NONE	*NO	IBM-supplied User Profile
	QTFTP	*NONE	*NO	IBM-supplied User Profile
	QTMHHTTP1	*NONE	*NO	HTTP Server CGI User Profile
	QTMHHTTP	*NONE	*NO	HTTP Server User Profile
	QTMPLPD	*NONE	*NO	ALLOW REMOTE LPR REQUESTERS
	QTSTRQS	*NONE	*NO	Test Request User Profile
	QUSER	*NONE	*NO	Work Station User
	QWSERVICE	*NONE	*NO	
	QYCMCIMOM	*NONE	*NO	IBM-supplied User Profile
	QYPSJSVR	*NONE	*NO	IBM-supplied User Profile

### Implications

User profiles should be assigned to specific persons and not to job functions, so you can maintain accountability over any actions performed on your system with a profile.

If users are assigned User Classes that are greater than their needs, they will have access to unnecessary system functions and resources via the 'special authorities' associated with that User Class.

The following table summarises the *default* special authorities assigned to each User Class. Note that these default authorities may be altered in individual User profiles.

For example, if profile *Joe* has a User Class of \*PGMR, and the \*SAVSYS Special Authority is *removed* from the profile, *Joe* will not have the authority to perform save & restore functions. Similarly, if the \*SECADM Special Authority is *added* to profile *Joe*, he will be able to perform security administration functions on the system even though he only has a User Class of \*PGMR.

Please consult the table in report [Profiles with Special Authorities](#) for details of the respective functions of these authorities.

User Class	Default Special Authorities
*PGMR	(*JOBCTL, *SAVSYS)
*SECADM	(*JOBCTL, *SAVSYS, *SECADM)
*SECOFR	(*ALLOBJ, *AUDIT, *IOSYSCFG, *JOBCTL, *SAVSYS, *SECADM, *SERVICE, *SPLCTL)
*SYSOPR	(*JOBCTL, *SAVSYS)
*USER	(no special authorities by default)

### Risk Rating

Medium to High. (dependent on users' job functions)

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

### Recommended Action

---

You should ensure that User profiles are assigned to specific persons and not to job functions.

User Classes other than \*USER should be checked to confirm that they are consistent with the person's job function. In general, most end-users should be assigned a User Class of \*USER.

Ensure you do not remove any intended special authorities from those IBM-supplied (Q..) profiles that are used internally by OS/400 itself.

The number of profiles with a User Class of \*SECOFR or \*SECADM should be kept to a minimum.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 4. Profiles with Special Authorities

The following reports summarise and list *all* Special Authorities assigned to the profiles defined to your system. I.e. they include Special Authorities granted *directly* to the profile ('Group' field is blank) as well as authorities that are inherited *indirectly* through Group membership.

The first report is [Grouped by Profile Name](#) and the second is [Grouped by Special Authority](#).

### Notes:

- All profiles are User profiles except those ending in '(G)', which are Group profiles;
- All groups are Primary groups except those ending in '(S)', which are Supplemental groups.
- A value of 'Yes' in the 'Profile Disabled?' column indicates that the profile is disabled, or it's password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

### Section Summary

#### All Accounts

32.1% (18) of the profiles on your system have one (or more) special authorities assigned to them:

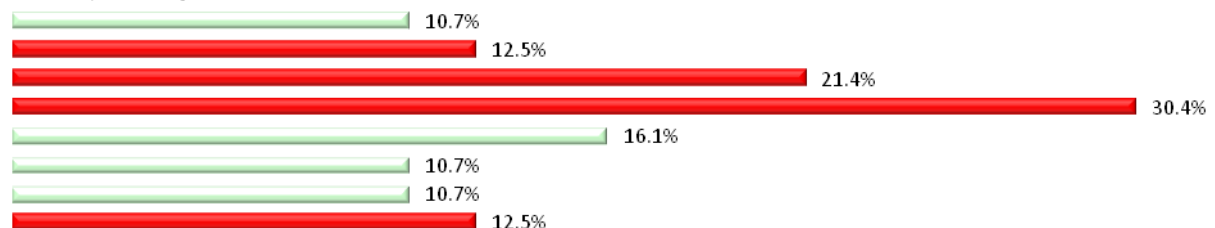
- 10.7% (6) can access all system resources (\*ALLOBJ)
- 12.5% (7) can amend auditing values on the system (\*AUDIT)
- 21.4% (12) can change system configuration lists (\*IOSYSCFG)
- 30.4% (17) can control jobs, IPL the system, start/stop sub-systems etc. (\*JOBCTL)
- 16.1% (9) can save and restore programs and files (\*SAVSYS)
- 10.7% (6) have security administration (\*SECADM) privileges
- 10.7% (6) have access to 'service' functions (\*SERVICE)
- 12.5% (7) can control 'spool' functions (\*SPLCTL)

#### Excluding Disabled Accounts

10.7% (6) of profiles have one (or more) special authorities assigned to them:

- 5.4% (3) can access all system resources (\*ALLOBJ)
- 10.7% (6) can amend auditing values on the system (\*AUDIT)
- 10.7% (6) can change system configuration lists (\*IOSYSCFG)
- 10.7% (6) can control jobs, IPL the system, start/stop sub-systems etc. (\*JOBCTL)
- 7.1% (4) can save and restore programs and files (\*SAVSYS)
- 5.4% (3) have security administration (\*SECADM) privileges
- 5.4% (3) have access to 'service' functions (\*SERVICE)
- 10.7% (6) can control 'spool' functions (\*SPLCTL)

#### Industry Average Comparison (All Accounts)



### Implications

If users are assigned special authorities greater than their needs, they will have unnecessary access to system functions, which increases the risk of unauthorised access to systems and data.

The following table lists the various special authorities and their functions.

Special Authority	Function
*ALLOBJ	User can access <i>all</i> system resources
*AUDIT	User can change auditing characteristics on the system
*IOSYSCFG	User can change system configuration lists (V3R1 onwards)
*JOBCTL	User can control jobs, IPL the system, start/stop sub-systems
*SAVSYS	User can save & restore files & programs (e.g. can take an object to another AS/400 system,

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

save the object & view the data)  
\*SECADM User can create and change profiles & access rights  
\*SERVICE User can perform 'alter' functions. Can provide a 'back-door' to security  
\*SPLCTL User can control spool functions

### Notes.

Access to specific resources, such as system commands, programs and job queues can also be restricted at resource-level. This means for example, that:

- A profile may have the \*JOBCTL special authority, but is prevented from IPL-ing the system because it does not have the required execute authority for the PWRDWNSYS command;
- A profile has the \*SPLCTL special authority, but is restricted to selected spool queues.

With the exception of the resources listed under report section [Object and Data Authorities for Selected Objects](#), *SekChek* does not report on resource-level security.

### Risk Rating

---

Medium to High. (dependent on users' job functions)

### Recommended Action

---

All profiles with special authorities should be checked to confirm that they are consistent with the person's job function.

Ensure you do not remove any intended special authorities from those IBM-supplied (Q..) profiles that are used internally by OS/400 itself.

In general, end-users should not be given access to 'special authorities'.

## Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

### Grouped by Profile Name

Profile Name	Profile Disabled?	Special Authority	Via Group
AUDITOR1		*AUDIT	
		*AUDIT	GROUP1
		*IOSYSCFG	GROUP1
		*JOBCTL	
		*JOBCTL	GROUP1
		*SPLCTL	
		*SPLCTL	GROUP1
AUDITOR2		*AUDIT	
		*AUDIT	GROUP1
		*IOSYSCFG	GROUP1
		*JOBCTL	
		*JOBCTL	GROUP1
		*SAVSYS	
		*SPLCTL	
		*SPLCTL	GROUP1
GROUP1(G)		*AUDIT	
		*IOSYSCFG	
		*JOBCTL	
		*SPLCTL	
QCLUSTER	Yes	*IOSYSCFG	
QLPAUTO	Yes	*ALLOBJ	
		*IOSYSCFG	
		*JOBCTL	
		*SAVSYS	
		*SECADM	
QLPINSTALL	Yes	*ALLOBJ	
		*IOSYSCFG	
		*JOBCTL	
		*SAVSYS	
		*SECADM	
QPGMR	Yes	*JOBCTL	
		*SAVSYS	
QPM400	Yes	*IOSYSCFG	
		*JOBCTL	
QRJE	Yes	*JOBCTL	
QSECOFR		*ALLOBJ	
		*AUDIT	
		*IOSYSCFG	
		*JOBCTL	
		*SAVSYS	
		*SECADM	
		*SERVICE	

## Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

Profile Name	Profile Disabled?	Special Authority	Via Group
		*SPLCTL	
QSRV	Yes	*JOBCTL	
		*SERVICE	
QSRVAGT	Yes	*IOSYSCFG	
		*JOBCTL	
		*SERVICE	
QSRVBAS	Yes	*JOBCTL	
QSYS	Yes	*ALLOBJ	
		*AUDIT	
		*IOSYSCFG	
		*JOBCTL	
		*SAVSYS	
		*SECADM	
		*SERVICE	
		*SPLCTL	
QSYSOPR	Yes	*JOBCTL	
		*SAVSYS	
QTCP	Yes	*JOBCTL	
SMURF		*ALLOBJ	
		*AUDIT	
		*IOSYSCFG	
		*JOBCTL	
		*SAVSYS	
		*SECADM	
		*SERVICE	
		*SPLCTL	
TERRYJ		*ALLOBJ	
		*AUDIT	
		*AUDIT	GROUP1
		*IOSYSCFG	
		*IOSYSCFG	GROUP1
		*JOBCTL	
		*JOBCTL	GROUP1
		*SAVSYS	
		*SECADM	
		*SERVICE	
		*SPLCTL	
		*SPLCTL	GROUP1

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

### Grouped by Special Authority

Special Authority	Profile Name	Profile Disabled?	Via Group
*ALLOBJ	QLPAUTO	Yes	
	QLPINSTALL	Yes	
	QSECOFR		
	QSYS	Yes	
	SMURF		
	TERRYJ		
*AUDIT	AUDITOR1		
	AUDITOR1		GROUP1
	AUDITOR2		
	AUDITOR2		GROUP1
	GROUP1(G)		
	QSECOFR		
	QSYS	Yes	
	SMURF		
	TERRYJ		
	TERRYJ		GROUP1
*IOSYSCFG	AUDITOR1		GROUP1
	AUDITOR2		GROUP1
	GROUP1(G)		
	QCLUSTER	Yes	
	QLPAUTO	Yes	
	QLPINSTALL	Yes	
	QPM400	Yes	
	QSECOFR		
	QSRVAGT	Yes	
	QSYS	Yes	
	SMURF		
	TERRYJ		
	TERRYJ		GROUP1
*JOBCTL	AUDITOR1		
	AUDITOR1		GROUP1
	AUDITOR2		
	AUDITOR2		GROUP1
	GROUP1(G)		
	QLPAUTO	Yes	
	QLPINSTALL	Yes	
	QPGMR	Yes	
	QPM400	Yes	
	QRJE	Yes	
	QSECOFR		
	QSRV	Yes	
	QSRVAGT	Yes	

## Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

Special Authority	Profile Name	Profile Disabled?	Via Group
	QSRVBAS	Yes	
	QSYS	Yes	
	QSYSOPR	Yes	
	QTCP	Yes	
	SMURF		
	TERRYJ		
	TERRYJ		GROUP1
*SAVSYS	AUDITOR2		
	QLPAUTO	Yes	
	QLPINSTALL	Yes	
	QPGMR	Yes	
	QSECOFR		
	QSYS	Yes	
	QSYSOPR	Yes	
	SMURF		
	TERRYJ		
*SECADM	QLPAUTO	Yes	
	QLPINSTALL	Yes	
	QSECOFR		
	QSYS	Yes	
	SMURF		
	TERRYJ		
*SERVICE	QSECOFR		
	QSRV	Yes	
	QSRVAGT	Yes	
	QSYS	Yes	
	SMURF		
	TERRYJ		
*SPLCTL	AUDITOR1		
	AUDITOR1		GROUP1
	AUDITOR2		
	AUDITOR2		GROUP1
	GROUP1(G)		
	QSECOFR		
	QSYS	Yes	
	SMURF		
	TERRYJ		
	TERRYJ		GROUP1

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 5. Password Change Intervals Greater than 30 Days

### Section Summary

#### All Accounts

98.2% (55) of the profiles on your system are not forced to change their password every 30 days (or less):

- 92.9% (52) are not forced to change their password every 60 days (or less)
- 92.9% (52) are not forced to change their password every 90 days (or less)
- 92.9% (52) are not forced to change their password every 180 days (or less)
- 92.9% (52) are never required to change their password

#### Excluding Disabled Accounts

28.6% (16) of the profiles on your system are not forced to change their password every 30 days (or less):

- 23.2% (13) are not forced to change their password every 60 days (or less)
- 23.2% (13) are not forced to change their password every 90 days (or less)
- 23.2% (13) are not forced to change their password every 180 days (or less)
- 23.2% (13) are never required to change their password

#### All Administrator (\*SECADM) Accounts

83.3% (5) of administrator profiles are not forced to change their password every 30 days (or less):

- 83.3% (5) are not forced to change their password every 60 days (or less)
- 83.3% (5) are not forced to change their password every 90 days (or less)
- 83.3% (5) are not forced to change their password every 180 days (or less)
- 83.3% (5) are never required to change their password

#### Administrator Accounts (Excluding Disabled Accounts)

33.3% (2) of administrator profiles are not forced to change their password every 30 days (or less):

- 33.3% (2) are not forced to change their password every 60 days (or less)
- 33.3% (2) are not forced to change their password every 90 days (or less)
- 33.3% (2) are not forced to change their password every 180 days (or less)
- 33.3% (2) are never required to change their password

#### Industry Average Comparison (> 30 days)



Note.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or it's password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

### Section Detail

Profile Name	Password Change Interval	User Class	Group?	*SECADM	Disabled
AUDITOR1	45	*USER	*NO		
AUDITOR2	45	*USER	*NO		
GROUP1	45	*USER	*YES		
QANZAGENT	0	*SYSOPR	*NO		Yes
QAUTPROF	0	*USER	*NO		
QBRMS	0	*USER	*NO		Yes
QCLUMGT	0	*USER	*NO		Yes
QCLUSTER	0	*USER	*NO		Yes
QCOLSRV	0	*USER	*NO		
QDBSHR	0	*USER	*NO		
QDBSHRDO	0	*USER	*NO		

## Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

Profile Name	Password Change Interval	User Class	Group?	*SECADM	Disabled
QDFTOWN	0	*USER	*NO		
QDIRSRV	0	*USER	*NO		Yes
QDLFM	0	*USER	*NO		Yes
QDOC	0	*USER	*NO		
QDSNX	0	*USER	*NO		Yes
QEJB	0	*USER	*NO		
QEJBSVR	0	*USER	*NO		Yes
QFNC	0	*USER	*NO		Yes
QGATE	0	*USER	*NO		Yes
QIBMHELP	0	*SYSOPR	*NO		Yes
QIPP	0	*USER	*NO		
QLPAUTO	0	*SYSOPR	*NO	Yes	Yes
QLPINSTALL	0	*SYSOPR	*NO	Yes	Yes
QLWISVR	0	*USER	*NO		Yes
QMGTC	0	*USER	*NO		Yes
QMSF	0	*USER	*NO		
QNETSPLF	0	*USER	*NO		Yes
QNFSANON	0	*USER	*NO		Yes
QNTF	0	*USER	*NO		Yes
QPEX	0	*USER	*NO		Yes
QPGMR	0	*PGMR	*NO		Yes
QPM400	0	*USER	*NO		Yes
QRJE	0	*PGMR	*NO		Yes
QSECOFR	0	*SECOFR	*NO	Yes	
QSNADS	0	*USER	*NO		Yes
QSPL	0	*USER	*NO		Yes
QSPLJOB	0	*USER	*NO		Yes
QSRV	0	*PGMR	*NO		Yes
QSRVAGT	0	*SYSOPR	*NO		Yes
QSRVBAS	0	*PGMR	*NO		Yes
QSYS	0	*SECOFR	*NO	Yes	Yes
QSYSOPR	0	*SYSOPR	*NO		Yes
QTCM	0	*USER	*NO		Yes
QTCP	0	*SYSOPR	*NO		Yes
QTFTP	0	*USER	*NO		
QTMHHTP1	0	*USER	*NO		Yes
QTMHHTTP	0	*USER	*NO		Yes
QTMPLPD	-1	*USER	*NO		Yes
QTSTRQS	0	*USER	*NO		Yes
QUSER	0	*USER	*NO		Yes
QWSERVICE	0	*USER	*NO		Yes
QYCMCIMOM	0	*USER	*NO		
QYPSJSVR	0	*USER	*NO		Yes

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Profile Name	Password Change Interval	User Class	Group?	*SECADM	Disabled
TERRYJ	0	*SECOFR	*NO	Yes	

### Implications

If users are not required to change their passwords on a frequent basis, their passwords are likely to become known to other employees and potential intruders. The user profile could then be used to gain unauthorised access to systems and data until the real user changes the password to a new one.

The password change interval is typically defined as a System Value (QPWDEXPITV), although this system-wide setting can be overridden at user profile level. A password change interval other than '0' indicates that the value is defined at the user profile level.

A password change interval of '-1' means that the system does not enforce regular password changes.

A value of '0' in the password change interval column indicates that, although the user is forced to change his password according to the system-wide default (System Value '[QPWDEXPITV](#)'), the default is set to a value greater than 30 days or to \*NOMAX (users are not required to change their passwords).

### Risk Rating

Medium to High.

### Recommended Action

Password change intervals for these user profiles should be brought in-line with the generally accepted standard of between 30 and 60 days.

You should also ensure that the QPWDEXPITV System Value is set to a value of '60' or less (currently \*NOMAX).

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 6. Group Profiles and their Members

### Section Summary

There are a total of 1 group profiles, containing the following members, defined on your system.

*Note:*

*The value in column 'P/S' determines whether the Group profile listed under 'Group Name' is the user's Primary (P) group or a Supplemental (S) group.*

### Section Detail

Group Name	P/S	Profile Name	Object Owner	Group Authority	Profile Owner
GROUP1	P	AUDITOR1	*USRPRF	*NONE	Auditor
	P	AUDITOR2	*USRPRF	*NONE	Auditor
	P	TERRYJ	*USRPRF	*NONE	Security Officer

### Implications

Group profiles are used to give multiple users the same set of access authorities. Although a user can have only one Primary group, she can be a member of up to 15 Supplemental groups.

If a user is defined to a Group with access authorities greater than her needs, the user will have access to unnecessary system functions and information resources.

The Object Owner column indicates who owns any new objects created by the user:

- \*USRPRF The User profile owns new objects it creates;
- \*GRPPRF The user's Primary Group profile owns new objects created by the user and is given \*ALL authority to the objects. The user profile is not given any specific authority to new objects it creates.

If the Object Owner is \*USRPRF, the Group Authority field determines the authority given to the Group profile for any new objects created by the user:

- \*NONE No specific authority;
- \*ALL All management and data authorities;
- \*CHANGE Authority to change objects;
- \*USE Authority to view objects;
- \*EXCLUDE The Group profile is specifically denied access to new objects created by the user.

### Risk Rating

High. (if users are assigned to inappropriate Groups, or Groups are given inappropriate authorities for new objects created by users.)

### Recommended Action

You should check the Groups to which the listed User profiles belong and ensure they are consistent with the user's job function.

You should also confirm that Object Owners and Group Authorities have been appropriately defined for any new objects created by the user.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

### 7. Redundant Groups

#### Section Detail

---

The following group profiles do not contain any members and may be redundant:

\*\* No data found. \*\*

#### Section Detail

---

The following group profiles are referenced in the listed user profiles, but the groups were not found on your system:

\*\* No data found. \*\*

#### Implications

---

No security implications. The above reports highlight an integrity problem in your system's security file.

If a user profile refers to a group that does not exist, the situation could prevent the user from signing on to your system. Both of the above situations were most likely caused by the deletion of user profiles and/or groups without a corresponding clean-up of associated profiles.

#### Risk Rating

---

None. A housekeeping issue only.

#### Recommended Action

---

In the case where a Group profile is referenced in user profiles but the group profile does not exist, you should amend or remove the reference to the group in the listed user profiles.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 8. Passwords Equal to Profile Name

### Section Summary

#### All Accounts

3.6% (2) of the profiles on your system have a password equal to the profile name.

#### Excluding Disabled Accounts

3.6% (2) of the profiles on your system have a password equal to the profile name.

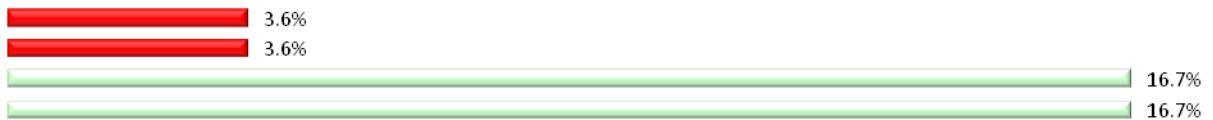
#### All Administrator (\*SECADM) Accounts

16.7% (1) of administrator profiles have a password equal to the profile name.

#### Administrator Accounts (Excluding Disabled Accounts)

16.7% (1) of administrator profiles have a password equal to the profile name.

#### Industry Average Comparison



#### Note.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or its password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

### Section Detail

Profile Name	Last Logon	Profile Owner	*SECADM	Disabled
AUDITOR2	01-Aug-2010	Auditor		
QSECOFR	25-Aug-2010	Security Officer	Yes	

### Implications

Weak passwords, such as one that is equal to the profile name, increase the risk of unauthorised access to your system. The particular resources an intruder could gain access to depends on the privileges assigned to the Profile.

Weak password controls also result in a loss of accountability for actions performed on your system.

### Risk Rating

High.

### Recommended Action

The profiles should be reviewed and their owners encouraged to sign-on and change their passwords to one that is private to them.

'Initial' passwords should always be set to random and unique values, and never to common default values, such as 'PASSWORD' and 'ABCDEFGH'.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 9. Profiles with Expired Passwords

### Section Summary

3.6% (2) of the profiles on your system have expired passwords.

Note.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or it's password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

### Section Detail

Profile Name	Last Logon	Profile Owner	Disabled
SMURF	12-Jul-2010	Security Officer	
TERRYJ	15-Aug-2010	Security Officer	

### Implications

These user profiles have default/'initial' passwords set by the security administrator, which may be easy for an intruder to guess. It could also be an indication that the profiles are no longer in use and are redundant.

### Risk Rating

Low to High. (dependent on the installation standard for selecting 'initial' passwords)

### Recommended Action

The profiles should be reviewed and their owners encouraged to sign-on and change their 'initial' password to one that is private to them, or deleted if no longer required.

'Initial' passwords should always be set to random and unique values, and never to common default values, such as 'PASSWORD' and 'ABCDEFG'.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 10. Passwords, 30 Days and Older

### Section Summary

#### All Accounts

25.0% (14) of the profiles on your system have not had their passwords changed in the last 30 days:

- 19.6% (11) have not had their passwords changed in the last 60 days
- 17.9% (10) have not had their passwords changed in the last 90 days
- 7.1% (4) have not had their passwords changed in the last 180 days
- 3.6% (2) have not had their passwords changed in the last 360 days
- 0.0% (0) have not had their passwords changed in the last 2 years

#### Excluding Disabled Accounts

7.1% (4) of the profiles on your system have not had their passwords changed in the last 30 days:

- 5.4% (3) have not had their passwords changed in the last 60 days
- 5.4% (3) have not had their passwords changed in the last 90 days
- 3.6% (2) have not had their passwords changed in the last 180 days
- 3.6% (2) have not had their passwords changed in the last 360 days
- 0.0% (0) have not had their passwords changed in the last 2 years

#### All Administrator (\*SECADM) Accounts

16.7% (1) of administrator profiles have not had their passwords changed in the last 30 days:

- 16.7% (1) have not had their passwords changed in the last 60 days
- 16.7% (1) have not had their passwords changed in the last 90 days
- 16.7% (1) have not had their passwords changed in the last 180 days
- 16.7% (1) have not had their passwords changed in the last 360 days
- 0.0% (0) have not had their passwords changed in the last 2 years

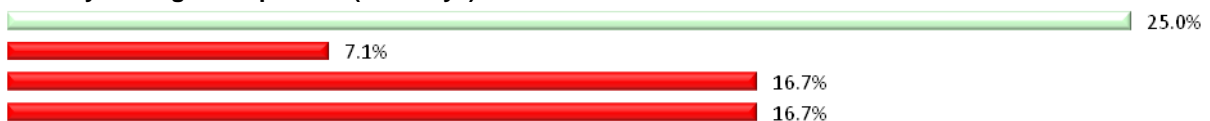
#### Administrator Accounts (Excluding Disabled Accounts)

16.7% (1) of administrator profiles have not had their passwords changed in the last 30 days:

- 16.7% (1) have not had their passwords changed in the last 60 days
- 16.7% (1) have not had their passwords changed in the last 90 days
- 16.7% (1) have not had their passwords changed in the last 180 days
- 16.7% (1) have not had their passwords changed in the last 360 days
- 0.0% (0) have not had their passwords changed in the last 2 years

The password for the QSECOFR profile was last changed 23 days ago.

#### Industry Average Comparison (> 30 days)



#### Note.

This is an exception report, so only lists profiles whose passwords have not changed in the last 30 days. I.e. if a profile's password was changed 29 days ago (or more recently) it will not be listed in the report section.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or it's password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

### Section Detail

Password Last Changed	Profile Name	Profile Owner	User Class	*SECADM	Disabled
11-Aug-2009	SMURF	Security Officer	*SECOFR	Yes	
17-Aug-2009	QDFTOWN	Default Owner for System Objects	*USER		
14-Feb-2010	QYPSJSVR	IBM-supplied User Profile	*USER		Yes
01-Mar-2010	QGATE	IBM-supplied User Profile	*USER		Yes
08-Mar-2010	QTMHHTTP	HTTP Server User Profile	*USER		Yes

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Password Last Changed	Profile Name	Profile Owner	User Class	*SECADM	Disabled
08-Apr-2010	QIBMHELP	IBM Eclipse Online Help	*SYSOPR		Yes
13-Apr-2010	QRJE	IBM-supplied User Profile	*PGMR		Yes
18-Apr-2010	QDSNX	IBM-supplied User Profile	*USER		Yes
19-Apr-2010	QTCP	Internal TCP/IP User Profile	*SYSOPR		Yes
14-May-2010	QYCMCIMOM	IBM-supplied User Profile	*USER		
06-Jun-2010	QSPL	Internal Spool User Profile	*USER		Yes
07-Jul-2010	QSRV	Service User Profile	*PGMR		Yes
12-Jul-2010	QTSTRQS	Test Request User Profile	*USER		Yes
01-Aug-2010	AUDITOR2	Auditor	*USER		

### Implications

This could indicate that these users are not required to change their passwords on a frequent basis, or that they are inactive or redundant. These profiles most likely appear on other reports.

### Risk Rating

Medium to High. (dependent on the strength of password controls)

### Recommended Action

The profiles should be reviewed and deleted if they are redundant and no longer required. Otherwise, their password change intervals should be brought in-line with installation standards.

A generally accepted standard is to force users to change their passwords every 30-60 days.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 11. Last Logons, 30 Days and Older

### Section Summary

#### All Accounts

92.9% (52) of the profiles on your system have not been used in the last 30 days:

- 89.3% (50) have not been used in the last 60 days
- 89.3% (50) have not been used in the last 90 days
- 89.3% (50) have not been used in the last 180 days
- 89.3% (50) have not been used in the last 360 days
- 89.3% (50) have not been used in the last 2 years
- 89.3% (50) have never been used

#### Excluding Disabled Accounts

23.2% (13) of the profiles on your system have not been used in the last 30 days:

- 19.6% (11) have not been used in the last 60 days
- 19.6% (11) have not been used in the last 90 days
- 19.6% (11) have not been used in the last 180 days
- 19.6% (11) have not been used in the last 360 days
- 19.6% (11) have not been used in the last 2 years
- 19.6% (11) have never been used

#### All Administrator (\*SECADM) Accounts

66.7% (4) of administrator profiles have not been used in the last 30 days:

- 50.0% (3) have not been used in the last 60 days
- 50.0% (3) have not been used in the last 90 days
- 50.0% (3) have not been used in the last 180 days
- 50.0% (3) have not been used in the last 360 days
- 50.0% (3) have not been used in the last 2 years

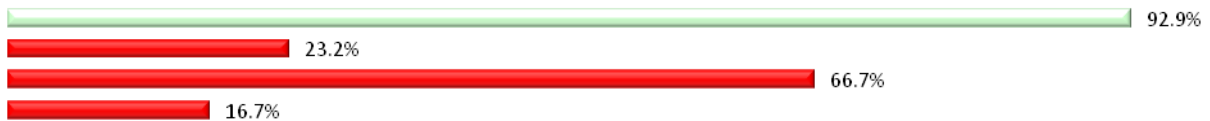
#### Administrator Accounts (Excluding Disabled Accounts)

16.7% (1) of administrator profiles have not been used in the last 30 days:

- 0.0% (0) have not been used in the last 60 days
- 0.0% (0) have not been used in the last 90 days
- 0.0% (0) have not been used in the last 180 days
- 0.0% (0) have not been used in the last 360 days
- 0.0% (0) have not been used in the last 2 years

The last logon for the QSECOFR account was 9 days ago.

#### Industry Average Comparison (> 30 days)



Note.

This is an exception report, so only lists profiles that have not logged on in the last 30 days. I.e. if a profile logged in 29 days ago (or more recently) it will not be listed in the report section.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or its password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

### Section Detail

Last Logon	Profile Name	User Class	Group?	*SECADM	Disabled
	QANZAGENT	*SYSOPR	*NO		Yes
	QAUTPROF	*USER	*NO		
	QBRMS	*USER	*NO		Yes
	QCLUMGT	*USER	*NO		Yes

## Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

Last Logon	Profile Name	User Class	Group?	*SECADM	Disabled
	QCLUSTER	*USER	*NO		Yes
	QCOLSRV	*USER	*NO		
	QDBSHR	*USER	*NO		
	QDBSHRDO	*USER	*NO		
	QDFTOWN	*USER	*NO		
	QDIRSRV	*USER	*NO		Yes
	QDLFM	*USER	*NO		Yes
	QDOC	*USER	*NO		
	QDSNX	*USER	*NO		Yes
	QEJB	*USER	*NO		
	QEJBSVR	*USER	*NO		Yes
	QFNC	*USER	*NO		Yes
	QGATE	*USER	*NO		Yes
	QIBMHELP	*SYSOPR	*NO		Yes
	QIPP	*USER	*NO		
	QLPAUTO	*SYSOPR	*NO	Yes	Yes
	QLPINSTALL	*SYSOPR	*NO	Yes	Yes
	QLWISVR	*USER	*NO		Yes
	QMGTC	*USER	*NO		Yes
	QMSF	*USER	*NO		
	QNETSPLF	*USER	*NO		Yes
	QNFSANON	*USER	*NO		Yes
	QNTP	*USER	*NO		Yes
	QPEX	*USER	*NO		Yes
	QPGMR	*PGMR	*NO		Yes
	QPM400	*USER	*NO		Yes
	QRJE	*PGMR	*NO		Yes
	QSNADS	*USER	*NO		Yes
	QSPL	*USER	*NO		Yes
	QSPLJOB	*USER	*NO		Yes
	QSRV	*PGMR	*NO		Yes
	QSRVAGT	*SYSOPR	*NO		Yes
	QSRVBAS	*PGMR	*NO		Yes
	QSYS	*SECOFR	*NO	Yes	Yes
	QSYSOPR	*SYSOPR	*NO		Yes
	QTCM	*USER	*NO		Yes
	QTCP	*SYSOPR	*NO		Yes
	QTFTP	*USER	*NO		
	QTMHHTP1	*USER	*NO		Yes
	QTMHHTTP	*USER	*NO		Yes
	QTMPLPD	*USER	*NO		Yes
	QTSTRQS	*USER	*NO		Yes
	QUSER	*USER	*NO		Yes

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Last Logon	Profile Name	User Class	Group?	*SECADM	Disabled
	QWSERVICE	*USER	*NO		Yes
	QYCMCIMOM	*USER	*NO		
	QYPSJSVR	*USER	*NO		Yes
12-Jul-2010	SMURF	*SECOFR	*NO	Yes	
01-Aug-2010	AUDITOR2	*USER	*NO		

### Implications

Some of these profiles may be inactive and therefore redundant. Inactive profiles are a prime target for intruders because if their passwords are compromised, they can be used with little fear of detection.

### Risk Rating

Low to Medium.

### Recommendations

The list of profiles should be reviewed and redundant entries should be deleted from the system.

Profiles that are required in the future, but not in the short term, should be disabled until next required.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 12. Invalid Signon Attempts Greater than 3

### Section Summary

---

#### All Accounts

0.0% (0) of the profiles on your system have 'invalid sign-on attempts' greater than 3.

#### Excluding Disabled Accounts

0.0% (0) of the profiles on your system have 'invalid sign-on attempts' greater than 3.

#### Industry Average Comparison

| 0.0%

| 0.0%

#### Note.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or it's password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

### Section Detail

---

\*\* No data found. \*\*

### Implications

---

'Invalid sign-on attempts' indicate the number of unsuccessful attempts at signing on to your system with the listed accounts. The value is reset to '0' *after* a successful sign-on to the system.

Consistently high values could be an indication that an intruder is attempting to guess user passwords to gain access to your system.

### Risk Rating

---

Medium to High. (dependent on the value assigned to the [QMAXSIGN](#) System Value and the strength of password controls).

### Recommended Action

---

You should check report [System Values](#) to confirm that the QMAXSIGN System Value is set to a value of '3' or less.

You should also try to determine the reason for high numbers of 'invalid sign-on attempts', perhaps by speaking to the profile owner.

If you suspect an intruder is attempting to gain access to your system, you should query the system's audit trails to identify the device(s) from which the high number of logon attempts originate. See [System Values](#) to determine the auditing features that are active on your system.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 13. Profiles Allowed Simultaneous Device Sessions

### Section Summary

#### All Accounts

100.0% (56) of the profiles on your system are not prevented from signing on to multiple work-stations at the same time.

#### Excluding Disabled Accounts

30.4% (17) of the profiles on your system are not prevented from signing on to multiple work-stations at the same time.

#### Industry Average Comparison



Note.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or it's password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

### Section Detail

Profile Name	Profile Owner	Limit Device Sessions?	User Class	Group?	Disabled
AUDITOR1	Auditor	*SYSVAL	*USER	*NO	
AUDITOR2	Auditor	*SYSVAL	*USER	*NO	
GROUP1	Test Group	*SYSVAL	*USER	*YES	
QANZAGENT	Trace Analyzer Agent Server	*NO	*SYSOPR	*NO	Yes
QAUTPROF	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QBRMS	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QCLUMGT	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QCLUSTER	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QCOLSRV	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QDBSHR	Internal Data Base User Profile	*SYSVAL	*USER	*NO	
QDBSHRDO	Internal Data Base User Profile	*SYSVAL	*USER	*NO	
QDFTOWN	Default Owner for System Objects	*SYSVAL	*USER	*NO	
QDIRSRV	System Directory Services Server User Profile	*NO	*USER	*NO	Yes
QDLFM	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QDOC	Internal Document User Profile	*SYSVAL	*USER	*NO	
QDSNX	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QEJB	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QEJBSVR	IBM-supplied User Profile	*NO	*USER	*NO	Yes
QFNC	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QGATE	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QIBMHELP	IBM Eclipse Online Help	*NO	*SYSOPR	*NO	Yes
QIPP	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QLPAUTO	IBM-supplied User Profile	*SYSVAL	*SYSOPR	*NO	Yes
QLPINSTALL	IBM-supplied User Profile	*SYSVAL	*SYSOPR	*NO	Yes
QLWISVR		*SYSVAL	*USER	*NO	Yes
QMGTC	IBM-supplied User Profile	*NO	*USER	*NO	Yes

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Profile Name	Profile Owner	Limit Device Sessions?	User Class	Group?	Disabled
QMSF	Mail Server Framework Profile	*SYSVAL	*USER	*NO	
QNETSPLF	Internal Spool Network Profile	*SYSVAL	*USER	*NO	Yes
QNFSANON	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QNTF	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QPEX	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QPGMR	Programmer and Batch User	*SYSVAL	*PGMR	*NO	Yes
QPM400	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QRJE	IBM-supplied User Profile	*SYSVAL	*PGMR	*NO	Yes
QSECOFR	Security Officer	*SYSVAL	*SECOFR	*NO	
QSNADS	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QSPL	Internal Spool User Profile	*SYSVAL	*USER	*NO	Yes
QSPLJOB	Internal Spool User Profile	*SYSVAL	*USER	*NO	Yes
QSRV	Service User Profile	*SYSVAL	*PGMR	*NO	Yes
QSRVAGT	IBM-supplied User Profile	*NO	*SYSOPR	*NO	Yes
QSRVBAS	Basic Service User Profile	*SYSVAL	*PGMR	*NO	Yes
QSYS	Internal System User Profile	*SYSVAL	*SECOFR	*NO	Yes
QSYSOPR	System Operator	*SYSVAL	*SYSOPR	*NO	Yes
QTCM	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QTCP	Internal TCP/IP User Profile	*SYSVAL	*SYSOPR	*NO	Yes
QTFTP	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QTMHHTTP1	HTTP Server CGI User Profile	*SYSVAL	*USER	*NO	Yes
QTMHHTTP	HTTP Server User Profile	*SYSVAL	*USER	*NO	Yes
QTMPLPD	ALLOW REMOTE LPR REQUESTERS	*SYSVAL	*USER	*NO	Yes
QTSTRQS	Test Request User Profile	*SYSVAL	*USER	*NO	Yes
QUSER	Work Station User	*SYSVAL	*USER	*NO	Yes
QWSERVICE		*SYSVAL	*USER	*NO	Yes
QYCMCIMOM	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QYPSJSVR	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
SMURF	Security Officer	*SYSVAL	*SECOFR	*NO	
TERRYJ	Security Officer	*SYSVAL	*SECOFR	*NO	

## Implications

If 'limit device sessions = \*NO' the profile can be signed on to multiple workstations at the same time. This increases the risk of unauthorised access to the system because:

- An intruder could access the system via these user profiles without detection, even if the profile is currently being used;
- If the owner has more than one active session, it is likely that one or more of these sessions are unattended and could be used to gain unauthorised access to the system.

A value of \*SYSVAL for 'Limit Device Sessions' indicates that, although the profile has been assigned the system-wide default for limit device sessions (System Value [QLMTDEVSSM](#)), the default does not prevent simultaneous sign-ons.

## Risk Rating

Low to Medium. (unless password controls for these profiles are weak)

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

### Recommended Action

---

The profiles should be checked to ensure that there is a valid need for them to have the capability of signing-on to multiple workstations at the same time. If there is no real need, the profiles should be changed to ensure that 'limit device sessions' = \*SYSVAL.

Also, you should check report [System Values](#) to confirm that the QLMTDEVSSN System Value is set to a value of '1' (prevent simultaneous sign-ons).

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 14. Profiles with Limited Capability

### Section Summary

#### All Accounts

98.2% (55) of the profiles on your system do not have 'limited capability = \*YES':

- 98.2% (55) have 'limited capability = \*NO'
- 0.0% (0) have 'limited capability = \*PARTIAL'

#### Excluding Disabled Accounts

30.4% (17) of the profiles on your system do not have 'limited capability = \*YES':

- 30.4% (17) have 'limited capability = \*NO'
- 0.0% (0) have 'limited capability = \*PARTIAL'

#### Industry Average Comparison (limited capability <> YES)



Note.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or its password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

### Section Detail

Profile Name	Limited Capability?	User Class	Group?	Disabled
AUDITOR1	*NO	*USER	*NO	
AUDITOR2	*NO	*USER	*NO	
GROUP1	*NO	*USER	*YES	
QANZAGENT	*NO	*SYSOPR	*NO	Yes
QAUTPROF	*NO	*USER	*NO	
QBRMS	*NO	*USER	*NO	Yes
QCLUMGT	*NO	*USER	*NO	Yes
QCLUSTER	*NO	*USER	*NO	Yes
QCOLSRV	*NO	*USER	*NO	
QDBSHR	*NO	*USER	*NO	
QDBSHRDO	*NO	*USER	*NO	
QDFTOWN	*NO	*USER	*NO	
QDLFM	*NO	*USER	*NO	Yes
QDOC	*NO	*USER	*NO	
QDSNX	*NO	*USER	*NO	Yes
QEJB	*NO	*USER	*NO	
QEJBSVR	*NO	*USER	*NO	Yes
QFNC	*NO	*USER	*NO	Yes
QGATE	*NO	*USER	*NO	Yes
QIBMHELP	*NO	*SYSOPR	*NO	Yes
QIPP	*NO	*USER	*NO	
QLPAUTO	*NO	*SYSOPR	*NO	Yes
QLPINSTALL	*NO	*SYSOPR	*NO	Yes
QLWISVR	*NO	*USER	*NO	Yes
QMGTC	*NO	*USER	*NO	Yes

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Profile Name	Limited Capability?	User Class	Group?	Disabled
QMSF	*NO	*USER	*NO	
QNETSPLF	*NO	*USER	*NO	Yes
QNFSPANON	*NO	*USER	*NO	Yes
QNTF	*NO	*USER	*NO	Yes
QPEX	*NO	*USER	*NO	Yes
QPGMR	*NO	*PGMR	*NO	Yes
QPM400	*NO	*USER	*NO	Yes
QRJE	*NO	*PGMR	*NO	Yes
QSECOFR	*NO	*SECOFR	*NO	
QSNADS	*NO	*USER	*NO	Yes
QSPL	*NO	*USER	*NO	Yes
QSPLJOB	*NO	*USER	*NO	Yes
QSRV	*NO	*PGMR	*NO	Yes
QSRVAGT	*NO	*SYSOPR	*NO	Yes
QSRVBAS	*NO	*PGMR	*NO	Yes
QSYS	*NO	*SECOFR	*NO	Yes
QSYSOPR	*NO	*SYSOPR	*NO	Yes
QTCM	*NO	*USER	*NO	Yes
QTCP	*NO	*SYSOPR	*NO	Yes
QTFTP	*NO	*USER	*NO	
QTMHHTP1	*NO	*USER	*NO	Yes
QTMHHTTP	*NO	*USER	*NO	Yes
QTMPLPD	*NO	*USER	*NO	Yes
QTSTRQS	*NO	*USER	*NO	Yes
QUSER	*NO	*USER	*NO	Yes
QWSERVICE	*NO	*USER	*NO	Yes
QYCMCIMOM	*NO	*USER	*NO	
QYPSJSVR	*NO	*USER	*NO	Yes
SMURF	*NO	*SECOFR	*NO	
TERRYJ	*NO	*SECOFR	*NO	

### Implications

Users with 'limited capability = \*NO' have the ability to change their *initial program*, initial menu and current library. These users are not limited to the functions contained in the menu and can execute system commands.

Users with 'limited capability = \*PARTIAL' have the ability to change their initial menu, are not limited to the functions contained in the menu and can execute system commands.

Profiles without 'limited capability = \*YES' could be used to bypass your intended security controls in the system. In general, end-users should not require 'unlimited capability'.

### Risk Rating

High. (if incorrectly specified)

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

### Recommended Action

---

The list of profiles should be reviewed and 'unlimited capability' removed where it is not required.

Where certain users require access to system commands to perform their job function, Resource-level security should be carefully reviewed to ensure their access rights to system resources and commands is reasonable and not excessive.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

# 15. Profiles with Attention-Key Programs

## Section Summary

---

### All Accounts

0.0% (0) of the profiles on your system have 'limited capability = \*YES' and an Attention-Key program which is not equal to \*SYSVAL.

### Excluding Disabled Accounts

0.0% (0) of the profiles on your system have 'limited capability = \*YES' and an Attention-Key program which is not equal to \*SYSVAL.

Note.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or it's password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

## Section Detail

---

\*\* No data found. \*\*

## Implications

---

Users with 'limited capability = \*YES' are normally restricted to the functions contained in their [menu](#) and do not have access to system commands.

However, an in-house developed Attention key program has the potential to give the user access to the command line and the ability to enter system commands. This could undermine the intended security controls over these users.

## Risk Rating

---

Medium. (dependent on the function of the Attention-Key program)

## Recommended Action

---

The list of profiles should be reviewed and the function of the Attention key program(s) determined. If the Attention key program provides access to the command line, Resource-level security should be reviewed for the profile, to ensure the user does not have access to sensitive system resources.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 16. Profiles without Signon (Display) Information

### Section Summary

#### All Accounts

100.0% (56) of the profiles on your system do not receive details of previous sign-on activity when they logon to your system.

#### Excluding Disabled Accounts

30.4% (17) of the profiles on your system do not receive details of previous sign-on activity when they logon to your system.

#### Industry Average Comparison



Note.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or its password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

### Section Detail

Profile Name	Profile Owner	Display Sign-on Information?	User Class	Group?	Disabled
AUDITOR1	Auditor	*SYSVAL	*USER	*NO	
AUDITOR2	Auditor	*SYSVAL	*USER	*NO	
GROUP1	Test Group	*SYSVAL	*USER	*YES	
QANZAGENT	Trace Analyzer Agent Server	*NO	*SYSOPR	*NO	Yes
QAUTPROF	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QBRMS	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QCLUMGT	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QCLUSTER	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QCOLSRV	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QDBSHR	Internal Data Base User Profile	*SYSVAL	*USER	*NO	
QDBSHRDO	Internal Data Base User Profile	*SYSVAL	*USER	*NO	
QDFTOWN	Default Owner for System Objects	*SYSVAL	*USER	*NO	
QDIRSRV	System Directory Services Server User Profile	*NO	*USER	*NO	Yes
QDLFM	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QDOC	Internal Document User Profile	*SYSVAL	*USER	*NO	
QDSNX	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QEJB	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QEJBSVR	IBM-supplied User Profile	*NO	*USER	*NO	Yes
QFNC	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QGATE	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QIBMHELP	IBM Eclipse Online Help	*NO	*SYSOPR	*NO	Yes
QIPP	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QLPAUTO	IBM-supplied User Profile	*SYSVAL	*SYSOPR	*NO	Yes
QLPINSTALL	IBM-supplied User Profile	*SYSVAL	*SYSOPR	*NO	Yes
QLWISVR		*SYSVAL	*USER	*NO	Yes
QMGTC	IBM-supplied User Profile	*NO	*USER	*NO	Yes

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Profile Name	Profile Owner	Display Sign-on Information?	User Class	Group?	Disabled
QMSF	Mail Server Framework Profile	*SYSVAL	*USER	*NO	
QNETSPLF	Internal Spool Network Profile	*SYSVAL	*USER	*NO	Yes
QNFSANON	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QNTPL	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QPEX	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QPGMR	Programmer and Batch User	*SYSVAL	*PGMR	*NO	Yes
QPM400	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QRJE	IBM-supplied User Profile	*SYSVAL	*PGMR	*NO	Yes
QSECOFR	Security Officer	*SYSVAL	*SECOFR	*NO	
QSNADS	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QSPL	Internal Spool User Profile	*SYSVAL	*USER	*NO	Yes
QSPLJOB	Internal Spool User Profile	*SYSVAL	*USER	*NO	Yes
QSRV	Service User Profile	*SYSVAL	*PGMR	*NO	Yes
QSRVAGT	IBM-supplied User Profile	*NO	*SYSOPR	*NO	Yes
QSRVBAS	Basic Service User Profile	*SYSVAL	*PGMR	*NO	Yes
QSYS	Internal System User Profile	*SYSVAL	*SECOFR	*NO	Yes
QSYSOPR	System Operator	*SYSVAL	*SYSOPR	*NO	Yes
QTCM	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
QTCP	Internal TCP/IP User Profile	*SYSVAL	*SYSOPR	*NO	Yes
QTFTP	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QTMHHTTP1	HTTP Server CGI User Profile	*SYSVAL	*USER	*NO	Yes
QTMHHTTP	HTTP Server User Profile	*SYSVAL	*USER	*NO	Yes
QTMPLPD	ALLOW REMOTE LPR REQUESTERS	*SYSVAL	*USER	*NO	Yes
QTSTRQS	Test Request User Profile	*SYSVAL	*USER	*NO	Yes
QUSER	Work Station User	*SYSVAL	*USER	*NO	Yes
QWSERVICE		*SYSVAL	*USER	*NO	Yes
QYCMCIMOM	IBM-supplied User Profile	*SYSVAL	*USER	*NO	
QYPSJSVR	IBM-supplied User Profile	*SYSVAL	*USER	*NO	Yes
SMURF	Security Officer	*SYSVAL	*SECOFR	*NO	
TERRYJ	Security Officer	*SYSVAL	*SECOFR	*NO	

### Implications

If 'Display Sign-on Information' is set to \*NO, the user will not receive details of previous sign-on activity or invalid attempts to sign-on with his profile, when he signs-on to the system. Successful intruders could use these profiles without detection by their owners.

If Display Sign-on Information contains a value of \*SYSVAL, although the profile uses the system-wide default for display sign-on information (System Value '[QDSPSGNINF](#)') the default does not ensure that previous sign-on details are displayed when users logon to your system.

### Risk Rating

Low to Medium. (dependent on the strength of security controls in general, and on System Values that prevent the selection of trivial passwords)

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

### Recommended Action

---

Ensure that previous sign-on activity is displayed for users by setting the '**QDSPGNINF**' System Value to '1' and changing the 'Display Sign-on Information' field in the above profiles to '\*SYSVAL'.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

### 17. Group and IBM-Supplied Profiles

#### Section Summary

25.0% (14) of the profiles on your system are Group and IBM-supplied profiles that do not have a password of \*NONE.

#### Section Detail

Profile Name	Profile Owner	User Class	Status	Group?
GROUP1	Test Group	*USER	*ENABLED	*YES
QAUTPROF	IBM-supplied User Profile	*USER	*ENABLED	*NO
QCLUMGT	IBM-supplied User Profile	*USER	*DISABLED	*NO
QCOLSRV	IBM-supplied User Profile	*USER	*ENABLED	*NO
QDBSHR	Internal Data Base User Profile	*USER	*ENABLED	*NO
QDBSHRDO	Internal Data Base User Profile	*USER	*ENABLED	*NO
QDFTOWN	Default Owner for System Objects	*USER	*ENABLED	*NO
QDOC	Internal Document User Profile	*USER	*ENABLED	*NO
QEJB	IBM-supplied User Profile	*USER	*ENABLED	*NO
QIPP	IBM-supplied User Profile	*USER	*ENABLED	*NO
QMSF	Mail Server Framework Profile	*USER	*ENABLED	*NO
QSECOFR	Security Officer	*SECOFR	*ENABLED	*NO
QTFTP	IBM-supplied User Profile	*USER	*ENABLED	*NO
QYCMCIMOM	IBM-supplied User Profile	*USER	*ENABLED	*NO

#### Implications

Some types of profile, such as Group profiles and some of the IBM-supplied (Q..) profiles, are never used to sign-on to a system. They are typically used for grouping together those users with similar access requirements, or used internally by OS/400 itself.

In certain cases, if these types of profile are enabled, with a password assigned to them, they present intruders with unnecessary opportunities to exploit security on your system.

Many organisations prefer to disable these profiles, to prevent the risk of them being used to sign-on to the system, by setting their passwords to \*NONE.

#### Risk Rating

Medium.

#### Recommended Action

If any of the above profiles are not used to sign-on to your system, you should ensure they are disabled by setting their password to \*NONE.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

### 18. Initial Programs and Menus

This report details the initial programs and menus assigned to the profiles defined in your security file.

A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or its password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.

Profile Name	Initial Program	IP Library	Initial Menu	IM Library	User Class	Disabled
AUDITOR1	*NONE		MAIN	*LIBL	*USER	
AUDITOR2	*NONE		MAIN	*LIBL	*USER	
GROUP1	*NONE		MAIN	*LIBL	*USER	
QANZAGENT	*NONE		MAIN	*LIBL	*SYSOPR	Yes
QAUTPROF	*NONE		MAIN	*LIBL	*USER	
QBRMS	*NONE		MAIN	*LIBL	*USER	Yes
QCLUMGT	*NONE		MAIN	*LIBL	*USER	Yes
QCLUSTER	*NONE		MAIN	*LIBL	*USER	Yes
QCOLSRV	*NONE		MAIN	*LIBL	*USER	
QDBSHR	*NONE		MAIN	*LIBL	*USER	
QDBSHRDO	*NONE		MAIN	*LIBL	*USER	
QDFTOWN	*NONE		MAIN	*LIBL	*USER	
QDIRSRV	*NONE		MAIN	*LIBL	*USER	Yes
QDLFM	*NONE		MAIN	*LIBL	*USER	Yes
QDOC	*NONE		MAIN	*LIBL	*USER	
QDSNX	*NONE		MAIN	*LIBL	*USER	Yes
QEJB	*NONE		MAIN	*LIBL	*USER	
QEJBSVR	*NONE		MAIN	*LIBL	*USER	Yes
QFNC	*NONE		MAIN	*LIBL	*USER	Yes
QGATE	*NONE		MAIN	*LIBL	*USER	Yes
QIBMHELP	*NONE		MAIN	*LIBL	*SYSOPR	Yes
QIPP	*NONE		MAIN	*LIBL	*USER	
QLPAUTO	QLPINATO	QSYS	*SIGNOFF		*SYSOPR	Yes
QLPINSTALL	*NONE		MAIN	*LIBL	*SYSOPR	Yes
QLWISVR	*NONE		MAIN	*LIBL	*USER	Yes
QMGTC	*NONE		MAIN	*LIBL	*USER	Yes
QMSF	*NONE		MAIN	*LIBL	*USER	
QNETSPLF	*NONE		MAIN	*LIBL	*USER	Yes
QNFSANON	*NONE		MAIN	*LIBL	*USER	Yes
QNTP	*NONE		MAIN	*LIBL	*USER	Yes
QPEX	*NONE		MAIN	*LIBL	*USER	Yes
QPGMR	*NONE		MAIN	*LIBL	*PGMR	Yes
QPM400	*NONE		MAIN	*LIBL	*USER	Yes
QRJE	*NONE		MAIN	*LIBL	*PGMR	Yes
QSECOFR	*NONE		MAIN	*LIBL	*SECOFR	
QSNADS	*NONE		MAIN	*LIBL	*USER	Yes
QSPL	*NONE		MAIN	*LIBL	*USER	Yes

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Profile Name	Initial Program	IP Library	Initial Menu	IM Library	User Class	Disabled
QSPLJOB	*NONE		MAIN	*LIBL	*USER	Yes
QSRV	*NONE		MAIN	*LIBL	*PGMR	Yes
QSRVAGT	*NONE		MAIN	*LIBL	*SYSOPR	Yes
QSRVBAS	*NONE		MAIN	*LIBL	*PGMR	Yes
QSYS	*NONE		MAIN	*LIBL	*SECOFR	Yes
QSYSOPR	*NONE		SYSTEM	*LIBL	*SYSOPR	Yes
QTCM	*NONE		MAIN	*LIBL	*USER	Yes
QTCP	*NONE		MAIN	*LIBL	*SYSOPR	Yes
QTFTP	*NONE		MAIN	*LIBL	*USER	
QTMHHTP1	*NONE		MAIN	*LIBL	*USER	Yes
QTMHHTP	*NONE		MAIN	*LIBL	*USER	Yes
QTMPLPD	*NONE		MAIN	*LIBL	*USER	Yes
QTSTRQS	*NONE		MAIN	*LIBL	*USER	Yes
QUSER	*NONE		MAIN	*LIBL	*USER	Yes
QWSERVICE	*NONE		MAIN	*LIBL	*USER	Yes
QYCMCIMOM	*NONE		MAIN	*LIBL	*USER	
QYPSJSVR	*NONE		MAIN	*LIBL	*USER	Yes
SMURF	*NONE		MAIN	*LIBL	*SECOFR	
TERRYJ	*NONE		MAIN	*LIBL	*SECOFR	

### Implications

An initial program is often used to set up the application environment or ensure the user can only run one program and never sees a menu.

The initial menu is the first menu the user sees after signing on to the system. It is displayed after the user's initial program has executed.

### Risk Rating

Medium to High.

### Recommended Action

The list of profiles should be reviewed to ensure that users' initial programs and menus do not compromise security and are appropriate for their job functions.

To avoid problems resulting from changes to library lists, you should consider specifying the library name containing the initial programs and menus, rather than \*LIBL.

It is possible to restrict users to specific applications using the initial program restriction; however, there is always the possibility that the application itself may allow the user access to other applications or the command line itself.

It is important to determine the functionality of the applications, and to consider the possibility that bugs may exist in the code, which could allow users access to the command line. In addition, we recommend that you verify the permissions over the library that the program belongs to and confirm that the program is effectively the one that was intended to run (for example, a library with inadequate resource-level security may allow someone to replace the genuine program with a modified version, which provides users with unintended functionality).

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

### 19. Disabled Profiles

#### Section Summary

69.6% (39) of the profiles on your system are disabled (or their password is set to '\*NONE') and should be checked.

#### Section Detail

Profile Name	Last Logon	User Class	Profile Owner	Disabled	Password =*NONE
QANZAGENT		*SYSOPR	Trace Analyzer Agent Server		Yes
QBRMS		*USER	IBM-supplied User Profile		Yes
QCLUMGT		*USER	IBM-supplied User Profile	Yes	
QCLUSTER		*USER	IBM-supplied User Profile		Yes
QDIRSRV		*USER	System Directory Services Server User Profile		Yes
QDLFM		*USER	IBM-supplied User Profile		Yes
QDSNX		*USER	IBM-supplied User Profile		Yes
QEJBSVR		*USER	IBM-supplied User Profile		Yes
QFNC		*USER	IBM-supplied User Profile		Yes
QGATE		*USER	IBM-supplied User Profile		Yes
QIBMHELP		*SYSOPR	IBM Eclipse Online Help		Yes
QLPAUTO		*SYSOPR	IBM-supplied User Profile		Yes
QLPINSTALL		*SYSOPR	IBM-supplied User Profile		Yes
QLWISVR		*USER		Yes	Yes
QMGTC		*USER	IBM-supplied User Profile		Yes
QNETSPLF		*USER	Internal Spool Network Profile		Yes
QNFSANON		*USER	IBM-supplied User Profile		Yes
QNTP		*USER	IBM-supplied User Profile		Yes
QPEX		*USER	IBM-supplied User Profile		Yes
QPGMR		*PGMR	Programmer and Batch User		Yes
QPM400		*USER	IBM-supplied User Profile		Yes
QRJE		*PGMR	IBM-supplied User Profile		Yes
QSNADS		*USER	IBM-supplied User Profile		Yes
QSPL		*USER	Internal Spool User Profile		Yes
QSPLJOB		*USER	Internal Spool User Profile		Yes
QSRV		*PGMR	Service User Profile		Yes
QSRVAGT		*SYSOPR	IBM-supplied User Profile		Yes
QSRVBAS		*PGMR	Basic Service User Profile		Yes
QSYS		*SECOFR	Internal System User Profile		Yes
QSYSOPR		*SYSOPR	System Operator		Yes
QTCM		*USER	IBM-supplied User Profile	Yes	Yes
QTCP		*SYSOPR	Internal TCP/IP User Profile		Yes
QTMHHTTP1		*USER	HTTP Server CGI User Profile		Yes
QTMHHTTP		*USER	HTTP Server User Profile		Yes
QTMPLPD		*USER	ALLOW REMOTE LPR REQUESTERS		Yes
QTSTRQS		*USER	Test Request User Profile		Yes

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Profile Name	Last Logon	User Class	Profile Owner	Disabled	Password =*NONE
QUSER		*USER	Work Station User		Yes
QWSERVICE		*USER		Yes	Yes
QYPSJSVR		*USER	IBM-supplied User Profile		Yes

### Implications

No security risk. A housekeeping issue only.

Profiles are disabled because their status has been set to 'disabled' or their password has been set to '\*NONE'. The listed profiles cannot be used to login to your system.

### Risk Rating

None.

### Recommended Action

You should determine whether these profiles are still required by their owners.

If they are still required, the owners should be contacted and their profiles re-enabled. If they are redundant and no longer required, they should be deleted from the system.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

## 20. Damaged Profiles

### Section Summary

---

0.0% (0) of the profiles on your system may be damaged and should be checked.

### Section Detail

---

\*\* No data found. \*\*

### Implications

---

No security risk.

### Risk Rating

---

None.

### Recommended Action

---

These profiles should be checked to confirm that they are damaged. If so they should be deleted and/or recreated.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 21. Profiles Created in the Last 90 Days

### Section Summary

#### All Profiles

8.9% (5) of user profiles were created in the last 360 days:

- 8.9% (5) were created in the last 30 days
- 8.9% (5) were created in the last 60 days
- 8.9% (5) were created in the last 90 days
- 8.9% (5) were created in the last 180 days
- 8.9% (5) were created in the last 360 days
- 91.1% (51) were created more than a year ago

#### All Administrator Profiles

33.3% (2) of administrator profiles were created in the last 360 days:

- 0.0% (2) were created in the last 30 days
- 33.3% (2) were created in the last 60 days
- 33.3% (2) were created in the last 90 days
- 33.3% (2) were created in the last 180 days
- 33.3% (2) were created in the last 360 days
- 66.7% (4) were created more than a year ago

*Note: This is an exception report, so it only lists user profiles that were created in the last 90 days. For details of profiles created more than 90 days ago, see column 'Account\_Created' in table [\\_All\\_User\\_Accounts](#) in the MS-Access database.*

*A value of 'Yes' in the 'Disabled' column indicates that the profile is disabled, or its password is set to '\*NONE'. These profiles cannot be used to login to your system. See report [Disabled Profiles](#) for a complete list of disabled profiles.*

### Section Detail

Create Date	Profile Name	Profile Owner	User Class	Group?	Disabled
10-Aug-2010	AUDITOR1	Auditor	*USER	*NO	
10-Aug-2010	AUDITOR2	Auditor	*USER	*NO	
10-Aug-2010	GROUP1	Test Group	*USER	*YES	
10-Aug-2010	SMURF	Security Officer	*SECOFR	*NO	
10-Aug-2010	TERRYJ	Security Officer	*SECOFR	*NO	

### Implications

The authorisation of new profiles, as well as changes to existing profiles, are key management controls that underpin the security of system and information resources.

If profiles are defined without management's knowledge or authorisation, they could be used to gain illegal access to your system resources with little fear of detection.

### Risk Rating

High (if user profiles are defined without appropriate management authorisation).

### Recommended Action

You should ensure management authorisation was formally provided prior to defining these user profiles. Supporting documentation should minimally include: a reason for creating the profile; the system resources required by the profile owner.

Before management gives an employee access to a user profile they should ensure the employee is made aware of the organisation's security policies and the employee's responsibilities for system security.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

Independent audits of new profiles should be conducted on a regular basis to ensure management controls are appropriate and are being applied in a consistent and effective manner.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 22. Programs with Adopted Authorities

### Section Detail

The following report lists the programs that adopt the authority of selected profiles on your system:

Adopted Profile	Program Name	Library	Program Type	Program Description
QSECOFR	CDRCVRT	QSYS2		
QSECOFR	CDRGCCN	QSYS2		
QSECOFR	CDRGCTL	QSYS2		
QSECOFR	CDRGESP	QSYS2		
QSECOFR	CDRGRDC	QSYS2		
QSECOFR	CDRSCSP	QSYS2		
QSECOFR	QFICHECK	QSYS2		
QSECOFR	QFIEXIT1	QSYS2		
QSECOFR	QLPEXIT1	QSYS2		
QSECOFR	QPGGENCA	QPFR	CLP	
QSECOFR	QPGGENCH	QPFR	PLI	
QSECOFR	QPTSLW	QPFR	RPG	
QSECOFR	QPTSRTMP	QPFR	CLP	
QSECOFR	QPTTNSCY	QPFR	CLP	
QSECOFR	QPTTNSRB	QPFR	CLP	
QSECOFR	QPTTNSRP	QPFR	CLP	
QSECOFR	QQMPWW	QSQL		
QSECOFR	QSQEXIT1	QSYS2		
QSECOFR	QSQIMAIN	QSQL		
QSECOFR	QZSCGETP	QSYS		
QSECOFR	QZSCRTDE	QSYS		
QSECOFR	SEKASPGM	SEKCHEK	CLP	
QSYS	CPRIVS	SYSIBM	CLE	SQL FUNCTION CPRIVILEGES
QSYS	PRIVILEGES	SYSIBM	CLE	SQL FUNCTION PRIVILEGES
QSYS	QDTS21ID	QDEVTOOLS	CLP	
QSYS	QDTS21IR	QDEVTOOLS	CLP	
QSYS	QDTS21IX	QDEVTOOLS	CLP	
QSYS	QHXEX0I1	QCAEXP	CLP	
QSYS	QPZA000038	QHTTPSVR	CLP	
QSYS	QTMFCOM1	QTCP	CPPLE	
QSYS	QTMFFTRC	QTCP	CPPLE	
QSYS	QTMMDUTL	QTCP	CPPLE	
QSYS	QTMMSUTL	QTCP	CPPLE	
QSYS	QTMSAPIUTL	QTCP	CPPLE	
QSYS	QTMSEXIT	QTCP	CPPLE	
QSYS	QTMSFWD	QTCP	CPPLE	
QSYS	QTMSHADM	QTCP		
QSYS	QTMSHADV	QTCP		
QSYS	QTMSINET	QTCP	CPPLE	

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Adopted Profile	Program Name	Library	Program Type	Program Description
QSYS	QTMSJOBS	QTCP	CPPLE	
QSYS	QTMSMALI	QTCP		
QSYS	QTMSMCP5	QTCP		
QSYS	QTMSMCVB	QTCP		
QSYS	QTMSMCVF	QTCP		
QSYS	QTMSMDIR	QTCP		
QSYS	QTMSMIEX	QTCP		
QSYS	QTMSMRNM	QTCP		
QSYS	QTMSMTAC	QTCP		
QSYS	QTMSMTAP	QTCP		
QSYS	QTMSMTCC	QTCP		
QSYS	QTMSMTNM	QTCP		
QSYS	QTMSMTPP	QTCP		
QSYS	QTMSMTPT	QTCP		
QSYS	QTMSSCAT	QTCP	CPPLE	
QSYS	QTMSSCHD	QTCP	CPPLE	
QSYS	QTMSSLIP	QTCP	CPPLE	
QSYS	QTMSSRCD	QTCP	CPPLE	
QSYS	QTMSSRCP	QTCP	CPPLE	
QSYS	QTMSSSUB	QTCP	CPPLE	
QSYS	QTMSSSTRC	QTCP	CPPLE	
QSYS	QTMSTEST	QTCP		
QSYS	QTMSTUTL	QTCP	CPPLE	
QSYS	QTMXCOM1	QTCP	CPPLE	
QSYS	QTMXCONV	QTCP		
QSYS	QTMXEXIT	QTCP	CPPLE	
QSYS	QTMXRAC	QTCP		
QSYS	QTMXRAP	QTCP		
QSYS	QTMXRACC	QTCP		
QSYS	QUHEXIT	QHLPSYS	CLP	
QSYS	SCHEMAS	SYSIBM	CLE	SQL FUNCTION SCHEMAS
QSYS	USERS	SYSIBM	CLE	SQL FUNCTION USERS

### Implications

AS/400's Adopted authority feature allows users to adopt the authority of a program's owner while the program is running. It allows users to be given *temporary* (indirect) authority to objects, while under the control of a program with restricted functionality, rather than having *permanent* and direct access to the objects concerned.

The user's normal authority to the object(s) is used when the program ends.

Note that this report only lists programs adopting the authority of those profiles you selected during the scan of data from the AS/400 machine.

### Risk Rating

Medium to High.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

### Recommended Action

---

You should ensure that:

- The profiles do not give unnecessary and excessive authorities to the listed programs;
- Users do not have unnecessary (\*EXECUTE) authority to these programs;
- The function of a program with adopt authority does not allow users to access objects outside the control of the program (e.g. the ability to execute system commands).

# Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 23. Object and Data Authorities for Selected Objects

### Section Detail

The following report lists the Object and Data Authorities, granted to users, groups, and the public, for selected objects on your system (the objects that were selected during the extract of data from the AS/400 machine):

Object Name	Library Name	Profile	Group?	* * * * * A R A U D E * O O O O O A R A U D E B B B B B U E D P L X J J J J J T A D D T E O M E A R L D C P G X L E M U R T I T F G T E S E T T R											Authorisation List
ADDAUTLE	QSYS	*PUBLIC		Y					Y			Y	*NONE		
ADDAUTLE	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
ADDLIBLE	QSYS	*PUBLIC		Y					Y			Y	*NONE		
ADDLIBLE	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGAUD	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGAUD	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGAUT	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGAUT	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGAUTLE	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGAUTLE	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGCURLIB	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGCURLIB	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGDLOAUD	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGDLOAUD	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGDSTPWD	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGDSTPWD	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGNETA	QSYS	*PUBLIC											*NONE		
CHGNETA	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGOBJAUD	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGOBJAUD	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGOBJOWN	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGOBJOWN	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGOBJPGP	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGOBJPGP	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGOWN	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGOWN	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGPGP	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGPGP	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGPWD	QSYS	*PUBLIC		Y					Y			Y	*NONE		
CHGPWD	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE		
CHGSYSVAL	QSYS	*PUBLIC											*NONE		
CHGSYSVAL	QSYS	QPGMR	*NO	Y					Y			Y	*NONE		
CHGSYSVAL	QSYS	QSRV	*NO	Y					Y			Y	*NONE		

# Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

Object Name	Library Name	Profile	Group?	* * * * * * * * * * *											Authorisation List
				O	B	J	O	P	R	T	S	T	A	R	
CHGSYSVAL	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
CHGSYSVAL	QSYS	QSYSOPR	*NO	Y							Y			Y	*NONE
CHGUSRAUD	QSYS	*PUBLIC		Y							Y			Y	*NONE
CHGUSRAUD	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
CHGUSRPRF	QSYS	*PUBLIC		Y							Y			Y	*NONE
CHGUSRPRF	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
CRTAUTHLR	QSYS	*PUBLIC													*NONE
CRTAUTHLR	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
CRTAUTL	QSYS	*PUBLIC		Y							Y			Y	*NONE
CRTAUTL	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
CRTUSRPRF	QSYS	*PUBLIC		Y							Y			Y	*NONE
CRTUSRPRF	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
DLTAUTHLR	QSYS	*PUBLIC		Y							Y			Y	*NONE
DLTAUTHLR	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
DLTAUTL	QSYS	*PUBLIC		Y							Y			Y	*NONE
DLTAUTL	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
DLTUSRPRF	QSYS	*PUBLIC		Y							Y			Y	*NONE
DLTUSRPRF	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
DSPAUTHLR	QSYS	*PUBLIC		Y							Y			Y	*NONE
DSPAUTHLR	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
EDTAUTL	QSYS	*PUBLIC		Y							Y			Y	*NONE
EDTAUTL	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
EDTOBJAUT	QSYS	*PUBLIC		Y							Y			Y	*NONE
EDTOBJAUT	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
GRTOBJAUT	QSYS	*PUBLIC		Y							Y			Y	*NONE
GRTOBJAUT	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
GRTUSRAUT	QSYS	*PUBLIC		Y							Y			Y	*NONE
GRTUSRAUT	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
PWRDWNSYS	QSYS	*PUBLIC													*NONE
PWRDWNSYS	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
PWRDWNSYS	QSYS	QSYSOPR	*NO	Y							Y			Y	*NONE
RMVAUTLE	QSYS	*PUBLIC		Y							Y			Y	*NONE
RMVAUTLE	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
RSTAUT	QSYS	*PUBLIC													*NONE
RSTAUT	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
RSTLIB	QSYS	*PUBLIC													*NONE
RSTLIB	QSYS	QSYS	*NO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	*NONE
RSTOBJ	QSYS	*PUBLIC													*NONE

# Security Analysis: TESTBED AS400

System: S65E570C  
 Analysis Date: 03-Sep-2010

CONFIDENTIAL

Object Name	Library Name	Profile	Group?	* * * * *	* * * * *	* * * * *	* * * * *	* * * * *	Authorisation List
				O O O O O	A R A U D E				
				B B B B B	U E D P L X				
				J J J J J	T A D D T E				
				O M E A R L D					C
				P G X L E M					U
				R T I T F G					T
				S E T					E
RSTOBJ	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
RSTUSRPRF	QSYS	*PUBLIC							*NONE
RSTUSRPRF	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
RTVAUTLE	QSYS	*PUBLIC		Y	Y			Y	*NONE
RTVAUTLE	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
RVKOBJAUT	QSYS	*PUBLIC		Y	Y			Y	*NONE
RVKOBJAUT	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
SAVLIB	QSYS	*PUBLIC		Y	Y			Y	*NONE
SAVLIB	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
SAVOBJ	QSYS	*PUBLIC		Y	Y			Y	*NONE
SAVOBJ	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
SAVSECDTA	QSYS	*PUBLIC		Y	Y			Y	*NONE
SAVSECDTA	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
SAVSYS	QSYS	*PUBLIC		Y	Y			Y	*NONE
SAVSYS	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
STRDFU	QSYS	*PUBLIC		Y	Y			Y	*NONE
STRDFU	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
STRSQL	QSYS	*PUBLIC		Y	Y			Y	*NONE
UPDDTA	QSYS	*PUBLIC		Y	Y			Y	*NONE
UPDDTA	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
WRKAUTL	QSYS	*PUBLIC		Y	Y			Y	*NONE
WRKAUTL	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
WRKOBJOWN	QSYS	*PUBLIC		Y	Y			Y	*NONE
WRKOBJOWN	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE
WRKUSRPRF	QSYS	*PUBLIC		Y	Y			Y	*NONE
WRKUSRPRF	QSYS	QSYS	*NO	Y Y Y Y Y	Y Y Y Y Y				*NONE

## Implications

Private authorities are granted to specific users and groups and determine the type of access they have to objects. Public authority (\*PUBLIC) is given to users and groups without specific private authorities to the object.

There are two categories of authority:

- Object authorities - define the operations that can be performed on the object as a whole;
- Data authorities - define the operations that can be performed on the contents of the object.

The following table lists the various authorities and their meanings:

Object Authorities	Name	Function
*OBJOPR	Object Operational	Look at the description of an object. Use the object as per the user's data authorities.
*OBJMGT	Object Management	Specify security for the object.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

		Move or rename the object.
*OBJEXIST	Object Existence	Delete the object. Free storage of the object. Perform save & restore operations for the object. Transfer ownership of the object.
*OBJALTER	Object Alter	Add, clear, initialise & reorganise members of the database files. Alter & add attributes of database files.
*OBJREF	Object Reference	Specify a database file as the parent in a referential constraint.
*AUTLMGT	Authorisation List Management	Add and remove users and their authorities from the authorisation list.

### Data Authorities

*READ	Read	Display the contents of the object (i.e. view records in a file).
*ADD	Add	Add entries to an object (i.e. add records to a file).
*UPD	Update	Change the entries in an object.
*DLT	Delete	Remove entries from an object (i.e. delete records from a file).
*EXECUTE	Execute	Run a program, service program, or SQL package.

Inappropriately defined authorities give users unnecessary access to programs and data, which can seriously undermine security of your system and information resources.

You should bear in mind however that there is more than one way a user can gain authority to objects on an AS/400 system. These are summarised below:

- The System-Value QSECURITY is set to less than 30 (see [System Values](#));
- The user has the Special Authority \*ALLOBJ (see [Profiles with Special Authorities](#));
- The user has the required private or public authority to the object (see above);
- The user has authority to the object via the object's authorisation list (see above);
- Via (program) [adopt authority](#) to the object;
- The user belongs to a group with any of the above authorities.

The table below lists the functions of some of the more common OS/400 commands.

<b>Object</b>	<b>Function</b>
ADDAUTLE	Add a user to an authorization list and specify authority to all objects on the list.
ADDLIBLE	Add entries to the library list for a job.
CHGAUTLE	Change users' authorities to the objects on an authorization list.
CHGCURLIB	Change current library.
CHGDSTPWD	Reset the DST or the QSECOFR password to the default password shipped with the system.
CHGNETA	Change network attributes for Job Action Network Attribute, Client Request Access Network Attribute and DDM (distributed data management) Network Attribute.
CHGOBJOWN	Change ownership of an object.
CHGSYSVAL	Change system value.
CHGUSRPRF	Change user profile.
CRTAUTL	Create authorization list.
CRTUSRPRF	Create user profile.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

---

<b>Object</b>	<b>Function</b>
DLTAUTHLR	Delete Authority holder.
DLTAUTL	Delete an entire authorization list.
DLTUSRPRF	Delete a user profile from the system.
DSPAUTHLR	Display all authority holders on the system.
EDTAUTL	Change and remove users and their authorities on an authorization list.
GRTOBJAUT	Specifically give authority to named users over objects.
GRTUSRAUT	Copy private authorities from one user profile to another user profile.
RMVAUTLE	Remove a user from an authorization list.
RSTLIB	Restore to the system one library or a group of libraries that was saved by the Save Library (SAVLIB) command.
RSTOBJ	Restore to the system a single object, or a group of objects, in a single library, that were saved on diskette, tape, optical volume, or in a save file by using a single command.
RVKOBJAUT	Remove one or more authorities given to a user.
SAVLIB	Save a copy of one or more libraries.
SAVOBJ	Save a copy of a single object or a group of objects located in the same library.
STRSQL	Start the interactive SQL program.
STRDFU	A powerful editor and data manipulation utility.
UPDDTA	Create and run a temporary DFU (Data File Utility) program.
WRKAUTL	Work with authorization lists from a list display.
WRKOBJOWN	Work with objects owned by a user profile.
WRKUSRPRF	Work with user profiles by entering options on a list display.

### Risk Rating

---

Medium to High. (if authorities are excessive)

### Recommended Action

---

You should ensure that:

- The private authorities for users and groups to the listed objects are appropriate and not excessive;
- The public (\*PUBLIC) authority for the objects is appropriate.

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 24. Network Services

### Section Summary

There are 206 active services on your system.

### Section Detail

The following table lists the active services in the Service Table:

Service Name	Port	Protocol	Description	Alias
APPCoverTCPIP	397	tcp	APPC over TCP/IP (connection provider)	appcovertcpip
				appc-tcpip
				APPC-TCPIP
APPCoverTCPIP	397	udp	APPC over TCP/IP (datagram provider)	appcovertcpip
				APPC-TCPIP
				appc-tcpip
as400-cluster	5550	tcp	cluster inetd port	AS400-CLUSTER
as400-cluster	5550	udp	cluster inetd port	AS400-CLUSTER
as400-clusterbase	5551	tcp	base cluster communications port	AS400-CLUSTERBASE
as400-clusterbase	5551	udp	base cluster communications port	AS400-CLUSTERBASE
as-admin-http	2001	tcp	AS400 Admin HTTP server	www-http-admin
as-admin-http	2001	udp	AS400 Admin HTTP server	www-http-admin
as-admin-https	2010	tcp	AS400 Admin HTTPs server	www-https-admin
as-admin-https	2010	udp	AS400 Admin HTTPs server	www-https-admin
as-central	8470	tcp	Central Server	ASCENTRAL
				ascentral
				AS-CENTRAL
as-central-s	9470	tcp	Secure Central Server	ASCENTRALS
				ascentrals
				AS-CENTRAL-S
as-database	8471	tcp	Database Server	ASDATABASE
				asdatabase
				AS-DATABASE
as-database-s	9471	tcp	Secure Database Server	ASDATABASES
				asdatabases
				AS-DATABASE-S
as-debug	4026	tcp	GRAPHICAL DEBUG SERVER	AS-DEBUG
as-dtaq	8472	tcp	Data Queue Server	ASDTAQ
				asdtaq
				AS-DTAQ
as-dtaq-s	9472	tcp	Secure Data Queue Server	ASDTAQS
				asdtajs
				AS-DTAQ-S
as-edrsq1	4402	tcp	AS400 EDRSQL server	AS-EDRSQL
as-file	8473	tcp	File Server	

## Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Service Name	Port	Protocol	Description	Alias
as-file-s	9473	tcp	Secure File Server	ASFILES asfiles AS-FILE-S
as-mgtctrl	5555	tcp	Management Central - No Encryption	
as-mgtctrl-cs	5577	tcp	Management Central - Encrypt/Clt/Svr Auth	
as-mgtctrlj	5544	tcp	Management Central Java - No Encryption	
as-mgtctrl-ss	5566	tcp	Management Central - Encrypt/Server Auth	
as-netdrive	8477	tcp	Network Drive Server	ASNETDRIVE asnetdrive AS-NETDRIVE

~~truncated, sample only~~

### **Service Name.**

The identifying label of the service.

### **Alias.**

Alternate names by which a service can be identified.

### **Description.**

The *text* identifying the Service Table listing.

### **Port.**

The port number of the local end of the socket.

### **Protocol.**

The name of the transport protocol. Typically *tcp* or *spx*.

## Implications

Network services expose your system in 3 ways:

- Services such as telnet (port 23) and ftp (port 21) transmit user passwords in clear text format, which makes them vulnerable to access via 'sniffer' software;
- Services such as finger (port 79), provide intruders with useful information about your system, such as details of inactive user accounts, which can be used to gain access to your system;
- Thirdly, every network service may have known and unknown security loopholes and risks.

## Risk Rating

Medium to High. (If inappropriate network services are made available)

## Recommended Action

You should check the list of network services to ensure they are valid and required. *The best general advice is if you do not really need a service, rather disable it or remove it from your system.*

You should also check the software versions you are using and consider upgrading to the latest version available from your vendor.

# Security Analysis: TESTBED AS400

System: S65E570C  
Analysis Date: 03-Sep-2010

CONFIDENTIAL

## 25. Other Considerations

### ***Sign-On Error Messages***

Consider changing the sign-on error message IDs CPF1107 and CPF1120 to make them more generic in content, as the standard messages give potential intruders vital clues as to whether he has provided a wrong profile name or wrong password to the system. A suggestion is to change them both to "Sign-on information is not correct".

### ***TCP/IP Services***

Ensure you are satisfied with security controls for TCP/IP services, such as TELNET, FTP and SMTP. Some examples of potential security exposures are:

- Passwords for FTP and TELNET are not encrypted when they are sent between the client and the server systems. This makes your system more vulnerable to password theft via 'line sniffing';
- The QMAXSIGN system value (which defines the maximum number of invalid sign-on attempts) does not apply to FTP;
- Although the QMAXSIGN system value applies to TELNET, its effectiveness is reduced if you set up your system to configure virtual devices automatically (QAUTOVRT=0).

As a general rule, TCP/IP servers should be disabled if not required.

### ***Resource Security***

Ensure that Resource-level security is correctly implemented for:

- Libraries
- Files
- Programs
- System commands
- User profile authorities
- Group authorities
- Public authorities
- Object ownership
- Adopted authorities
- Devices
- Output queues
- Job queues

Users should only be granted access to those resources that they need to perform their job functions.

### ***IBM-Supplied User Profiles***

Ensure passwords for IBM-supplied user profiles are not set to installation 'defaults'. In earlier versions of OS/400, the password was shipped the same as the user profile name.

For profiles that will not be used to sign-on to the system, setting **PASSWORD=\*NONE** prevents the risk of intruders 'guessing' their passwords. Because they are well known, the IBM-supplied profiles are obvious targets for intruders.

### ***Policies and Standards***

If you regularly find inconsistencies in security profiles and access rules, it is most probably due to a lack of formalised policies and standards or to a lack of clearly assigned responsibility for system ownership and security administration. *A permanent and lasting solution to security can only be achieved if these underlying issues are properly addressed.*

#### *Disclaimer.*

*These security analysis reports should be used as a guide and support tool only, in the speedy and frequent identification of security weaknesses and potential exposures. Although based on generally accepted security practices, they do not replace the need for sound judgment in defining and applying security standards for your particular organisation. Please consult the "AS/400 Security Reference Guide" or the product vendor for assistance in interpreting the results from this program.*

© 1996-2012 SekChek IPS. All rights reserved.

SekChek is a registered trademark of SekChek IPS. \* AS/400 is a trademark of the IBM Corporation.