iSecurity Compliance Evaluator

User Guide
Version 1.35

www.razlee.com

Contents

About this Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on IBM i systems. However, any user with basic knowledge of IBM i operations will be able to make full use of this product after reading this book.

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal IBM i experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

This user guide, together with the iSecurity Installation Guide, is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: http://www.adobe.com/. You can also read and print pages from the manual using any modern web browser.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the- box" security. To learn more about the iSecurity Suite, visit our website at http://www.razlee.com/.

Intended Audience

The Compliance EvaluatorUser Guide document was developed for users, system administrators and security administrators responsible for the implementation and management of security on IBM® AS/400 systems. However, any user with a basic knowledge of System i operations is able to make full use of this document following study of this User Guide.

NOTE: Deviations from IBM® standards are employed in certain circumstances in order to enhance clarity or when standard IBM® terminology conflicts with generally accepted industry conventions.

This document may also serve for new versions' upgrade approval by management.

Conventions Used in the Document

Menu options, field names, and function key names are written in **Courier New Bold**.

Links (internal or external) are emphasized with underline and blue color as follows: "About this Manual" on page 5.

Commands and system messages of IBM i® (OS/400®), are written in ***Bold Italic***.

Key combinations are in Bold and separated by a dash, for example: **Enter**, **Shift-Tab**.

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

STRACT **> 81 > 32**

meaning: Syslog definitions activated by typing ***STRACT***and selecting option: **81** then option: **32**.

Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press Enter or Field Exit
- To move from one field to another without changing the contents press Tab
- To view options for a data field together with an explanation, press F4
- To accept the data displayed on the screen and continue, press Enter

The following function keys may appear on data entry screens.

- **F1**: **Help** Display context-sensitive help
- **F3**: **Exit** End the current task and return to the screen or menu from which the task was initiated
- **F4**: **Prompt** Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
- **F6**: **Add New** Create a new record or data item
- **F8**: **Print** Print the current report or data item
- **F9**: **Retrieve** Retrieve the previously-entered command
- **F12**: **Cancel** Return to the previous screen or menu without updating

Legal Notice

This document is provided by Raz-Lee Security for information purposes only and is not a legal binding document.

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

This document contains highly confidential information, which is proprietary to Raz-Lee Security Ltd. and/or its affiliates (hereafter, "Raz-Lee"). No part of this document's contents may be used, copied, disclosed or conveyed to any third party in any manner whatsoever without prior written permission from Raz-Lee. The information included in this document is intended for your knowledge and for negotiation purposes only. Raz-Lee makes no implicit representations or warranties with respect to such information. The information included in this document is subject to change without notice. Any decision to rely on the information contained herein shall be at your sole responsibility, and Raz-Lee will not accept any liability for your decision to use any information or for any damages resulting therefrom. Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you.

All registered or unregistered trademarks, product names, logos and other service marks mentioned within this document are the property of Raz-Lee or their respective owners. Nothing contained herein shall be construed as conferring by implication, estoppels, or otherwise any license or right, either express or implied, under any patent or trademark of Raz-Lee or any third party. No use of any trademark may be made without the prior written authorization of Raz-Lee. This document and all of its contents are protected intellectual property of Raz-Lee. Any copying, reprinting, reuse, reproduction, adaptation, distribution or translation without the prior written permission of Raz-Lee is prohibited.

Please check your End User License Agreement (EULA) for terms and Conditions.

Contacts

Raz-Lee Security Inc. www.razlee.com
Marketing: marketing@razlee.com 1-888-RAZLEE-4 (1-888-7295334)
Support: support@razlee.com 1-888-RAZLEE-2 (1-888-7295332)

Overview

What is Compliance Evaluator?

Compliance Evaluator enables companies to easily obtain a quick, concise picture of the compliance status of their System i servers.

By providing compliance scores for individual servers, **Compliance Evaluator** is the ideal product for top and middle-level IT management.

Compliance Evaluator executes a focused set of pre-packaged and site-defined compliance reports, enabling the report output to be viewed either on a PC via the iSecurity™ GUI interface or as Excel email attachments.

What are the components of Compliance Evaluator?

Compliance Evaluator consists of three major components:

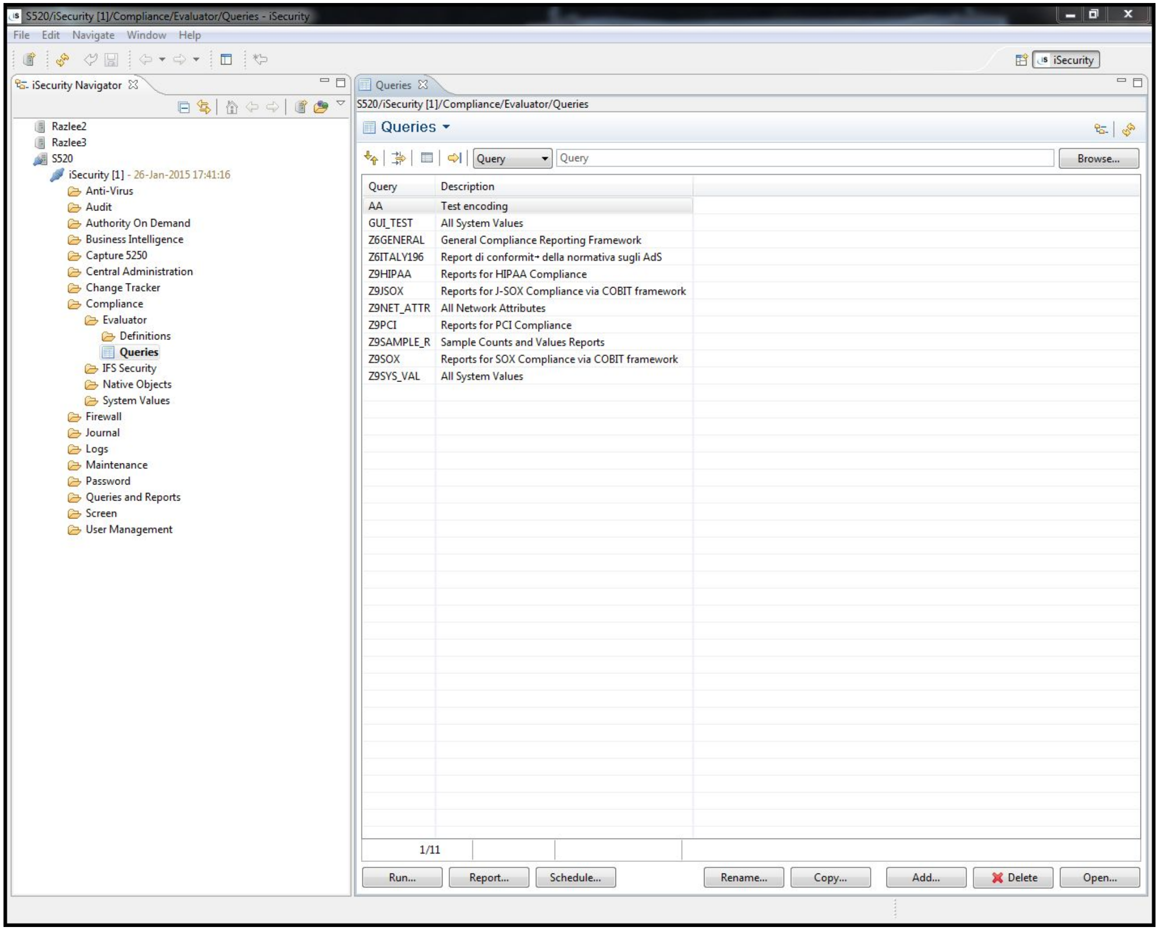
1. **Compliance Report Checks**. These checks are defined via the **Compliance Evaluator** user interface accessible via the iSecurity GUI. A number of pre-defined Compliance Report Checks are supplied with the product. These reports focus on the major compliance regulations such as PCI, SOX and HIPAA.
2. **Network Attributes and System Values definitions.** Each site can easily define scores for each of the Network Attributes and System Values, as well as unique scores for particular systems (for example a set of scores for a Production system, another set for a Test system, and so on).
3. **Excel Report Templates**. Technical users of **Compliance Evaluator**, for example system administrators, can define Excel-format report templates which will be used to automatically generate the requested reports in an Excel format compatible with site standards. It is recommended that at the outset the site use the product-supplied Excel report templates.

Implementing Compliance Evaluator

Compliance Evaluator is shipped with a number of pre-defined compliance checks. Each Check consists of a set of Detail and/or Counts reports which will execute when the **Run** button on the bottom left of the main product window is clicked.

Define or Edit a Compliance Check

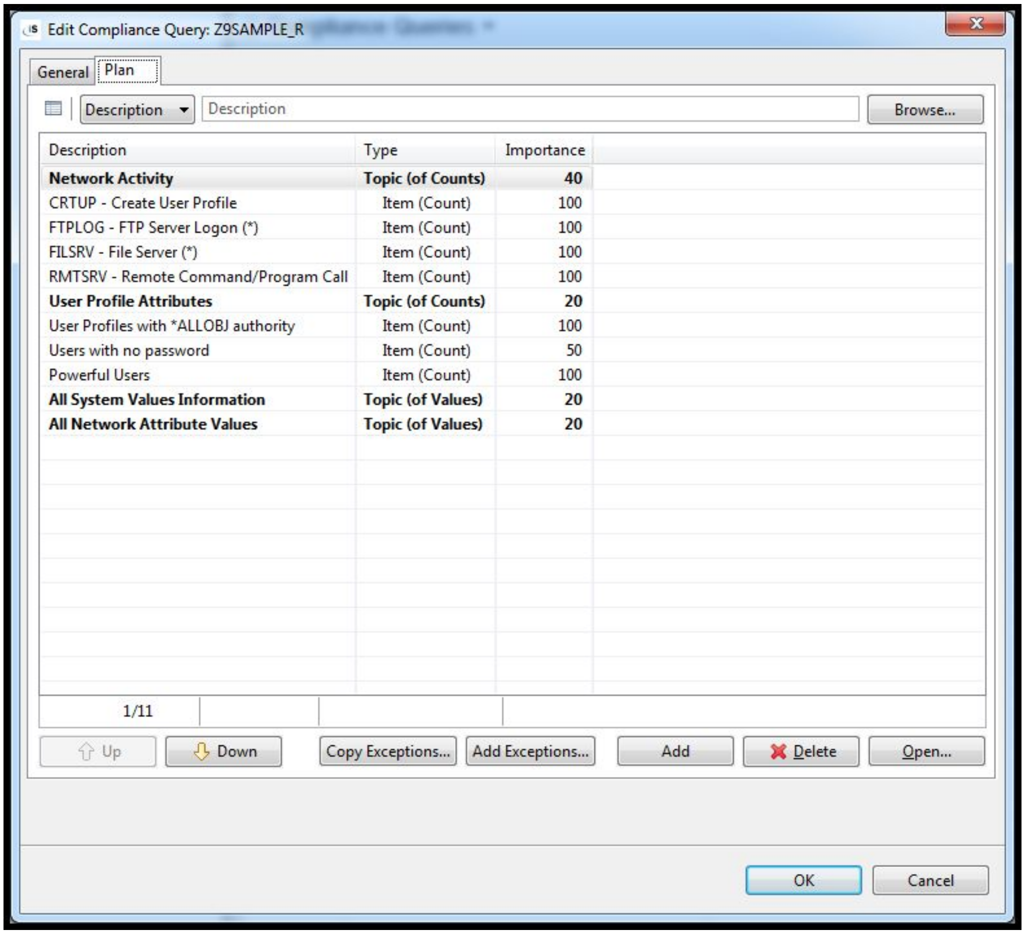
1. Open the **Compliance** node on the GUI tree, click **Evaluator** and then double-click **Queries**. The **Queries** window appears.



Query	Description
AA	Test encoding
GUI_TEST	All System Values
Z6GENERAL	General Compliance Reporting Framework
Z6ITALY196	Report di conformit+ della normativa sugli AdS
Z9HIPAA	Reports for HIPAA Compliance
Z9JSOX	Reports for J-SOX Compliance via COBIT framework
Z9NET_ATTR	All Network Attributes
Z9PCI	Reports for PCI Compliance
Z9SAMPLE_R	Sample Counts and Values Reports
Z9SOX	Reports for SOX Compliance via COBIT framework
Z9SYS_VAL	All System Values

Compliance Evaluator Checks

2. This manual will focus on explaining how Z9SAMPLE_R is defined; double-click on Z9SAMPLE_R or select Z9SAMPLE_R and click **Open.** Note that checks can also be deleted, copied, renamed, and so on.
3. The **Edit Compliance Query** dialog for Z9SAMPLE_R appears.



Description	Type	Importance
Network Activity	**Topic (of Counts)**	**40**
CRTUP - Create User Profile	Item (Count)	100
FTPLOG - FTP Server Logon (*)	Item (Count)	100
FILSRV - File Server (*)	Item (Count)	100
RMTSRV - Remote Command/Program Call	Item (Count)	100
User Profile Attributes	**Topic (of Counts)**	**20**
User Profiles with *ALLOBJ authority	Item (Count)	100
Users with no password	Item (Count)	50
Powerful Users	Item (Count)	100
All System Values Information	**Topic (of Values)**	**20**
All Network Attribute Values	**Topic (of Values)**	**20**

Edit Compliance Query

The above report **Z9SAMPLE_R** has 4 sections (lines appear in **bold**) which are weighted 40-20-20-20 correspondingly, totaling 100%. Note that had we assigned 100 to each of the 4 sections, Compliance Evaluator automatically normalizes these values so that the relative weights in the final report will be 25 for each of these sections.

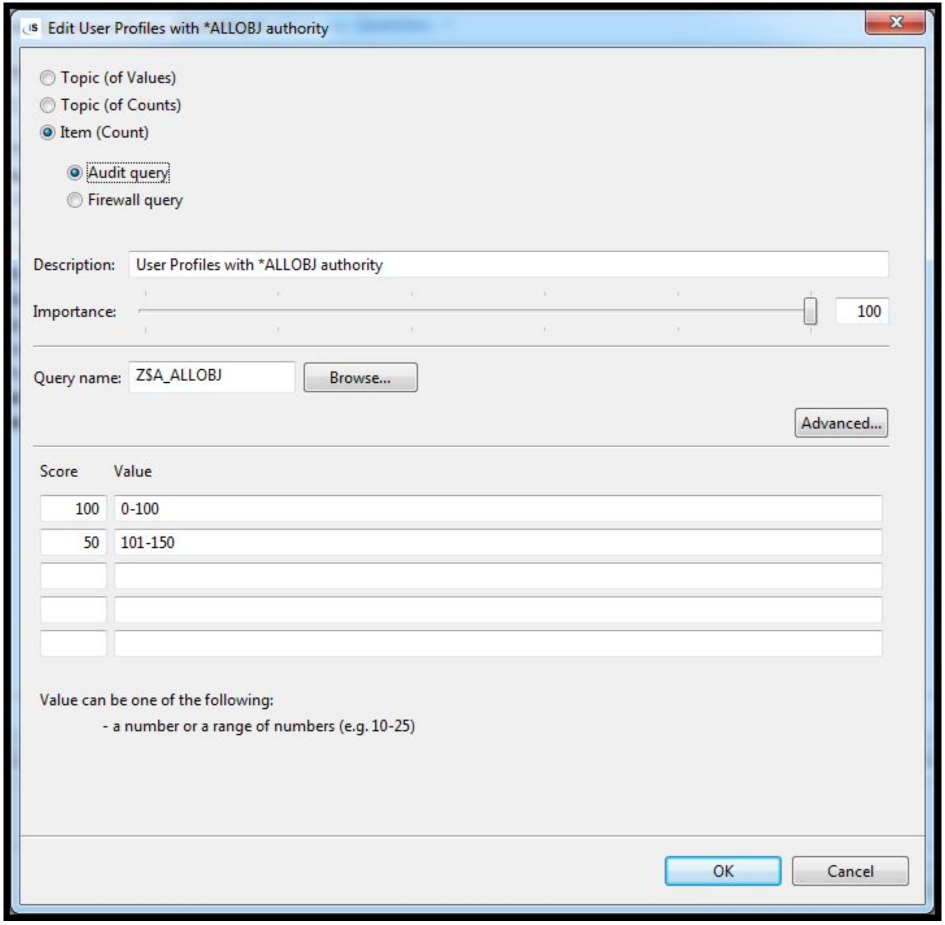
Relative weights can also be assigned to the Item (Count) reports which as a whole make up the Topic (of Counts) section of the Compliance Check. In the screen above, the **User Profiles with *ALLOBJ authority** report and the **Users with no Password** report each contribute (after normalization) 33.3% of the relative importance of the output section named **User Profile Attributes**.

Topic (of Values) reports are either $S=System Values or $T=Network Attributes **Audit** reports which produce multiple lines of output. These reports DO NOT need to be preceded by a Topic (of Counts) line.

All other **Firewall** and **Audit** reports produce a single numerical output which is a Count of the subject of the report (for example, the number of **Users with no Password**). These reports produce a single line of output in the final report; a set of such Item (Count) lines must be preceded by a single Topic (of Counts) line.

Edit Item (Count) reports

1. Select an Item (Count) type report and double-click it or click the **Open** button to edit. Recall that Item (Count) reports consist of a single numerical output which is, in this case, the number of **User Profiles with *ALLOBJ authority**.



○ Topic (of Values)
○ Topic (of Counts)
● Item (Count)

● Audit query
○ Firewall query

Description: User Profiles with *ALLOBJ authority

Importance: 100

Query name: Z$A_ALLOBJ

Score	Value
100	0-100
50	101-150

Value can be one of the following:
- a number or a range of numbers (e.g. 10-25)

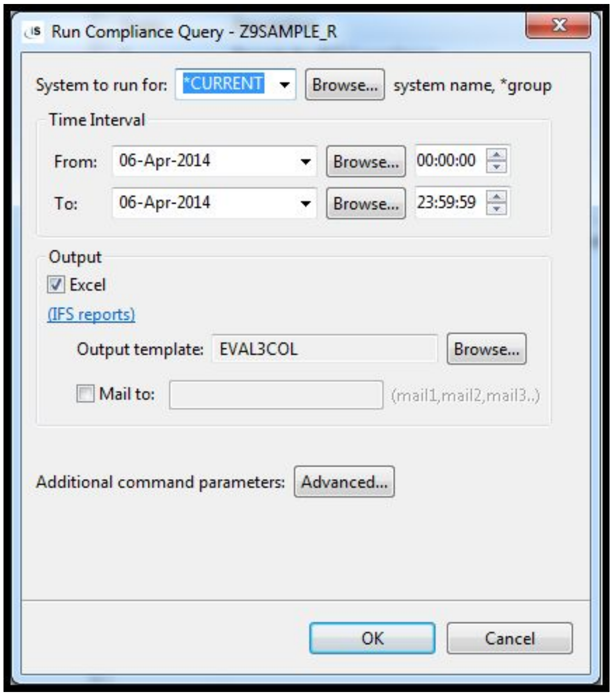
Edit Item(Count) reports

2. Define an importance rating for this particular report, which will be used to define the relative weight of this report within the Topic (of Counts).
3. Define ranges of values and a score for each value or range of values. This score represents the weight of this particular report within Topic (of counts). For example, if 105 users have *ALLOBJ authority, the score for this report is 50.

Running Reports

1. In order for the reports to run correctly you should:
    a. Review the query definitions, checking that the filter conditions specified are appropriate for your site. Query definition names will be similar to Z$A_DEFPW; that is they begin with "Z", are followed by the audit type, in this case $A, and following the "_" have up to 6 characters. To edit the filter conditions in the GUI, simple edit the query from "Queries and Reports"→ "Audit Queries".
    b. The libraries listed below appear in some of the filter conditions and should be updated with information specific to your site. Use Option 32. General Groups from the main **Audit** menu, or Audit→"General Groups" to update the lists of libraries:
        1. LIBRARIES/PRODLIB- list of production libraries at your site.
        2. LIBRARIES/SYSTLIB- list of system libraries at your site.
        3. LIBRARIES/KEYSLIB- list of libraries containing key encryption codes at your site.
        4. USERS/PRODUSER- list of authorized users with access to production systems at your site.
        5. USERS/KEYSUSER- list of users who are authorized to access the list of encryption keys

Run the Compliance query by clicking **Run** and defining the time interval, the system to collect data from and the output format.



Run Compliance Query - Z9SAMPLE_R

System to run for: *CURRENT system name, *group

Time Interval

From: 06-Apr-2014 00:00:00

To: 06-Apr-2014 23:59:59

Output

☑ Excel

(IFS reports)

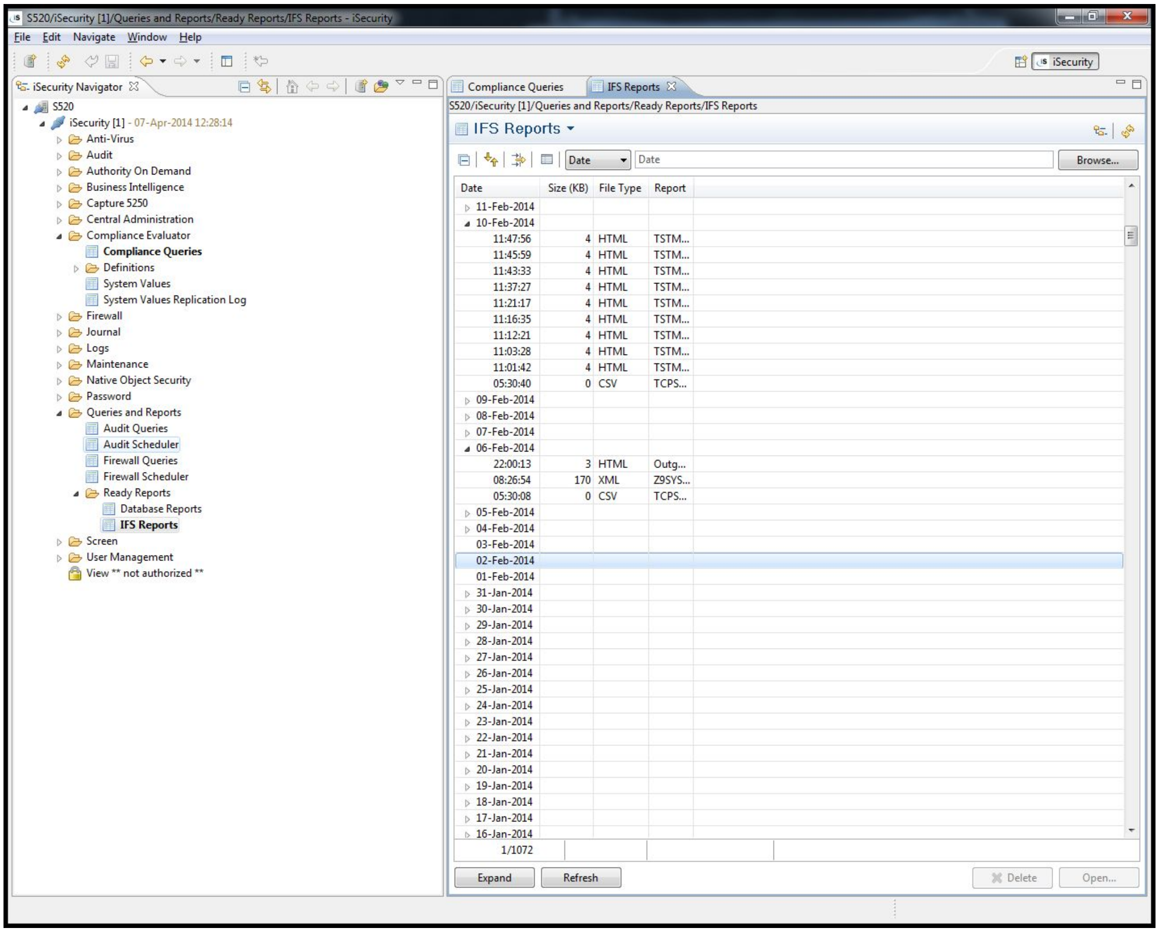
Output template: EVAL3COL

□ Mail to: (mail1,mail2,mail3..)

Additional command parameters:

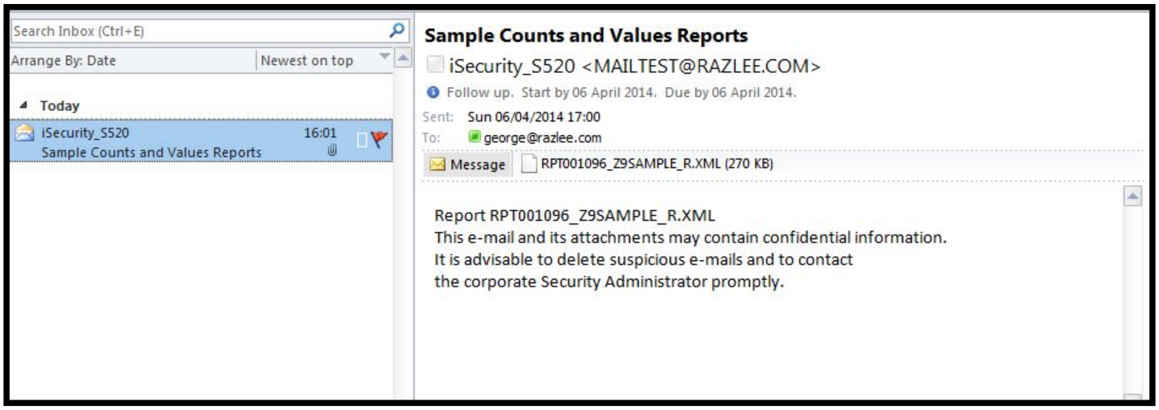
Collect Compliance Check

2. When selecting Excel output (with or without an e-mail address), the report is stored in your system's IFS area. The report can be viewed directly from the GUI by going to **Queries and Reports → Ready Reports → IFS Reports**).



Date	Size (KB)	File Type	Report
▷ 11-Feb-2014			
◢ 10-Feb-2014			
11:47:56	4	HTML	TSTM...
11:45:59	4	HTML	TSTM...
11:43:33	4	HTML	TSTM...
11:37:27	4	HTML	TSTM...
11:21:17	4	HTML	TSTM...
11:16:35	4	HTML	TSTM...
11:12:21	4	HTML	TSTM...
11:03:28	4	HTML	TSTM...
11:01:42	4	HTML	TSTM...
05:30:40	0	CSV	TCPS...
▷ 09-Feb-2014			
▷ 08-Feb-2014			
▷ 07-Feb-2014			
◢ 06-Feb-2014			
22:00:13	3	HTML	Outg...
08:26:54	170	XML	Z9SYS...
05:30:08	0	CSV	TCPS...
▷ 05-Feb-2014			
▷ 04-Feb-2014			
03-Feb-2014			
02-Feb-2014			
01-Feb-2014			
▷ 31-Jan-2014			
▷ 30-Jan-2014			
▷ 29-Jan-2014			
▷ 28-Jan-2014			
▷ 27-Jan-2014			
▷ 26-Jan-2014			
▷ 25-Jan-2014			
▷ 24-Jan-2014			
▷ 23-Jan-2014			
▷ 22-Jan-2014			
▷ 21-Jan-2014			
▷ 20-Jan-2014			
▷ 19-Jan-2014			
▷ 18-Jan-2014			
▷ 17-Jan-2014			
▷ 16-Jan-2014			

View IFS Reports from the GUI



Sample Counts and Values Reports

iSecurity_S520 <MAILTEST@RAZLEE.COM>

Follow up. Start by 06 April 2014. Due by 06 April 2014.

Sent: Sun 06/04/2014 17:00

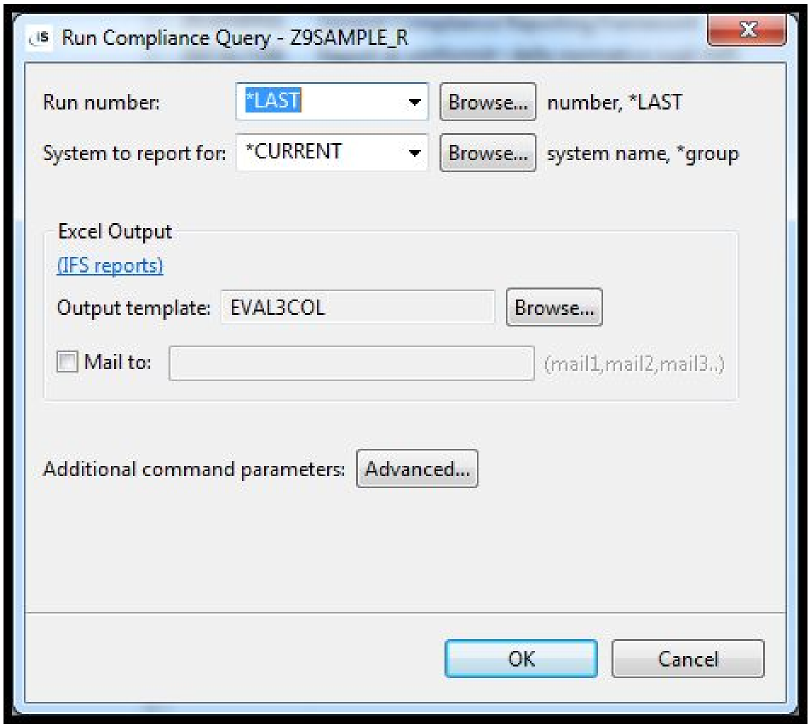
To: george@razlee.com

RPT001096_Z9SAMPLE_R.XML (270 KB)

Report RPT001096_Z9SAMPLE_R.XML
This e-mail and its attachments may contain confidential information.
It is advisable to delete suspicious e-mails and to contact
the corporate Security Administrator promptly.

Excel Report Sent to Email

3. To view the Compliance query, click **Report**. Select Run number by ID or date, system to report for, output parameters and click **OK** to confirm.



Run Compliance Query - Z9SAMPLE_R

Run number: *LAST Browse... number, *LAST

System to report for: *CURRENT Browse... system name, *group

Excel Output

(IFS reports)

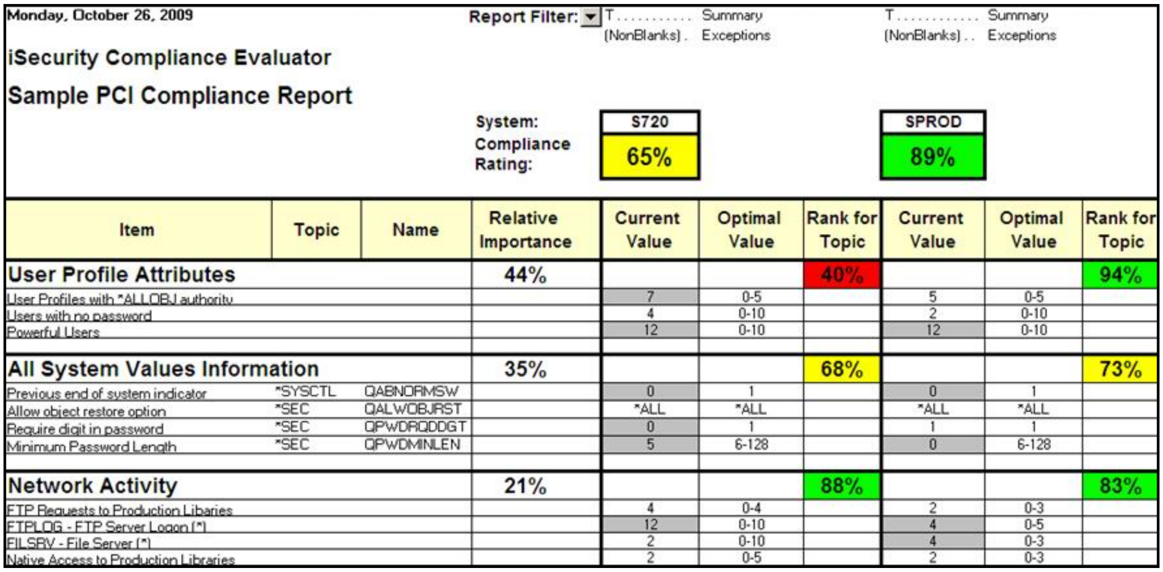
Output template: EVAL3COL Browse...

□ Mail to: (mail1,mail2,mail3..)

Additional command parameters: Advanced...

Run Compliance Check

4. The report will be displayed as an Excel spreadsheet on your PC. The report can be manipulated, saved to the PC's hard disk, and so on.



Monday, October 26, 2009

Report Filter: T........... (NonBlanks) . Summary Exceptions T............ (NonBlanks) . . Summary Exceptions

iSecurity Compliance Evaluator

Sample PCI Compliance Report

				System: Compliance Rating:	S720 65%			SPROD 89%		
Item	**Topic**	**Name**	**Relative Importance**	**Current Value**	**Optimal Value**	**Rank for Topic**	**Current Value**	**Optimal Value**	**Rank for Topic**
User Profile Attributes			**44%**			40%			94%
User Profiles with *ALLOBJ authority				7	0-5		5	0-5	
Users with no password				4	0-10		2	0-10	
Powerful Users				12	0-10		12	0-10	
All System Values Information			**35%**			68%			73%
Previous end of system indicator	*SYSCTL	QABNORMSW		0	1		0	1	
Allow object restore option	*SEC	QALWOBJRST		*ALL	*ALL		*ALL	*ALL	
Require digit in password	*SEC	QPWDRQDDGT		0	1		1	1	
Minimum Password Length	*SEC	QPWDMINLEN		5	6-128		0	6-128	
Network Activity			**21%**			88%			83%
FTP Requests to Production Libaries				4	0-4		2	0-3	
FTPLOG - FTP Server Logon (*)				12	0-10		4	0-5	
FILSRV - File Server (*)				2	0-10		4	0-3	
Native Access to Production Libraries				2	0-5		2	0-3	

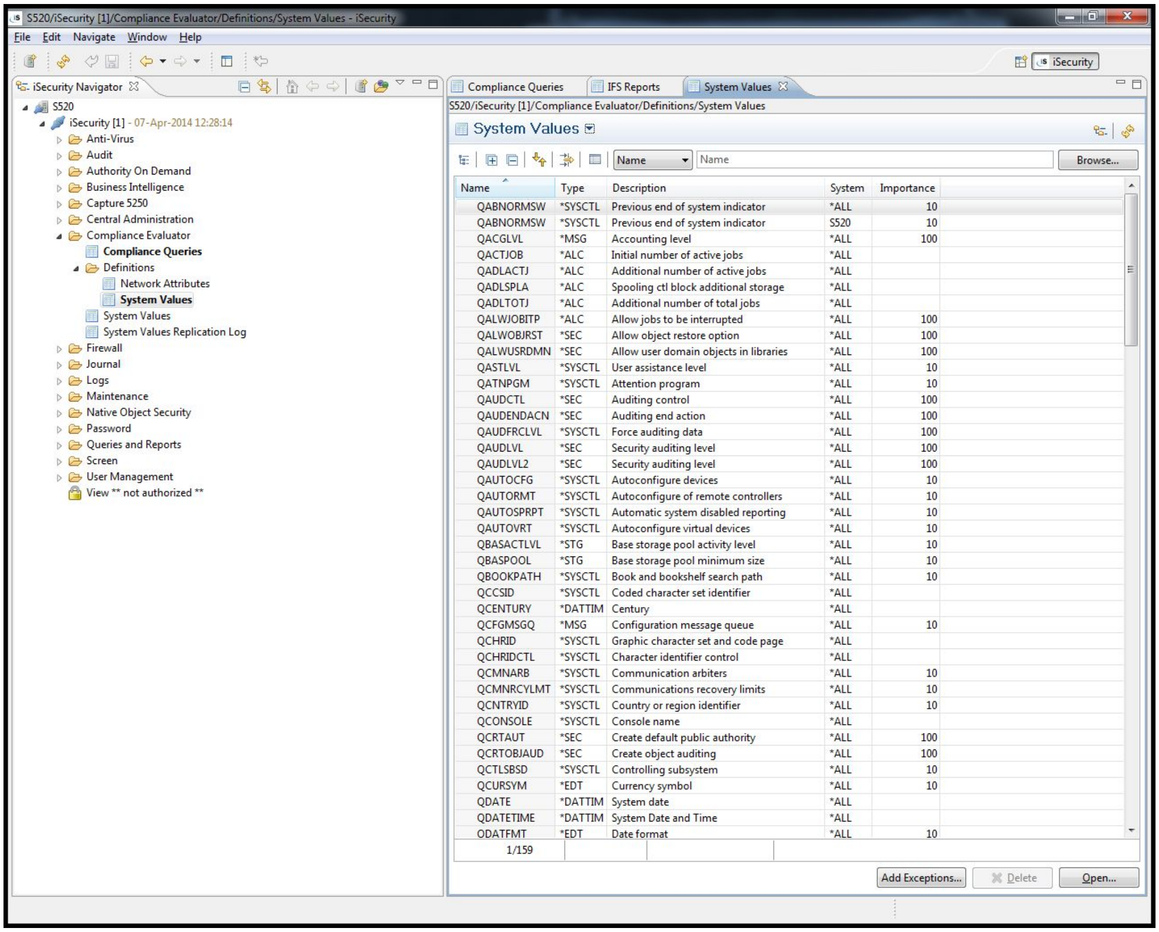
Excel Report

Network Attributes and System Values

Clicking the **Network Attributes** or the **System Values** tree nodes will list the appropriate information, including a short description, the relevant systems and the value's importance.

The list can be manipulated like any iSecurity GUI table, including sorting by any of the columns, filtering, and so on.

In the screenshot below, the definition for QABNORMSW appears twice, once for system S520 and once for all other systems. This means that the scoring for System Value QABNORMSW has been defined differently for S520 (which could be our TEST system).



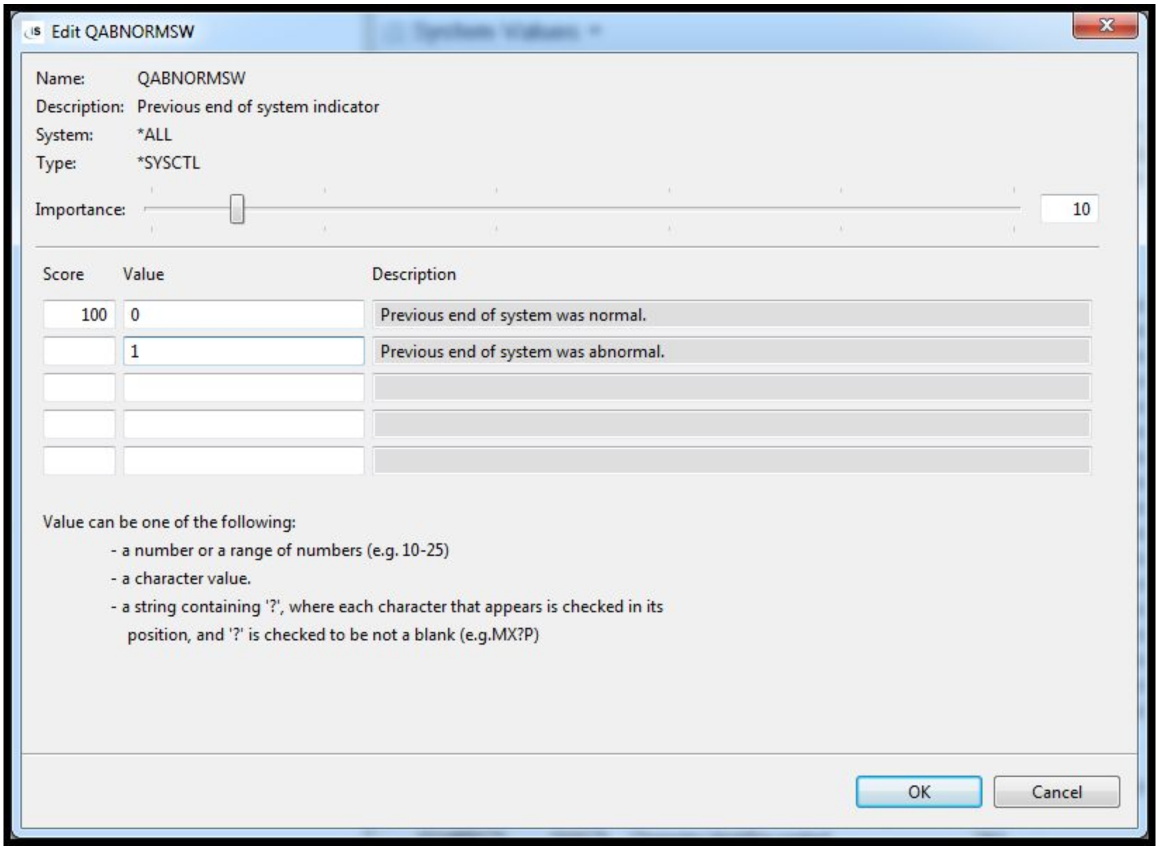
Name	Type	Description	System	Importance
QABNORMSW	*SYSCTL	Previous end of system indicator	*ALL	10
QABNORMSW	*SYSCTL	Previous end of system indicator	S520	10
QACGLVL	*MSG	Accounting level	*ALL	100
QACTJOB	*ALC	Initial number of active jobs	*ALL	
QADLACTJ	*ALC	Additional number of active jobs	*ALL	
QADLSPLA	*ALC	Spooling ctl block additional storage	*ALL	
QADLTOTJ	*ALC	Additional number of total jobs	*ALL	
QALWJOBITP	*ALC	Allow jobs to be interrupted	*ALL	100
QALWOBJRST	*SEC	Allow object restore option	*ALL	100
QALWUSRDMN	*SEC	Allow user domain objects in libraries	*ALL	100
QASTLVL	*SYSCTL	User assistance level	*ALL	10
QATNPGM	*SYSCTL	Attention program	*ALL	10
QAUDCTL	*SEC	Auditing control	*ALL	100
QAUDENDACN	*SEC	Auditing end action	*ALL	100
QAUDFRCLVL	*SYSCTL	Force auditing data	*ALL	100
QAUDLVL	*SEC	Security auditing level	*ALL	100
QAUDLVL2	*SEC	Security auditing level	*ALL	100
QAUTOCFG	*SYSCTL	Autoconfigure devices	*ALL	10
QAUTORMT	*SYSCTL	Autoconfigure of remote controllers	*ALL	10
QAUTOSPRPT	*SYSCTL	Automatic system disabled reporting	*ALL	10
QAUTOVRT	*SYSCTL	Autoconfigure virtual devices	*ALL	10
QBASACTLVL	*STG	Base storage pool activity level	*ALL	10
QBASPOOL	*STG	Base storage pool minimum size	*ALL	10
QBOOKPATH	*SYSCTL	Book and bookshelf search path	*ALL	10
QCCSID	*SYSCTL	Coded character set identifier	*ALL	
QCENTURY	*DATTIM	Century	*ALL	
QCFGMSGQ	*MSG	Configuration message queue	*ALL	10
QCHRID	*SYSCTL	Graphic character set and code page	*ALL	
QCHRIDCTL	*SYSCTL	Character identifier control	*ALL	
QCMNARB	*SYSCTL	Communication arbiters	*ALL	10
QCMNRCYLMT	*SYSCTL	Communications recovery limits	*ALL	10
QCNTRYID	*SYSCTL	Country or region identifier	*ALL	10
QCONSOLE	*SYSCTL	Console name	*ALL	
QCRTAUT	*SEC	Create default public authority	*ALL	100
QCRTOBJAUD	*SEC	Create object auditing	*ALL	100
QCTLSBSD	*SYSCTL	Controlling subsystem	*ALL	10
QCURSYM	*EDT	Currency symbol	*ALL	10
QDATE	*DATTIM	System date	*ALL	
QDATETIME	*DATTIM	System Date and Time	*ALL	
QDATFMT	*EDT	Date format	*ALL	10

System Values

Edit Network Attributes/System Values

Importance and score can be edited according to the site's policies and auditor's requirements.

To edit, select a Network Attribute or System Value and double-click it or click **Open**.



Edit QABNORMSW

Name: QABNORMSW
Description: Previous end of system indicator
System: *ALL
Type: *SYSCTL

Importance: 10

Score	Value	Description
100	0	Previous end of system was normal.
	1	Previous end of system was abnormal.

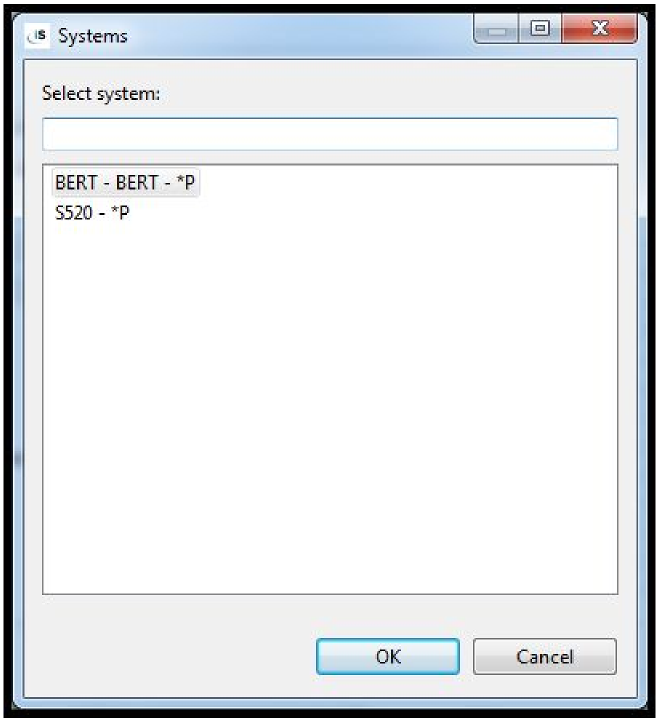
Value can be one of the following:

- a number or a range of numbers (e.g. 10-25)
- a character value.
- a string containing '?', where each character that appears is checked in its position, and '?' is checked to be not a blank (e.g.MX?P)

Edit a particular System Value

Add Exceptions

1. To add score exceptions for a specific Network Attribute or System Value, select its definition (in the line where system is *ALL) and click **Add Exceptions**.
2. Click **Browse…** to select the exception system.



Add Exceptions

3. Select a System, and edit the score as required. Click **OK** to confirm.