iSecMap

Version 3.08

As of June 2026

Kisco Systems LLC
54 Danbury Road, #439
Ridgefield, CT 06877

Phone:	**(518) 897-5002**
E-mail:	**Sales@Kisco.com**
WWW:	**https://www.kisco.com**
Customer Support:	**https://www.kisco.com/ism/support**

Table Of Contents

Introduction . . . 1
- Overview . . . 1
  - What's New in Release 3 . . . 2
  - What Was New in Release 2 . . . 3
- Installation and Security . . . 4
- Kisco Software Support . . . 4
- World Wide Web Support . . . 5

The MASTER Menu . . . 6
- Note on logging . . . 7

Audit Module . . . 8
- Audit Notes . . . 9
- Security System Values . . . 11
- User Profiles . . . 14
- Group Profiles . . . 17
- Authorization Lists . . . 20
- All Libraries . . . 23
- Objects in a Library . . . 26
- IFS Path Objects . . . 30
- Exit Point Registrations . . . 33
- IFS Path Shares . . . 36
- Function Usage . . . 38
- Environment Variables . . . 41

Reporting Module . . . 44

Monitor Module . . . 46
- Starting The Security Monitor . . . 47
- Ending The Security Monitor . . . 48
- Checking The Security Monitor . . . 49
- Run Monitor Immediately . . . 49
- Path Share Monitor . . . 50

Assessment Module . . . 53
- System Values . . . 54
- System Access . . . 57
  - Library Selection . . . 59
- Adopted Authority . . . 61
- User Profiles . . . 64
- Network Services . . . 66
- Authorization Lists . . . 67
- Exception Notes . . . 69
- Assessment Summary . . . 69

Installation and Configuration . . . 70
- Installation from Download . . . 70
- Release Upgrade Installation . . . 70
- Configuring Email for iSecMap . . . 70
- The Install Menu . . . 71
- Display installation status . . . 73
- Change installation status . . . 74
- Permanent installation . . . 74
- Print additional documentation . . . 75
- Display Software Version Information . . . 75
- Work With iSecMap Users . . . 76
- Install Kisco PTF Package . . . 77
- Send Test Email Message . . . 78
- iSecMap Global Settings . . . 79

Introduction

iSecMap is a security administration tool for your IBM i computer system (Power System running IBM i, i5, iSeries and AS/400). Security on the IBM i system is implemented with multiple facets including system values, user profiles, group profiles, authorization lists, library security, exit points, object security and IFS (Integrate File System) security and more. iSecMap is a collection of tools that will help you keep track of all changes in each of these areas. iSecMap will map the current security settings for your system and then allow you to check on security changes that happen on your system. It will also let you do a comprehensive security assessment and includes reporting on your current security configuration.

For the purposes of this documentation, your system will be referred to as an "**IBM i**" system. This term is used generically and applies to all systems in the IBM i family, including your **Power** system, **i5** system, **AS/400** system or your **iSeries**.

Overview

iSecMap now includes multiple modules to help you administer and understand how security is implemented on your system. These include an Audit Module, Reporting Module, Monitor Module and Assessment Module. Each is documented separately in this manual.

When installed, iSecMap will create a baseline of information about security on your system for the Audit Module. This will become your base of security and it represents how security is implemented on your system at the time when iSecMap was installed.

Over time, the Audit Module can then check each of the administered security areas to see if any changes have happened on your system. The changes are reported in detail and you can choose to either accept the new security setting or you can change the setting back to where it was to start with. If you accept a change, it then becomes part of the baseline security.

For library objects and IFS path objects security, you will have to choose which libraries and paths you want to monitor. For each library or IFS path, you can create a baseline at any time and then subsequently check for security changes. The same options to accept new security rules or update objects to change back to the original will be presented.

For the Reporting Module, once the security configuration has been identified, you can then run a series of reports to document that configuration. These can be used for audit purposes.

The Monitor Module will let you automatically check the current security configuration against your base line and report on any changes. This will take the form of an alert that can be issued by sending an email or text message with an indication of which area of system security needs checking.

The Assessment Module will compare your IBM i configuration settings against industry, IBM and Kisco standards and report areas where there are deviations. You can then document accepting those deviations or make adjustment to your configuration to bring your system into compliance.

When you install iSecMap, the user profiles QSECOFR and ISECMAP will be granted administrative authority to the iSecMap software. An Administrator for the software can grant access to the information to users and create additional Administrator profiles. See the section of this documentation on the INSTALL menu options.

What's New in Release 3

The following new features and capabilities have been added:

- A new Assessment module has been added which will look at your system security implementation and let you know where weaknesses exists. It will let you annotate reported weaknesses to indicate that you are aware of them and accept them for your situation.
- The menu structure has been reorganized to match up with the module approach of the new release.
- IFS Path Shares auditing has been added along with associated reporting.
- Function Usage auditing has been added added along with associated reporting.
- Environment Variable auditing has been added added along with associated reporting.
- An option has been added to the Monitor module that will force the monitor process to run immediately without affecting an active periodic monitor already running.

Release 3.03 included the following new features:

- All reports in iSecMap that can be downloaded as CSV files now have column headings added for each field.
- Tracking for exit point changes will now issue an alert if the registered program for any exit point changes.
- The Assessment module now has a new feature added that will assess authorization lists for weak security settings.
- The Monitor module now includes a new feature that lets you track which users are connected to the various file shares in the IFS on your system.

Release 3.07 included the following new features:

- If you are tracking objects within libraries (option 6 on the ISAUDIT menu), Journal Receiver objects are now excluded.
- The Path Share Monitor has been changed so that you can specify a date range when viewing Path Share history.
- Changing the security setting for a library has been made easier when tracking objects in selected libraries.
- Email alerts from the iSecMap Security Monitor have been improved to make them easier to read. The alerts also contain more information.
- When accepting or rejecting changes to the security baseline information, you can now add an explanatory note for future reference. These note are available in the Activity Log.

Release 3.08 included the following new features:

- Email alerts have been reformatted to make them easier to read with more information about the alert situation.
- All options on the ISAUDIT menu have been updated so request an explanatory note for the option taken whether to update the baseline or work with the security setting.
- The Activity Log will now show the note fields when they are available.
- The records captured in the Activity Log change with this release. Prior to this change, every time iSecMap discovered a baseline difference, a new log record was created. This could result in duplicate log records for the same event. With this change, log records for changes from the baseline will only be created when the change is either accepted or rejected.
- The CSV download option for the Activity Log now includes the note fields.
- When created a CSV output from any opton on the ISECLIST menu (Reports) the system name will be included in the CSV file.
- Two new management reports have been added:
    - An Activity Summary report is available for the Activity Log
    - An Assessment Summary report is available for the Assessment Module

  Both management reports include a CSV file output.

What Was New in Release 2

iSecMap had the following new features added to it when release 2 became available:

- Exit Point tracing now includes information about registered programs on each exit point.
- All iSecMap activity is now logged in a history log.
- The alert email subject line can now be specified by the customer.
- The library analysis process lets you see which libraries are being tracked before you select the library you want a report for.
- The library analysis process now lets you run the analysis for all registered libraries, not just one library at a time.
- The IFS analysis process lets you see which paths are being tracked before you select which path you want a report for.
- Reporting options have been improved to simplify selection of subsets to be reviewed.

Installation and Security

Specific installation instructions are covered in the section of this manual titled "Installation". To install your product on trial, follow those instructions. The initial installation will allow iSecMap to run on your system for a period of at least thirty days. At the end of the trial period, the software will no longer function.

When you decide to keep iSecMap, you must send payment to Kisco Systems LLC. At that time, Kisco must know the serial number for your system and the partition number where you have iSecMap installed. If you are not sure of your serial number, you can display it by using option #2 on the INSTALL menu.

When Kisco receives your payment and serial/partition numbers, they will issue a password to you. This password, when applied, will certify your copy of iSecMap and will permanently activate the software on your system. The password and certification instructions will be provided in writing by email.

Kisco Software Support

Kisco Systems LLC software support is available from 7am to 6pm eastern time. You can reach software support with the following methods:

Phone:	518-897-5002
Email:	support@kisco.com
Mail:	Kisco Systems LLC 54 Danbury Road, #439 Ridgefield, CT 06877

Off-hours support can be provided for all registered customers with advance notification. Contact our support staff at least 24 hours in advance when you think you will need off-hours support and we will provide instructions for contacting us during that time. If you have unscheduled off-hours support needs, you should place a phone call and send an email request. Support is generally available during off-hours.

Kisco Systems LLC provides unlimited software support during your first year of ownership. This includes the time during your free trial. Following the first year of ownership, there is a modest fee structure to maintain support for your software.

The Kisco support policy program works as follows:

1. First year support will continue to be FREE! This will include unlimited telephone support, unlimited E-mail support, free release updates and free license transfers.

2. After the first year, an annual charge will apply for support and software maintenance.

3. Support covered by this annual fee includes:

    a. Unlimited telephone support (518-897-5002)
    b. Unlimited E-mail support (Support@kisco.com)
    c. Defect analysis and correction
    d. Free updates to correct known defects (Kisco PTFs)
    e. Free license transfers (when you move to a different system)

4. Customers must be active on maintenance in order to get a license transfer for the software to a new serial number.

At the end of your first year of ownership, you will receive a quote from us for your next year's maintenance charge. To start the renewal process, accept the quote and an invoice will be sent to you.

World Wide Web Support

You can also use the World Wide Web to reach us and to obtain software support information. Just set your web browser to our web address at:

https://www.kisco.com

Support information specifically for iSecMap can be found at this address:

https://www.kisco.com/ism/support

At our Website, you will find:

- Product information about all Kisco software products for the IBM i.
- Customer support information including:
  - Latest release level information for all products
  - Technical bulletins
  - Frequently asked questions and answers
  - Problem reports including iSecMap PTF availability
  - Descriptions for recent enhancements to products
  - E-mail contact information for getting in touch with us
- Information about consulting services available from Kisco Systems LLC.
- Registration for automatic notification about iSecMap enhancements and changes.
- ..... and more

The first time you visit the Customer support section of our website for iSecMap, be sure to register for automatic notification. Once you are registered, we will automatically send Email notices to you about upgrades, enhancements and fixes for iSecMap as soon as they become available.

We invite you to visit our Website, use the contact features to let us know what you think. We're always looking for ways to better serve you, our customer.

The MASTER Menu

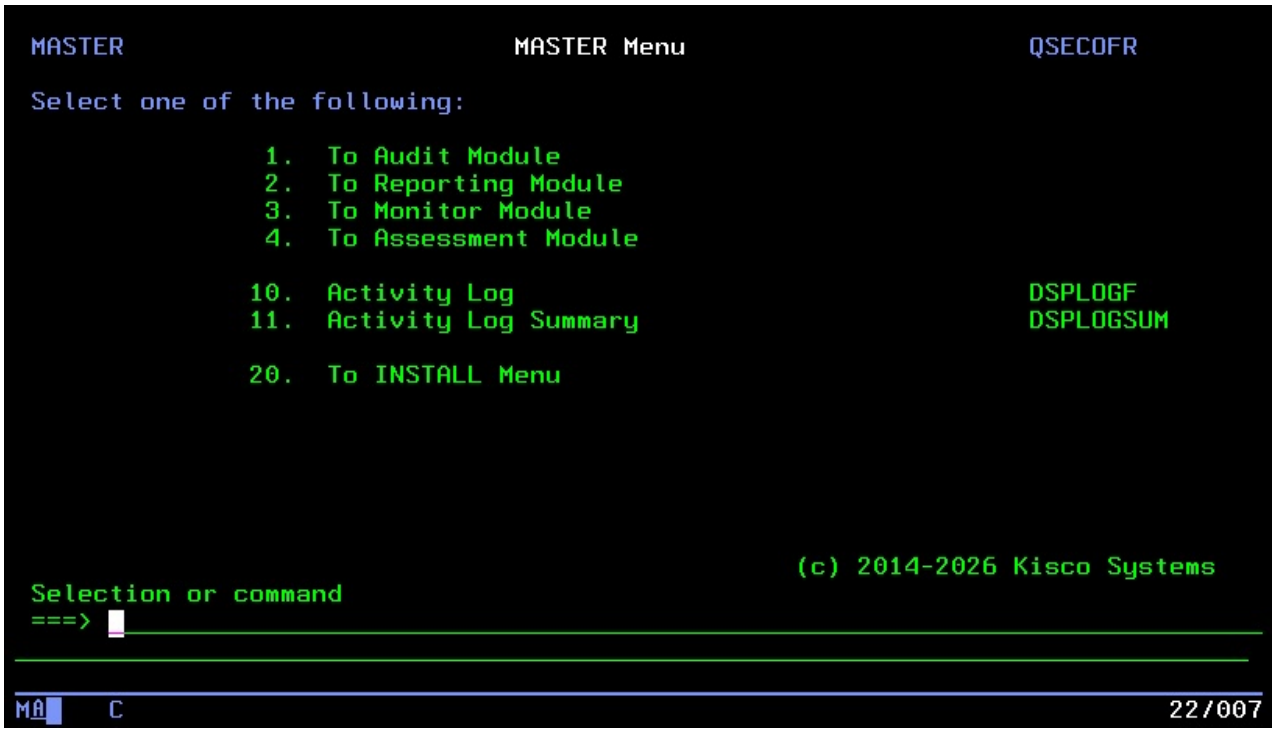
The main menu used by iSecMap is called MASTER and is found in the library ISECLIB. There are several ways to display the menu. You can issue the following GO command from any terminal session command line:

GO ISECLIB/MASTER

This method does not require that the library name be added to your library list. You can also add the library to your library list and display the menu with an easier format. To add the library to your library list and display the menu, enter the following two commands:

ADDLIBLE ISECLIB
GO MASTER

The main iSecMap menu appears as follows:



This is the starting point for all features in iSecMap. Select the option you want to reach the function you want to work with:

1.	Audit Module	Works with your current security implementation to detect changes made since the last time it was mapped.
2.	Reporting Module	Lets you create reports of the current security configuration on your system.
3.	Monitor Module	Lets you set up an automatic monitor to check for security environment changes and alert you when they have been made.

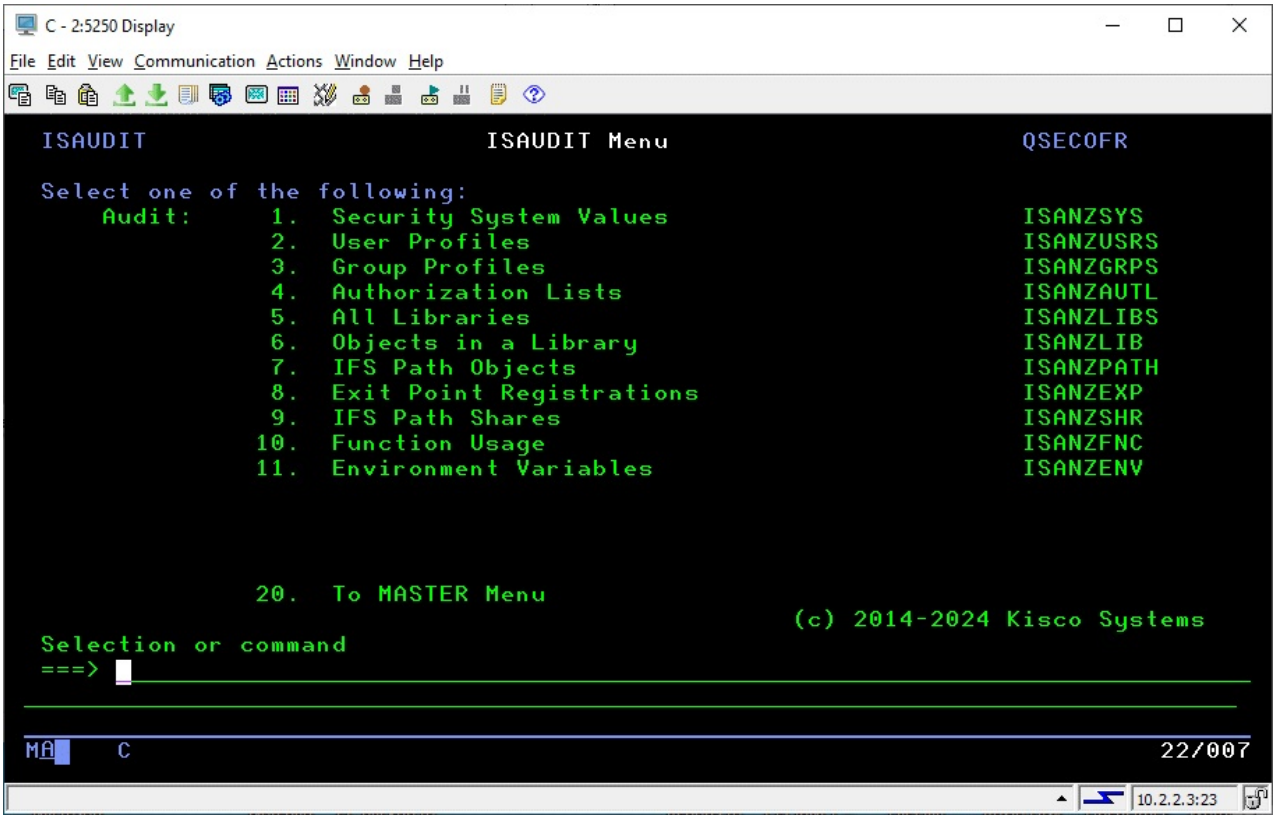
4.	Assessment Module	Lets you check your security implementation against IBM, Kisco and Industry Standards and report on potential weaknesses.
10.	Activity Log	Displays log entries from the iSecMap activity log. When displaying the Activity Log, two function key options are available for use: F6 Will prompt for a start and end date and then generate a CSV version of the Activity Log in the /kisco/ismdnload/ folder in the IFS on your system. F9 Will prompt for a specific date. When entered, all log entries prior to the date given will be purged from the log.
11.	Activity Log Summary	Generates a management summary report of all activity for a given range of dates provided. Output is also generated as a CSV file in the IFS on your system. More information is available using the HELP key (F1) when the command is prompted. **Note**: This report will only show log entries generated following the installation of iSecMap release 3.08 or later.
20.	INSTALL Menu	Transfers you to the INSTALL menu.

Note on logging: In order for logging to contain meaningful information for management reporting purposes, whenever a baseline value is detected, it should be either accepted into the baseline or changed back to its baseline value using iSecMap. If you make a change to the system setting without using iSecMap, the logging may be incomplete.

Each of the modules is discussed in a separate section of this user's guide.

Audit Module

When you select option 1 on the MASTER menu, the Audit Module menu will be shown as follows:



Each menu option handles the following functions. The right margin of the menu display shows the command that is run by that option. All commands are located in the application library named ISECLIB. Each function is described in more detail later in this manual:

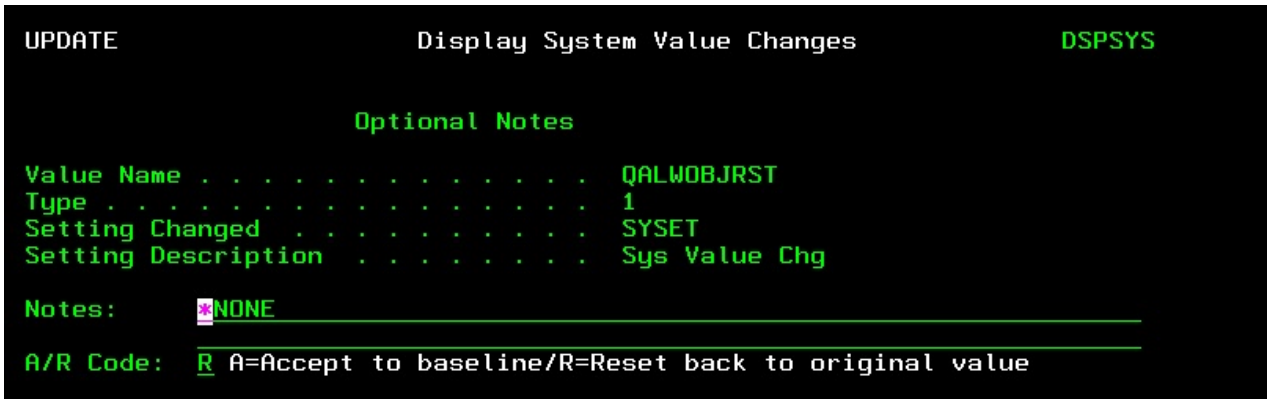
1.	Security System Values	Checks the current security related system values against the baseline and displays changes, with an optional report.
2.	User Profiles	Checks the current user profiles on your system against the baseline and displays changes, with an optional report.
3.	Group Profiles	Checks the current group profiles on your system against the baseline and displays changes, with an optional report.
4.	Authorization Lists	Checks all authorization lists on your system against the baseline and displays changes, with an optional report.
5.	All Libraries	Checks library level security for all libraries on your system against the baseline and displays changes, with an optional report.
6.	Objects in a Library	Checks object level security for all objects in a selected

		library on your system against the baseline and displays changes, with an optional report.
7.	IFS Path Objects	Checks object level security for all objects in a selected IFS path on your system against the baseline and displays changes, with an optional report.
8.	Exit Point Registrations	Checks all exit points on your system for changes in program registration.
9.	IFS Path Shares	Checks IFS paths that are configured to be shared to see if any new shared paths have been created or existing shared paths have been changed or removed.
10.	Function Usage	Checks configured Function registrations to see if any have been changed, added or removed.
11.	Environment Variables	Checks system level Environment Variable to see if any have been added, changed or removed.
20. To MASTER Menu		Switches back to the MASTER menu.

The following sections of this guide will describe how each of these audit functions works.

Audit Notes

Each of these menu options will give you an option to display the audit results in your terminal session with choices to either make changes to your baseline security information (option 8) or make changes to your security settings (option 9). When you choose to take an action, iSecMap will give you an opportunity to record a note about your decision. This will appear in your session on a screen that looks like this:



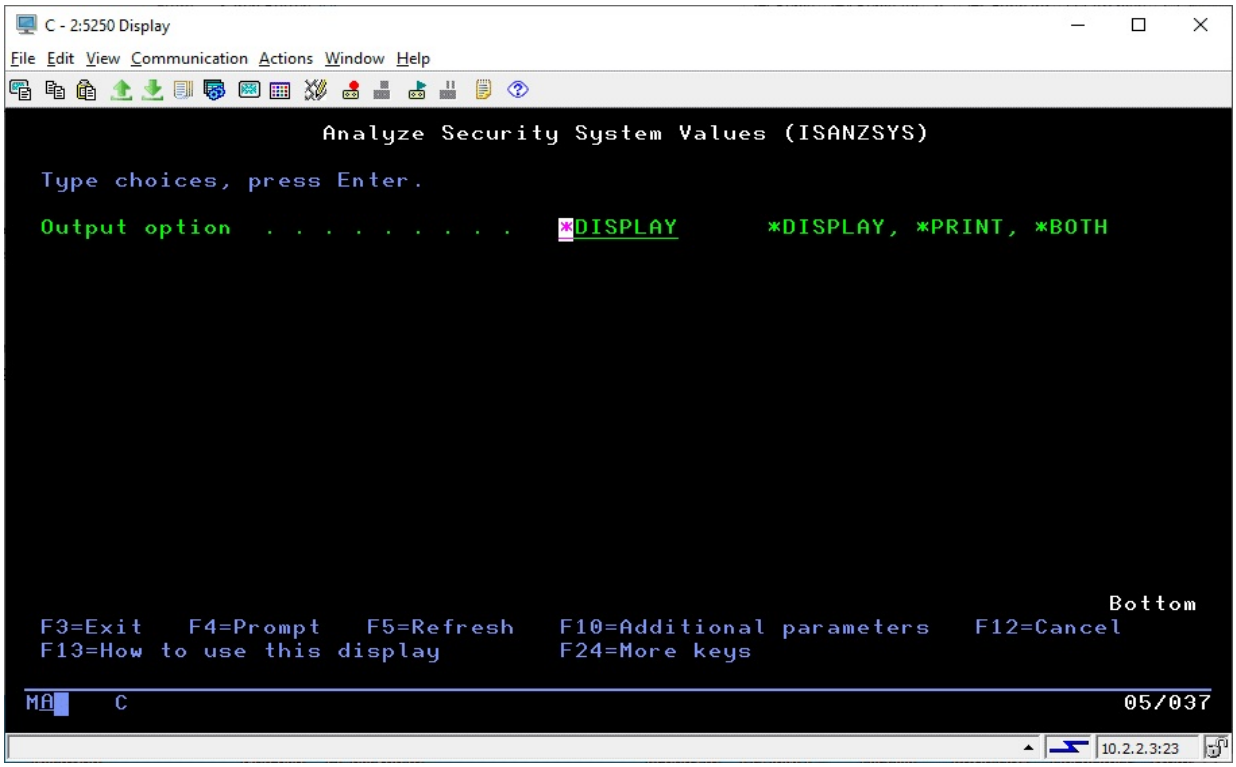
If you don't want to record a note, just press ENTER and your decision will be processed. To record a note, type it in the two fields provided and then press ENTER. These notes can later be reviewed using the Activity Log, option 10 on the MASTER menu.

The A/R Code at the bottom of this display indicates whether the change was accepted into the

baseline values or if it was rejected. When you select option 8 to accept the change into your baseline, this code is pre-filled with the value ‘A’. Choosing option 9 to work with the setting causes this value to be pre-filled with the value ‘R’.

Security System Values

A set of system values are used by the IBM i OS to control security on your system. Option #1 on the Audit menu works with this set of system values. When you select this option, the following parameter screen is shown:



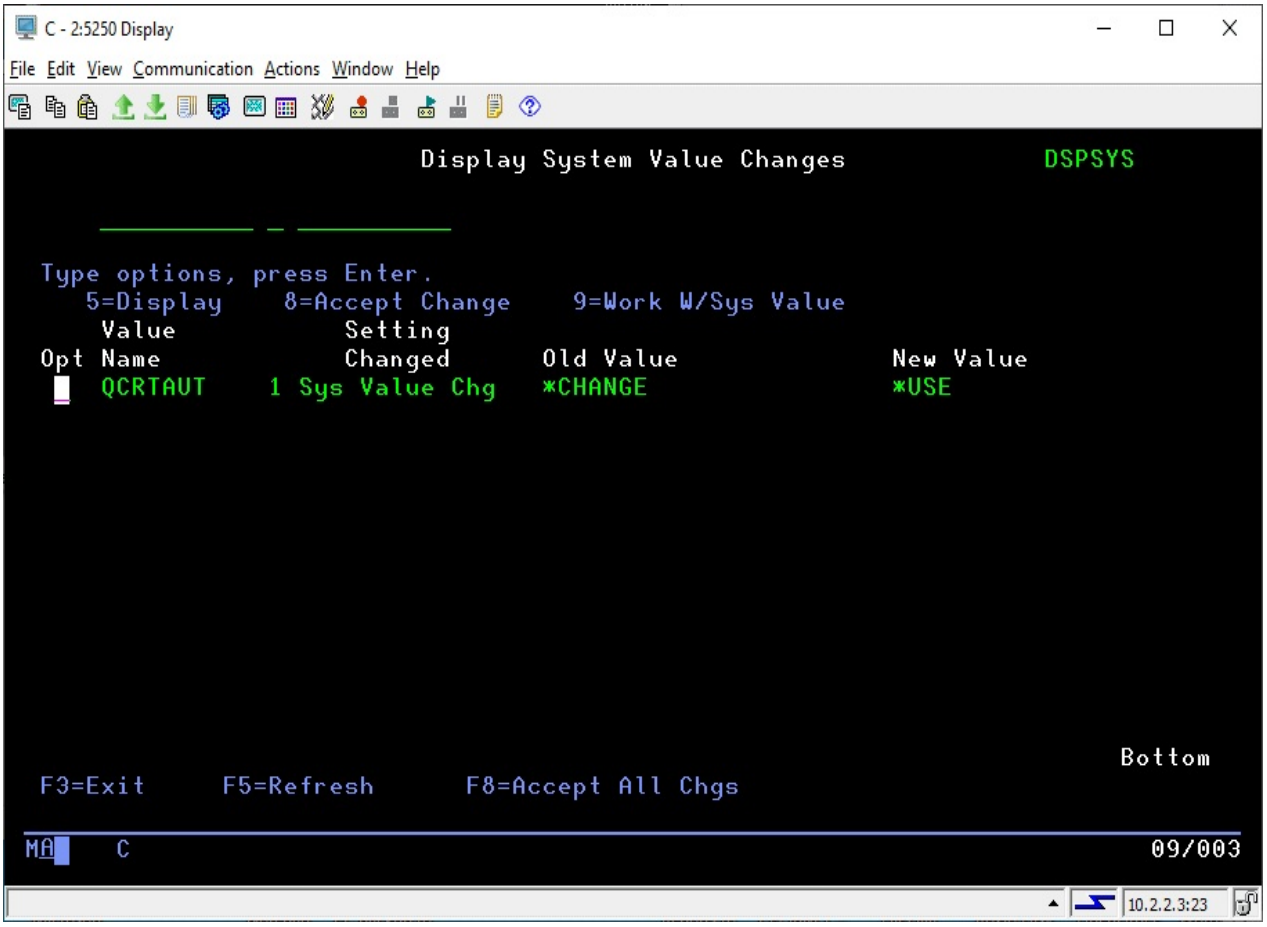
When this check of the security system values is run, you can choose the following output options:

*DISPLAY	The results of the system values check will be shown on your display session. You will be given a chance to work with the system values that have been changed and either set them to a different value or accept the new value into your baseline system value set.
*PRINT	A report of the system values check will be generated.
*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this, but the Analysis Option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to the system values are analyzed and presented, but the baseline set for system values is not changed.
*POST	The changes to the system values are analyzed and presented, but they are then also automatically accepted as the new baseline system values set.
*INIT	The current system values are posted directly to the baseline system values set with no report or display.

When you use the *DISPLAY option, the following will be displayed to show you all security system values that have changed since your baseline values were stored:



In this case, the system value QCRTAUT has been changed from *CHANGE to*USE. If there were no changes recorded, the display will show that fact.

If changes are shown, you can choose the following options:

5 Will just show you additional details. You may want to select this option when the system value changed contains more data than can be displayed on the initial list.

8 This option will let you accept the new system value and post it to your baseline for security system values.

9 This option will start a system function to work with the system value. Choose this option if you decide that you want to set the system value back to what it was originally or some other value.

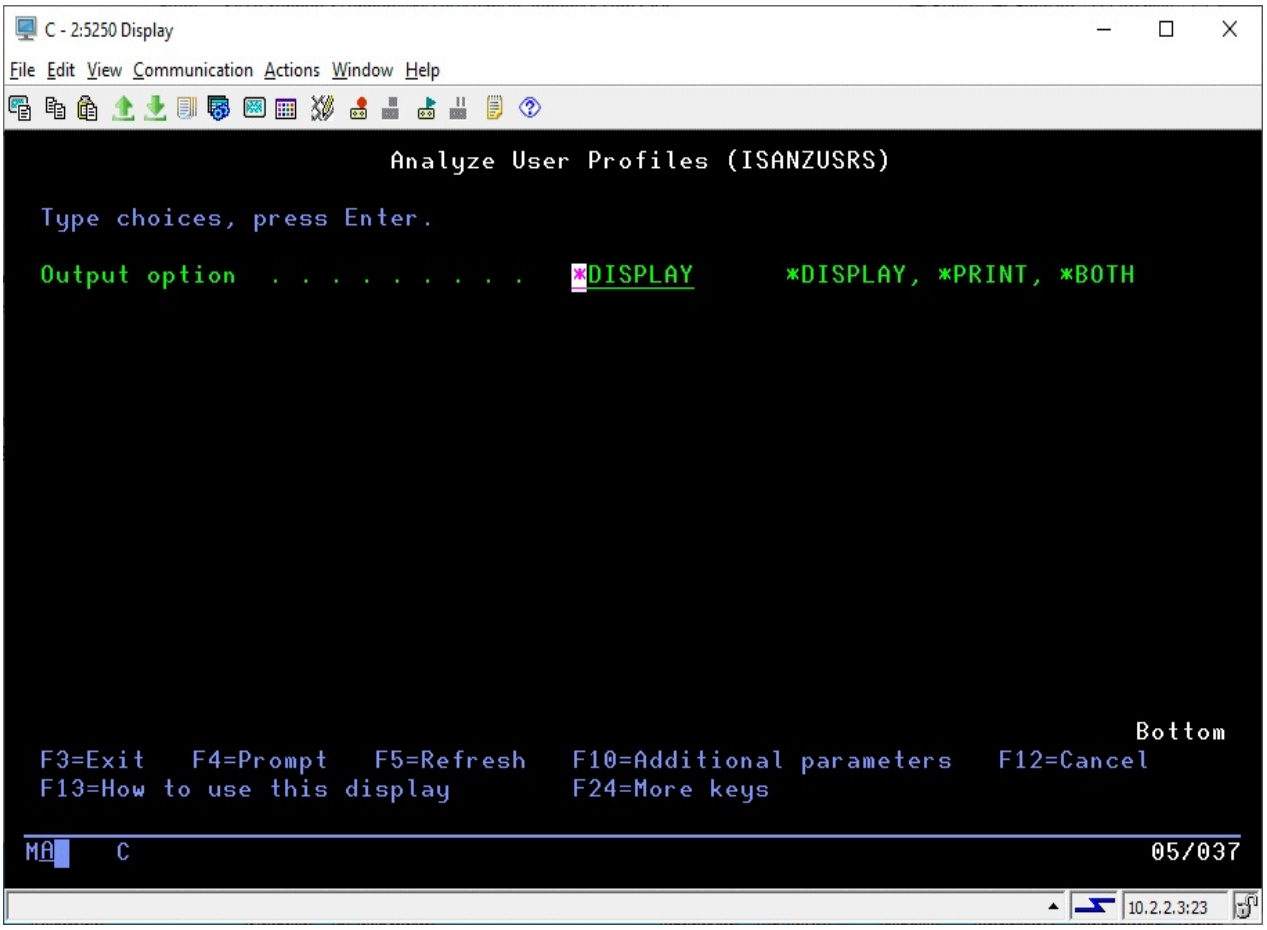
In addition to these line item options, you can also use the F8 function key to simply accept all changes. If you use this option, all changes will be accepted into the baseline security system values stored for your system. Using the F8 function key will also cause iSecMap to restart a new check of the current settings against the new baseline, the results will now be displayed.

When you have made all the changes that you want to make, you can use the F5 function key to refresh the display. The current system values will then be checked against the updated baseline, including any changes that you have posted, and the new results of the check will be displayed.

User Profiles

A key component of system security on the IBM i is the user profile. During installation, iSecMap stores a baseline of information about user profiles on your system along with key security values for each profile.

When you run option #2 on the Audit menu, iSecMap will check your current user profiles and compare them to the baseline information already stored. When you select the menu option, the following prompt will be shown:



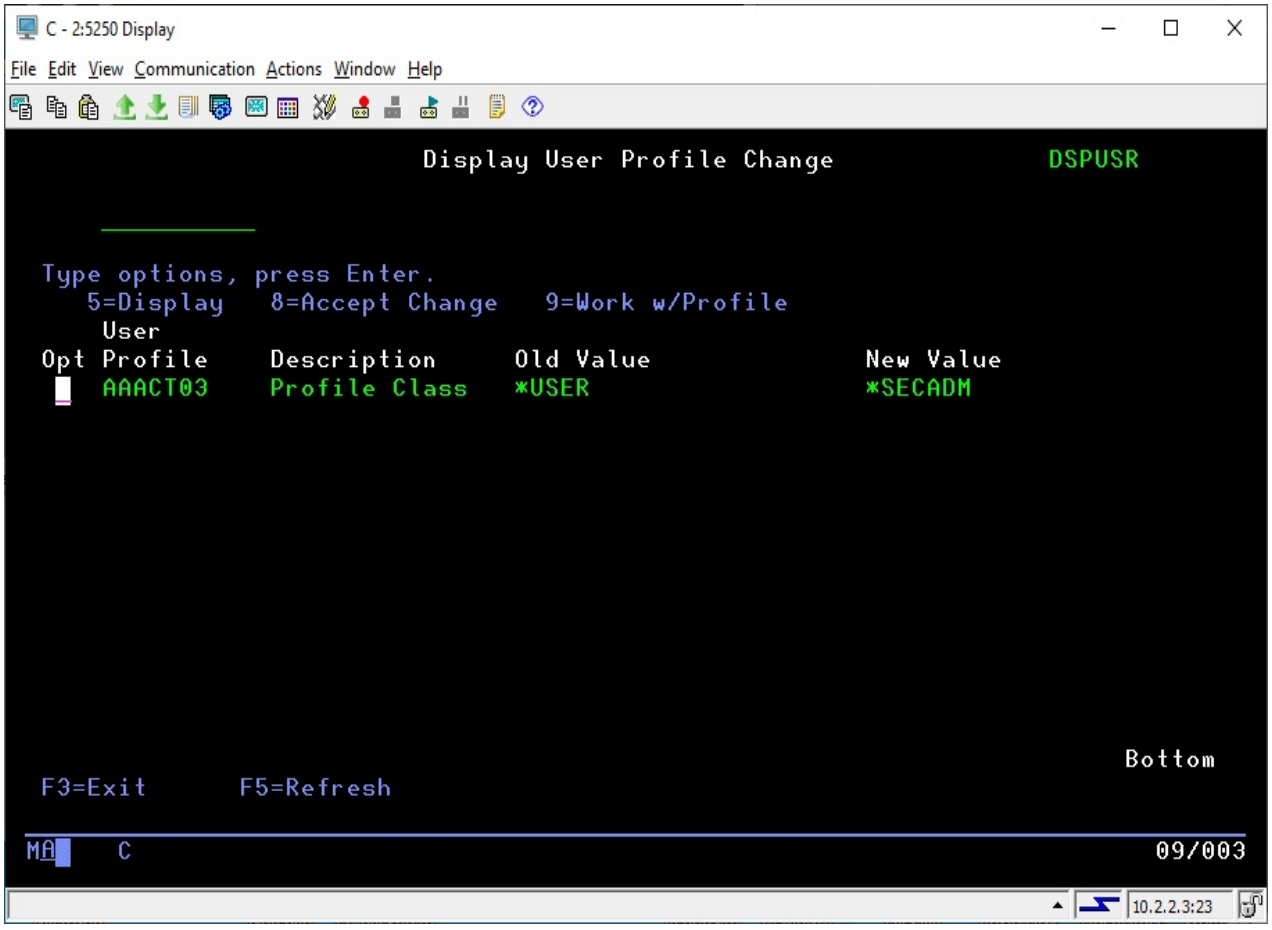
When this check of the user profiles is run, you can choose the following output options:

*DISPLAY	The results of the user profiles check will be shown on your display session. You will be given a chance to work with the profiles that have been changed and either set them to a different value or accept the new value into your baseline user profile set.
*PRINT	A report of the user profiles check will be generated.
*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this, but the Analysis Option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to the user profiles are analyzed and presented, but the baseline set for user profiles is not changed.
*POST	The changes to the user profiles are analyzed and presented, but they are then also automatically accepted as the new baseline user profile set.
*INIT	The current system values are posted directly to the baseline user profile set.

When the user profile check runs, if there are any differences between the current user profiles and the baseline, then the following display will appear:



In the case shown above, a user profile has been changed from a profile class of *USER to have security administrative authority (*SECADM).

If changes are shown, you can choose the following options:

5 Will just show you additional details. You may want to select this option when the User profile information changed contains more data than can be displayed on the initial list.

8 This option will let you accept the user profile change and post it to your baseline for user profiles.

9 This option will start a system function to maintain the user profile. Choose this option if

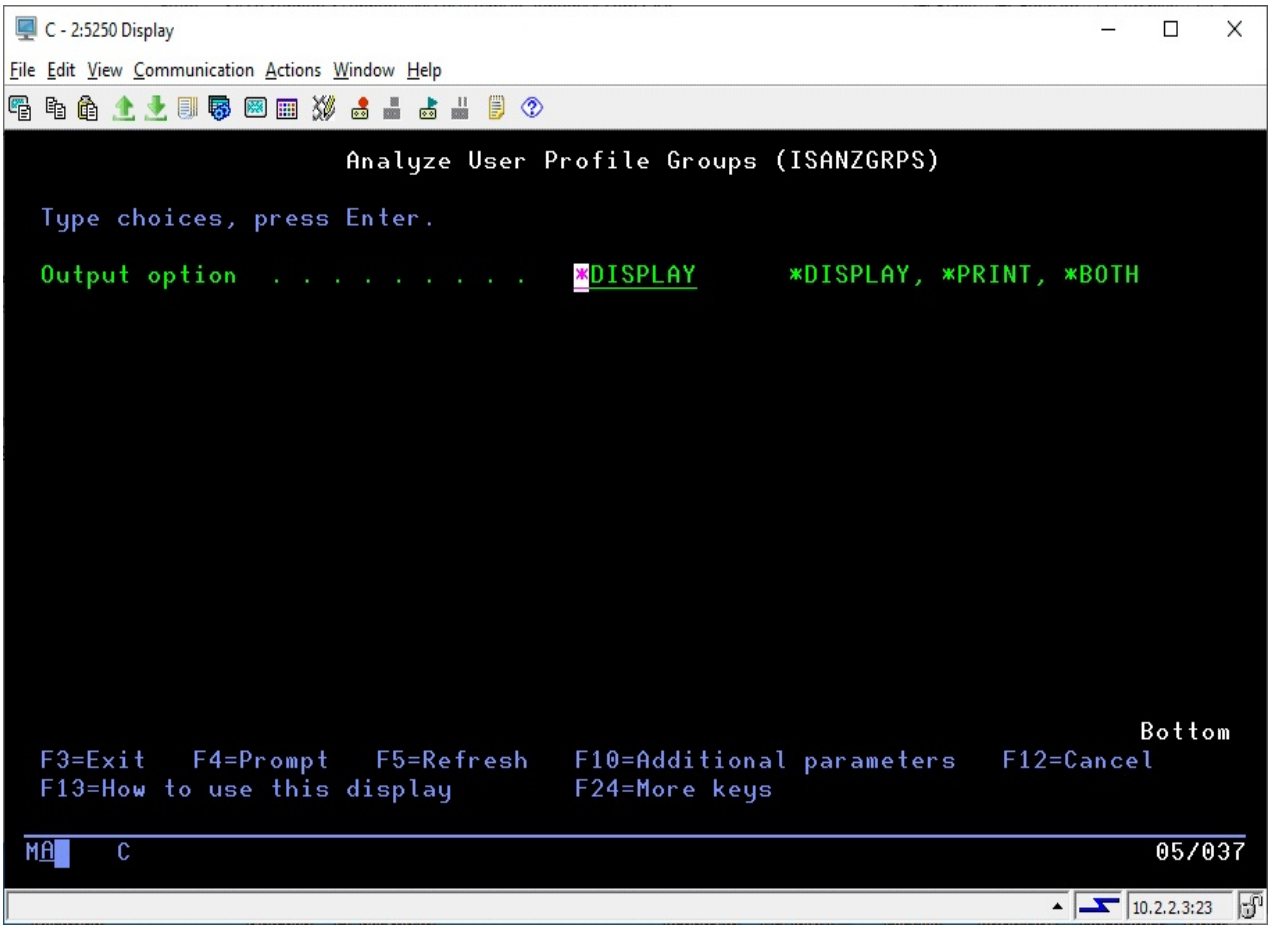
you decide that you want to set the User profile back to what it was originally.

Once you have made some changes to the user profile base, you can use the F5 refresh key to re-check the current user profiles against the updated baseline and see if there are any changes now remaining that need to be dealt with.

Group Profiles

Another key component of system security on the IBM i are the group user profiles. This includes both group profiles and supplemental group profiles. During installation, iSecMap stores a baseline of information about group user profiles on your system.

When you run option #3 on the Audit menu, iSecMap will check your current group profiles and compare them to the baseline information already stored. When you select the menu option, the following prompt will be shown:



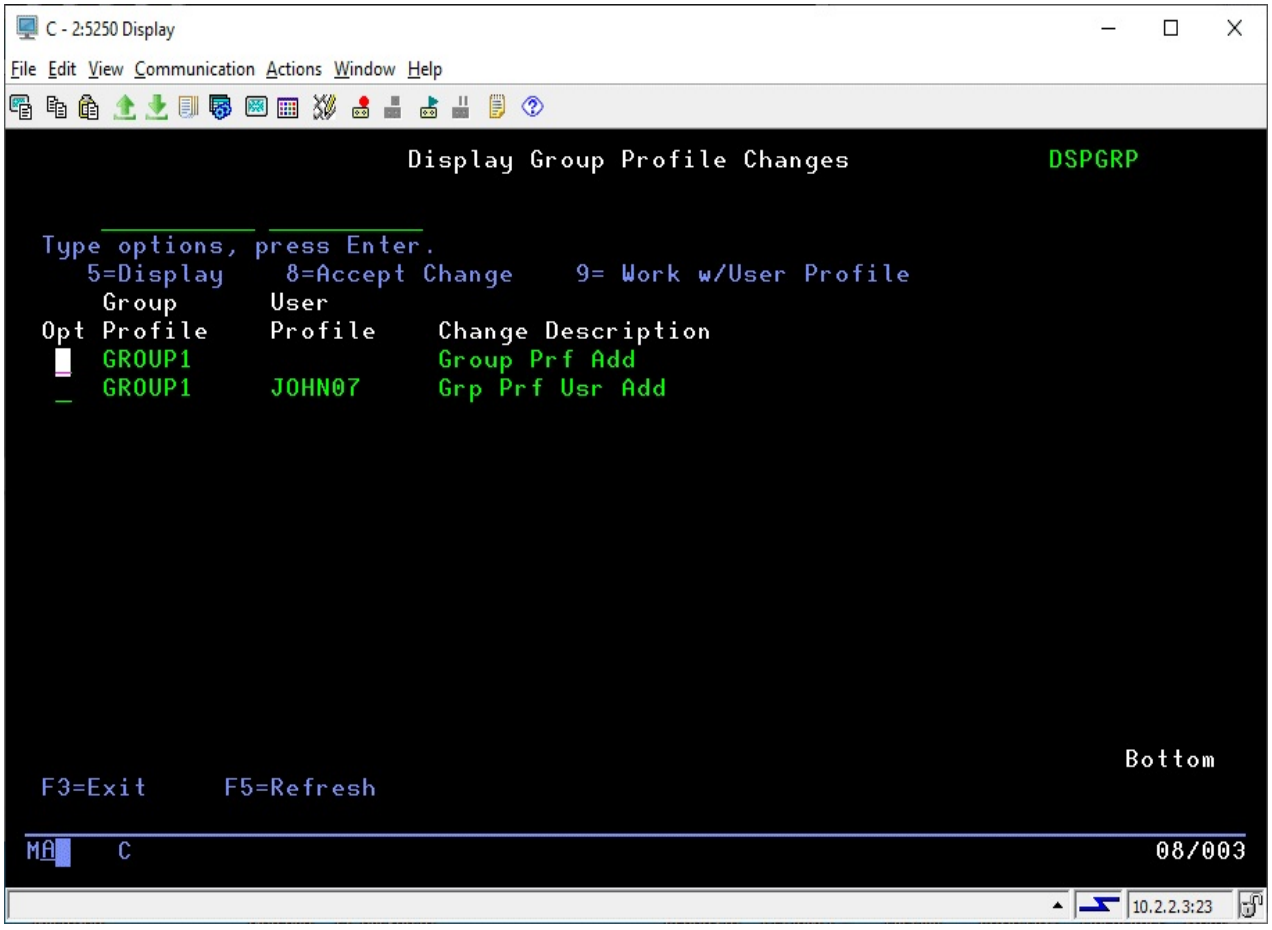
When this check of the group profiles is run, you can choose the following output options:

*DISPLAY	The results of the group profile check will be shown on your display session. You will be given a chance to work with the profiles that have been changed and either set them to a different value or accept the new value into your baseline group profile set.
*PRINT	A report of the group profile check will be generated.
*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this, but the Analysis Option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to the group profiles are analyzed and presented, but the baseline set for group profiles is not changed.
*POST	The changes to the group profiles are analyzed and presented, but they are then also automatically accepted as the new baseline group profile set.
*INIT	The current group profiles are posted directly to the baseline group profile set.

When the group profile check runs, if there are any differences between the current group profiles and the baseline, then the following display will appear:



In the above example, one new group has been created and one user profile has been assigned to the group.

If changes are shown, you can choose the following options:

5 Will just show you additional details.

8 This option will let you accept the user profile change and post it to your baseline for user profiles.

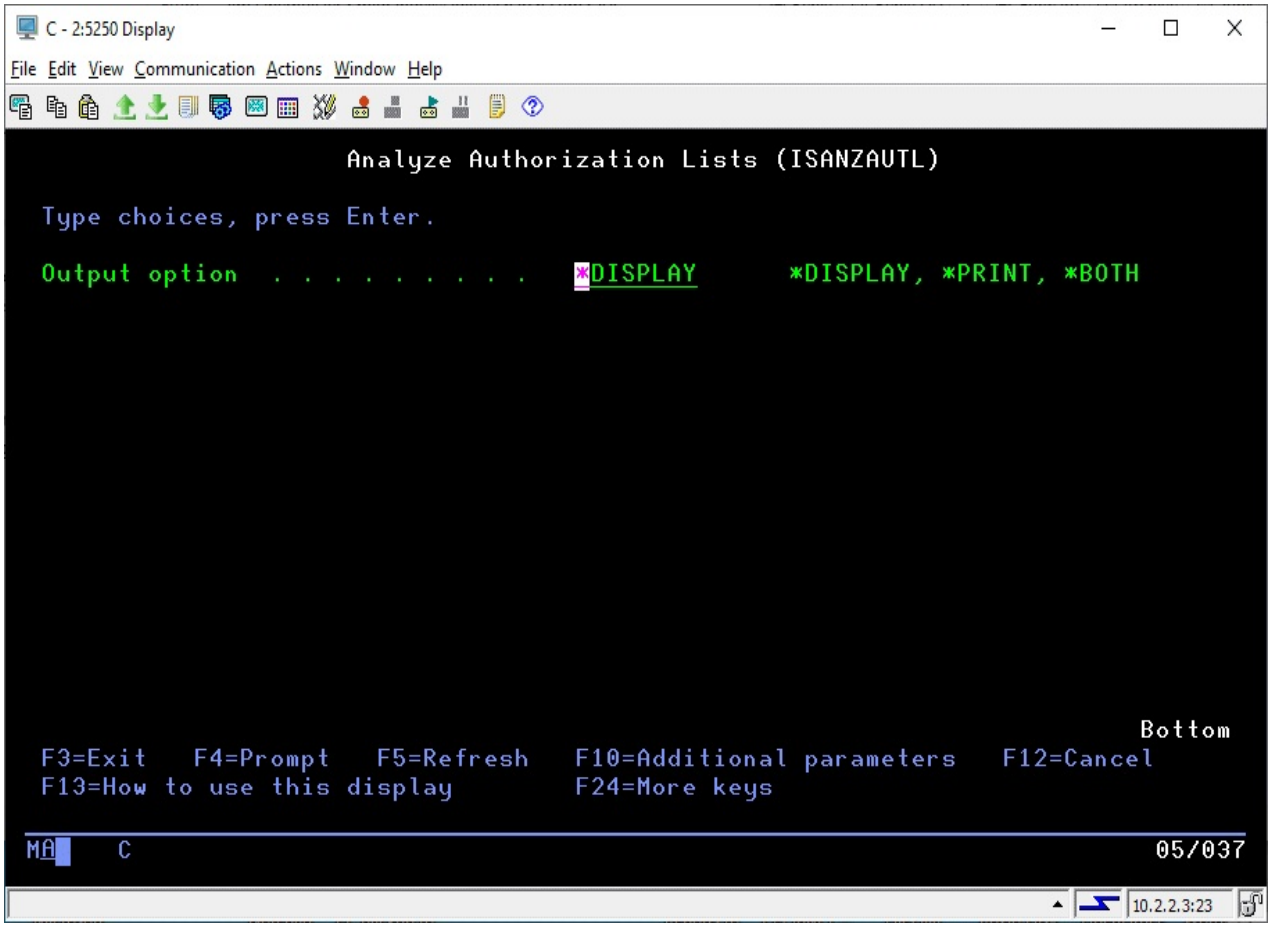
9 This option will start a system function to maintain the user profile. Choose this option if you decide that you want to set the User profile back to what it was originally. This option only works when a profile is shown in the User Profile column of the display.

Once you have made some changes to the group profile base, you can use the F5 refresh key to re-check the current group profiles against the baseline and see if there are any changes now remaining that need to be dealt with.

Authorization Lists

Another key component of system security on the IBM i are the authorization lists. These are special repositories of overall security permissions that can be used for object level security on your system. If an object is secured by a reference to an authorization list, then the system checks for access permissions in the list. During installation, iSecMap stores a baseline of information about authorization lists on your system.

When you run option #4 on the Audit menu, iSecMap will check your authorization lists and compare them to the baseline information already stored. When you select the menu option, the following prompt will be shown:



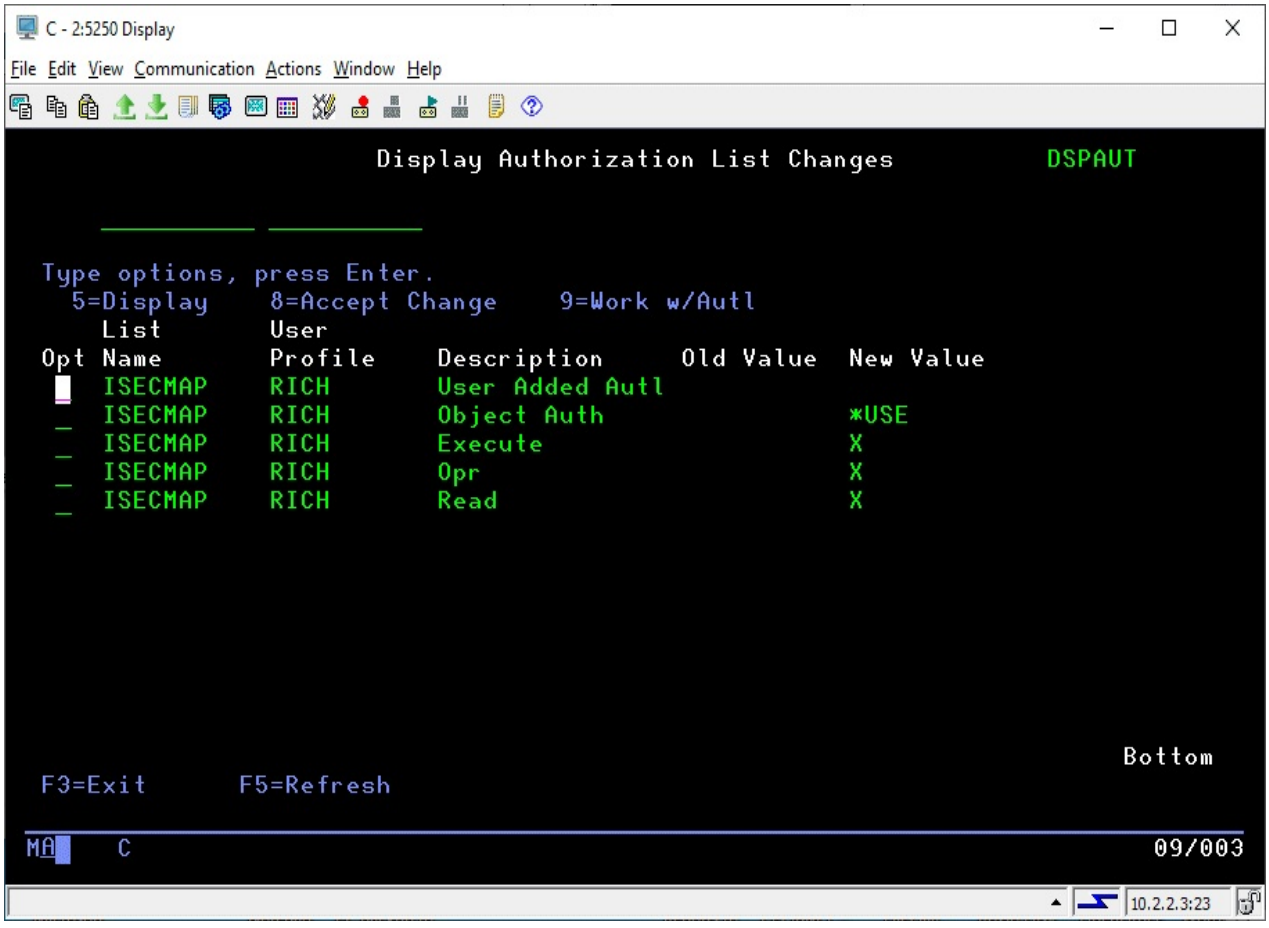
When this check of the authorization lists is run, you can choose the following output options:

*DISPLAY	The results of the authorization list check will be shown on your display session. You will be given a chance to work with the lists that have been changed and either set them to a different values or accept the new value into your baseline authorization list set.
*PRINT	A report of the authorization list check will be generated.
*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this, but the Analysis Option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to the authorization lists are analyzed and presented, but the baseline set for authorization lists is not changed.
*POST	The changes to the authorization list are analyzed and presented, but they are then also automatically accepted as the new baseline authorization list set.
*INIT	The current authorization lists are posted directly to the baseline authorization list set.

When the authorization list check runs, if there are any differences between the current authorization lists and the baseline, then the following display will appear:



In this example, a new user profile has been added to the authorization list that is used to secure the iSecMap software product. The display shows the user added and the specific permissions that have been set up for this new profile.

If changes are shown, you can choose the following options:

5 Will just show you additional details.

8 This option will let you accept the authorization list change and post it to your baseline for authorization lists.

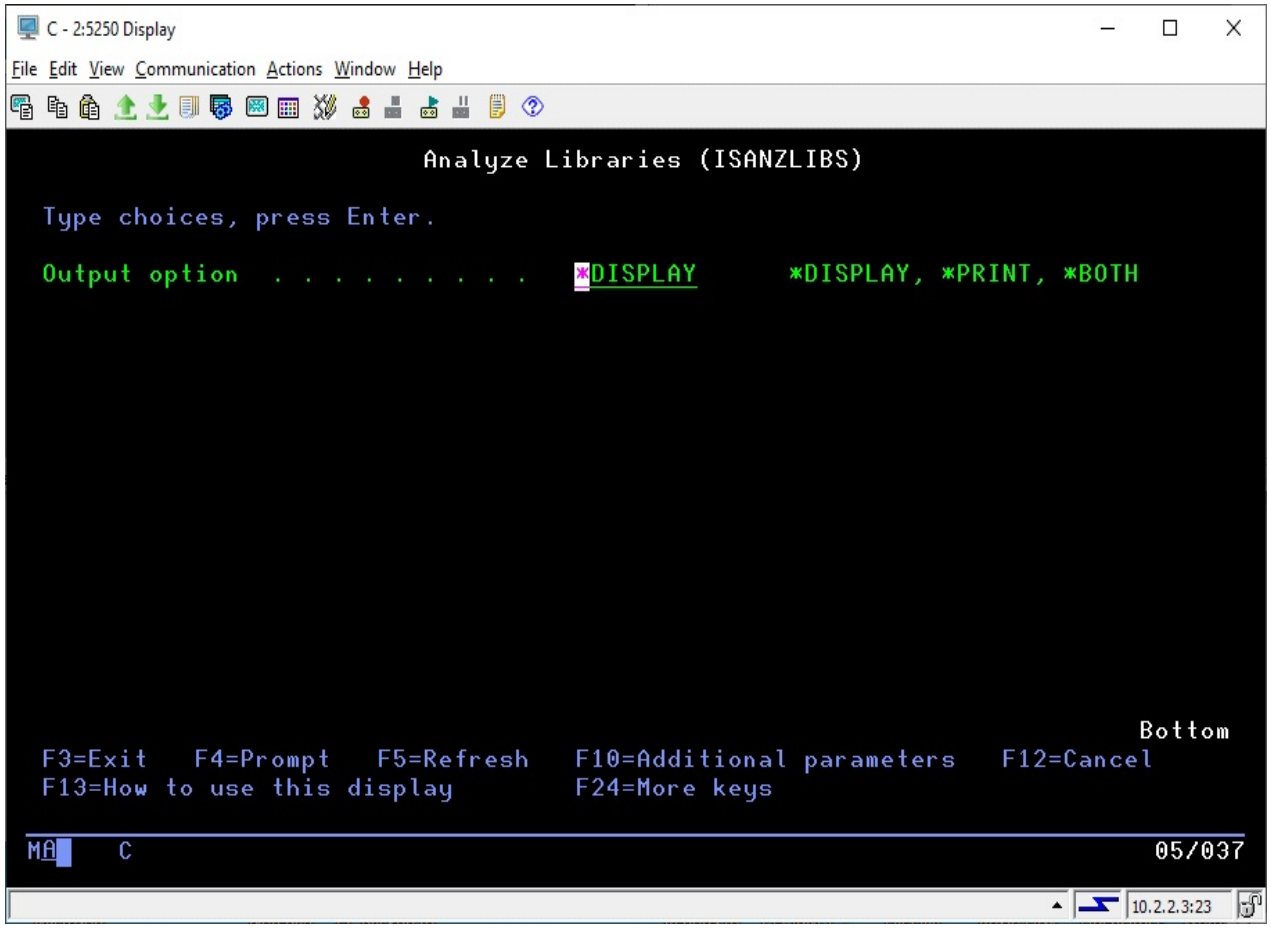
9 This option will start a system function to maintain the authorization list. Choose this option if you decide that you want to set change the authorization list that has been changed. You can change it back to back to what it was originally or make modifications to the permissions that have been granted.

Once you have made some changes to the authorization list base, you can use the F5 refresh key to re-check the current authorization lists against the baseline and see if there are any changes now remaining that need to be dealt with.

All Libraries

Security setting at the IBM i library level are used to apply to all accesses of objects within those libraries. Because of this, the security settings at the library level are also a very important aspect of IBM i security. During installation, iSecMap stores a baseline of information about library level security on your system.

When you run option #5 on the Audit menu, iSecMap will check your library security and compare it to the baseline information already stored. When you select the menu option, the following prompt will be shown:



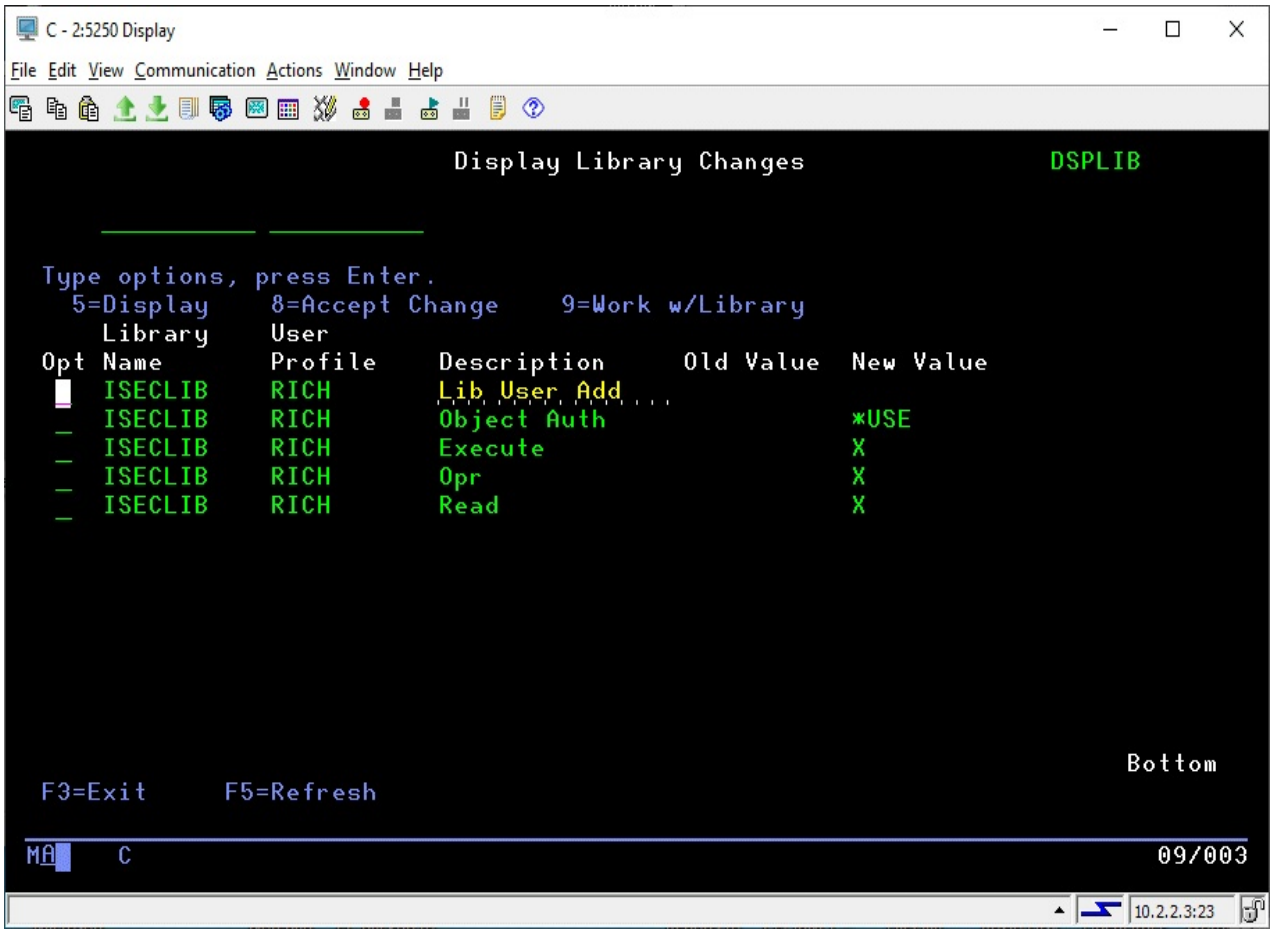
When this check of library security is run, you can choose the following output options:

*DISPLAY	The results of the library security check will be shown on your display session. You will be given a chance to work with the libraries that have been changed and either set them to a different values or accept the new value into your baseline library security set.
*PRINT	A report of the library security check will be generated.
*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this, but the Analysis Option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to library security are analyzed and presented, but the baseline set for library security is not changed.
*POST	The changes to library security are analyzed and presented, but they are then also automatically accepted as the new baseline library security set.
*INIT	The current library security is posted directly to the baseline library security set.

When the library security check runs, if there are any differences between the current library security and the baseline, then the following display will appear:



In the above example, the iSecMap application library ISECLIB has been changed to grant the user profile RICH use access to object in the library (not recommended as this library should always be controlled by the ISECMAP authorization list).

If changes are shown, you can choose the following options:

5 Will just show you additional details.

8 This option will let you accept the library security change and post it to your baseline for library security. This option can only be used on the first line for a listed user profile. The

description on the first line is always highlighted in yellow to make it easy to find.

9 This option will start a system function to maintain the security configuration for the library. Choose this option if you decide that you want to change the library security that has been altered. You can change it back to back to what it was originally or make modifications to the permissions that have been granted.

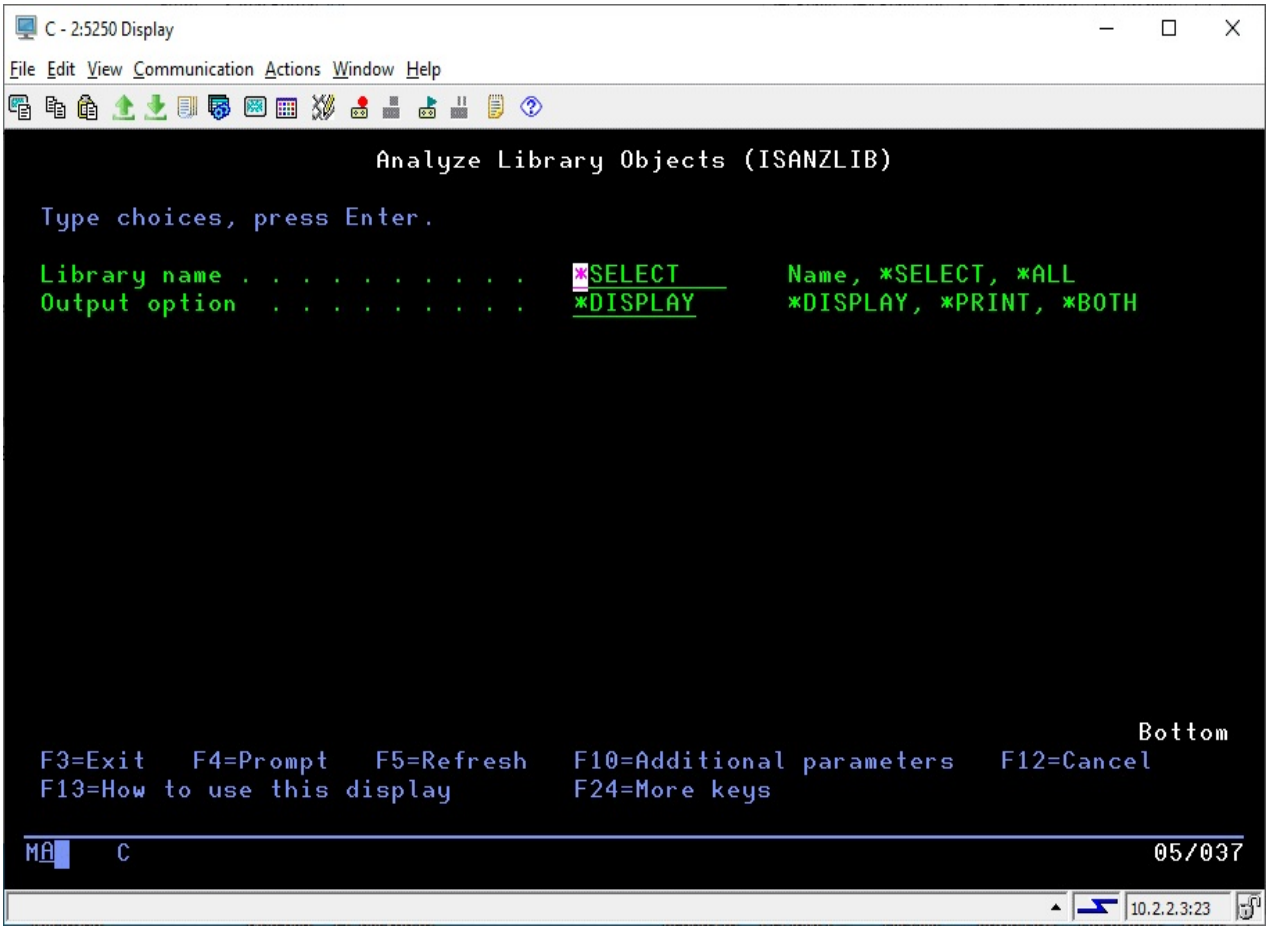
Once you have made some changes to the library security base, you can use the F5 refresh key to re-check the current library security against the baseline and see if there are any changes now remaining that need to be dealt with.

Objects in a Library

For certain libraries on your system, you will want to track security settings down to the object level within the library. iSecMap supports this. To establish a baseline for a library, that library must first be initialized. This initialization process creates the baseline for current security configuration for all objects in the library.

Once a baseline has been established, you can then check the current security settings for all objects against the stored baseline and see what has changed.

When you run option #6 on the Audit menu, iSecMap will check your library object security and compare to the baseline information already stored. When you select the menu option, the following prompt will be shown:



When this check of library object security is run, you can choose the following output options:

Library name — To process a specific library, enter that library name. The following special values can also be used:

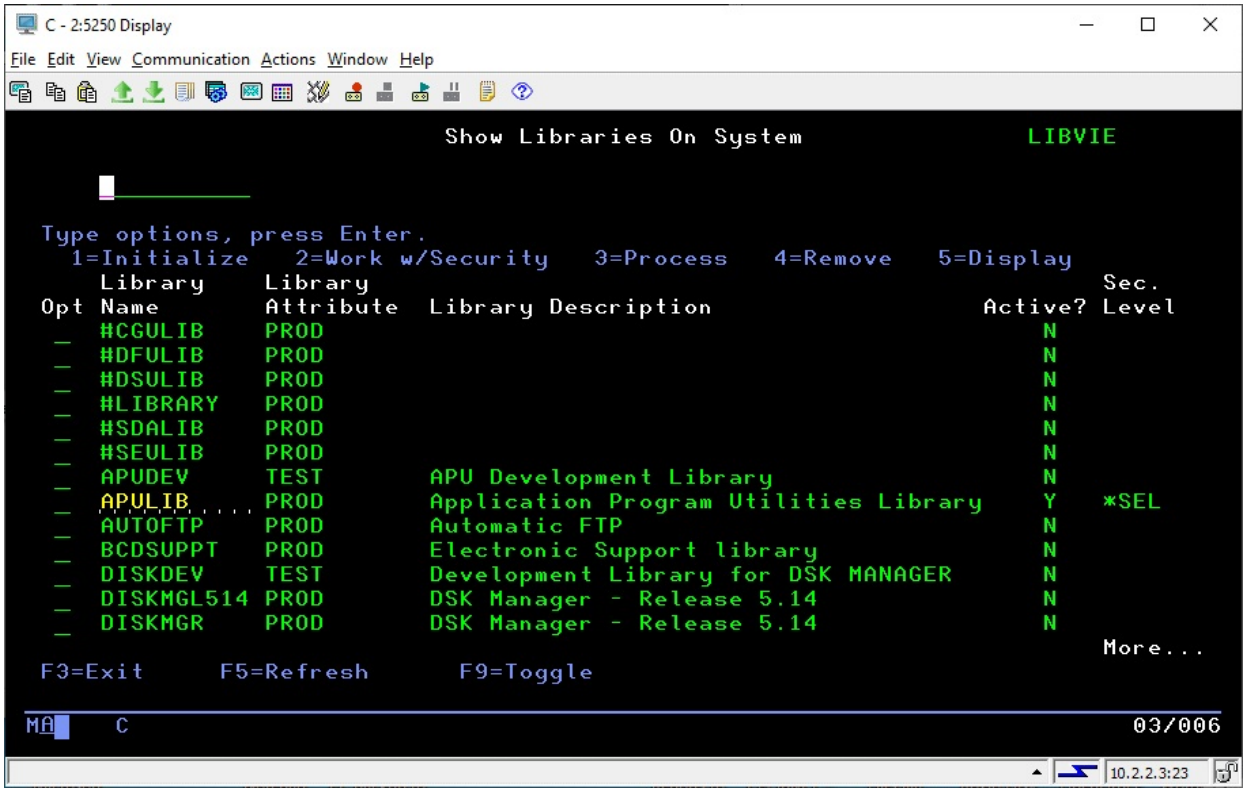
- *SELECT — Shows a list of all libraries on your system and lets you select which library you want.
- *ALL — The analysis process will be run for all libraries that have already been activated.

Output option	*DISPLAY	The results of the library object security check will be shown on your display session. You will be given a chance to work with the objects that have been changed and either set them to a different values or accept to new value into your baseline library object security set.
	*PRINT	A report of the library object security check will be generated.
	*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this, but the Analysis Option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to library object security are analyzed and presented, but the baseline set for library object security is not changed. This is the only option available when you choose a library name of *SELECT.
*POST	The changes to library object security are analyzed and presented, but they are then also automatically accepted as the new baseline library object security set.
*INIT	The current library object security is posted directly to the baseline library security set.

If you choose the *SELECT option for the library name, the following list of libraries is displayed:



If a library name is showing as highlighted with a Y in the Active? column, then that library has already been initialized and can be analyzed now. Any library showing without the highlight display has not yet been initialized and no baseline exists for it.

From this display, you can use the F9 Toggle function to limit the display to just those libraries that have already been initialized and can be analyzed now.

The options available for the listed libraries will be processed as follows:

1 - Initialize

The selected library will be initialized and added to the security baseline for the library objects. When you select option 1, an option will be presented that will allow you to the security level for the library. The options for this are:

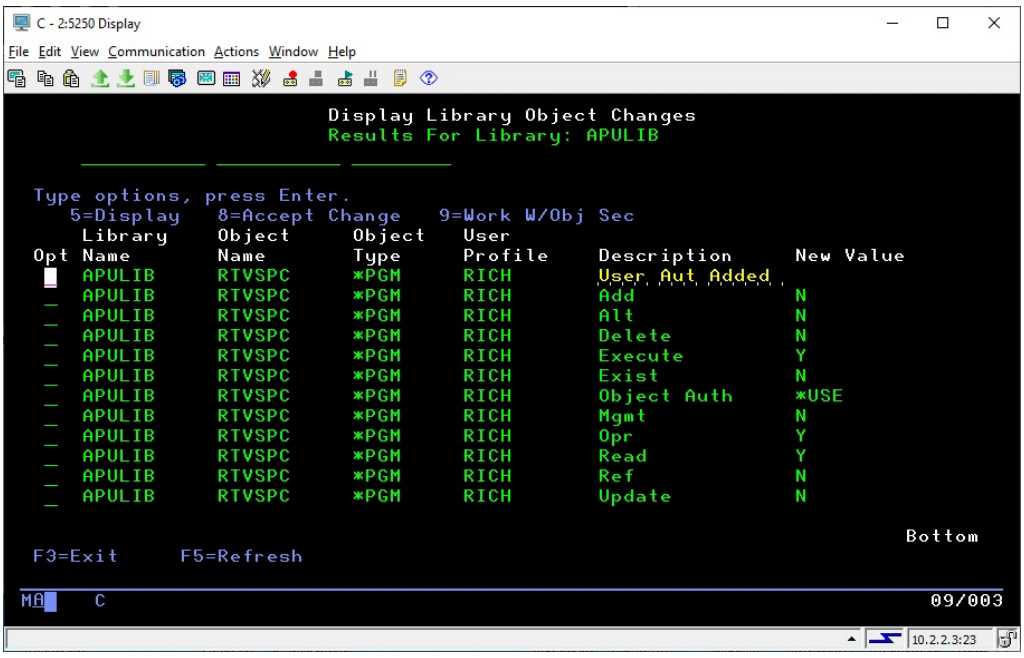
*SEL	The library will be included for audit purposes, but not for assessment purposes.
*ALL	All objects in the library will be included for both audit and assessment processing.
*DATA	All objects in the library will be included for audit processing but just the data objects will be included for assessment processing.
*NONE	The library will is excluded from assessment processing.

2 - Work w/Security

For a library that has already been selected, you can change the library security setting using this option.

3 - Process

For a library that has already been initialized, you can check the security configuration against the established baseline information using this option. A screen like the following will be displayed:



In this example, the library named APULIB was analyzed against the baseline information. One new user profile has been added to the security configuration for the RTVSPC *PGM object in this library. The details are shown on the display.

If changes are shown, you can choose the following options:

5 Will just show you additional details.

8 This option will let you accept the library object security change and post it to your baseline for library object security. This option can only be used on the first line for a listed user profile. The description on the first line is always highlighted in yellow to make it easy to find.

9 This option will start a system function to maintain the security configuration for the library object. Choose this option if you decide that you want to change the library object security that has been altered. You can change it back to back to what it was originally or make modifications to the permissions that have been granted.

Once you have made some changes to the library object security base, you can use the F5 refresh key to re-check the current library object security against the baseline and see if there are any changes now remaining that need to be dealt with.

4 - Remove

For a library that has been initialized and is being tracked by iSecMap, you can stop that tracking process using this option. The registration will be removed along with all current baseline information for the objects in the library.

5 - Display

Will display information about the registered library.

6 - Deselect

See option 4 above. This option performs the same function.

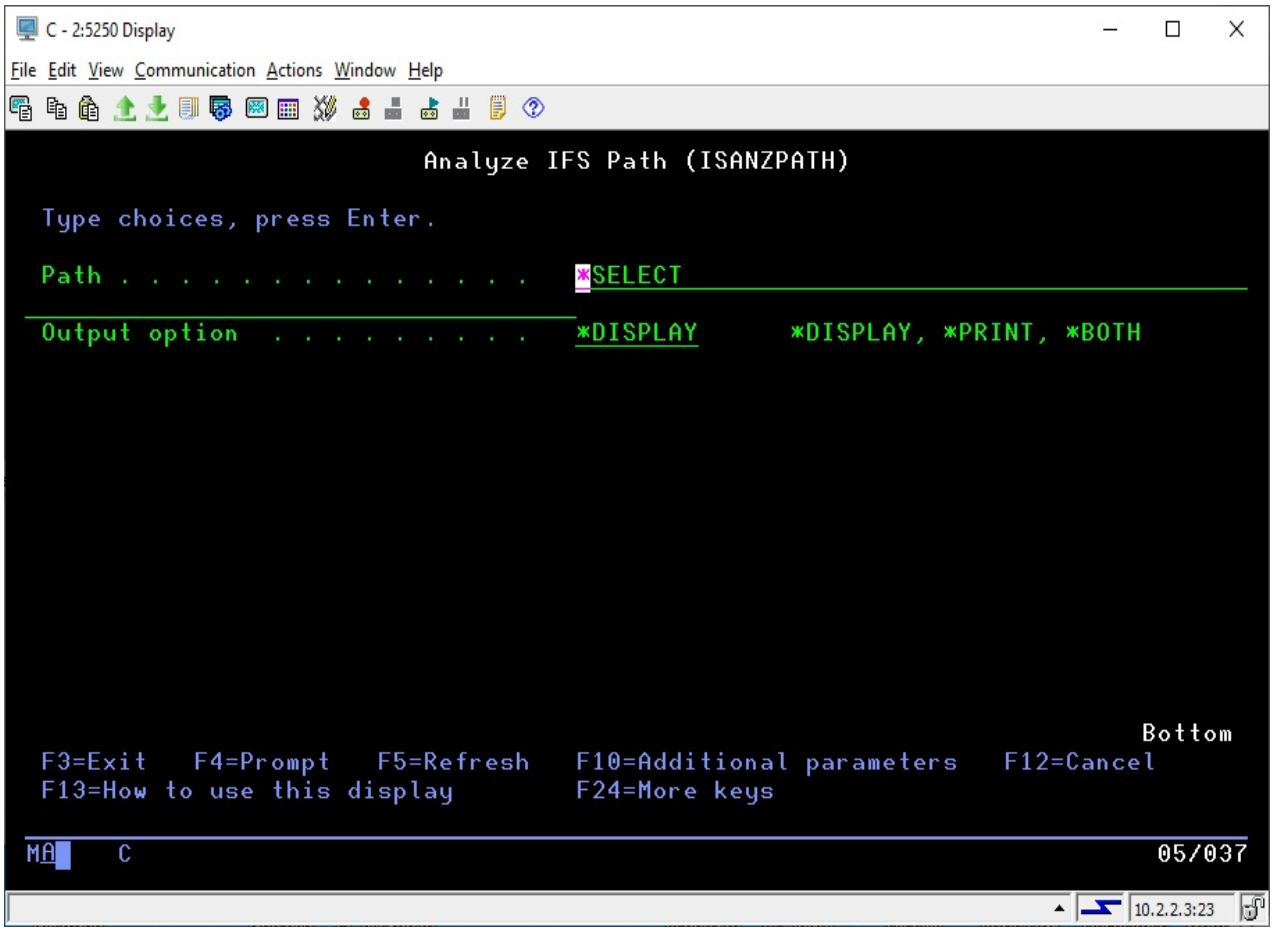
IFS Path Objects

For certain file paths in the Integrated File System (IFS) on your system, you will want to track security settings down to the object level within the path. iSecMap supports this. To establish a baseline for a path, that path must first be initialized. This initialization process creates the baseline for current security configuration for all objects in the path.

Note: iSecMap will only look at the actual files within the specified path. It will not look at files in sub-paths. If you want to monitor security at a sub-path, it must be identified separately as its own path.

Once a baseline has been established, you can then check the current security settings for all objects against the stored baseline and see what has changed.

When you run option #7 on the Audit menu, iSecMap will check your path object security and compare to the baseline information already stored. When you select the menu option, the following prompt will be shown:



Specify the path that you want to monitor. If this is the first time and you are initializing the baseline for the path, press the F10 key and use the *INIT option (see below). Make sure that your path parameter begins with a slash (/) character and keep in mind that this field is case sensitive. If you use the special value *SELECT, a list of registered paths will be displayed for you to choose from.

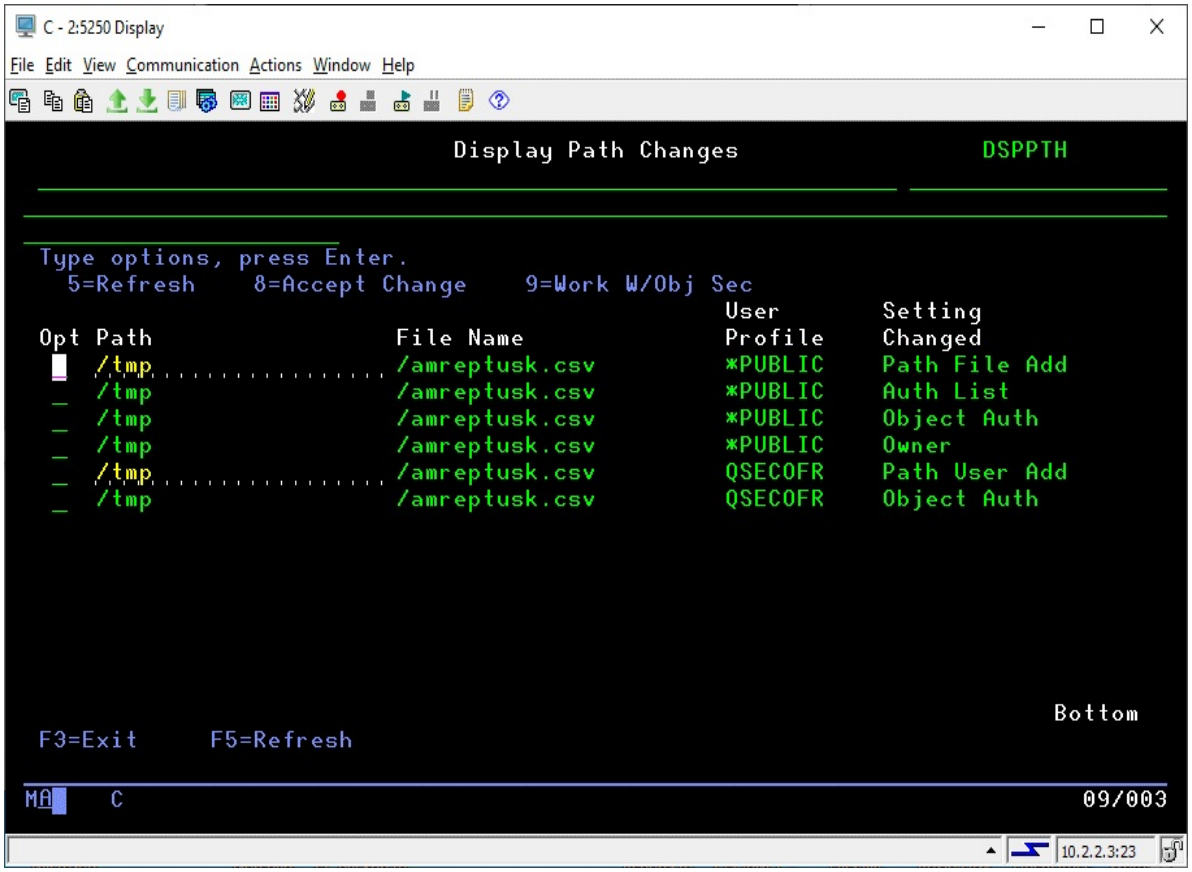
When this check of path security is run, you can choose the following output options:

*DISPLAY	The results of the path security check will be shown on your display session. You will be given a chance to work with the objects that have been changed and either set them to a different values or accept the new value into your baseline path security set.
*PRINT	A report of the path security check will be generated.
*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this (except in the case when you are initializing a path baseline), but the Analysis option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to path security are analyzed and presented, but the baseline set for path security is not changed.
*POST	The changes to path security are analyzed and presented, but they are then also automatically accepted as the new baseline security set for the path.
*INIT	The current path security is posted directly to the baseline security set for the path. This option must be used when initializing a new path for tracking.

When the path security check runs, if there are any differences between the current path security and the baseline, then the following display will appear:



In this example, the path named /tmp was analyzed against the baseline information. One file file has been added.

If changes are shown, you can choose the following options:

5 Will just show you additional details.

8 This option will let you accept the path object security change and post it to your baseline for path object security. This option can only be used on the first line for a listed user profile. The description on the first line is always highlighted in yellow to make it easy to find.

9 This option will start a system function to maintain the security configuration for the path object. Choose this option if you decide that you want to change the path object security that has been altered. You can change it back to back to what it was originally or make modifications to the permissions that have been granted.

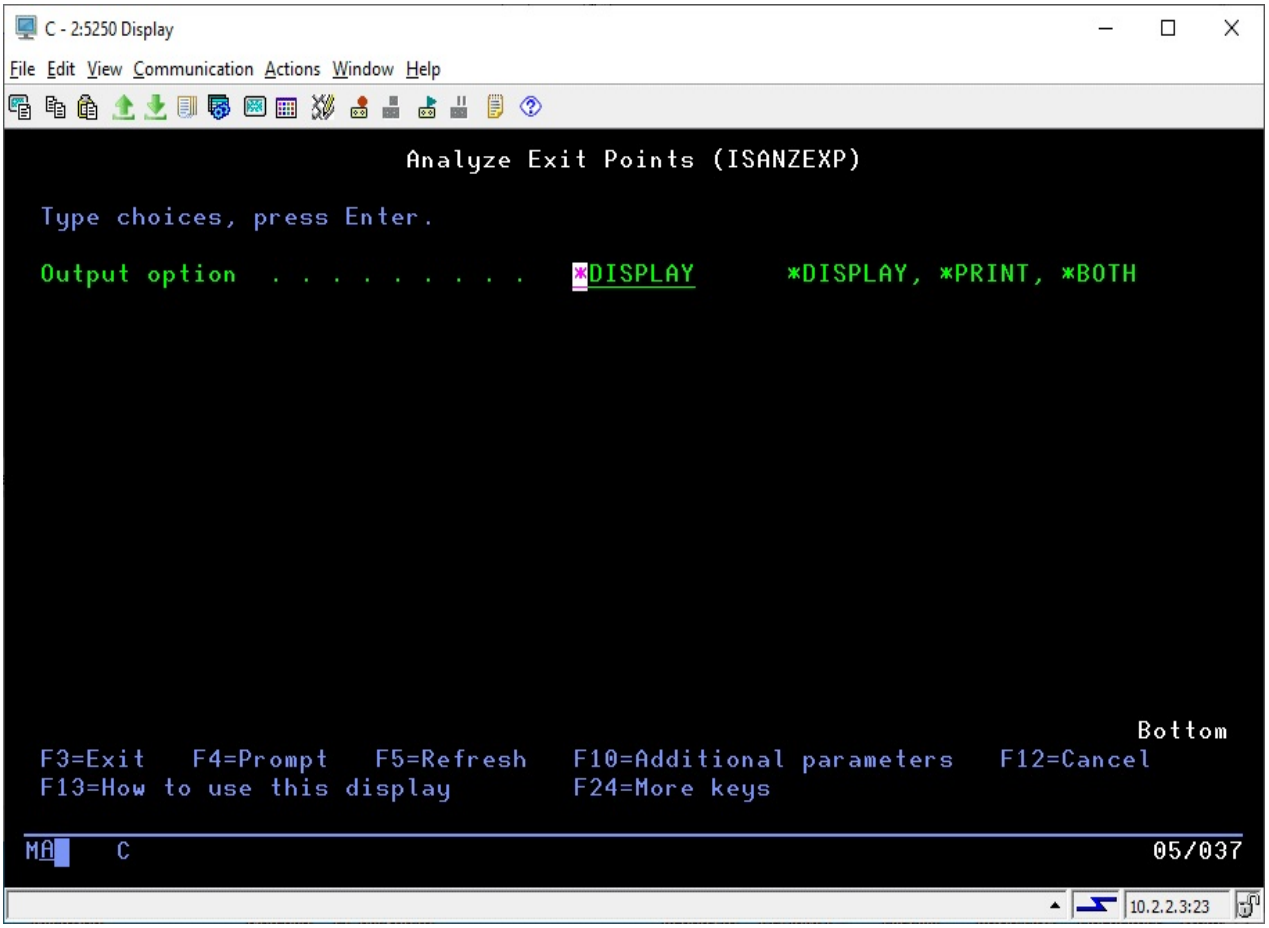
Once you have made some changes to the path object security base, you can use the F5 refresh key to re-check the current path object security against the baseline and see if there are any changes now remaining that need to be dealt with.

At any time, if you want to stop tracking a specific IFS path, you can use the RMVPATH command in library ISECLIB to do so. Prompt the command from the command line and just fill in the path that you want to remove from tracking in iSecMap.

Exit Point Registrations

Exit points are places in the IBM i OS where provision is made to call a user written routine at given points in normal OS operation. These can be used for security checking, additional processing for system functions and many other reasons. Because of the power involved with this tight association with the OS on your system, it is important that you watch for exit programs that may be added to your system without your prior approval and preparation. During installation, iSecMap stores a baseline of information about exit point registrations on your system.

When you run option #8 on the Audit menu, iSecMap will check your exit point registrations and compare them to the baseline information already stored. When you select the menu option, the following prompt will be shown:



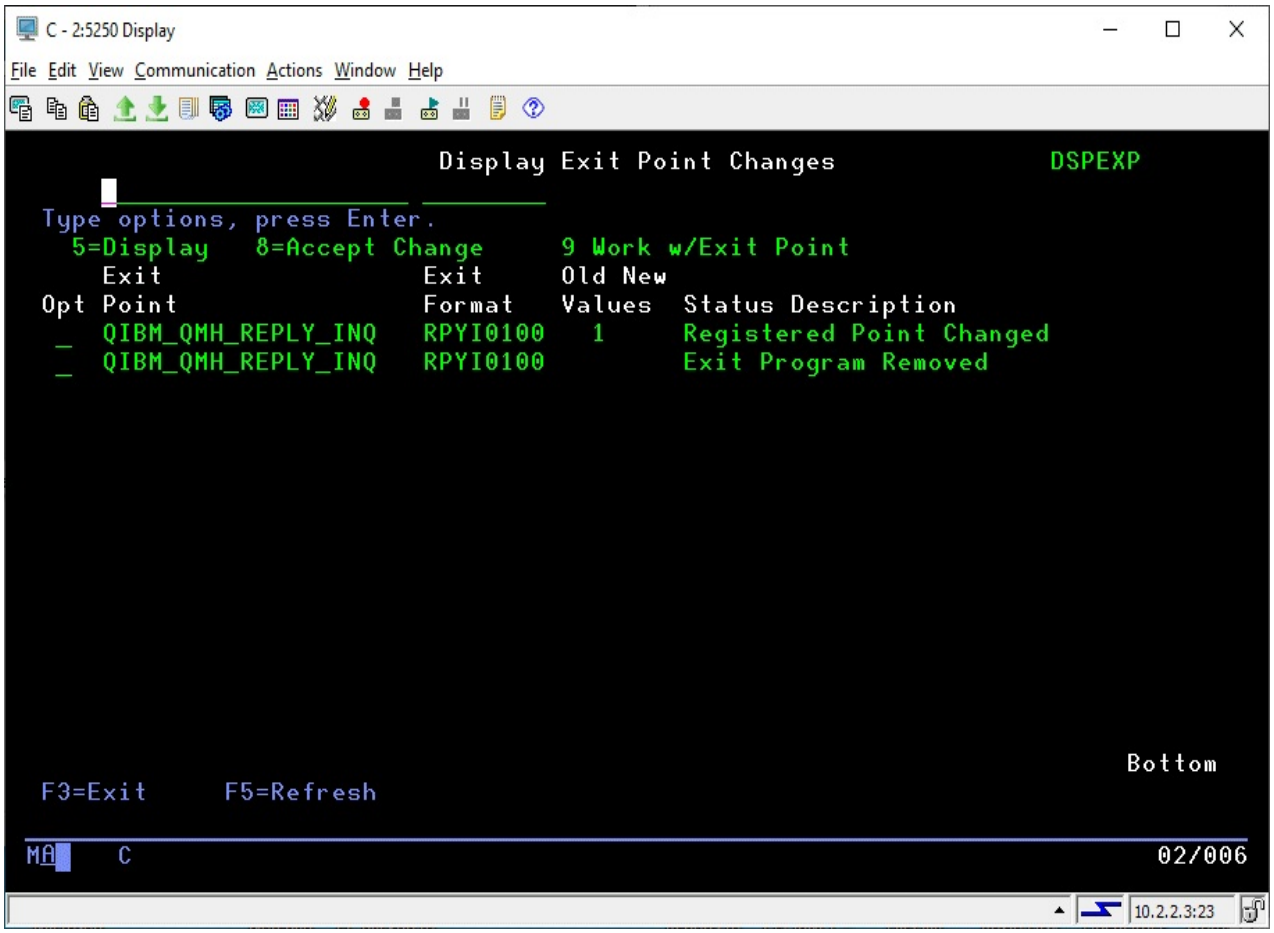
When this check of exit point registrations is run, you can choose the following output options:

*DISPLAY	The results of the exit point check will be shown on your display session. You will be given a chance to work with the exit points that have been changed and either set them to a different values or accept the new value into your baseline exit point registrations set.
*PRINT	A report of the exit point registrations check will be generated.
*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this, but the Analysis Option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to exit point registrations are analyzed and presented, but the baseline set is not changed.
*POST	The changes to exit point registrations are analyzed and presented, but they are then also automatically accepted as the new baseline set.
*INIT	The exit point registrations are posted directly to the baseline set.

When the exit point check runs, if there are any differences between the current exit points and the baseline, then the following display will appear:



In the above example the exit point referenced has been changed with a program registration having been removed. The number 1 indicates that a total 1 program is registered to this point. To see the details for the program registered, use option 5. Many exits allow for multiple registration.

If changes are shown, you can choose the following options:

5 Will just show you additional details.

8 This option will let you accept the exit point registration change and post it to your baseline

set.

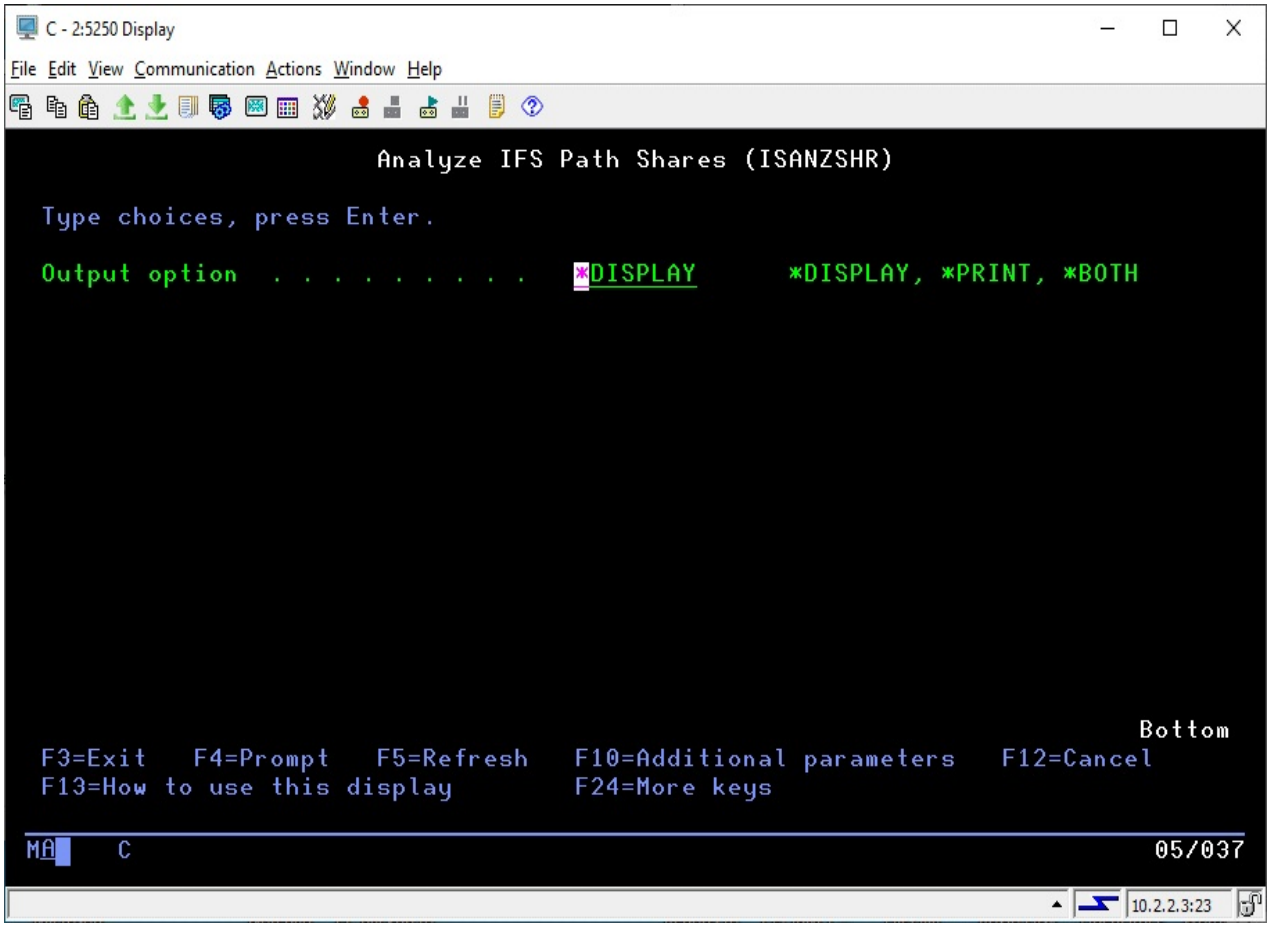
9 This option will start a system function to maintain the exit point registration for the named exit point. Choose this option if you decide that you want to change the program registration.

Once you have made some changes to the exit point base, you can use the F5 refresh key to re-check the current exit point registrations against the baseline and see if there are any changes now remaining that need to be dealt with.

IFS Path Shares

IFS Path Shares allow users to connect to files in the IFS using NetServer services. IFS Netserver Path Shares are controlled from IBM i Access Client Solutions "Navigator for i" (Nav). If you need to make changes to a share that was created but needs to be changed, this should be done using Nav. This is done by selecting "File Systems" (near the bottom of the list of options) and then "File Shares".

When you run option #8 on the Audit menu, iSecMap will check your current path shares and compare them to the baseline information already stored. When you select the menu option, the following prompt will be shown:



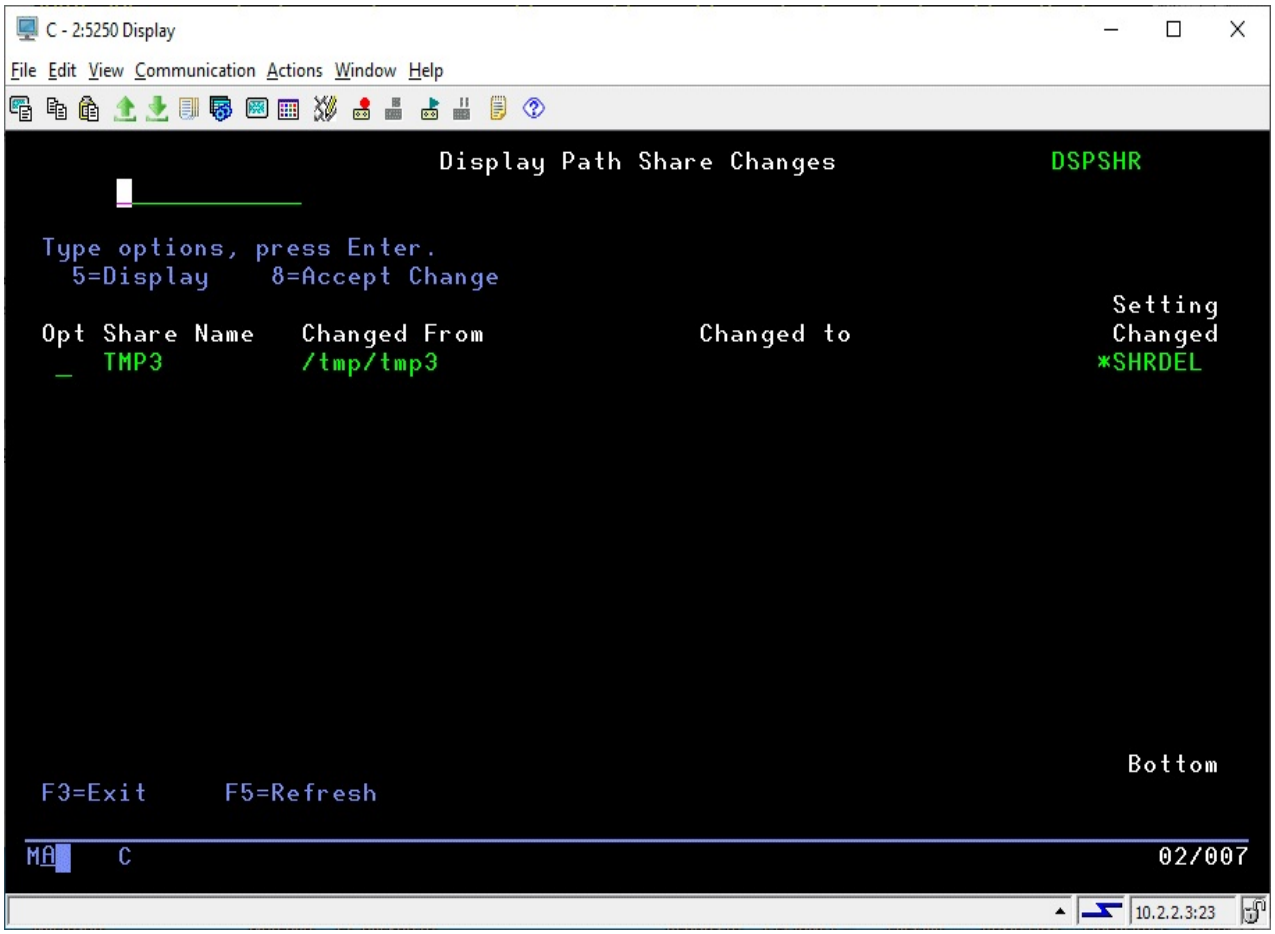
When this check of the path shares is run, you can choose the following output options:

*DISPLAY	The results of the path shares check will be shown on your display session. You will be given a chance to accept the share changes into your baseline set of path shares.
*PRINT	A report of the path shares check will be generated.
*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this, but the Analysis Option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to path shares are analyzed and presented, but the baseline set is not changed.
*POST	The changes to path shares are analyzed and presented, but they are then also automatically accepted as the new baseline set.
*INIT	The path shares are posted directly to the baseline set.

When the path share check runs, if there are any differences between the current shares and the baseline, then the following display will appear:



In the above example the share referenced has been removed. To see the details for the program registered, use option 5. Many exits allow for multiple registration.

If changes are shown, you can choose the following options:

5 Will just show you additional details.

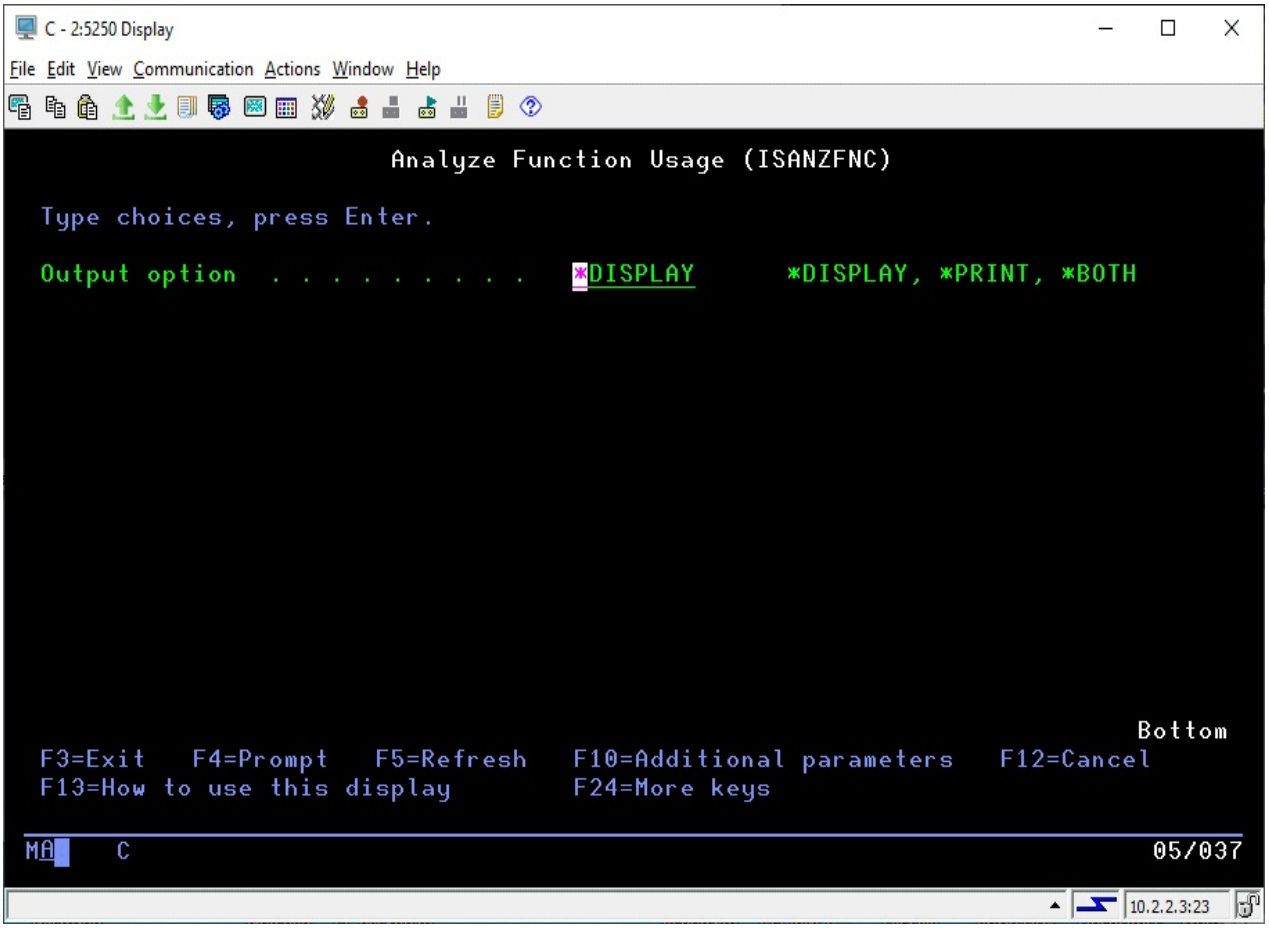
8 This option will let you accept the change and post it to your baseline set.

Once you have made some changes to the path shares base, you can use the F5 refresh key to re-check the current path shares against the baseline and see if there are any changes now remaining that need to be dealt with.

Function Usage

Function Usage is a feature of the IBM i OS that allows you to implement some rudimentary controls over network access functions such as FTP, File Server, etc. Function usage lets you restrict use of these functions by user profile, group profile or by profile authority. Given this power to control network access, it is important that your security implementation take this into account. The best way to control network access is by using exit points, but this is another way that is already built into the operating system.

When you run option #10 on the Audit menu, iSecMap will check your function usage settings and compare them to the baseline information already stored. When you select the menu option, the following prompt will be shown:



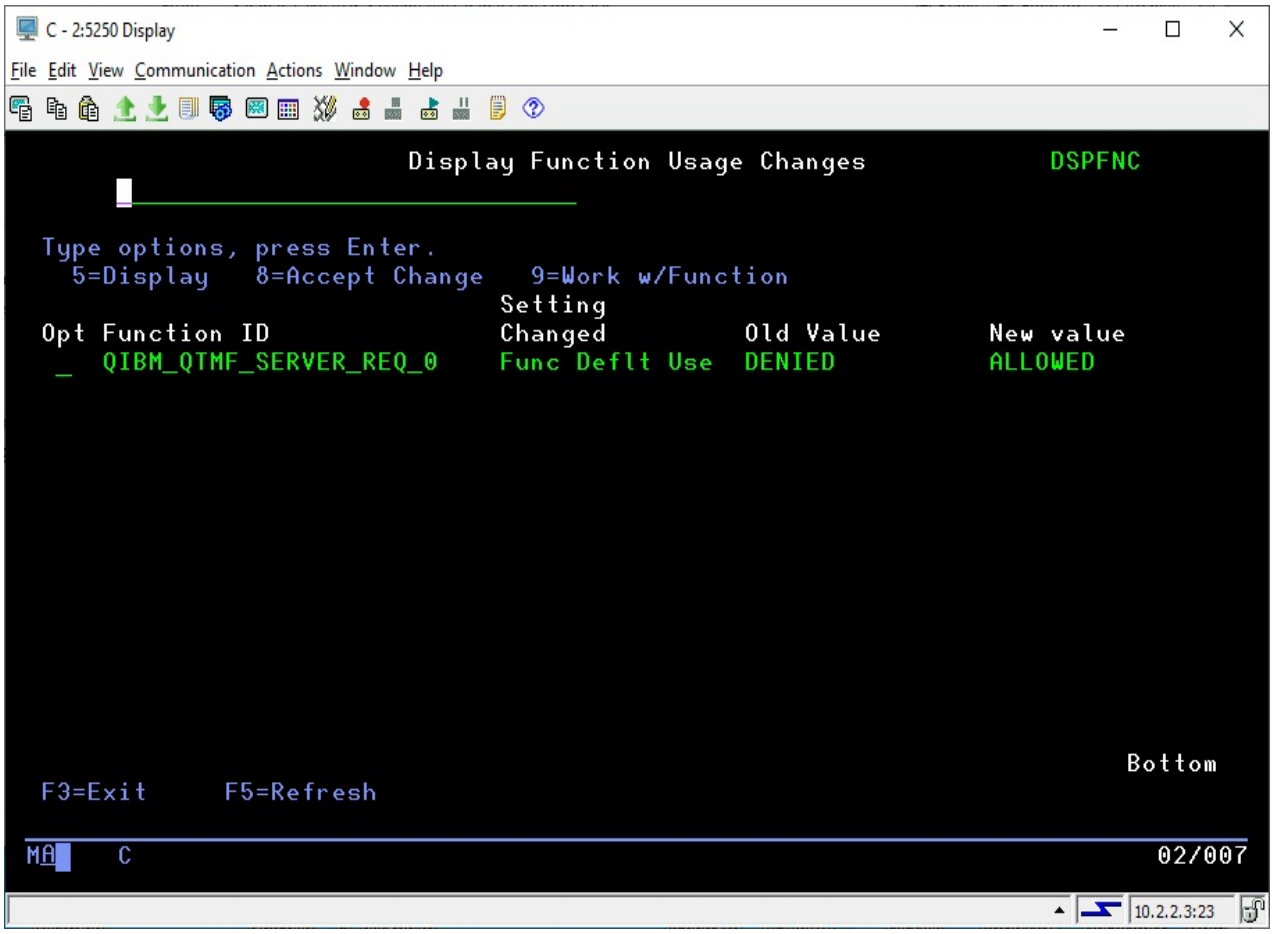
When this check of function usage is run, you can choose the following output options:

*DISPLAY	The results of the function usage check will be shown on your display session. You will be given a chance to work with the function usages that have been changed and either set them to a different values or accept the new value into your baseline function usage set.
*PRINT	A report of the function usage check will be generated.
*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this, but the Analysis Option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to function usages are analyzed and presented, but the baseline set is not changed.
*POST	The changes to function usages are analyzed and presented, but they are then also automatically accepted as the new baseline set.
*INIT	The exit point registrations are posted directly to the baseline set.

When the function usage check runs, if there are any differences between the current usages and the baseline, then the following display will appear:



In the above example the FTP server function referenced has been changed with access being opened up to anyone using FTP (maybe not a good idea?). To see the details for the change, use option 5.

If changes are shown, you can choose the following options:

5 Will just show you additional details.

8 This option will let you accept the function usage change and post it to your baseline set.

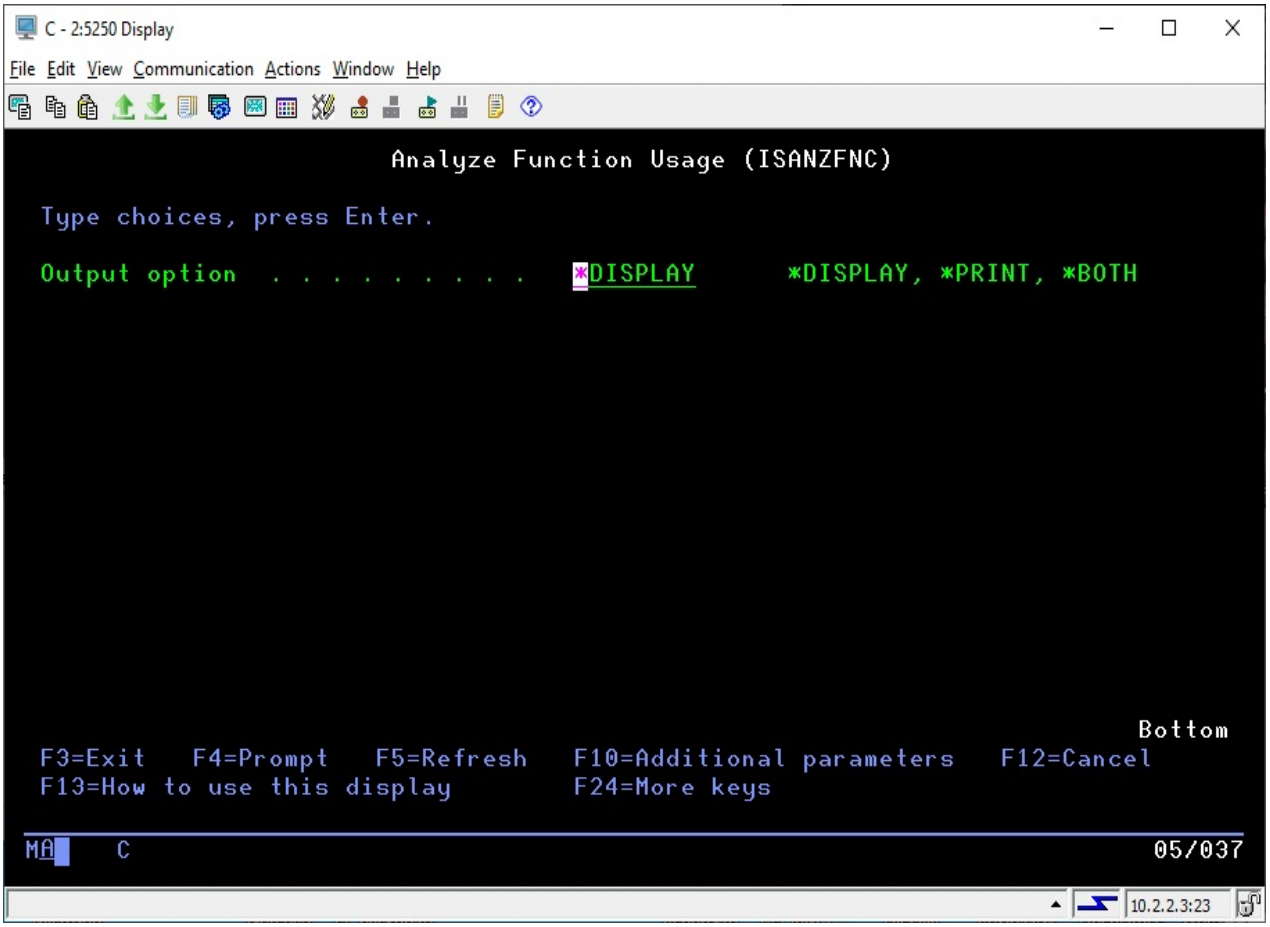
9 This option will start a system function to maintain the specific function usage. Choose this option if you decide that you want to change the usage back to what it was originally..

Once you have made some changes to the function usage base, you can use the F5 refresh key to re-check the current function usages against the baseline and see if there are any changes now remaining that need to be dealt with.

Environment Variables

Environment variables can be used to change the way applications and operating system functions work on your system. As such, it is important to know when they have been changed as some such changes could be malicious in intent. This feature in iSecMap will check on system level environment variables to let you know if any changes have been made.

When you run option #11 on the Audit menu, iSecMap will check your environment variable settings and compare them to the baseline information already stored. When you select the menu option, the following prompt will be shown:



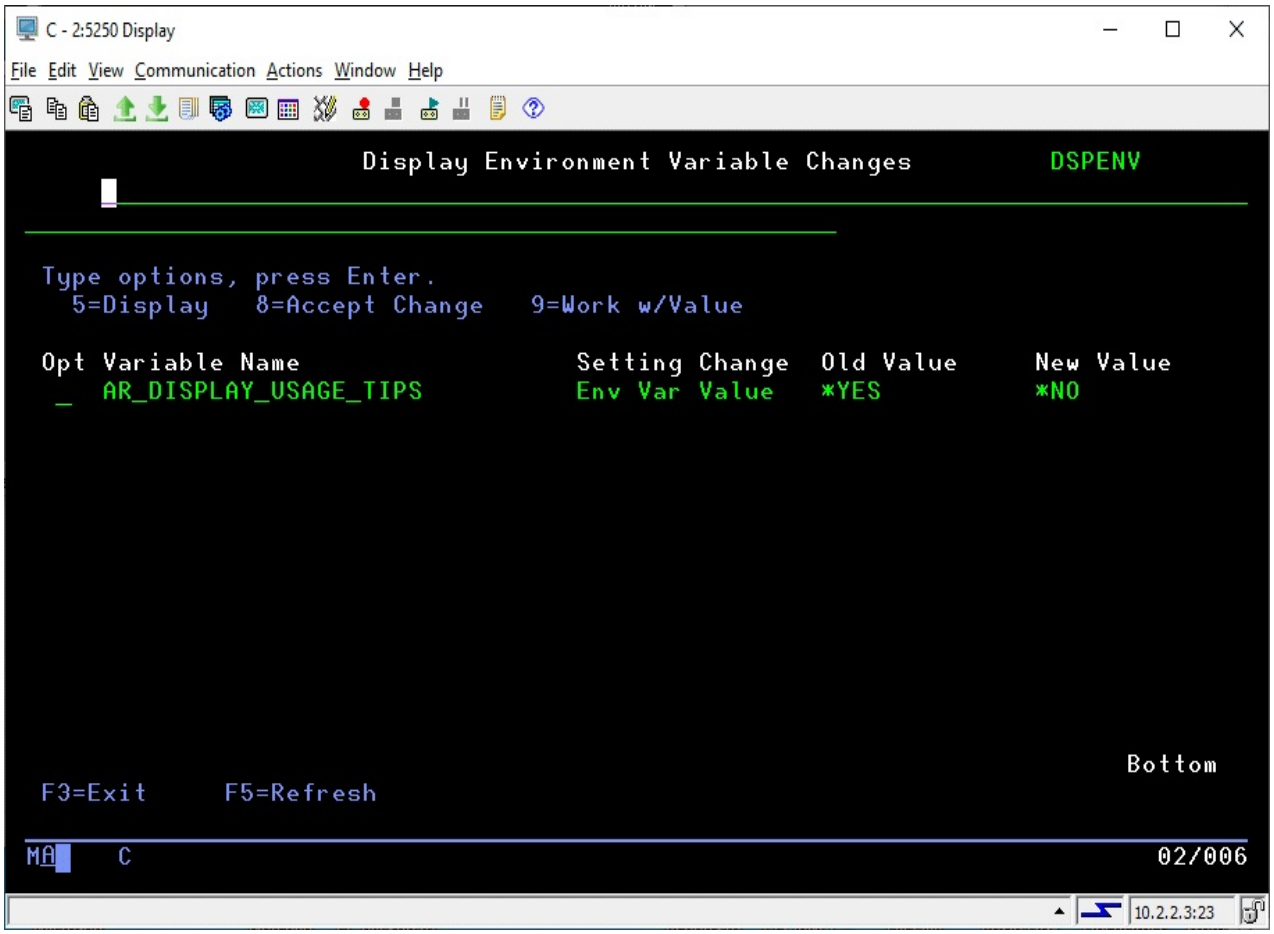
When this check of environment variables is run, you can choose the following output options:

*DISPLAY	The results of the environment variable check will be shown on your display session. You will be given a chance to work with the environment variables that have been changed and either set them to a different values or accept the new value into your baseline environment variables set.
*PRINT	A report of the environment variable check will be generated.
*BOTH	A report will be generated and the results will be displayed.

You can also use the F10 function key to access one additional parameter from this display. We do not recommend this, but the Analysis Option that is shown can be set if you desire:

*EDIT	This is the recommended default setting. The changes to environment variables are analyzed and presented, but the baseline set is not changed.
*POST	The changes to environment variables are analyzed and presented, but they are then also automatically accepted as the new baseline set.
*INIT	The environment variables are posted directly to the baseline set.

When the environment variable check runs, if there are any differences between the current variables and the baseline, then the following display will appear:



In the above example, the application environment value referenced has been changed. To see the details for the change, use option 5.

If changes are shown, you can choose the following options:

5 Will just show you additional details.

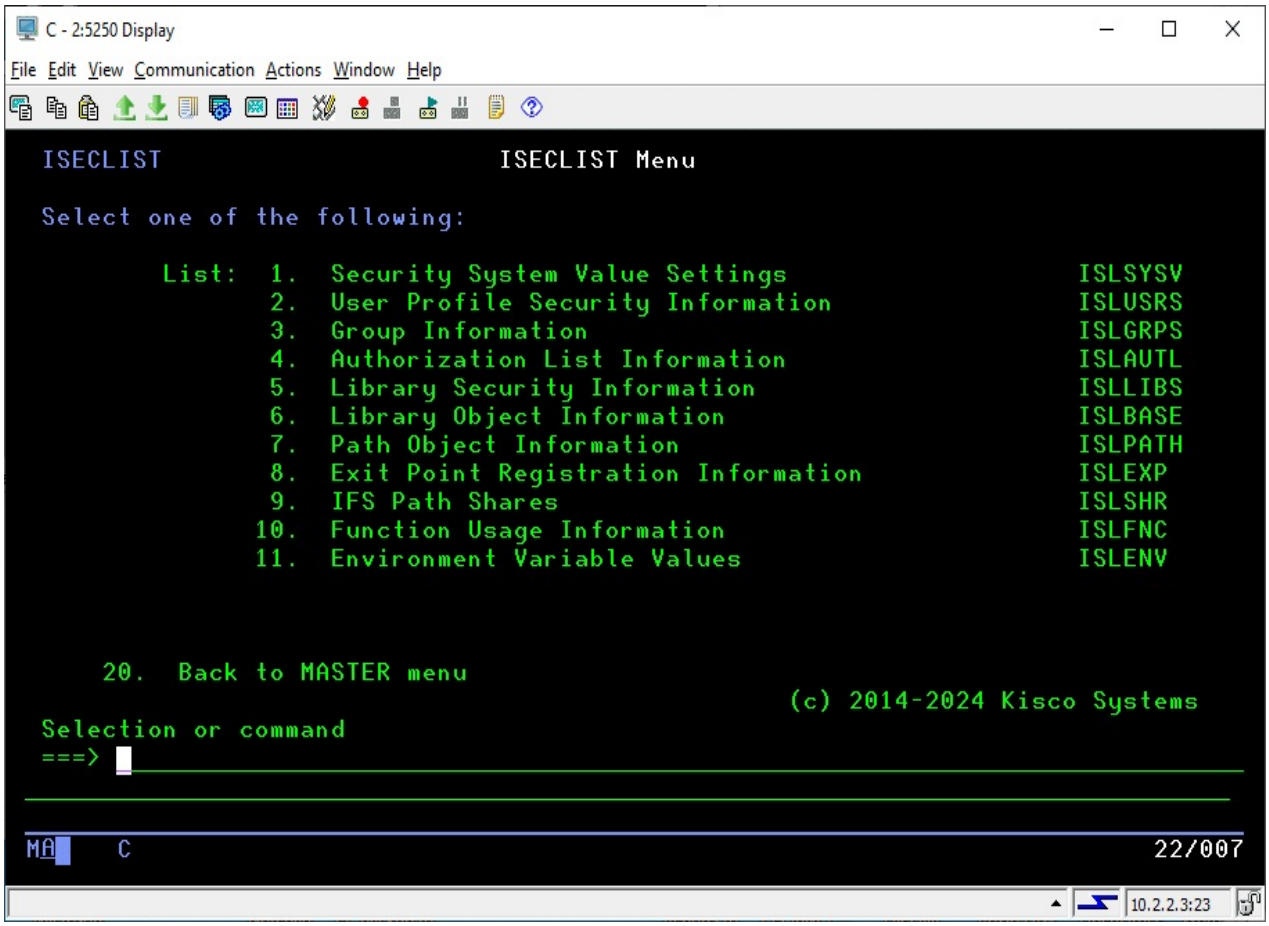
8 This option will let you accept the environment variable change and post it to your baseline set.

9 This option will start a system function to maintain the specific environment variable. Choose this option if you decide that you want to change the variable back to what it was originally..

Once you have made some changes to the environment variable base, you can use the F5 refresh key to re-check the current environment variables against the baseline and see if there are any changes now remaining that need to be dealt with.

Reporting Module

If you select option #2 from the MASTER menu, the Reports Menu will be displayed. From this report, you can generate reports for all of the current baseline information stored in iSecMap. The Reports Menu looks like this:



Each option on the menu is described here:

1.	Security System Value Settings	Shows all security related system values included in your system's baseline record in iSecMap.
2.	User Profile Security Information	Shows security related information currently in your baseline for user profiles. You can show a single profile, *ALL profiles, GENERIC* profiles or just profiles with *ALLOBJ authority (super users). When you select the *ALLOBJ option, if a user does not have *ALLOBJ on their profile but is granted this authority because of a group or supplemental group profile, it will be included on the list with a reference as to where the *ALLOBJ authority is given.
3.	Group Information	Shows all group profiles on your system with the

		individual profiles that are included in each group.
4.	Authorization List Information	Shows all authorization lists in your iSecMap baseline along with the individual profiles and their access rights defined in the authorization list.
5.	Library Security Information	Shows security related information for libraries in your baseline. You can show information for an individual library, *ALL libraries or a GENERIC* set of libraries.
6.	Library Object Information	For libraries that are registered to iSecMap for object level tracking, this option shows security related settings for the objects. You can run it an individual library or all registered libraries. The *SELECT option will let you see which libraries are registered so that you can select the library you want shown.
7.	Path Object Information	For IFS paths that are registered to iSecMap for object level tracking, this option shows security related settings for the objects. You can run this for an individual path or all registered paths. The *SELECT option will let you see which paths are registered so that you can select your path.
8.	Exit Point Registration Information	Shows all exit points in your iSecMap baseline. For those exits where exit programs are registered, each program is also shown under the exit point where it is registered.
9.	IFS Path Shares	Shows all IFS Path Shares in your iSecMap baseline. For each entry, the share name, type and path are shown.
10.	Function Usage Information	Shows all of the function usages in your iSecMap baseline. For each entry, the relevant settings are shown.
11.	Environment Variable Values	Shows all system level environment variable settings currently in your iSecMap baseline.

For each option, you can specify an output option with the following choices:

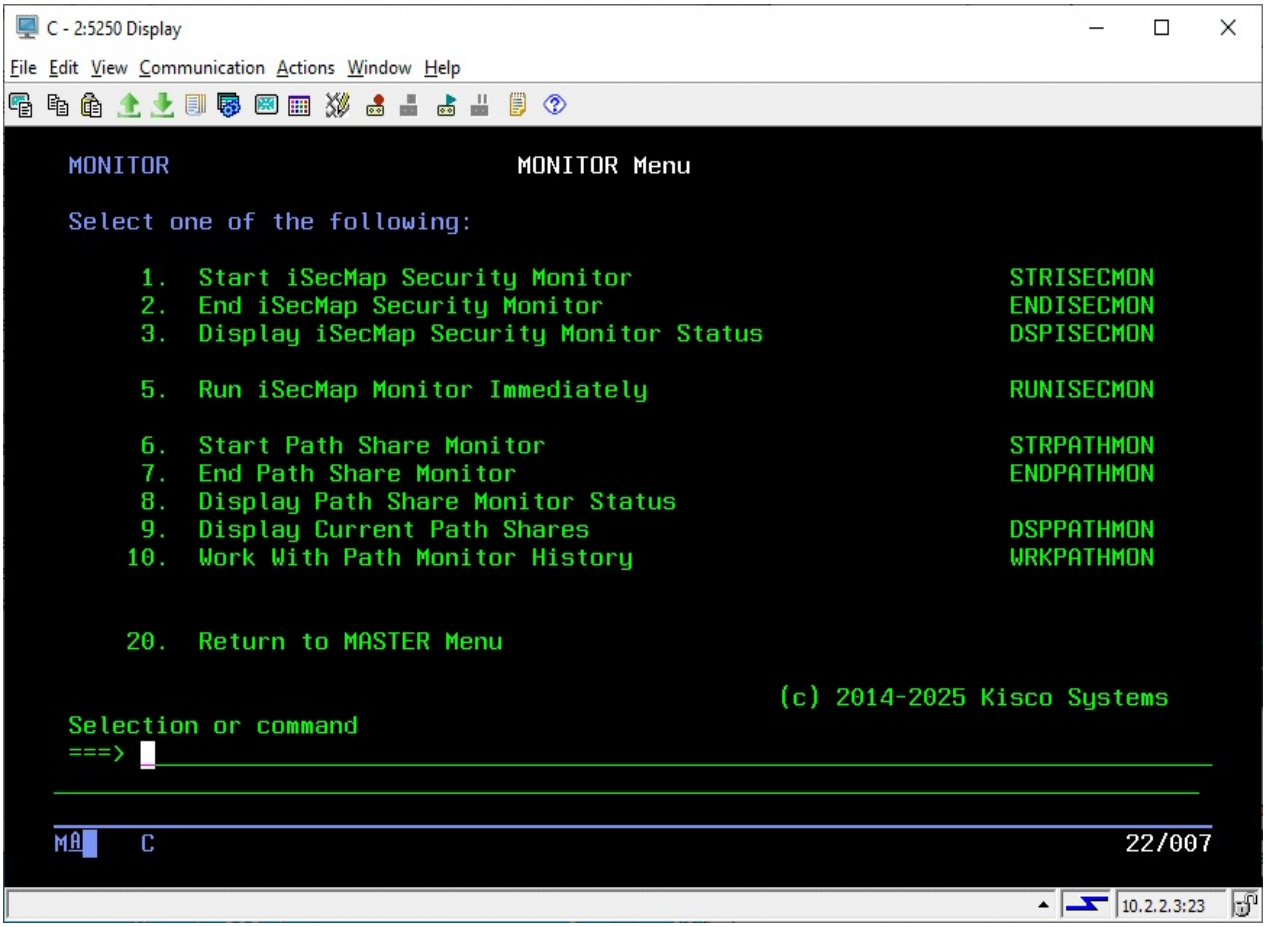
*PRINT	The output is created as a printed listing
*CSV	The output is created as a CSV file that you can download. All of the CSV files are stored in the /kisco/ismdnload/ path in the IFS on your system
*DISPLAY	You can view the current baseline information for each option interactively in your terminal session.

If you want to run reports in your own CL programs, the corresponding CL command for each report is shown on the right side of the menu display. All of these commands are in our application library named ISECLIB.

Monitor Module

iSecMap includes a feature that allows you to automatically monitor your base security settings. These include system values, user profiles, group profiles, authorization lists, library security, exit point registrations, IFS Path Shares, Function Usage and Environment Variables. You can also optionally monitor for changes in library object security and IFS path security for the libraries and paths that are already registered to iSecMap. When the monitor function is active, it will periodically check the current security settings for these areas against the baseline information stored for your system and any differences will be reported. Reporting is done by message to a message queue (such as the system operator message queue) and/or by email. Up to five messages can be sent and up to five email notices can be sent.

When you select option #3 from the MASTER menu, the Monitor Control menu will be displayed as follows:



The menu options are as follows:

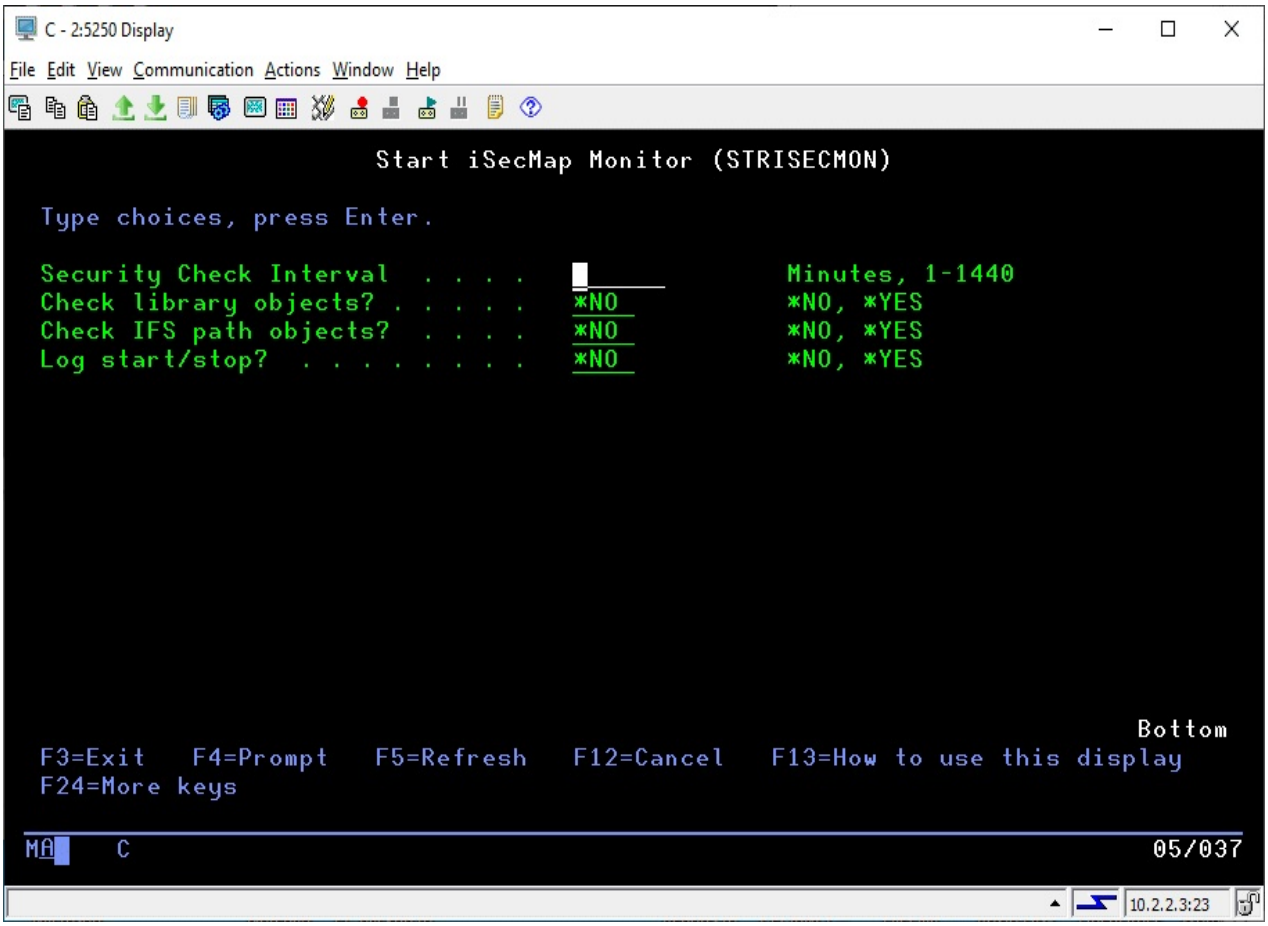
1 Starts the iSecMap Security Monitor running on your system
2 Ends the current Monitor that is running on your system
3 Displays the status of the iSecMap Security Monitor on your system
5 Runs iSecMap Monitor Immediately regardless of the schedule setup already
6 Starts the IFS Path Share Monitor
7 Ends an active IFS Path Share Monitor
8 Shows the status of the IFS Path Share Monitor to confirm if is it active or not

9 Displays any currently active IFS Path Shares when the Monitor is active
10 Shows the IFS Path Share history

Each of these is described in a separate section following here.

Starting The Security Monitor

For the Security Monitor to work, it must be started. When you select option #1 on the Monitor menu, the following prompt will be displayed:



Complete the parameters as follows:

Security Check Interval	Enter a number between 1 and 1440. This will be the frequency of the security check process. For example, if you use the number 15, then every 15 minutes, a batch job running in background will check the security settings on your system against their corresponding baseline information and report differences.
Check library objects?	Optionally check for library objects: *NO - no library objects will be checked

*YES - all libraries registered to iSecMap will have all objects checked for security changes whenever the monitor activates for its periodic cycle.

Check IFS path objects? Optionally check for IFS path objects:

*NO - no IFS path objects will be checked
*YES - all IFS paths registered to iSecMap will have all objects checked for security changes whenever the monitor activates for its periodic cycle.

Log start/stop? Control logging of monitor starts and stops:

*NO Monitor start and stop will not be logged in the iSecMap Activity Log.
*YES Monitor start and stop will be logged.

When security changes are identified by the iSecMap Security Monitor, notification messages will be sent to up to 5 message queues and/or to up to 5 email addresses. The notification message queues and email information is maintained using option #9 on the INSTALL menu. See that section of this documentation for specifics.

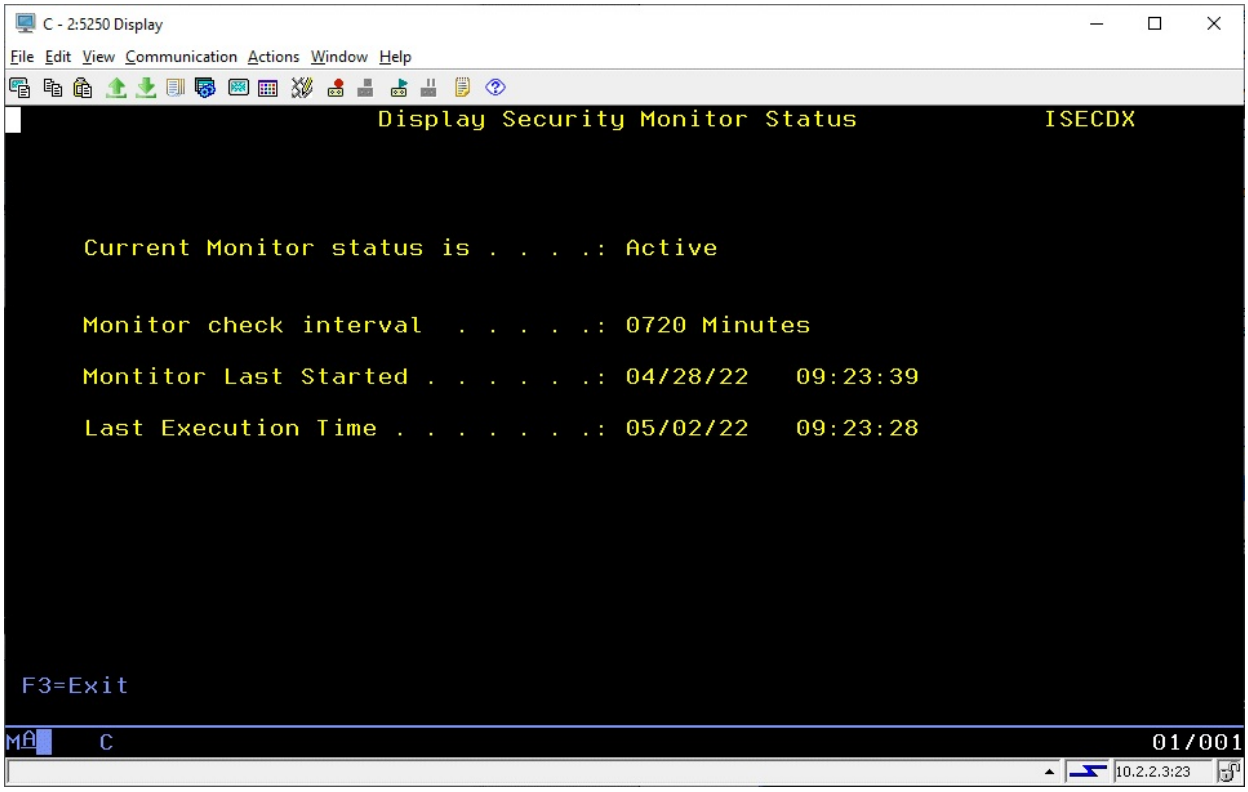
Note: When activating email notification, some configuration work may be required on your system.

Ending The Security Monitor

To end the Security Monitor once it has been started, just select menu option #2 from the Monitor menu and the task will end along with its associated sub-system.

Checking The Security Monitor

At any time, you can check the status of the Security Monitor by running option #3 from the Monitor menu. When you select this option, the following will be displayed:



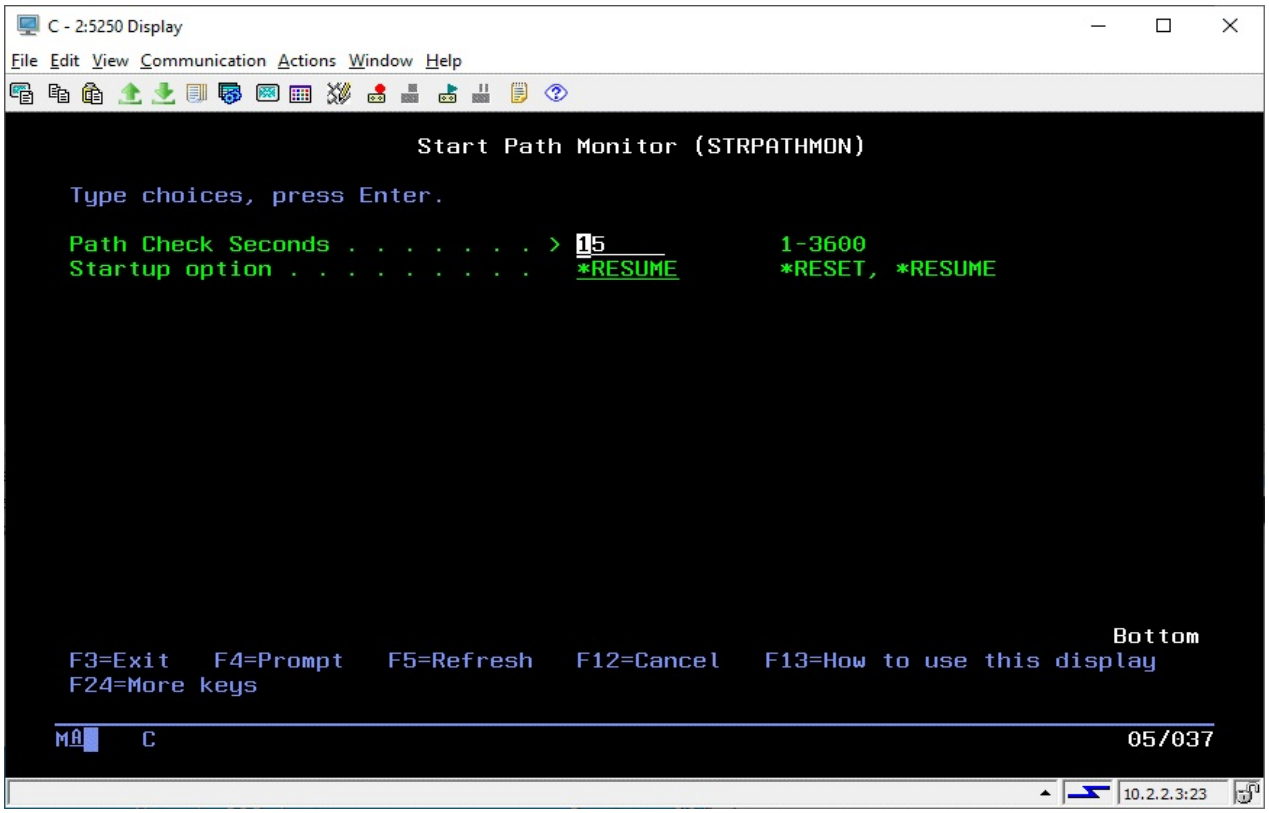
This will show you if the monitor is active and what the check interval is that the current monitor (or last one run) used. It will also show you when the monitor was last started and the last time the monitor cycled through its series of security checked (execution time).

Run Monitor Immediately

If you want to run a full check of your security settings immediately without waiting for the next scheduled run, you can use option #5. The check will run in the iSecMap subsystem and any required notifications will be issued.

Path Share Monitor

The Path Share Monitor will let you collect information about defined shares in the IFS on your system. This monitor will let you know who is connected to each share and how long they are connected to it. To start the Path Share Monitor, use option #6 on the MONITOR menu. The following will be shown:



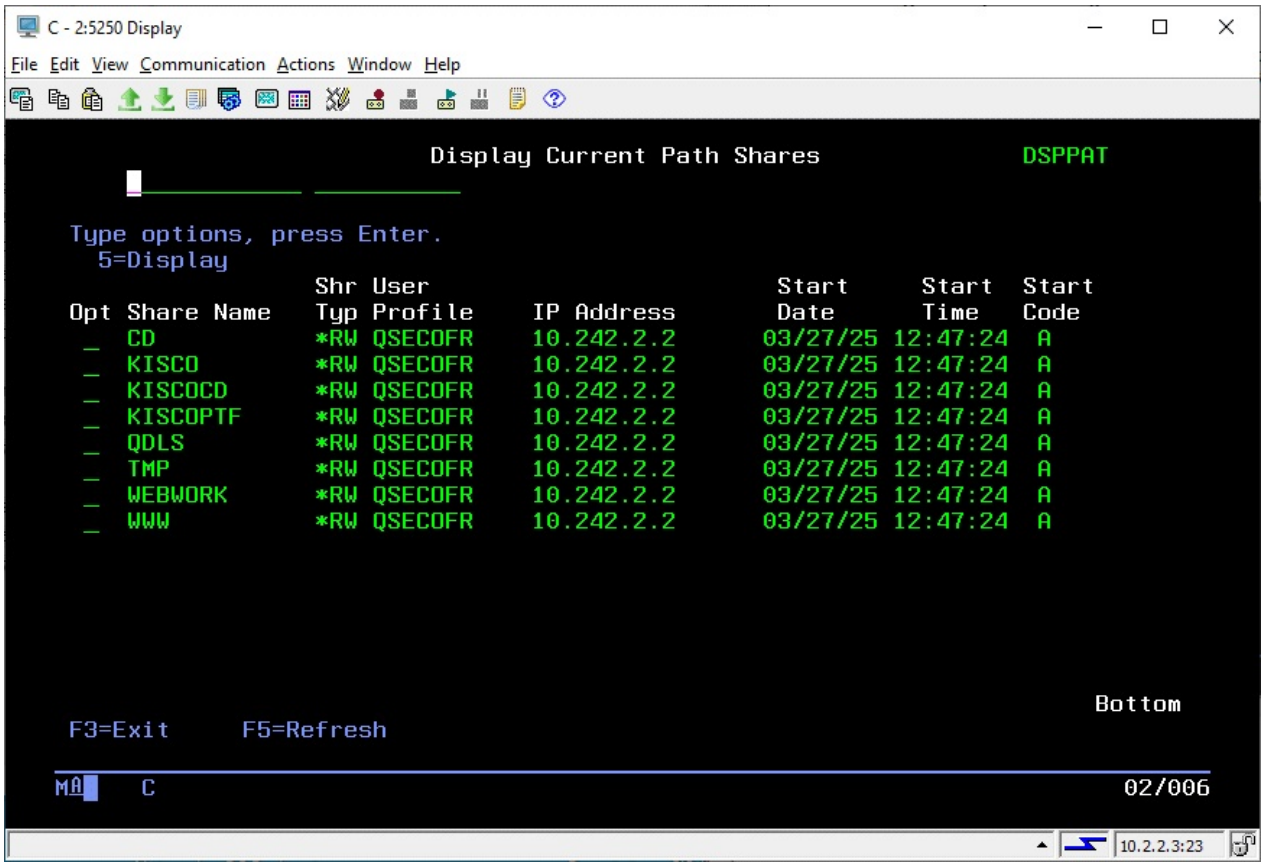
Fill in the parameters as follows:

Path Check Seconds	Enter a value between 1 and 3600. This is the time interval in seconds between montior checks. The monitor will wake up at each interval and check all defined path shares. Information about the current users will be captured.
Startup option	Choose the option you want when the Path Monitor is started:
*RESUME	The information captured about path shares will be continued from where it was when the monitor was last run.
*RESET	All historical information about path shares will be deleted beforestarting the monitor.

When the monitor is started, it will collect information about which users are actively connected to the IFS path shares on your system.

Options 7 and 8 on the MONITOR menu will let you control the Path Share Monitor. If a monitor is active, you can use option #6 to stop it from running. You can use option #8 to check to see if the monitor is currently running.

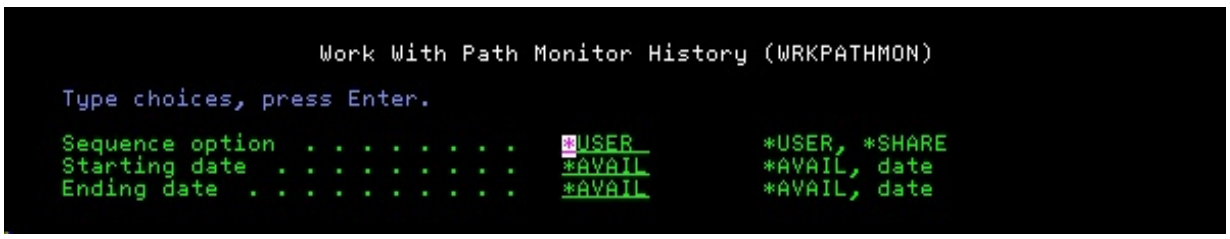
With the Path Share Monitor running, you can view the current path connections by using option #9 on the MONITOR menu. The following will be shown:



Use option 5 next to any detail line to see more details about the file share.

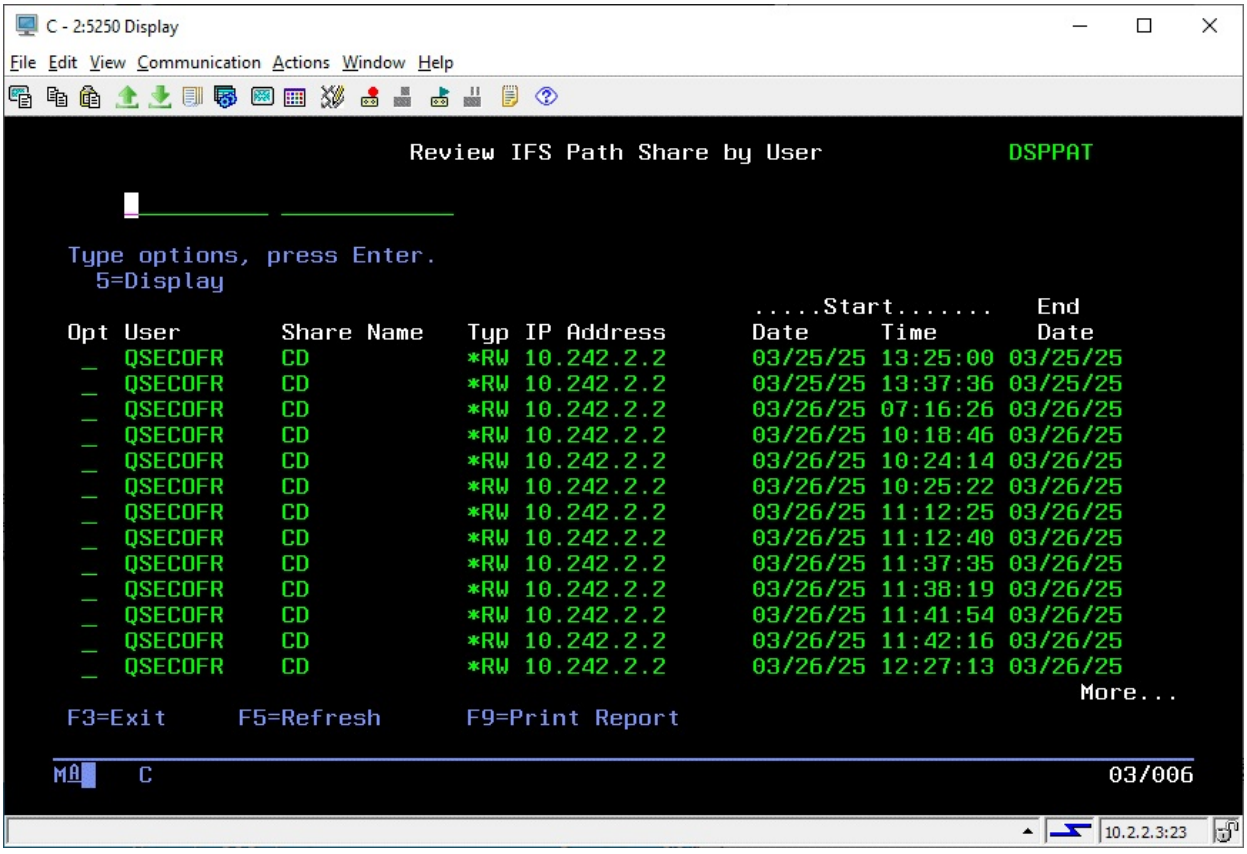
Whenever an active path share ends because the user has disconnected, the information about that share will be transferred to the path share history. Information will also be transferred whenever the monitor is intentionally ended.

You can view information from the history by using option #10 on the MONITOR menu.



The default view will be by user profile. To look at the history by IFS Share, change this option to the *SHARE option. If you want to limit the display to a range of dates, use the date range parameters.

The user profile option will appear as follows:



To see more details about each share, place a 5 next to it. The exact path will be shown along with the exact end time and how the share started and ended. Using the F9 function key will transfer this information into a listing.

Note: If a share is on file that started before this start date selected, it will not be included. Similarly, if a share started within the range selected but ended later than the range, it will not be included.

Assessment Module

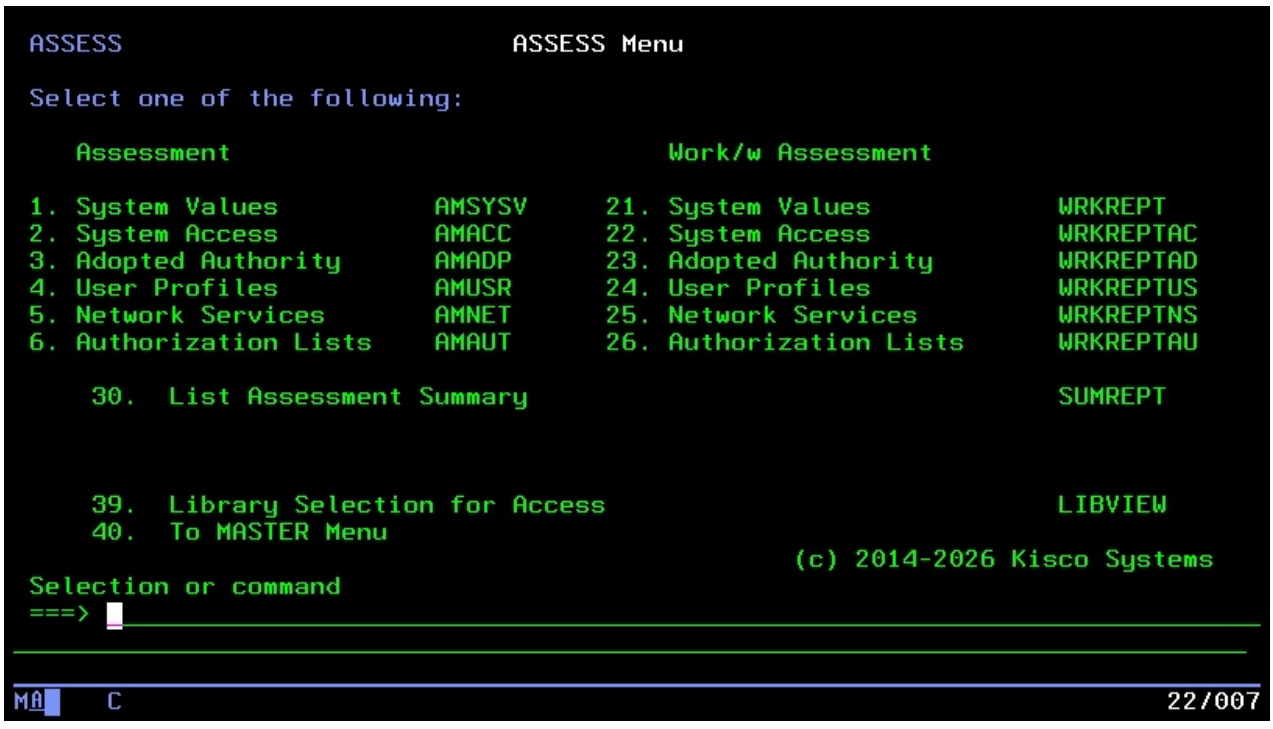
The Assessment Module can be used to check your current security configuration against IBM, Industry and Kisco standards for the best possible security implementation possible. Exceptions to the standards are highlighted and you can then either make changes to your security environment or document your acceptance of the differences highlighted.

There are five areas of assessment covered by iSecMap. These include:

1. System Values
2. System Access
3. Adopted Authority
4. User Profiles
5. Network Service
6. Authorization Lists

For each of these, there is the actual assessment process and then subsequent working with that assessment.

The Assessment Module is accessed from the Assessment menu by selecting option #4 on the MASTER menu.



The process to run each assessment is performed by the options 1 through 5 on the left side of the menu. When each assessment is run, one or more listing are generated and a downloadable CSV file for the results is generated in a folder named /kisco/ismdnload.

Each assessment area is covered separately in the following documentation.

System Values

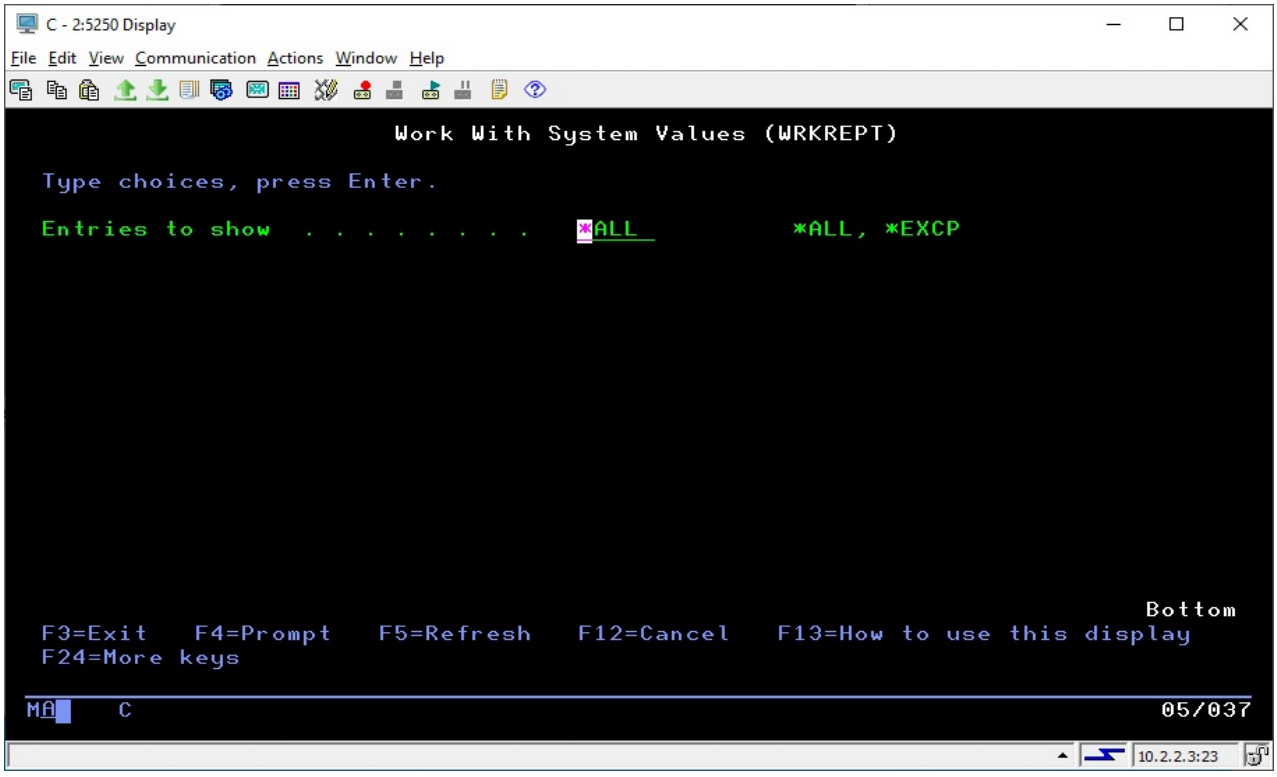
The system values assessment will compare your current security based system values with IBM, Kisco and Industry standards. When you run the assessment, two reports will be generated that will help with your understanding of the results. Also, a CSV file will be generated in the IFS based on the assessment results. The file is named /kisco/ismdnload/assesssv.csv.

The first report created will detail the exceptions identified. There is a column on the report for any exception notes. If a "Yes" appears here, this indicates that a note is on file for the exception and can be referenced using option 21 on the Assessment menu.

The second report is a listing of all of the security system values showing your current setting, the recommended setting, the source of the recommendation and any exceptions noted. The recommendation sources can include the following:

- CIS - The Center for Internet Security recommendations for IBM i
- IBM - IBM security recommendations
- KIS - Kisco security recommendations

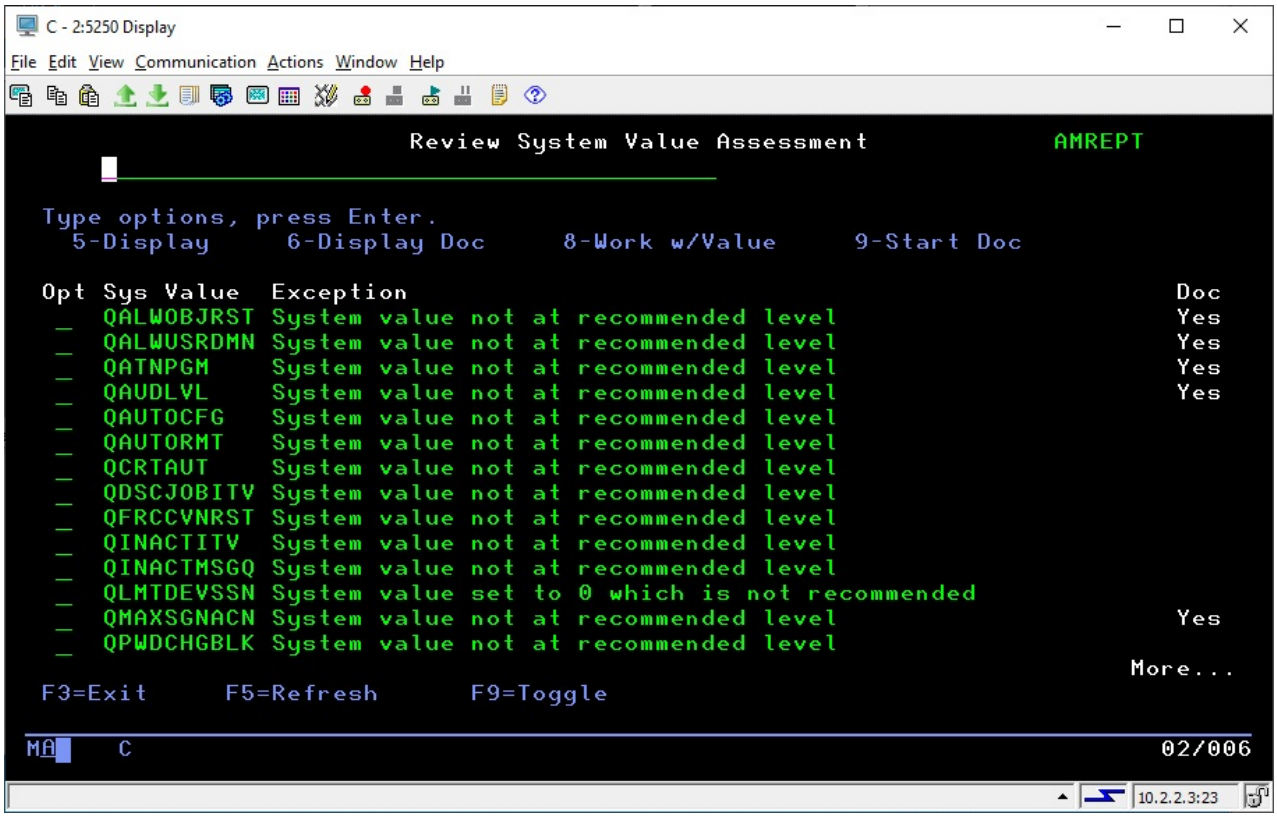
To work with the system value assessment, run menu option #21. You will be prompted for the following option:



Choose from the following options:

*ALL	All assessment exceptions will be shown
*EXCP	Only those exceptions that have not been documented will be shown

The results of the most recent assessment with always be shown as follows:



When a “Doc” column on the right side of the panel shows “Yes”, this indicates that the exception shown has a document associated with it that is already on file.

The following options can be selected for any of the exceptions shown:

5 Displays more details for the exception

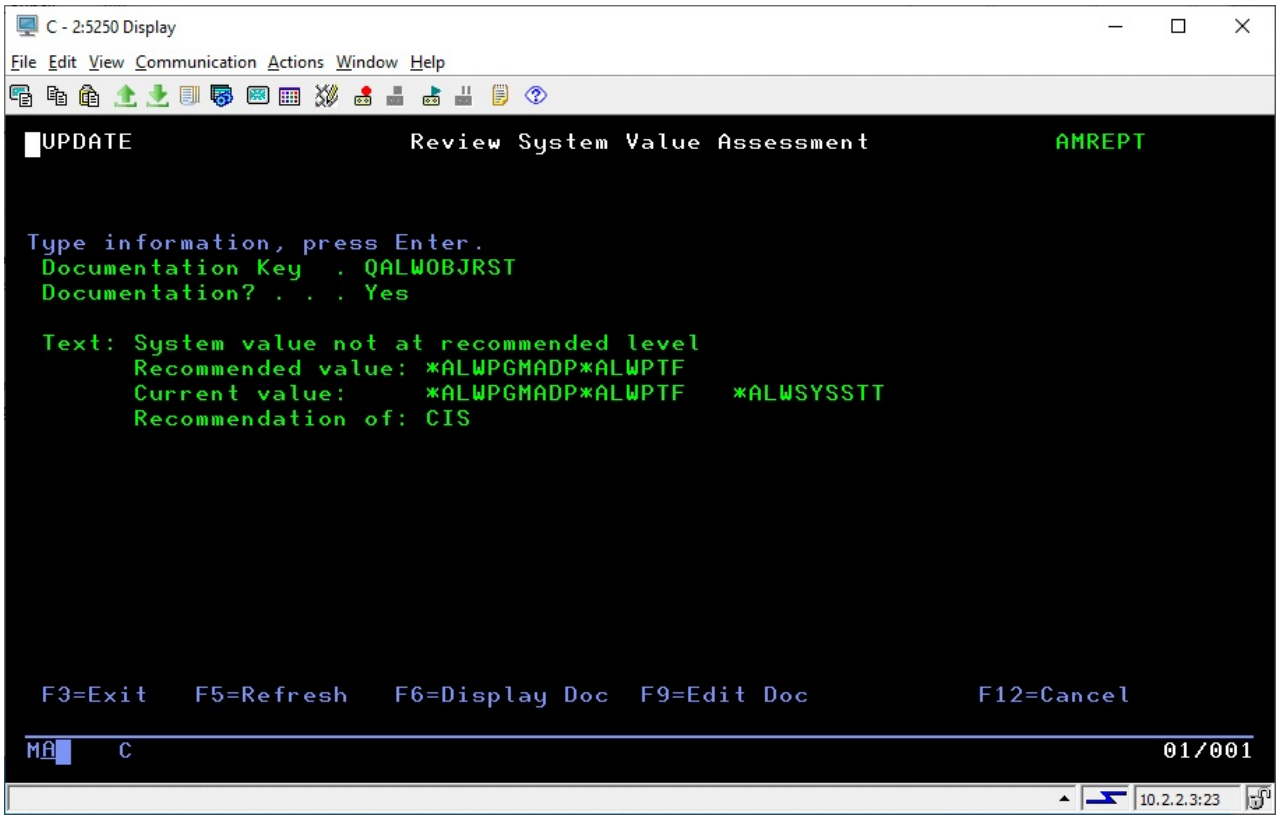
6 Displays the document on file for this exception

8 Lets you work with the system value to make changes

9 For an exception that has not been documented, you can create a document entry here.

There is also an F9 function key available to toggle the display between showing exceptions with documentation or only limiting the display to undocumented exceptions.

When you use option #5 to display more details, the following screen will be shown:



This will show more information about the exception. It also gives you the following function keys to use:

F6 Displays any document that is on file for this exception

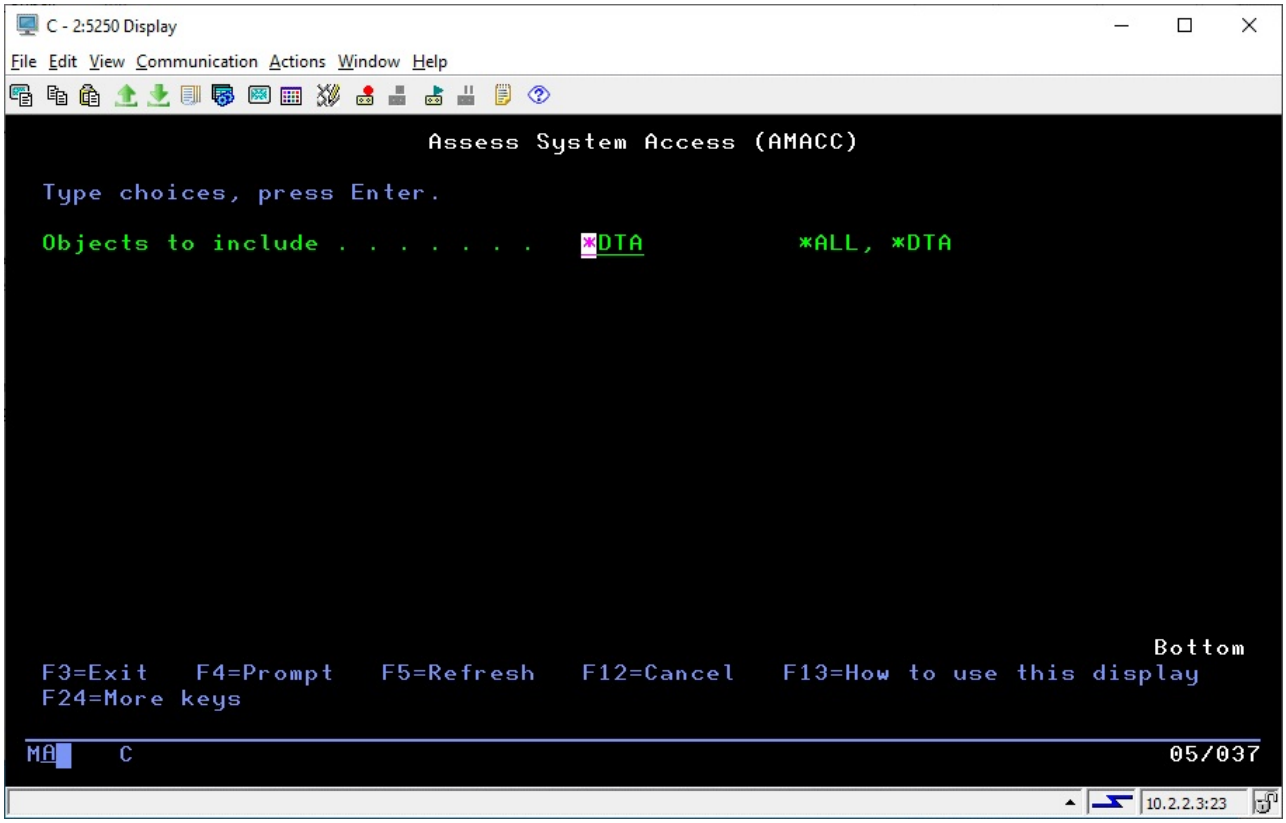
F9 Is a document is already available, you can edit it using this option. To create a new document, use option 9 on the previous display.

Once you have made adjustments as a result of the system value assessment, you can rerun the assessment and check the results to make sure the desired results have been met.

System Access

The System Access assessment checks your system for objects that are publicly accessible and issues a report on them. The assessment is limited to those libraries that are identified as being sensitive. This is done using menu option #39 on the ASSESS menu. See specific instructions for this process below. When the assessment runs, a report will be generated and a CSV file will be generated in the IFS based on the assessment results. The file is named /kisco/ismdnload/assesacc.csv.

Before you run this assessment, we recommend that you run option #5 on the Audit menu to make sure that all library information has been updated. To run the System Access assessment, select menu option #2 on the ASSESS menu and the following prompt will be shown:



Choose the option that you want to use for this access assessment process:

*DTA Only data file objects will be checked (*FILE)

*ALL All objects will be checked

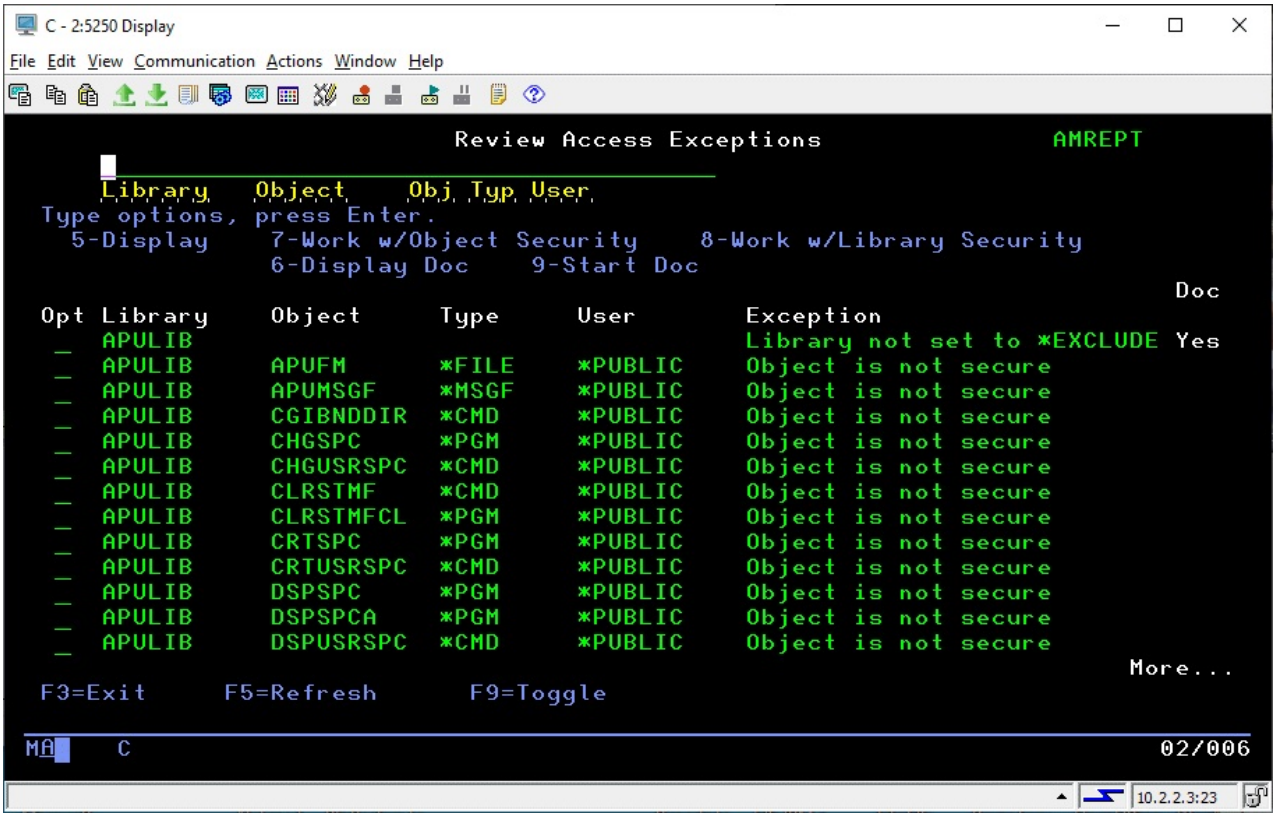
When you press ENTER, the assessment will run for the libraries that you have identified to be included.

To work with the system access assessment, run menu option #22. You will be prompted for the following options:

Choose from the following options:

*ALL	All assessment exceptions will be shown
*EXCP	Only those exceptions that have not been documented will be shown

The results of the most recent assessment with always be shown as follows:



When a “Doc” column on the right side of the panel shows “Yes”, this indicates that the exception shown has a document associated with it that is already on file.

The following options can be selected for any of the exceptions shown:

5	Displays more details for the exception
6	Displays the document on file for this exception
7	Lets you work with object security for a specific object (not valid on a line that just shows a library)

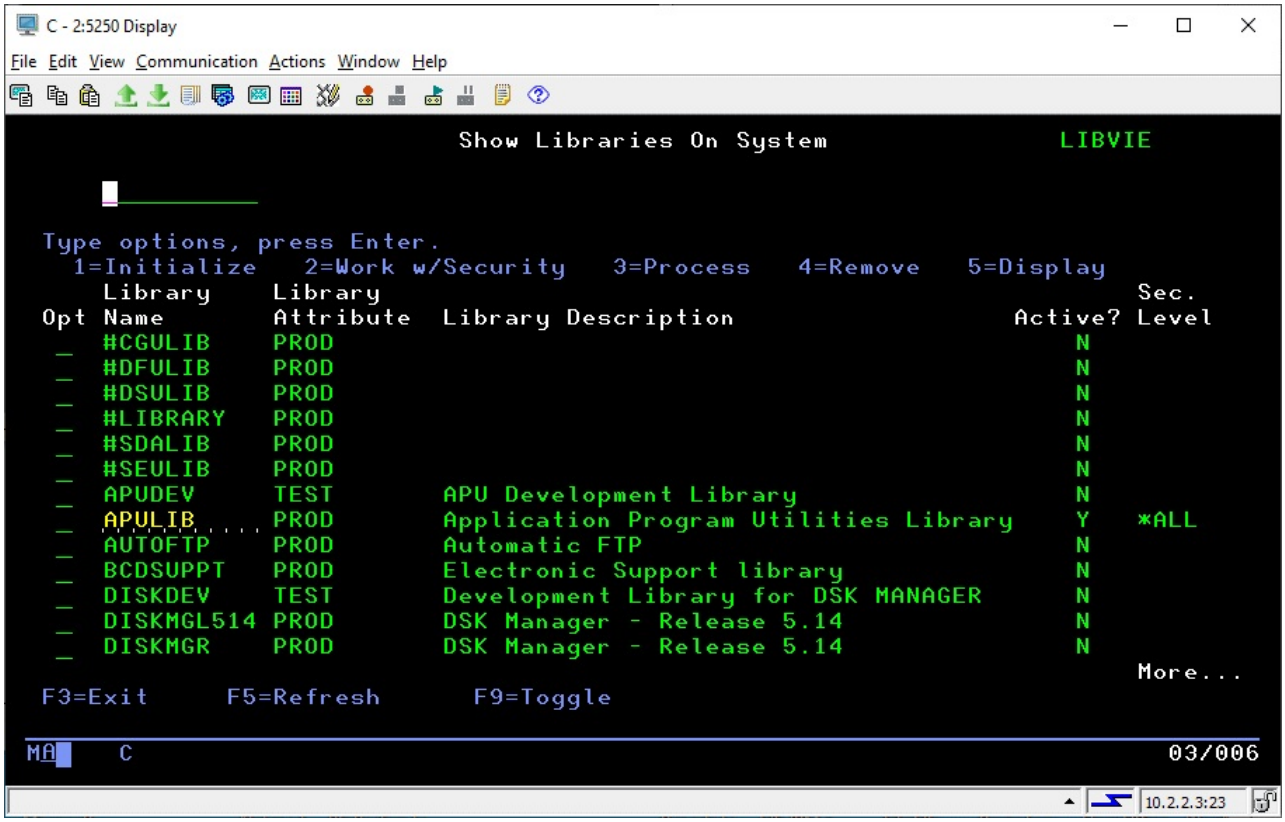
8 Lets you work with library security to make changes for the library (not valid on a line for a specific object)

9 For an exception that has not been documented, you can create a document entry here.

There is also an F9 function key available to toggle the display between showing exceptions with documentation or only limiting the display to undocumented exceptions.

Library Selection

For the System Access, you will have to indicate which specific libraries you want to be included for assessment purposes. To configure the libraries to be included, you can use option #39 on the Assessment menu. When you start this process, a list of current libraries on your system will be shown as follows:



Libraries that have been selected will be shown with a Y in the Active? column. The Sec. Level column must show a value of *ALL to be included for assessment. When a library is selected for assessment, you should be aware that it is also selected for object security auditing. When you start this process, you may see libraries already specified, but they will have the value *SEL in the Sec. Level setting. For those to be included for assessment purposes, this must be updated to *ALL.

An F9 function key is available that will switch between showing all libraries or just those that have already been selected showing a Y in the Active? column.

The following options can be selected to work on individual libraries shown on the display:

1 Initialize - the selected library is initialized for audit purposes and system access assessment.

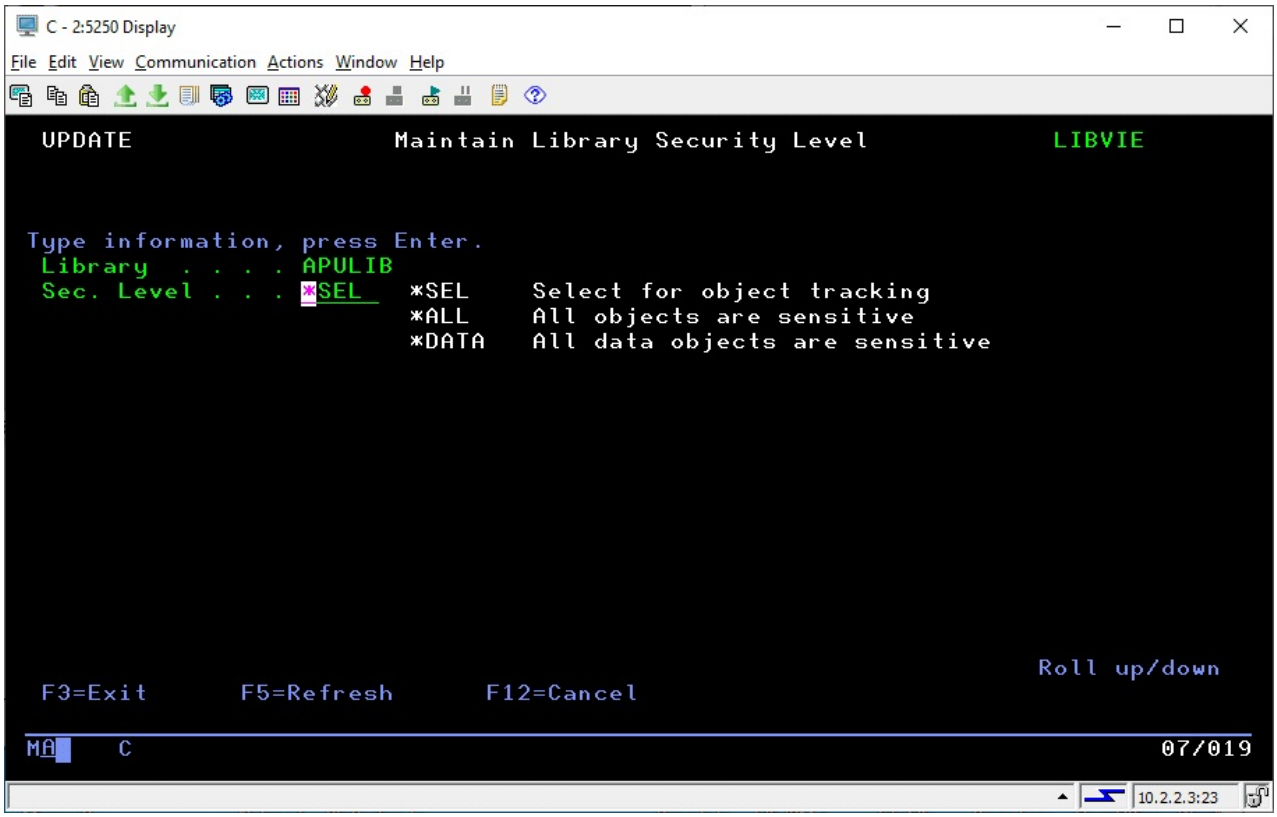
2 The security configuration for the selected library can be changed or removed from processing.

3 Will run an object audit against the current baseline of objects for this library.

4 Will remove a library from audit and assessment processing.

5 Will display information about the library.

To specify a library for inclusion for system access assessment, you must first initialize it using option 1. Once that has been done, the Sec. Level must be changed to *ALL. You can do this by placing a 2 next to the library after it has been initialized. The following will be displayed:



Set the Sec. Level as follows:

*SEL The library will be included for audit purposes, but not for assessment

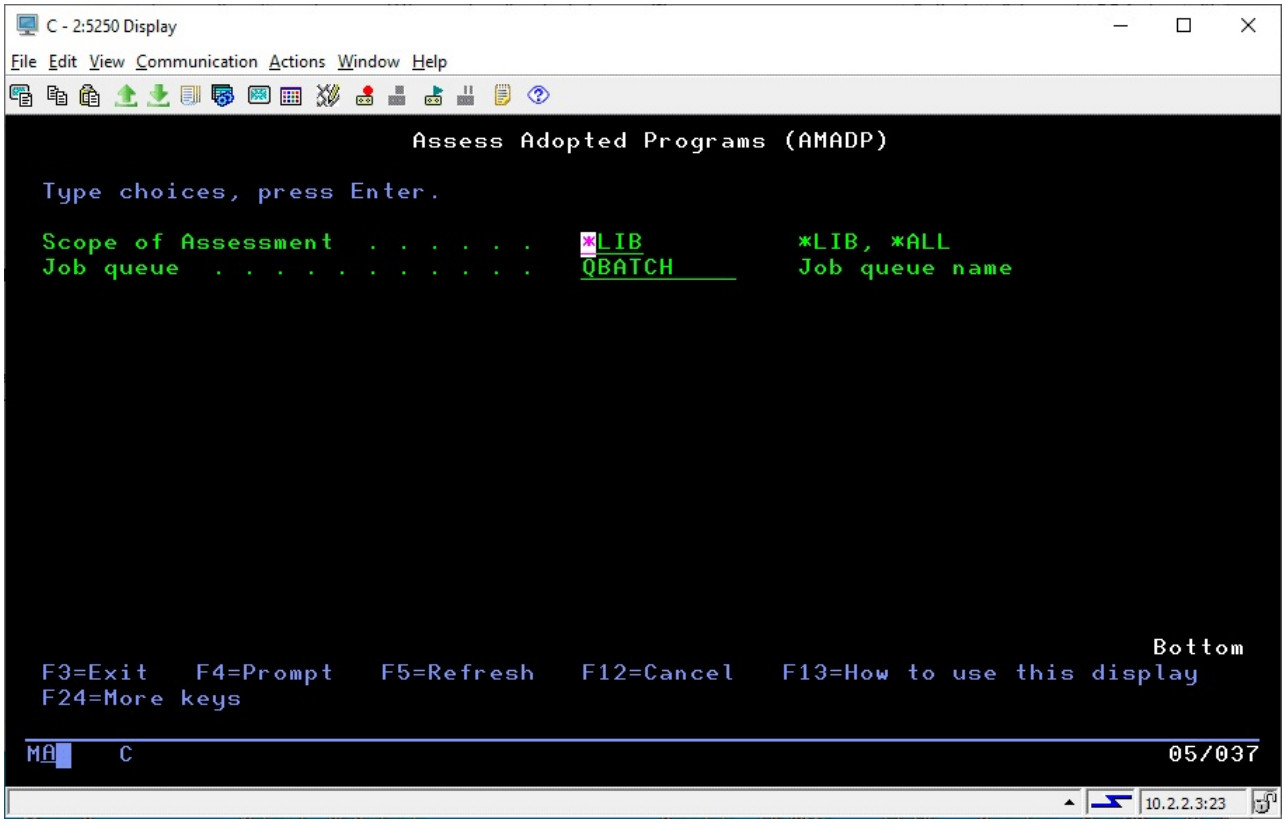
*ALL All objects in the library will be included for both audit and assessment processing

*DATA All objects in the library will be included for audit processing but just the data objects will be included for assessment processing.

Adopted Authority

The IBM i OS allows you to provide increased access to objects on your system for users who have very restricted user profiles. This allows an entry level clerk to use the Accounts Payable application at the program level while preventing them for open access to that same data. Along with this feature, however, there are inherent risks that need to be avoided. The Adopted Authority assessment tool will provide you with the ability to identify programs that adopt authority and also highlight those that have a further risk caused by giving the end user access to a command line.

To run an Adopted Authority assessment on your system, select option #3 on the Assessment Menu. The following options will be shown:



Choose the options as follows:

Scope of Assessment Select from the following options:

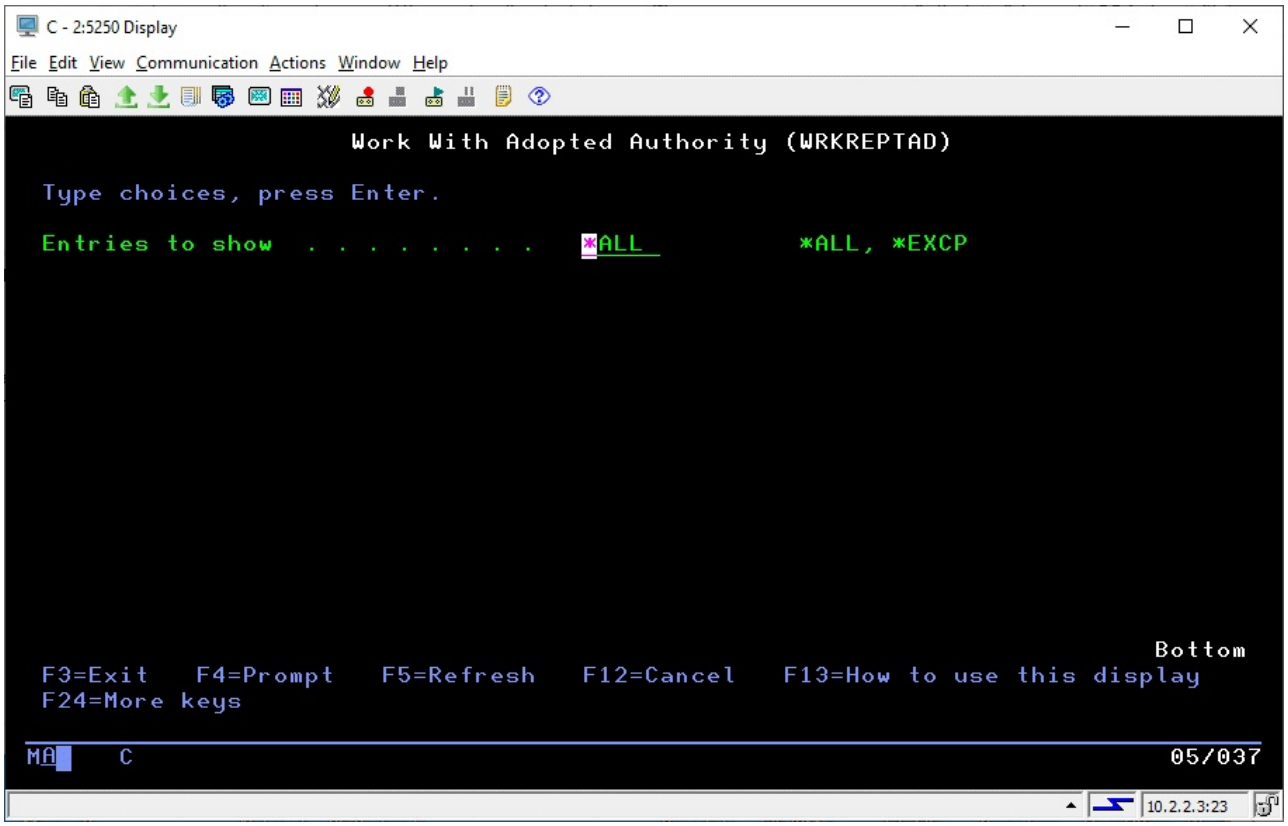
*LIB Only library level security will be checked - this will run faster than the *ALL option but will not include all possible risks.

*ALL All risks will be assessed during the process.

Job queue The Adopted Authority assessment can take a long time to run. It is best run in batch. Specify the batch job queue that you want to use here. The job queue must be available in your current session library list.

When the assessment runs, each program that adopts authority will be checked to make sure that it cannot be accessed publicly. When run with the *LIB option, the library where it resides will be checked to make sure that it has public *EXCLUDE access. When run with the *ALL option, additional checks will be made to any related authorization lists and group profile settings. All libraries on your system are checked, not just those selected for object audit and assessment processing. Results of the assessment will be issued on reports at the end of the assessment process.

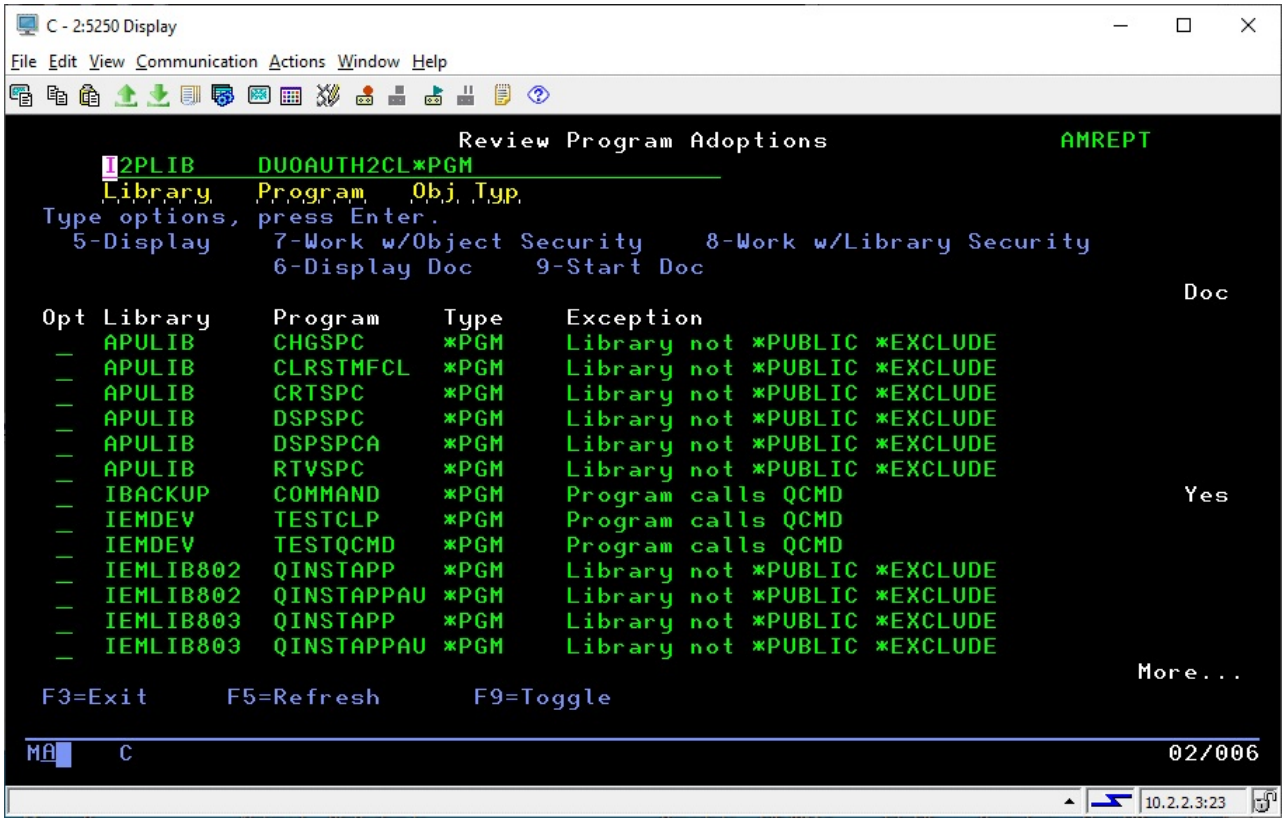
To review and work with the results of your assessment, use menu option #23. A screen similar to the following will be shown:



Choose from the following options:

*ALL	All assessment exceptions will be shown
*EXCP	Only those exceptions that have not been documented will be shown

The results of the most recent assessment with always be shown as follows:



Programs and service programs that adopt authority and also have security access exposures will be shown. In the above example, programs were selected where the library they reside in were not secure and some programs with adopted authority were found to contain calls to QCMD, a possible serious security risk.

If the word “Yes” appears in the Doc column on the right, then an exception note for the item shown has been created. You can use the F9 Toggle key to include or exclude those items where the risk has been documented.

The following options can be used on individual items in the list:

5 Displays the details for the listed object. If an exception note is on file, there are function keys available on the detail display to view and/or update the note.

6 Displays an existing exception note

7 Lets you work with the object security for the program

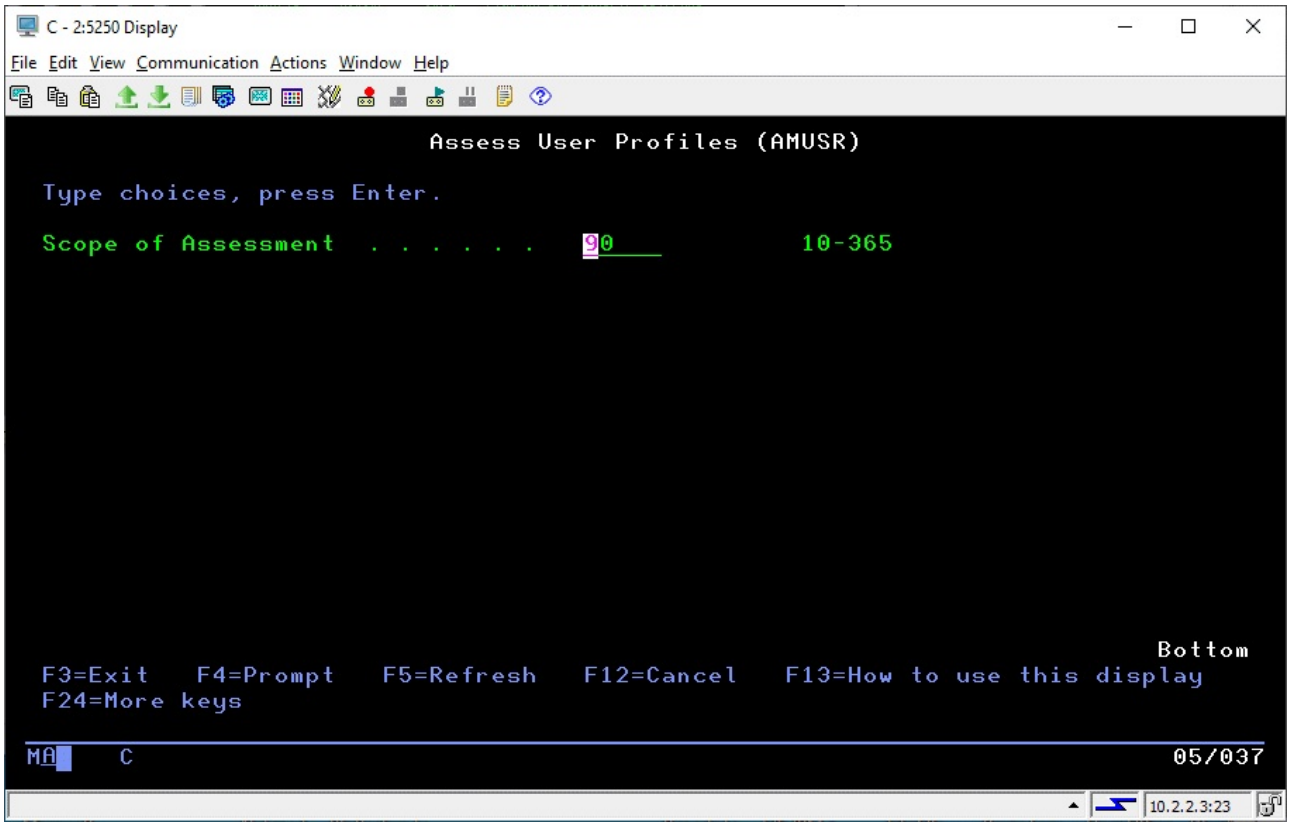
8 Lets you work with the library level security

9 Lets you start an exception note for the program

User Profiles

User profiles can also present security risks on your IBM i system. The Assessment tool can be used to examine the user profiles on your system and list known security weaknesses for each profile identified.

To run the user profile assessment, select option #4 on the Assessment menu. The following option will be shown:



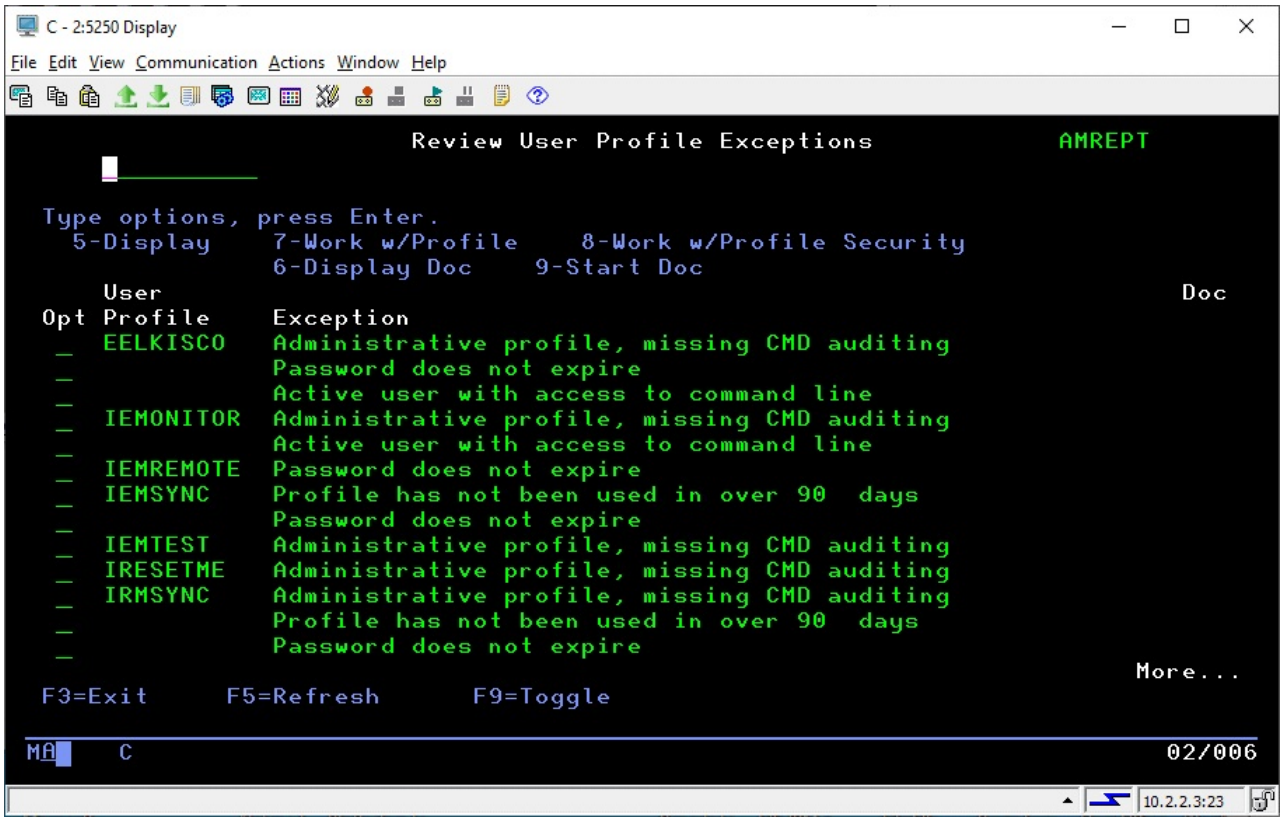
One of the user profile assessments will check for active profiles that have not been used in a given period of time. Enter the number of days unused that you want to use for this particular assessment. When you press ENTER, the user profile assessment will run.

To review the results of the user profile assessment, choose menu option #24. You will be prompted for the following options:

Choose from the following options:

*ALL	All assessment exceptions will be shown
*EXCP	Only those exceptions that have not been documented will be shown

The results of the most recent assessment with always be shown as follows:



In this example, several risks have been identified for the user profiles shown. Each of these exceptions should be investigated and a decision made as to whether the risk should be accepted. For those where you want to accept the risk, you should document your decision with an exception note. If the word "Yes" shows in the right hand column headed "Doc", then a note is already on file. You can use the F9 Toggle function key to suppress those with notes already on file.

The following options are available for each exception shown:

5 Displays the details for the listed object. If an exception note is on file, there are function keys available on the detail display to view and/or update the note.

6 Displays an existing exception note

7 Lets you work with the settings for the user profile shown

8 Lets you work with the user profile object security

9 Lets you start an exception note for the program

Network Services

The Network Services assessment checks several network related areas on your system for potential security risks. These include network attributes, Telnet attributes, FTP attributes and Exit Points. To run the Network Services assessment, just select option #5 from the Assessment menu. There are no parameter settings. When the assessment completes, a listing will be generated showing the results.

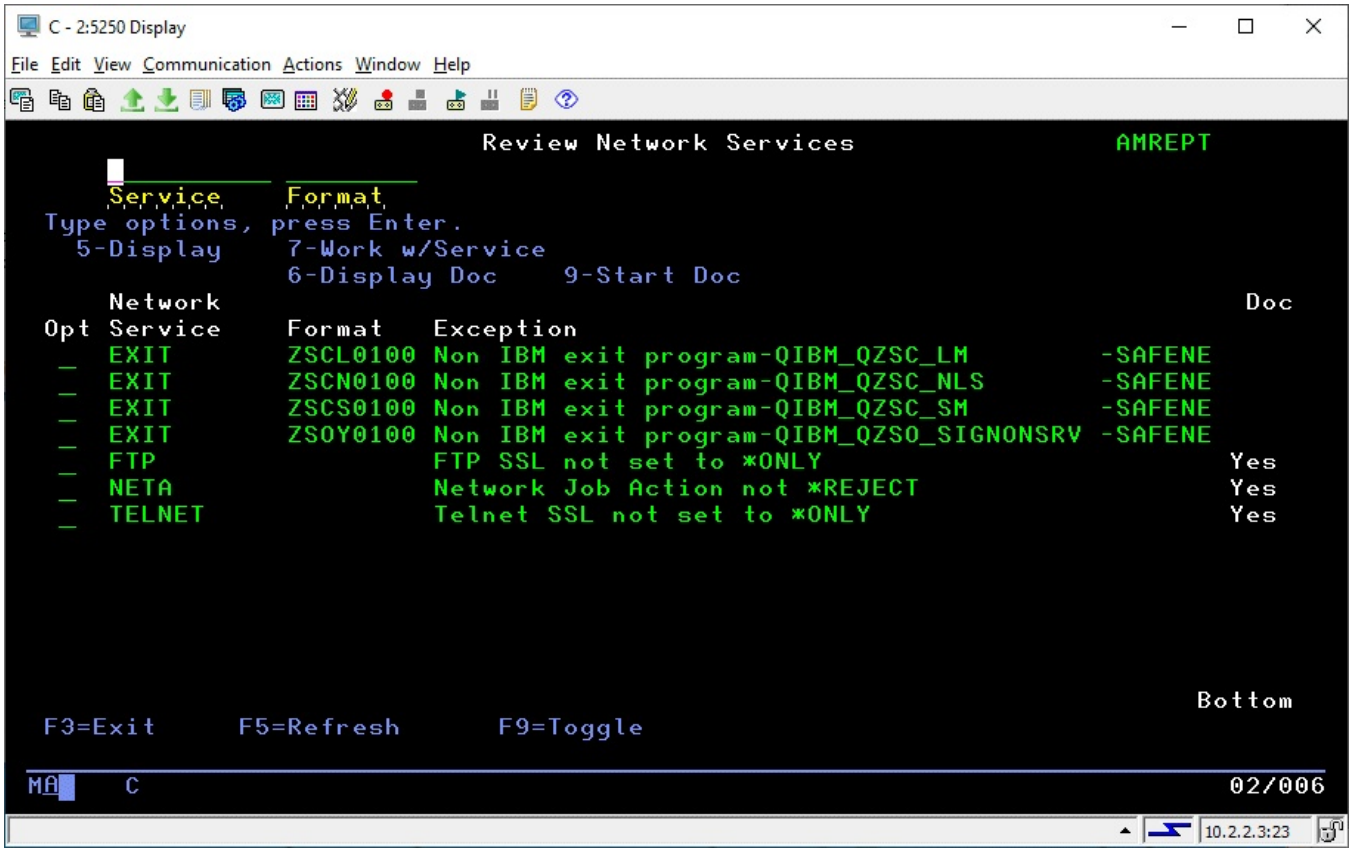
To work with the assessment, run menu option #25. You will be prompted for options.

Choose from the following options:

*ALL All assessment exceptions will be shown

*EXCP Only those exceptions that have not been documented will be shown

The results of the most recent assessment with always be shown as follows:



In this example, several exit point program registrations are shown along with an FTP, Network Attribute and Telnet exception. When the work "Yes" shows on the right column, that indicates that an exception note is on file for that exception. You can use the F9 Toggle function key to suppress the exceptions where notes are already on file.

The following options are available for each exception shown:

5 Displays the details for the listed object. If an exception note is on file, there are function keys available on the detail display to view and/or update the note. To see the full exit point registration information, you will need to use option 5.

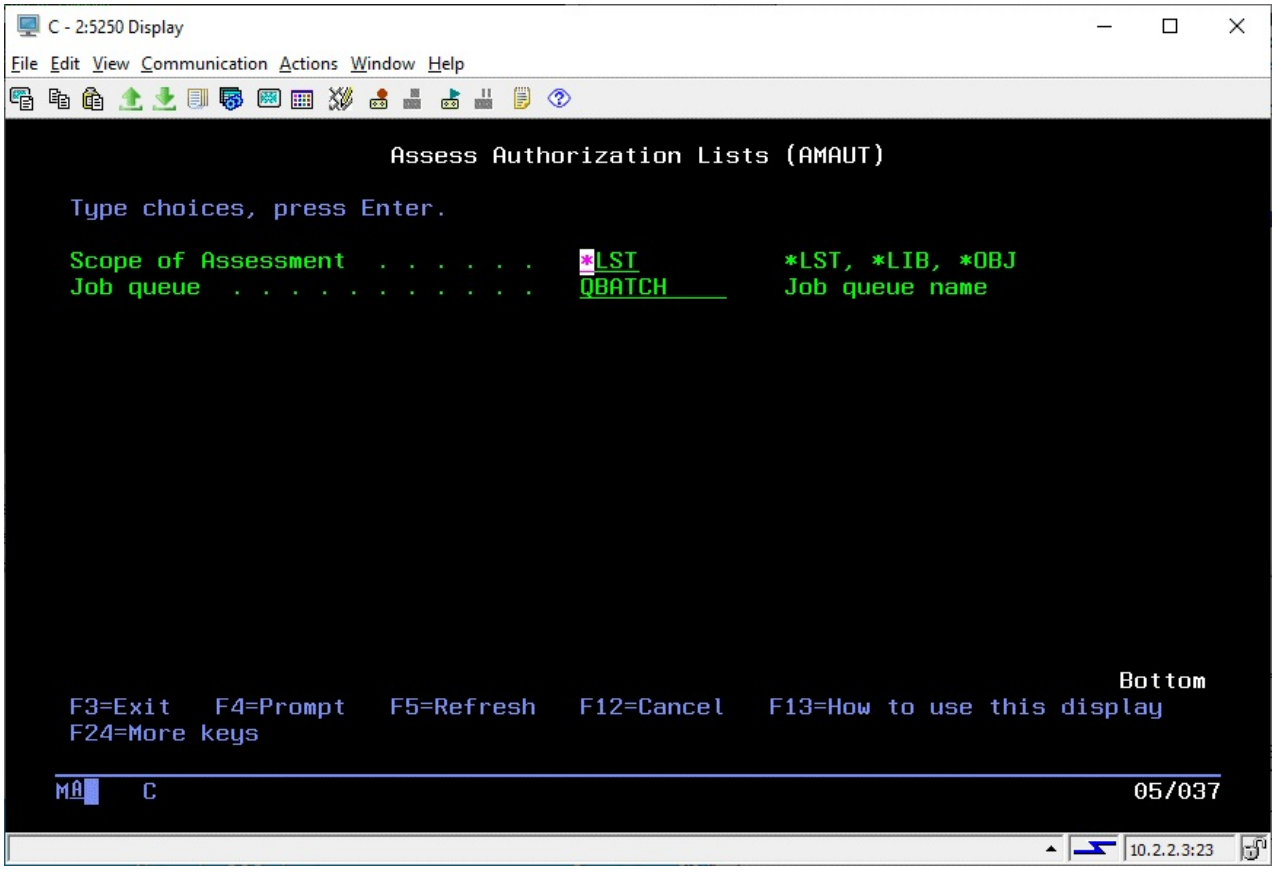
6 Displays an existing exception note

7 Lets you work with the settings for the network service shown. For exit points, you can view the exit point and the program registration. For the other three network services, you can view the setting in question and make changes if needed.

9 Lets you start an exception note for the network service

Authorization Lists

The Authorization Lists assessment checks all of the lists on your system and reports on any that have security weaknesses. When you run option #6 from the ASSESS menu, the following prompt will be shown:



The Scope of Assessment option controls how much assessment is done. You can choose from the following values:

*LST Only the authorization list objects themselves will be assessed.

*LIB Both the authorization list objects and any libraries that are secured by the

authorization list will be assessed.

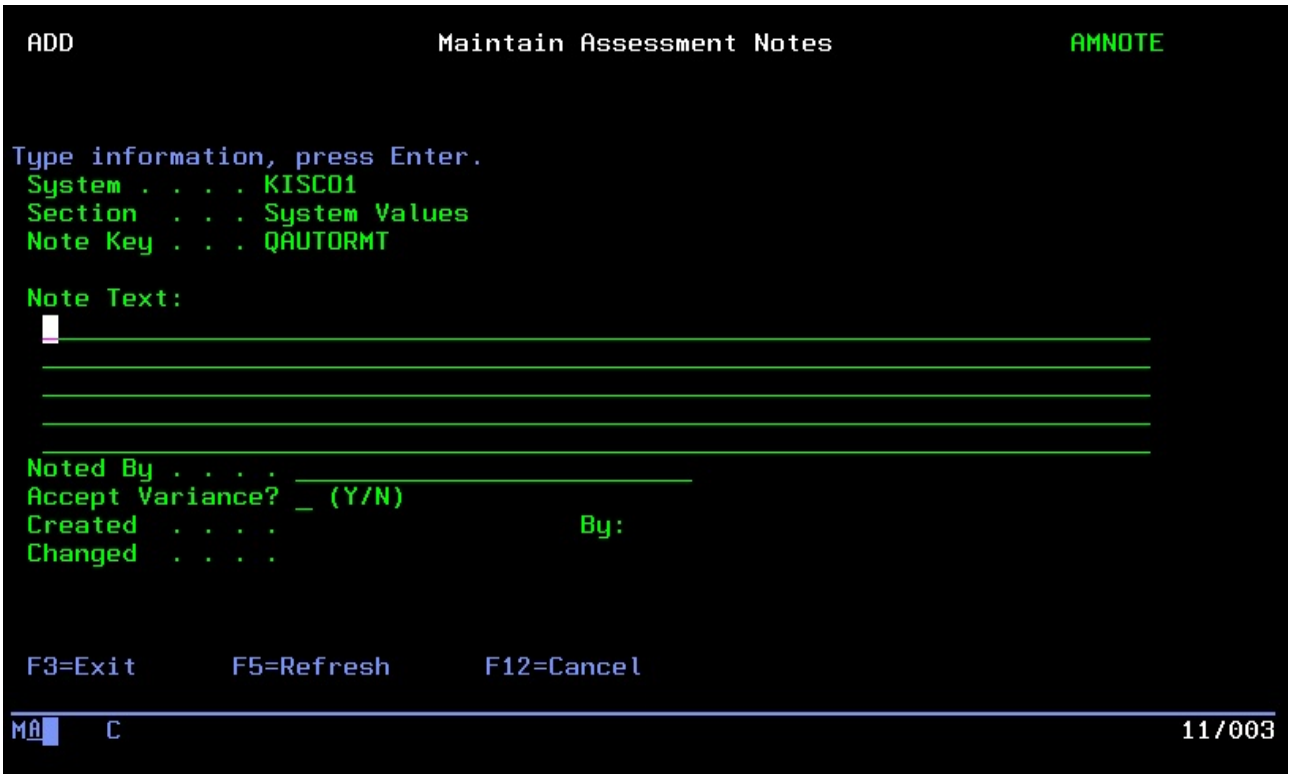
*OBJ The authorization list objects, any libraries that are secured by the authorization list and the objects within those libraries will be assessed.

The *LST option will run very quickly, the other two options will take longer to run. If you want to run the option in line rather than in batch, change the Job queue option to ' ' with the quotes.

Option #26 on the ASSESS menu will let you review the results of the most recent assessment.

Exception Notes

For each assessment review (menu options 21-26), there are options to create exception documentation (or exception notes). To start an exception note, the 9 option next to the exception shown will start the process. When you do, the following detail screen will be displayed:



To create the note, you must fill in the first line of the text note and the "Noted By" field. When you store the note, your user profile and the current date and time will also be stored. If the note is later changed, then the user profile and date and time of the change will also be recorded. This process is the same regardless of which assessment is being referred to. Be sure to indicate in the "Accept Variance?" field whether or not your note indicates that you are accepting this variance from best practices or not.

Assessment Summary

At any point, you can summarize the current assessment status using option 30 on the ASSESS menu. A report will be generated and the contents of the report will be placed into a CSV file in the IFA on your system. Whenever you rerun any assessment options (menu options 1-6), the Assessment Summary will change to take the new results into account.

Installation and Configuration

Before any iSecMap functions will work, the initial install procedure must be run. iSecMap can be installed from a download file obtained from the Internet. Installation instructions are included on the web page where the software is downloaded from.

Installation from Download

We recommend that you use the install instructions from the iSecMap Download web page.

https://www.kisco.com/ism/ismdload.html

After you download the install file from the website, print the Download page and use it as a check list while completing the installation.

Release Upgrade Installation

When Kisco Systems LLC completes work on a new Release of iSecMap, you will be notified of the availability for the new release. New releases are available as a download. You can use the same install instructions from the download page.

Configuring Email for iSecMap

To use the email features in iSecMap for email notification and alerts, you must first go to the INSTALL menu and run option #9. See the "iSecMap Global Settings" section of this manual below. The first three settings on this display must be configured along with the last setting. The second and last settings must be valid email addresses. The "Support email address" will be used to identify the sender of each email message only when the first parameter is set to *NO. The "Notify By Email" setting will be where the email will be sent and can include up to 5 different email addresses.

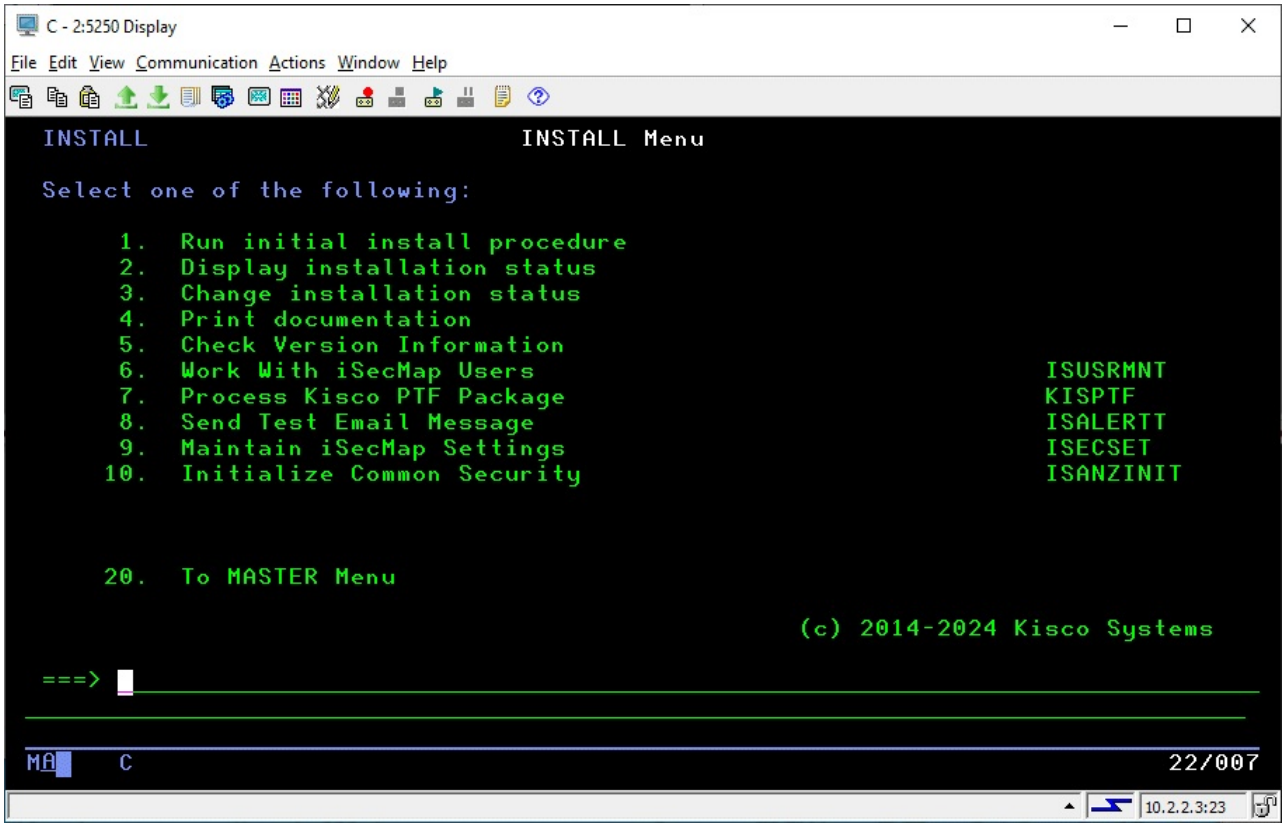
You can also find help for email configuration issues at our website at this address:

https://www.kisco.com/emailconfig.html

Once you have this configured, then use menu option #8 to send a test email to confirm that email gets delivered. There is more information about this test process in the "Send Test Email Message" section of this manual.

The Install Menu

When you select item 20 from the MASTER menu, the installation menu is displayed as follows:



Menu items perform the following functions. Each function is discussed in greater detail later in this document:

1. Run initial install procedure - DO NOT USE THIS OPTION unless directed to do so by Kisco Support staff. This option is automatically run during normal install processing.

2. Display installation status - Displays a screen showing the current installation status for the software.

3. Change installation status - Displays the current software installation status and allows for changes to be made.

4. Print documentation - Prints this documentation manual to the default print device.

5. Check Version Information - Displays information about the specific version of iSecMap that is installed on your system.

6. Work With iSecMap Users - Lets you control which user profiles can access iSecMap information and administer the software.

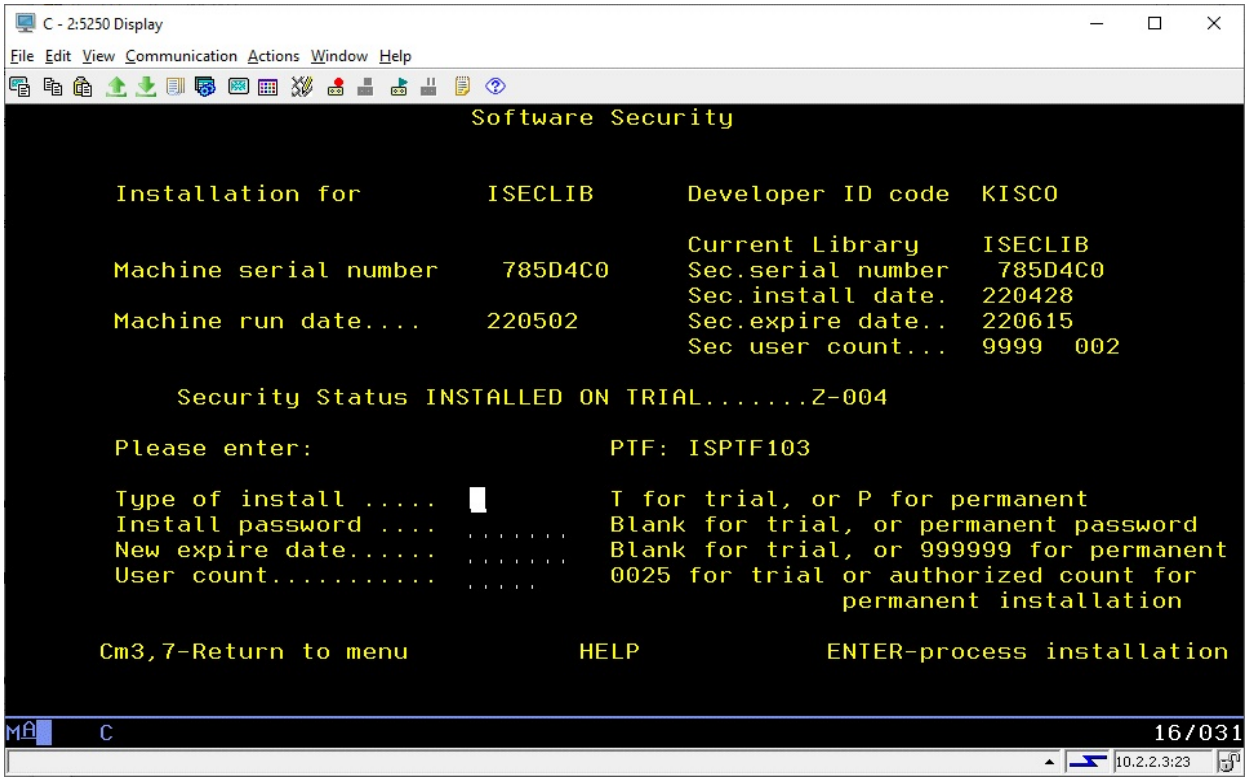
7. Install Kisco PTF package - Allows you to process a corrective PTF package received from Kisco for program fixes.

8. Send Test Email Message	Sends a test email message to the email address that you provide. Used when getting email notification configured.
9. Maintain iSecMap Settings	Lets you set up default settings for iSecMap.
10. Initialize Common Security	Initializes all common baseline information in iSecMap in a single process. (**Not recommended**)
20. To Main Menu -	Will display the iSecMap MASTER menu.

Details on each of these menu options are covered in the following sections of this documentation.

Display installation status

At any time, you can check the current installation status of your copy of iSecMap by selecting this menu option. You must be signed on with security authority of QSECOFR or equivalent. The following screen will be displayed:



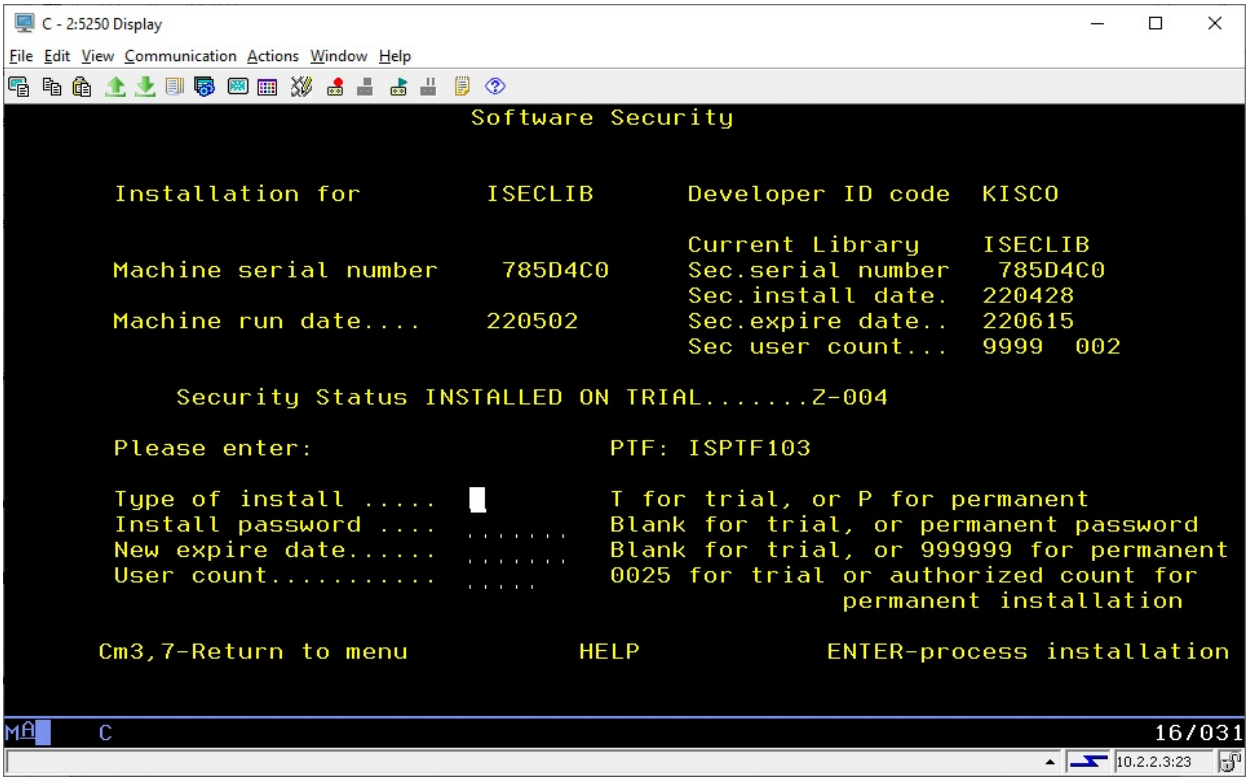
The message at the center of the screen indicates your current installation status. You should also check the Sec. expire date for an expired trial period. iSecMap may still show as installed on a trial basis but, if the trial is expired, it will no longer function.

The following are the possible status messages that can appear on this display:

Message	Explanation
Z-001 NOT INSTALLED	Trial installation not started
Z-002 TRIAL EXPIRED	Trial period has ended
Z-003 PERMANENTLY INSTALLED	Software is permanently installed
Z-004 INSTALLED ON TRIAL	Software is installed on trial
Z-005 PASSWORD NOT ACCEPTED	Password keyed is not valid
Z-006 WRONG LIBRARY	Programs must run from our library
Z-007 PLEASE RUN TRIAL INSTALL	Must have trial install before perm.
Z-008 INVALID INSTALL REQUEST	Must be P or T
Z-009 INVALID SECURITY (REC#6)	Call Kisco
Z-010 INVALID SECURITY (NO ZZ)	Call Kisco
Z-011 INVALID SECURITY (HASH.)	Call Kisco

Change installation status

To make changes to your installation status, use this menu option. The changes processed can include both a trial period extension and permanent installation. You must be signed on with QSECOFR security authority or equivalent. When you select this option, the following screen is displayed:



Trial extension

To extend a trial period, contact Kisco Systems LLC and request an extension. We will provide you with an extension password and new expiration date. On the above screen, enter the following:

Type of install	Enter 'T' for trial
Install password	Enter all six digits of the extension password provided, including any leading zeros
New expire date	Enter the new expiration date in the format YYMMDD (ie: Jan 12, 2014 would be 140112)
User count	Enter the number of users that you are authorized for from Kisco

When the parameter fields have been completed, press enter to reactivate your software.

Permanent installation

To permanently install your software package, use the permanent password provided by Kisco Systems LLC following receipt of payment. On the above screen, enter the following:

Type of install	Enter 'P' for permanent
Install password	Enter all six digits of the extension password provided, including any leading zeros
New expire date	Enter all 9's (ie: 999999)
User count	Enter the number of users that you are authorized for from Kisco

When the parameter fields have been completed, press enter. Your software is now permanently installed.

Print additional documentation

At any time, you can reproduce the additional documentation by using this menu option. A full copy of the additional documentation topics will be printed.

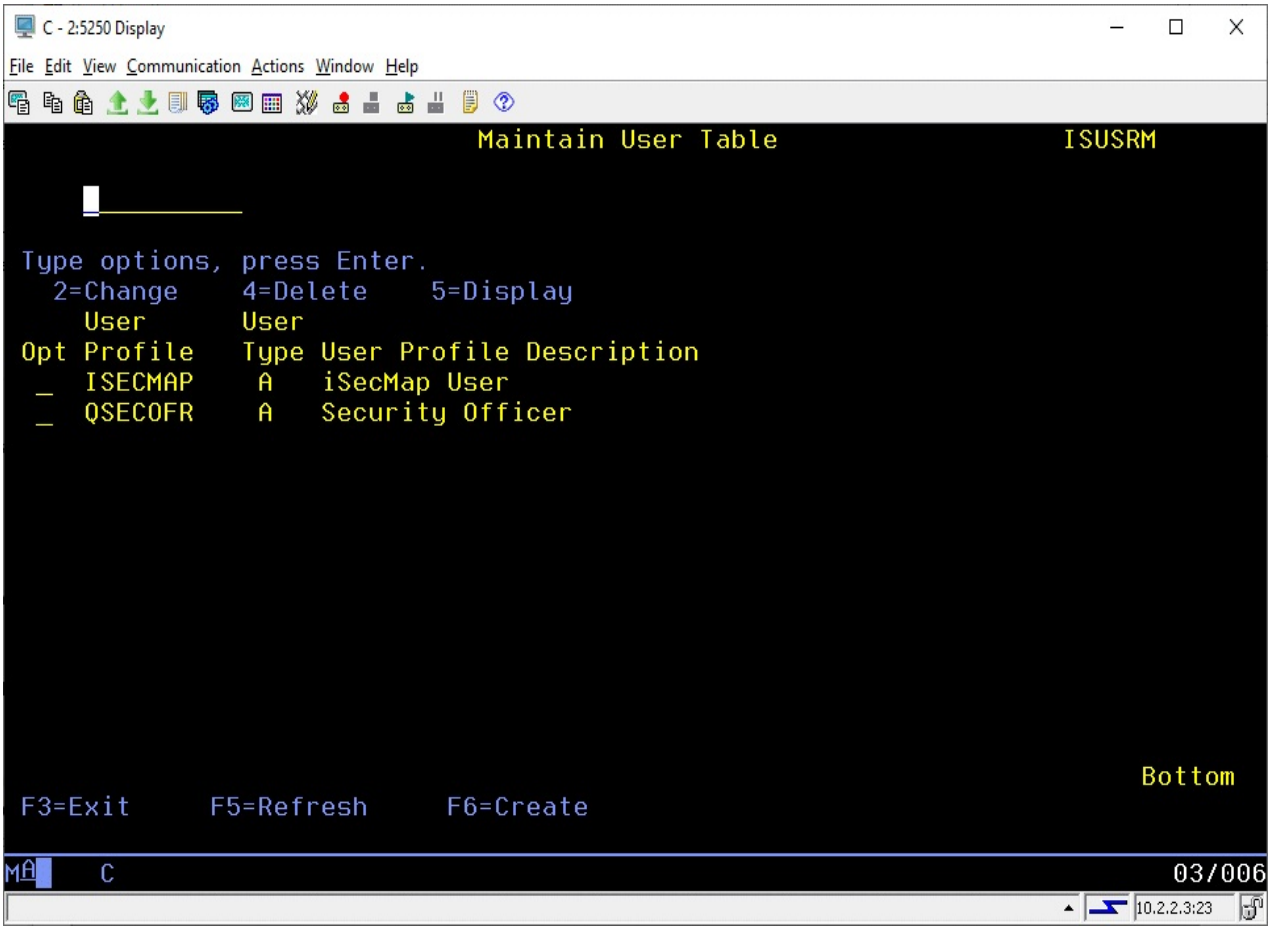
Display Software Version Information

This menu option will display the current release level and PTF information for your version of iSecMap. The developer may need to verify this when working with you on a support issue.

Work With iSecMap Users

iSecMap lets you grant access to the information in the software at two different levels, User level and Admin level. At the user level, you can look at the information but not make any changes. At the Admin level, you have full access to use the software. When the software is first installed, two user profiles are granted Admin access; QSECOFR and ISECMAP. These two cannot be deleted or changed. You can use option #6 on the INSTALL menu to work with the users.

When you start option #6, the following screen will be displayed:



In order to use this menu option, you must already be logged in as an Admin for iSecMap. Initially, this will be restricted to the QSECOFR profile.

To add a user profile to this list, use the F6 function key and enter the profile and account type. You must use a valid user profile for your system. User Type U will be for user accounts and A for Admin accounts. We recommend that you create at least one additional Admin account for iSecMap so that you can limit the number of times that the QSECOFR user profile is used on your system as an active account.

Install Kisco PTF Package

iSecMap supports distribution of program updates remotely via the Internet. When programs in iSecMap are updated or program fixes are required, Kisco Systems LLC can send the updates directly to you via the Internet. If needed, we will send E-mail to you with an attached PC file. This file, when loaded into a folder on your system, can be used to post program updates and changes to your copy of iSecMap.

When you receive a PTF update package from Kisco, you will be given an eight character PTF Package Name. To load and apply the PTF to your system, follow these steps:

Step# Instructions

1. Create a folder on your system named KISCO. You can do this with the following command:

   CRTFLR FLR(KISCO)

   Note: This folder only has to be created the first time you install a PTF. If you have other software products from Kisco Systems LLC, they all use this same folder.

2. From a PC that is attached to your system, move the PTF Package file that you received from Kisco into this folder. If you are not familiar with this process, please check the following URL at the Kisco website for specific instructions:

   https://www.kisco.com/pctoflr.htm

3. Sign on to any terminal or terminal session as QSECOFR or equivalent.

4. Make sure that no iSecMap functions are in use and that no users are logged into any iSecMap menu.

5. Type the following command:

   ISECLIB/KISPTF

   and press the F4 prompt key. You can also choose option #7 from the INSTALL menu.

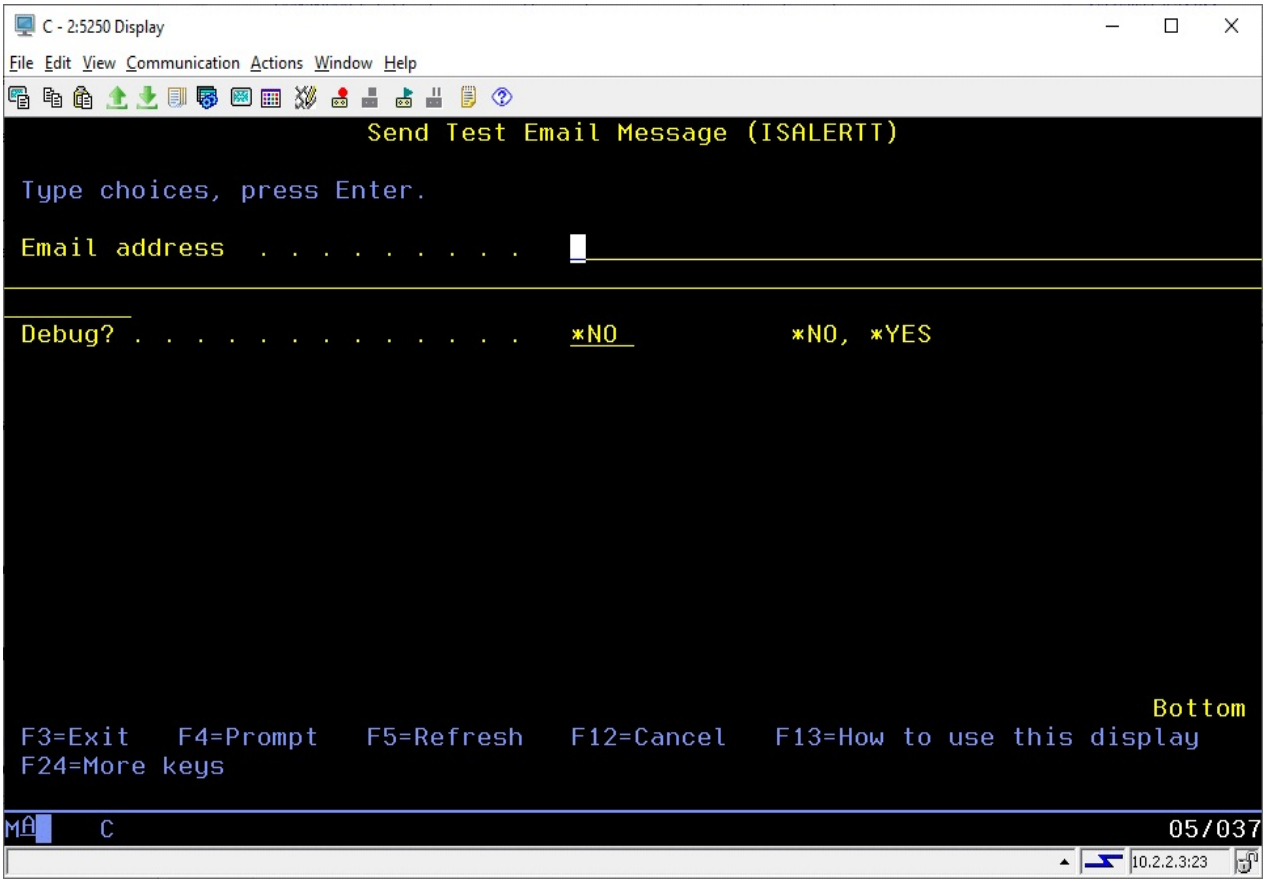
6. The command will prompt for two values. The first is the name of the iSecMap application library and should not be changed. The second parameter must contain the eight character name of the PTF Package File. When both parameters are set, press ENTER and the PTFs will be loaded and applied to your copy of iSecMap.

7. All Kisco PTFs are loaded so that the prior version of any program objects is saved. This will allow for the effects of a PTF to be reversed at a later time should a defect be identified in the PTF. This can only be done via direct instruction from a Kisco support representative.

During the PTF installation process, one or two printouts will be created. The first of these will be the PTF Cover Letter Documentation. The second is optional and, if printed, will be a fresh update of the additional documentation topics for all iSecMap changes. Kisco recommends that you read both documents before starting to use iSecMap again.

Send Test Email Message

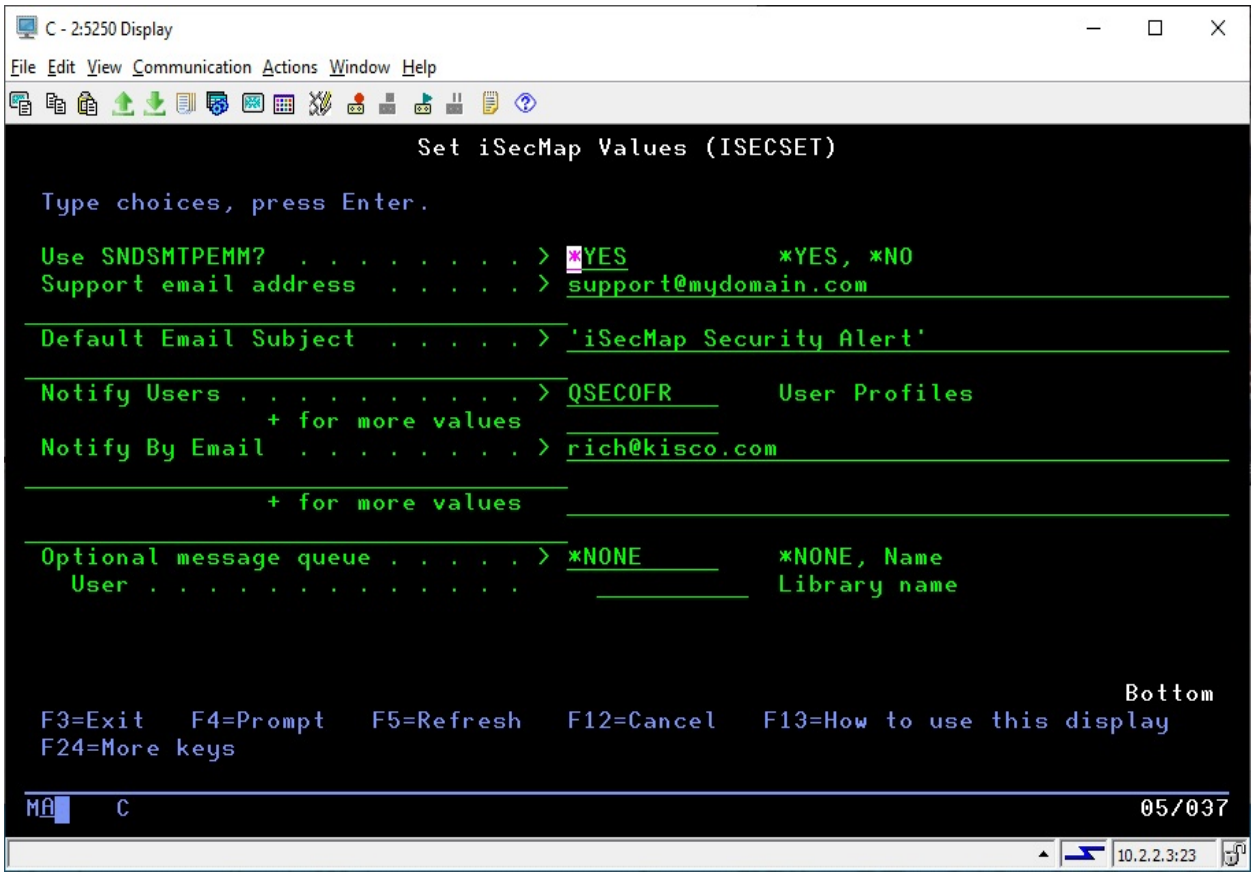
If you are going to use the iSecMap Security Monitor and you want to use notification by email, then you must first check to make sure that email transmission is working on your system. To send a test email using the iSecMap email notification feature, select option #8 on the INSTALL menu. The following prompt field will be shown:



Enter a valid email address where you want to send the test and press ENTER. If the email gets delivered, then you know that the process is configured correctly and will work. If no email arrives and you have the SNDSMTPEMM? option set to *NO (see option 9 above), rerun the test changing the DEBUG option to *YES. This will generate a short trace listing in to your terminal session output queue. Check this for more details. If you cannot determine that cause of the issue, send the listing to Kisco support for assistance.

iSecMap Global Settings

Choose menu option #9 from the INSTALL menu to set the global settings. The following prompt will be displayed:



Set these parameters as follows:

Use SNDSMTPEMM?	Lets you decide how you want outgoing email sent when using the iSecMap monitor feature. Choose one of these values:
*YES	All outbound email messages will be sent using the IBM i OS protocol based on the SNDSMTPEMM command (Recommended).
*NO	All outbound email messages will be sent using the legacy Kisco protocol which was in place prior to iSecMap Release 3.
Support email address	This field will default to *NONE. While set to *NONE, email notifications cannot be processed. To allow for email notifications, change this to a valid email address for your company. This will be the “from” email for all notifications and will receive any non-delivery notices for failed email transmissions.

Default Email Subject	Enter a default value that you want to use as the email subject when an alert is issued. If you are managing multiple systems, this setting can help you to differentiate alerts that are issued from different sources.
Notify Users	Enter up to 5 user profile names or message queue names. If you use message queues, the queues must exist in a library that is addressable from your system library list. If this value is set to *NONE, no message notifications will be processed on your system.
Notify By Email	Enter up to 5 email addresses for automatic notification purposes. If you leave this value set to *NONE, no email notifications will be processed on your system. **Note**: Before you can use email notification, a test email must be successfully sent from your system using option #8 on the INSTALL menu.