iSecurity Antivirus & Object Integrity Validation

User Guide

www.razlee.com

Contents

Contents 2

About this Manual 4

Intended Audience 4

Native IBM i (OS/400) User Interface 5

Conventions Used in the Document 5

Menus 5

Data Entry Screens 6

Legal Notice 6

Contacts 7

Setting Up Antivirus 8

Setting Antivirus Definitions 9

Defining Alerts 24

Excluding Objects from Scans 26

Connecting to ICAP Servers 32

Updating Virus Definitions 36

Preparing Virus Definition Sources 38

Performing or Scheduling Virus Definition Updates 41

Activating and De-Activating Real-Time Virus Detection 46

Scanning for Viruses 48

Scanning in Batch Mode 49

Scanning in Real-Time 57

Scheduling Virus Scans 59

Viewing Scan Results 62

Displaying Recent Virus Scan and Alert Logs 63

Viewing Quarantined Objects 65

Resetting the Scan Status of Objects 66

Viewing Older Scan Logs 67

Starting a New Log File 68

Validating Object Integrity 69

Reporting on Suspicious Objects 71

-

Managing Suspicious Objects 75
Message Codes for Anti-Virus 78
Installing the iSecurity ICAP Server on a PC 78

About this Manual

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

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

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

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

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

Intended Audience

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

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

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

Native IBM i (OS/400) User Interface

Antivirus is designed to be a user-friendly product for auditors, managers, security personnel and system administrators. The user interface follows standard IBM i CUA conventions. All product features are available via the menus, so you are never required to memorize arcane commands.

Many features are also accessible via the command line, for the convenience of experienced users.

Conventions Used in the Document

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

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

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

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

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

STRAV **> 81 > 32**

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

Menus

Product menus allow easy access to all features with a minimum of keystrokes. Menu option numbering and terminology is consistent throughout this product and with other Raz-Lee products. *To* select a menu option, simply type the option number and press **Enter**. The command line is available from nearly all product menus. If the command line does not appear (and your user profile allows use of the command line), press **F10** to display it.

Data Entry Screens

Data entry screens include many convenient features such as:

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

The following describes the different data entry screens.

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

The following function keys may appear on data entry screens.

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

Legal Notice

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

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

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

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

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

Manual Revised: Tuesday, July 19, 2022

Contacts

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

Setting Up Antivirus

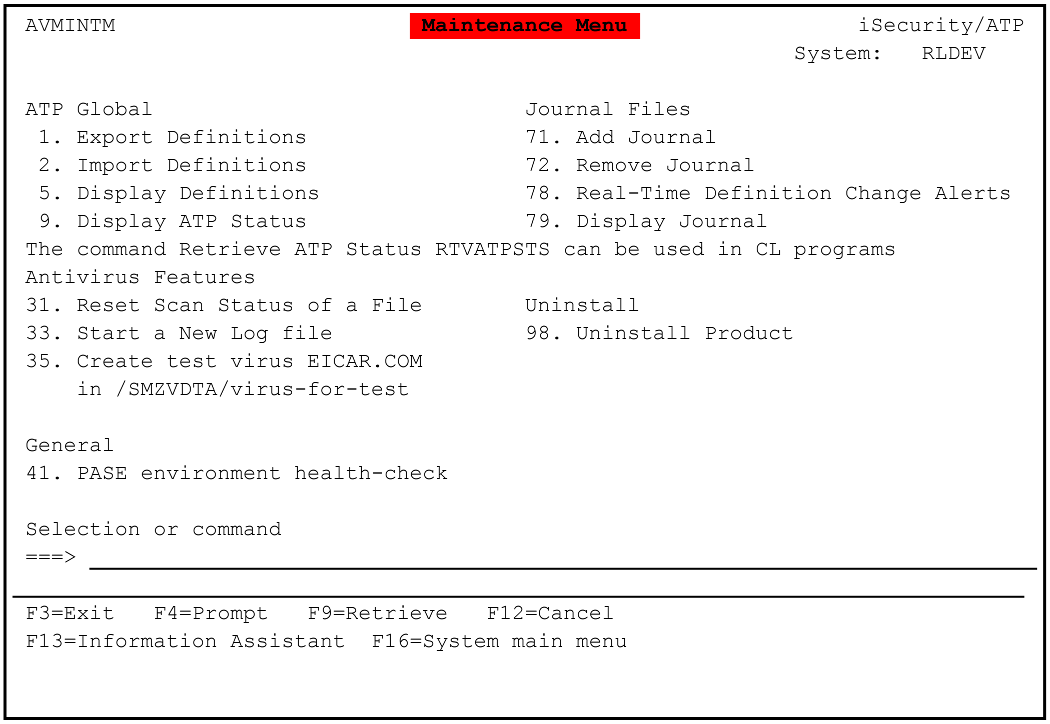
Antivirus uses several parameters and definitions. These need to be set before you run the first scans.

The steps include:

- "Setting Antivirus Definitions" on the facing page
- "Defining Alerts" on page 24
- "Excluding Objects from Scans" on page 26
- "Connecting to ICAP Servers" on page 32
- "Updating Virus Definitions" on page 36

Setting Antivirus Definitions

To **import, export, or display virus definitions**, select **`82. Maintenance Menu`** from the main menu. The **Maintenance Menu** appears:



```
AVMINTM                    Maintenance Menu                 iSecurity/ATP
                                                          System:   RLDEV

ATP Global                               Journal Files
 1. Export Definitions                   71. Add Journal
 2. Import Definitions                   72. Remove Journal
 5. Display Definitions                  78. Real-Time Definition Change Alerts
 9. Display ATP Status                   79. Display Journal
The command Retrieve ATP Status RTVATPSTS can be used in CL programs
Antivirus Features
31. Reset Scan Status of a File          Uninstall
33. Start a New Log file                 98. Uninstall Product
35. Create test virus EICAR.COM
    in /SMZVDTA/virus-for-test

General
41. PASE environment health-check

Selection or command
===> ____________________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

To **display a report of your current Antivirus definitions**, select **`5. Display Definitions`** from the Antivirus **Maintenance Menu** screen. The **Display Antivirus Definitions (DSPAVDFN)** screen appears, as shown in "Displaying Antivirus Definitions" on page 12.

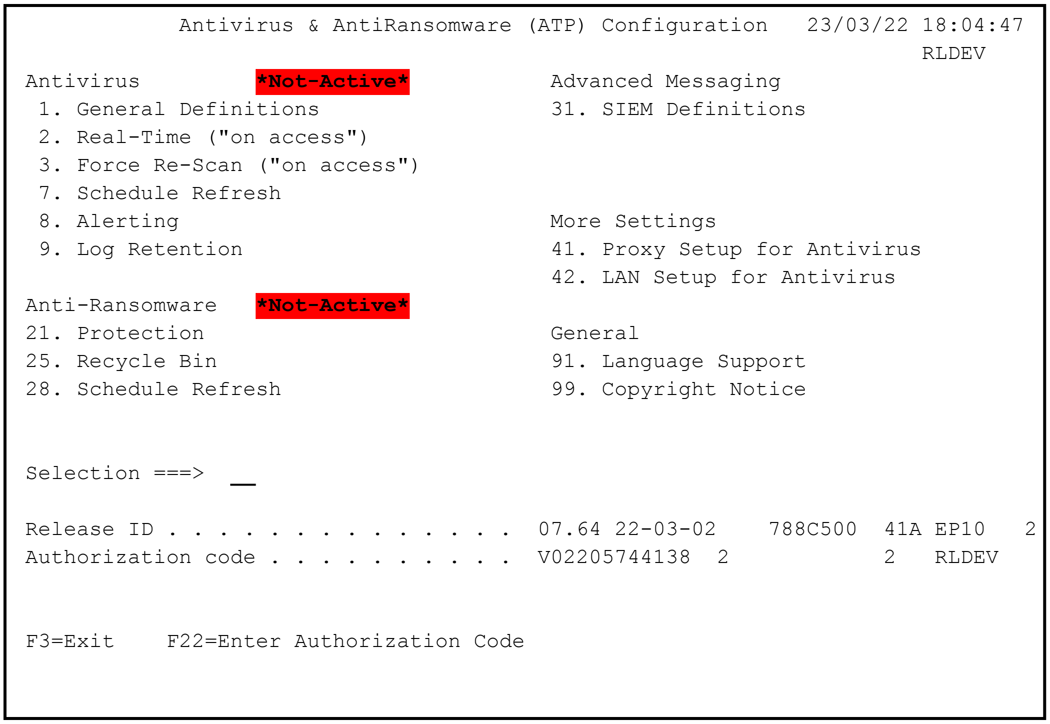
To **import definitions** from a file or library, select **`2. Import Definitions`** from the Antivirus **Maintenance Menu** screen. The **Import Antivirus Defns. (IMPAVDFN)** screen appears, as shown in "Importing Antivirus Definitions" on page 13.

To **export definitions** to a file or library, select **`1. Export Definitions`** from the Antivirus **Maintenance Menu** screen. The **Export Antivirus Defns. (EXPAVDFN)** screen appears, as shown in "Exporting Antivirus Definitions" on page 15.

To **see whether Anti-Virus and iSecurity Anti-Ransomware** are active, select **`9. Display ATP Status`** from the Anti-Virus **Maintenance Menu** screen. The information appears on the bottom line of the screen. You can also retrieve this information in Command Line programs with the *RTVATPSTS* command.

To **mark scanned objects as unscanned and vice versa**, select **`31. Reset Scan Status of a File`** from the Anti-Virus **Maintenance Menu** screen. The **Reset Scan Status (RSTSCNSTS)** screen appears, as shown in "Resetting the Scan Status of Objects" on page 66.

To **set definitions** for Antivirus to use, select **`81. System Configuration`** from the **Antivirus** main screen. The **Antivirus & AntiRansomware (ATP) Configuration** screen appears.



```
            Antivirus & AntiRansomware (ATP) Configuration   23/03/22 18:04:47
                                                                      RLDEV
Antivirus           *Not-Active*                  Advanced Messaging
 1. General Definitions                           31. SIEM Definitions
 2. Real-Time ("on access")
 3. Force Re-Scan ("on access")
 7. Schedule Refresh
 8. Alerting                                      More Settings
 9. Log Retention                                 41. Proxy Setup for Antivirus
                                                  42. LAN Setup for Antivirus
Anti-Ransomware     *Not-Active*
21. Protection                                    General
25. Recycle Bin                                   91. Language Support
28. Schedule Refresh                              99. Copyright Notice


Selection ===>  __

Release ID . . . . . . . . . . . . . .  07.64 22-03-02    788C500  41A EP10   2
Authorization code . . . . . . . . . .  V02205744138  2            2   RLDEV


F3=Exit    F22=Enter Authorization Code
```

To **set general definitions**, select **`1. General Definitions`**. The **Antivirus General Definitions** screen appears, as shown in "Setting General Definitions" on page 17.

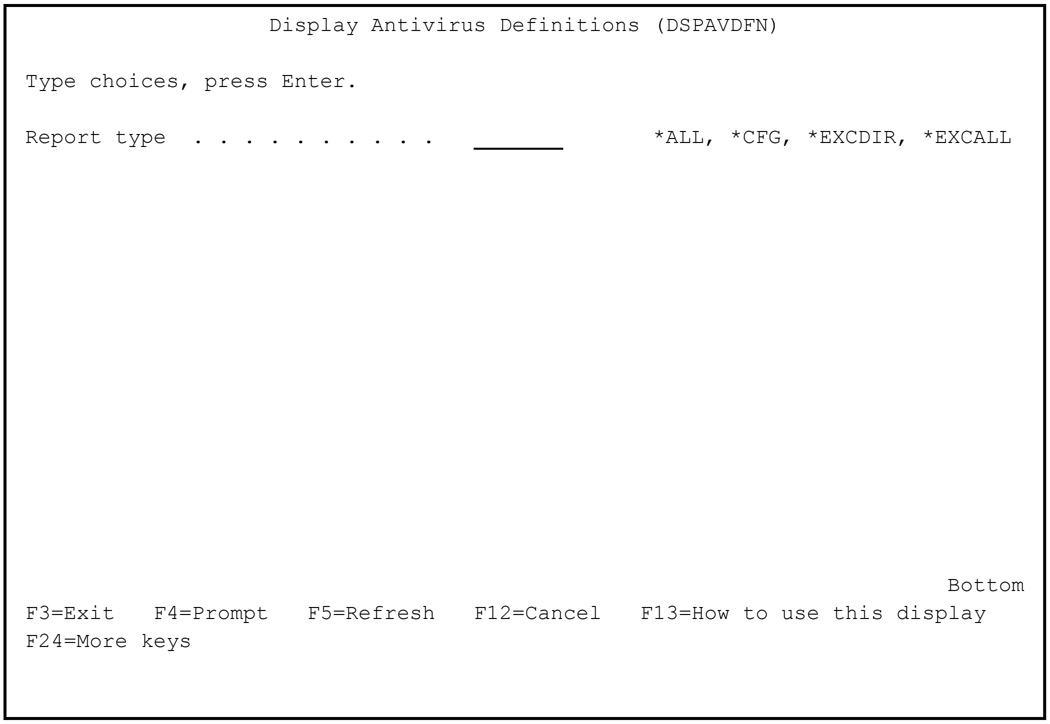
To **set definitions for real-time access**, select **`2. Real-Time ("on access")`**. The **"On Access" Definitions** screen appears, as shown in "Setting Definitions for Real-Time Access" on page 19.

To **enable a proxy server** for Antivirus, see the instructions shown in "Setting Proxy Definitions" on page 23.

To **define how and to whom Antivirus sends alerts** when an virus is detected, select **`8. Alerting.`** The Alerting screen appears, as shown in "Defining Alerts" on page 24.

Displaying Antivirus Definitions

To **display a report of your current Antivirus definitions**, select **`5. Display Definitions`** from the Antivirus **Maintenance Menu** screen (*STRAV>* **`82`**). The **Display Antivirus Definitions (DSPAVDFN)** screen appears:



```
                   Display Antivirus Definitions (DSPAVDFN)

Type choices, press Enter.

Report type  . . . . . . . . . .   _______       *ALL, *CFG, *EXCDIR, *EXCALL

























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

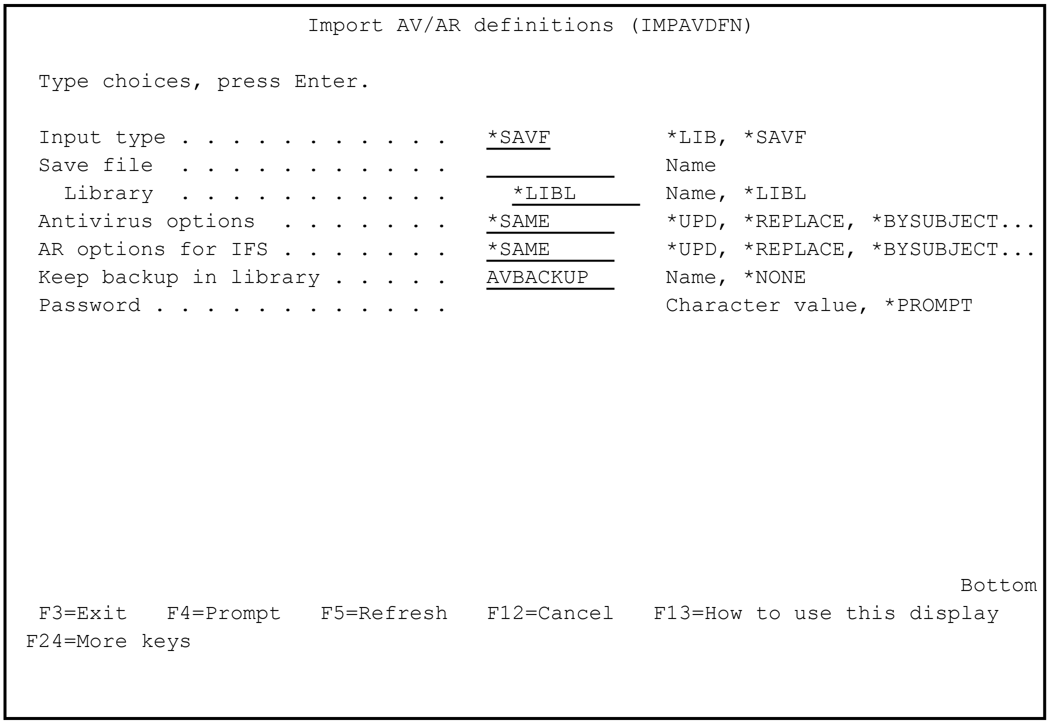
Enter the type of report in the **`Report Type`** field. Possible values are:

- **`*ALL`**: All fields, including information on directories and file extensions
- **`*CFG`**: Configuration parameters
- **`*EXCDIR`**: Directories and file extensions excluded from real-time Antivirus scans
- **`*EXCALL`**: Directories and file extensions excluded from all Antivirus scans

Importing Antivirus Definitions

You can import Antivirus definitions from a SAVF or library. This is useful in replicating definitions over multiple systems.

To **import definitions**, select `2. Import Definitions` from the Antivirus **Maintenance Menu** screen (*STRAV>* `82`). The **Import Antivirus Defns. (IMPAVDFN)** screen appears:



```
                        Import AV/AR definitions (IMPAVDFN)

 Type choices, press Enter.

 Input type . . . . . . . . . . .   *SAVF         *LIB, *SAVF
 Save file  . . . . . . . . . . .                 Name
   Library  . . . . . . . . . . .     *LIBL       Name, *LIBL
 Antivirus options  . . . . . . .   *SAME         *UPD, *REPLACE, *BYSUBJECT...
 AR options for IFS . . . . . . .   *SAME         *UPD, *REPLACE, *BYSUBJECT...
 Keep backup in library . . . . .   AVBACKUP      Name, *NONE
 Password . . . . . . . . . . . .                 Character value, *PROMPT











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

When it appears, the body of the screen has only the **`Input type`** field. The rest of the fields appear based on what is entered into it.

`Input type`

The type of object from which you are importing the definitions. Possible values are:

- **`*SAVF`**: A save file
- **`*LIB`**: A library

`Save file`

If the input type is **`*SAVF`**, the name of the save file.

Library

If the input type is ***SAVF**, the name of the library that contains the save file.

If the input type is ***LIB**, the name of the library.

Antivirus options

Possible values are:

- *SAME
- *UPD
- *REPLACE
- *BYSUBJECT

ATP options for IFS

Possible values are:

- *SAME
- *UPD
- *REPLACE
- *BYSUBJECT

Keep backup in library

The name of the library in which to keep a backup.

If you are not keeping a backup, set this to ***NONE**.

Password

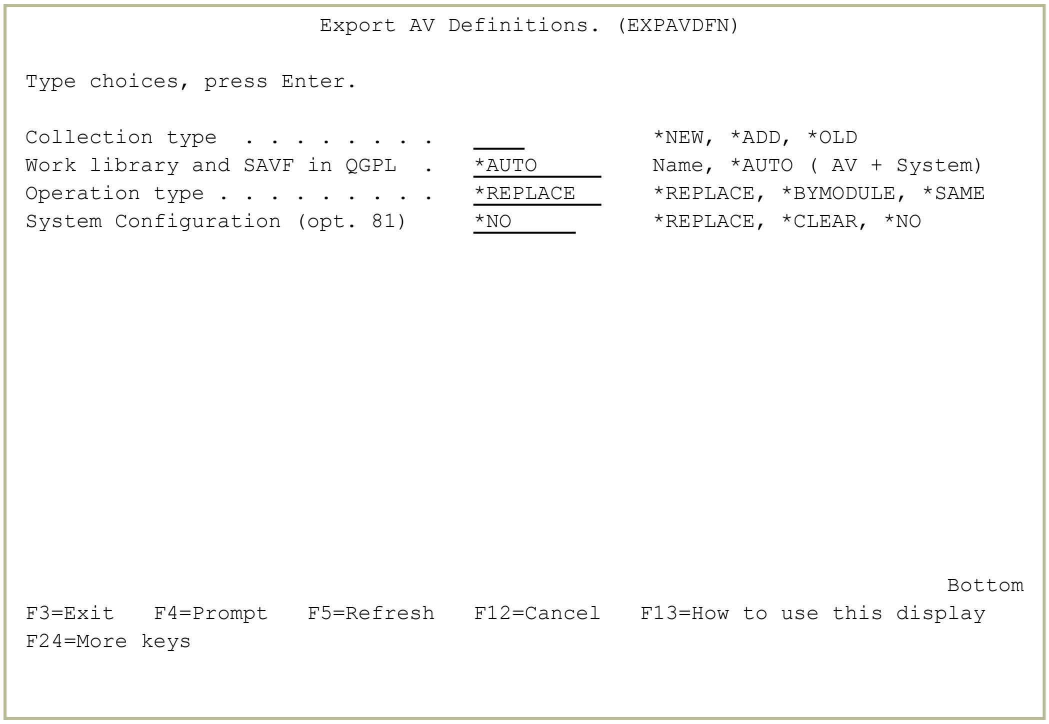
The password for the definitions source.

To prompt the user for the value, set this to ***PROMPT**.

Exporting Antivirus Definitions

You can export Antivirus definitions to a SAVF or library. This is useful in replicating definitions over multiple systems.

To **export definitions**, select **`1. Export Definitions`** from the Antivirus **Maintenance Menu** screen (*STRAV>* **`82`**). The **Export Antivirus Defns. (EXPAVDFN)** screen appears:



```
                       Export AV Definitions. (EXPAVDFN)

 Type choices, press Enter.

 Collection type  . . . . . . . .   ____            *NEW, *ADD, *OLD
 Work library and SAVF in QGPL  .   *AUTO           Name, *AUTO ( AV + System)
 Operation type . . . . . . . . .   *REPLACE        *REPLACE, *BYMODULE, *SAME
 System Configuration (opt. 81)     *NO             *REPLACE, *CLEAR, *NO

















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

The body of the screen has the following fields:

`Collection type`

Possible values are:

- **`*NEW`**:
- **`*ADD`**: Add definitions to an existing library
- **`*OLD`**: Use this option only with the support of support staff. It is only kept for compatibility.

`Work library and SAVF in QGPL`

The location of the library or SAVF. To use the default security settings, set this to **`*AUTO`**.

Operation type

Possible values are:

- ***REPLACE**: Replace all definitions
- ***BYMODULE**: Replace definitions by module
- ***SAME**: Do not replace definitions

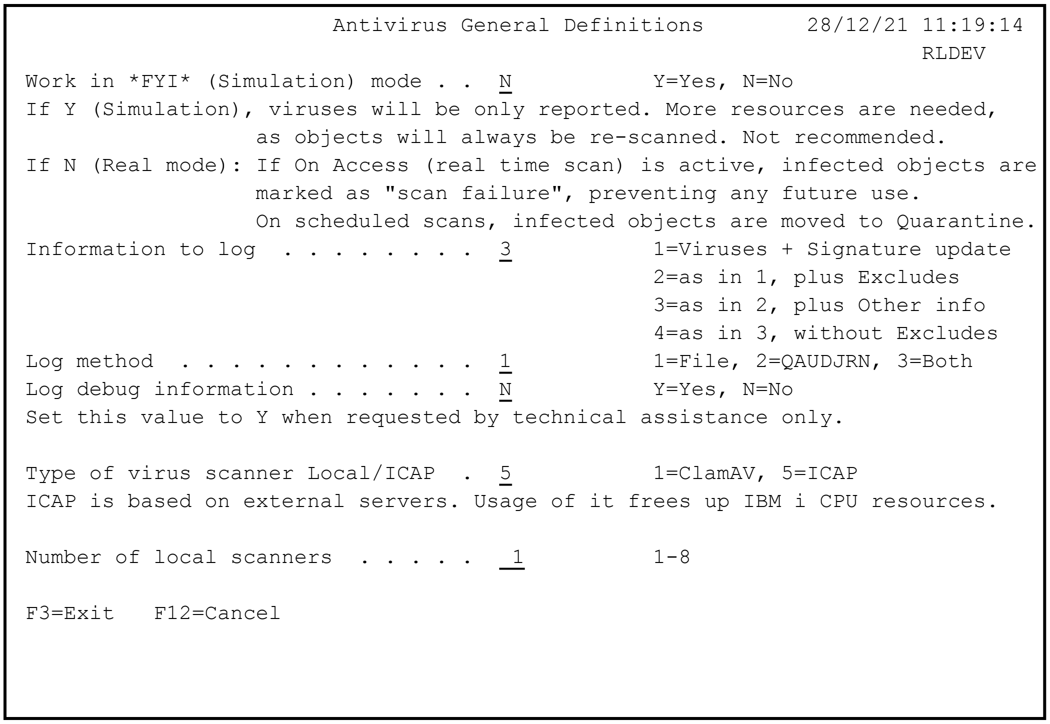
System Configuration (opt. 81)

Possible Values are:

- ***REPLACE**: Replace the existing SAVF and copy the new values
- ***CLEAR**: Replace the existing SAVF and clear the new values
- ***NO**: Export values as is

Setting General Definitions

To **set general definitions**, select **`1. General Definitions`** from the **Antivirus & AntiRansomware (ATP) Configuration** screen (*STRAV*> **`81`**). The **Antivirus General Definitions** screen appears.



```
                        Antivirus General Definitions       28/12/21 11:19:14
                                                                     RLDEV
Work in *FYI* (Simulation) mode . .  N           Y=Yes, N=No
If Y (Simulation), viruses will be only reported. More resources are needed,
                  as objects will always be re-scanned. Not recommended.
If N (Real mode): If On Access (real time scan) is active, infected objects are
                  marked as "scan failure", preventing any future use.
                  On scheduled scans, infected objects are moved to Quarantine.
Information to log  . . . . . . . .  3           1=Viruses + Signature update
                                                 2=as in 1, plus Excludes
                                                 3=as in 2, plus Other info
                                                 4=as in 3, without Excludes
Log method  . . . . . . . . . . . .  1           1=File, 2=QAUDJRN, 3=Both
Log debug information . . . . . . .  N           Y=Yes, N=No
Set this value to Y when requested by technical assistance only.

Type of virus scanner Local/ICAP  .  5           1=ClamAV, 5=ICAP
ICAP is based on external servers. Usage of it frees up IBM i CPU resources.

Number of local scanners  . . . . .  1           1-8

F3=Exit   F12=Cancel
```

The screen contains these fields:

Work in *FYI* (Simulation) Mode

In *FYI* (Simulation) Mode, Antivirus scans files and logs what it finds, but does not move files into Quarantine or mark them as scanned. This is useful in seeing what Antivirus would do when fully activated without having it tke action against files. Since files are not marked as having been scanned, all files are scanned each time, which consumes more resources, than if files marked as having been scanned are skipped.

Possible values are:

- **`Y`**: Work in Simulation mode
- **`N`**: Work normally, marking files as scanned and acting on them.

Information to log

Antivirus can log several different types of information:

- **1**: Detected viruses and Signature changes
- **2**:Unchanged and excluded objects
- **3**: All detected information
- **4**: All detected information except excluded objects

Log method

Whether to log to a standard file, to **QAUDJRN**, or both

- **1**: Log to a standard file (as shown in "Starting a New Log File" on page 68)
- **2**: Log to **QAUDJRN**
- **3**: Log to both

Log debug information

Whether to include debug information in logs. Do not set this to Y unless requested by technical assistance.

Type of virus scanner Local/ICAP

Whether to scan locally or using a remote system via the ICAP protocol, which uses fewer resources on the local system.

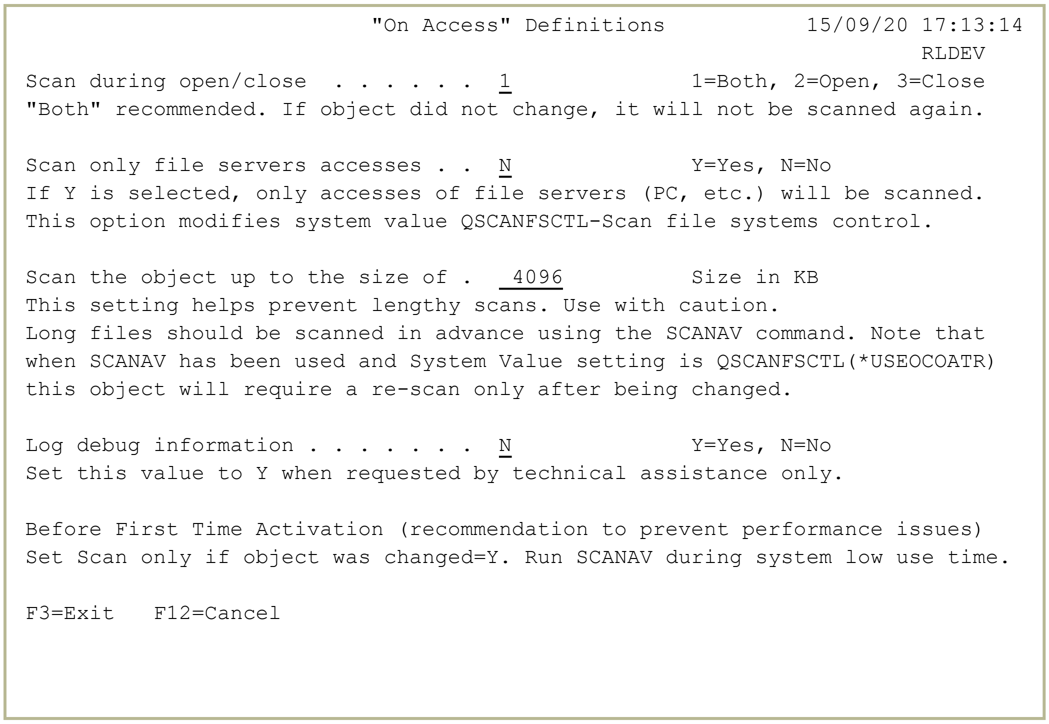
- **1**: Scan on the local system, using the ClamAV scanner
- **5**: Scan using a remote system using ICAP. Set further specifications for the ICAP scan via the **Work with ICAP Servers** screen, as shown in "Connecting to ICAP Servers" on page 32.

Number of local scanners

Up to eight scanners can run at the same time. Possible values are from **1** through **8**.

Setting Definitions for Real-Time Access

To **set definitions for real-time access**, select **`2. Real-Time ("on access")`** from the **Antivirus & AntiRansomware (ATP) Configuration** menu (*STRAV>* **`81`**). The **"On Access" Definitions** screen appears:



```
                           "On Access" Definitions          15/09/20 17:13:14
                                                                     RLDEV
Scan during open/close  . . . . . .  1              1=Both, 2=Open, 3=Close
"Both" recommended. If object did not change, it will not be scanned again.

Scan only file servers accesses . .  N              Y=Yes, N=No
If Y is selected, only accesses of file servers (PC, etc.) will be scanned.
This option modifies system value QSCANFSCTL-Scan file systems control.

Scan the object up to size of .   4096          Size in KB
This setting helps prevent lengthy scans. Use with caution.
Long files should be scanned in advance using the SCANAV command. Note that
when SCANAV has been used and System Value setting is QSCANFSCTL(*USEOCOATR)
this object will require a re-scan only after being changed.

Log debug information . . . . . . .  N              Y=Yes, N=No
Set this value to Y when requested by technical assistance only.

Before First Time Activation (recommendation to prevent performance issues)
Set Scan only if object was changed=Y. Run SCANAV during system low use time.

F3=Exit   F12=Cancel
```

The screen contains these fields:

`Scan during open/close`

Antivirus can scan files when they are opened, when they are closed, or both. Possible values are:

- **`1`**: Both (recommended)
- **`2`**: Open
- **`3`**: Close

`Scan only file servers accesses`

Determines whether Antivirus scans access attempts via the *WRKLNK* and *EDITF* commands or only accesses via the file server. This option modifies the system value ***QSCANFSCTL*** (Scan file systems control). Possible values are:

- **Y**: Only scan accesses via file servers
- **N**: Also scan access attempts via the *WRKLNK* and *EDITF* commands

Scan the object up to the size of ____

A size in KB. If this is set, objects larger than this size are not scanned in real time. They are marked as clean and a message appears in a log file showing that they would have been scanned.

This setting helps to prevent lengthy scans. It should be used with caution. Scan large files in advance with the *SCANAV* command. If *SCANAV* has been used and the system value setting is **QSCANFSCTL(*USEOCOATR)**, larger objects only require rescans after they are changed.

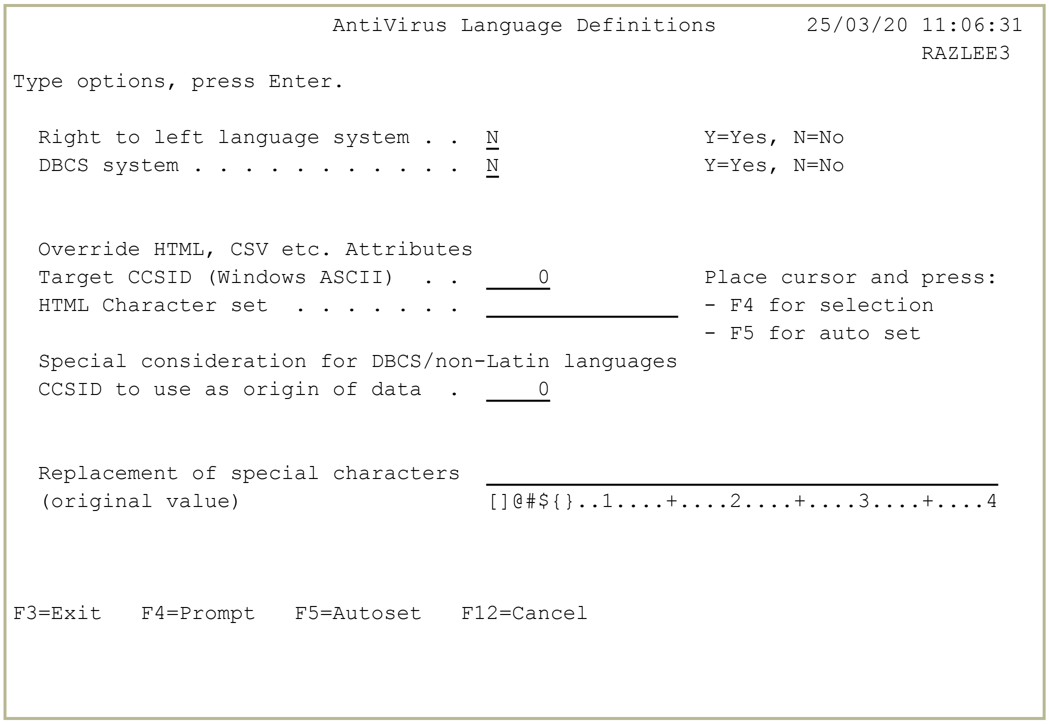
Log debug information

Whether debugging information is logged. This should only be done if requested by technical assistance, since it can generate large amount of information that usually is not useful. Possible values are:

- **Y**: Log the information. Use this only if technical support has requested it.
- **N**: Do not log the information. (Default)

Setting Language Support

To set how the interface language is supported, select **91. Language Support** from the AntiVirus & AntiRansomware (ATP) Configuration screen (*STRAV* **> 81**). The AntiVirus Language Definitions screen appears:



```
                         AntiVirus Language Definitions       25/03/20 11:06:31
                                                                       RAZLEE3
Type options, press Enter.

  Right to left language system . .  N                Y=Yes, N=No
  DBCS system . . . . . . . . . . .  N                Y=Yes, N=No


  Override HTML, CSV etc. Attributes
  Target CCSID (Windows ASCII)  . .      0            Place cursor and press:
  HTML Character set  . . . . . . .  _______________  - F4 for selection
                                                      - F5 for auto set
  Special consideration for DBCS/non-Latin languages
  CCSID to use as origin of data  .      0


  Replacement of special characters  ________________________________________
  (original value)                   []@#${}..1....+....2....+....3....+....4



F3=Exit   F4=Prompt   F5=Autoset   F12=Cancel
```

Enter values in the following fields:

Right to left language system

If the language is written from right to left (such as Hebrew or Arabic), set this field to **Y**. Otherwise, leave it at **N**.

DBCS system

If the language uses a Double Byte Character Set (such as Chinese or Japanese), set this field to **Y**.Otherwise, leave it at **N**.

Override HTML, CSV etc. Attributes

Two sub-fields specifying further aspects of language handling.

To set them automatically based on the language specified for your system, place the cursor in either field and press the F5 key.

To **select a language**, place the cursor in either field and press the **F4** key. The **Select Language Attributes** window appears, from which you can select the language from a predefined set of numeric CCSID codes representing the language.

CCSID to use as origin of data

To select a different language when receiving data, place the cursor in either field and press the **F4** key select the language from a predefined set of numeric CCSID codes representing the language.

Replacement of special characters

Use this field to replace characters when presenting text in this language.

In some languages, the keyboard settings are different. When creating an HTML file via one of the commands, such as ***DSPAULOG*** or ***DSPFWLOG***, the machine writes to a text file that HTML translator understands.

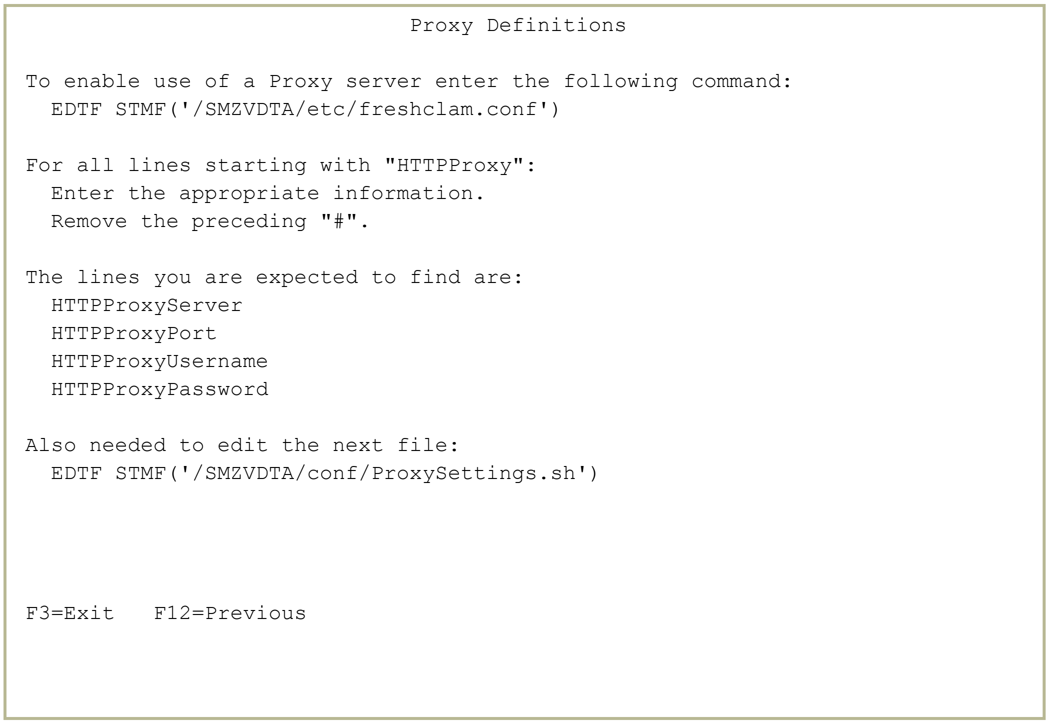
When, for example, a keyword for HTML has to be between " [keyword]", but the user notices that his text file looks like this ... "!keyword^", then, defining the field as follows:

```
Replacement of special characters.  !^
(original value)                    []@#$....1....+....2....+....3....+....4
```

This will obtain as result: "[keyword]" which will be readable to HTML.

Setting Proxy Definitions

To **enable the use of a proxy server** for Antivirus, you need to edit two files on the IBM i, as described on the **Proxy Definitions** screen (***STRAV>* `81 > 41`**).



```
                              Proxy Definitions

To enable use of a Proxy server enter the following command:
  EDTF STMF('/SMZVDTA/etc/freshclam.conf')

For all lines starting with "HTTPProxy":
  Enter the appropriate information.
  Remove the preceding "#".

The lines you are expected to find are:
  HTTPProxyServer
  HTTPProxyPort
  HTTPProxyUsername
  HTTPProxyPassword

Also needed to edit the next file:
  EDTF STMF('/SMZVDTA/conf/ProxySettings.sh')




F3=Exit   F12=Previous
```

Edit the **`freshclam.conf`** file with the command

EDTF STMF('/SMZVDTA/etc/freshclam.conf')
The file contains four lines beginning with the strings:

```
#HTTPProxyServer
#HTTPProxyPort
#HTTPProxyUsername
#HTTPProxyPassword
```

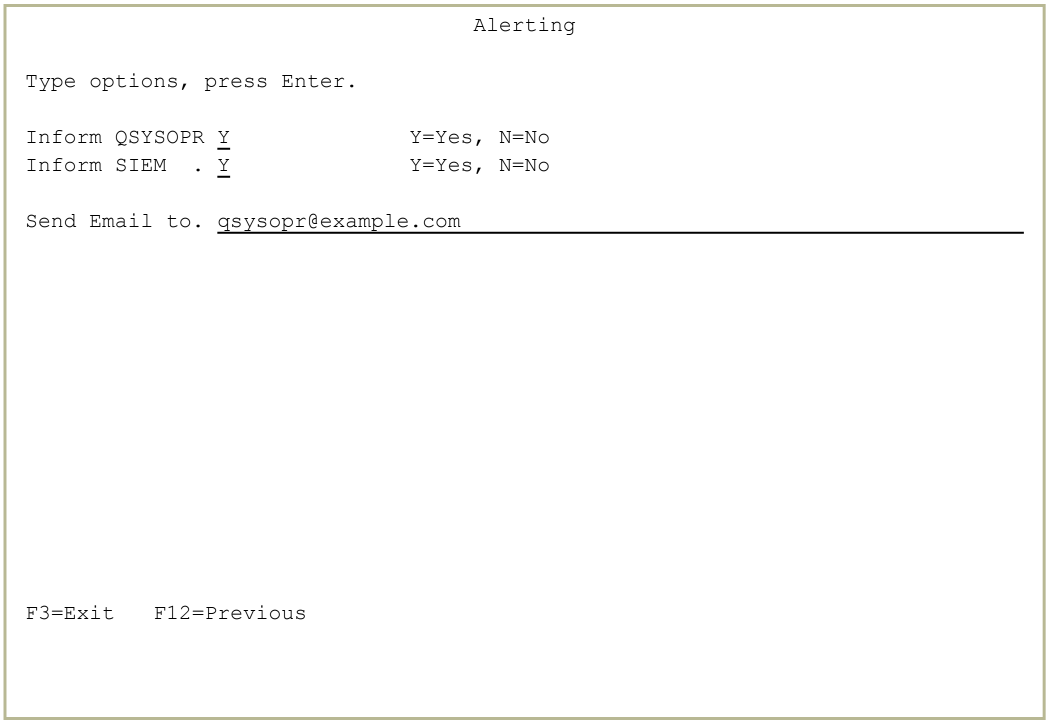
Remove the **#** character from each line.

Add the information for the **`Server`**, **`Port`**, **`Username`**, and **`Password`**, respectively.

Edit the **`ProxySettings.sh`** file with the command ***EDTF STMF ('/SMZVDTA/conf/ProxySettings.sh')***, which has lines corresponding to those in the first file.

Defining Alerts

To **define how and to whom Antivirus sends alerts** when an virus is detected, select **`8. Alerting`** from the **Antivirus & AntiRansomware (ATP) Configuration** screen (*STRAV>* **`81`**). The **Alerting** screen appears:



```
                                   Alerting

Type options, press Enter.

Inform QSYSOPR Y              Y=Yes, N=No
Inform SIEM  . Y              Y=Yes, N=No

Send Email to. qsysopr@example.com
















F3=Exit   F12=Previous
```

The body of the screen contains these fields:

`Inform QSYSOPR`

Whether to send a message to QSYSOPR when a virus is detected. Possible values are:

- **`Y`**: Send messages to QSYSOPR
- **`N`**: Do not send messages to QSYSOPR.

`Inform SIEM`

Whether to send alerts to SIEM systems when a virus is detected. You can set up to three SIEM systems for alerts via the **iSecurity/Base System Configuration** screen (*STRAUD>* **`81`**) as shown in the **Audit** manual.

Possible values are

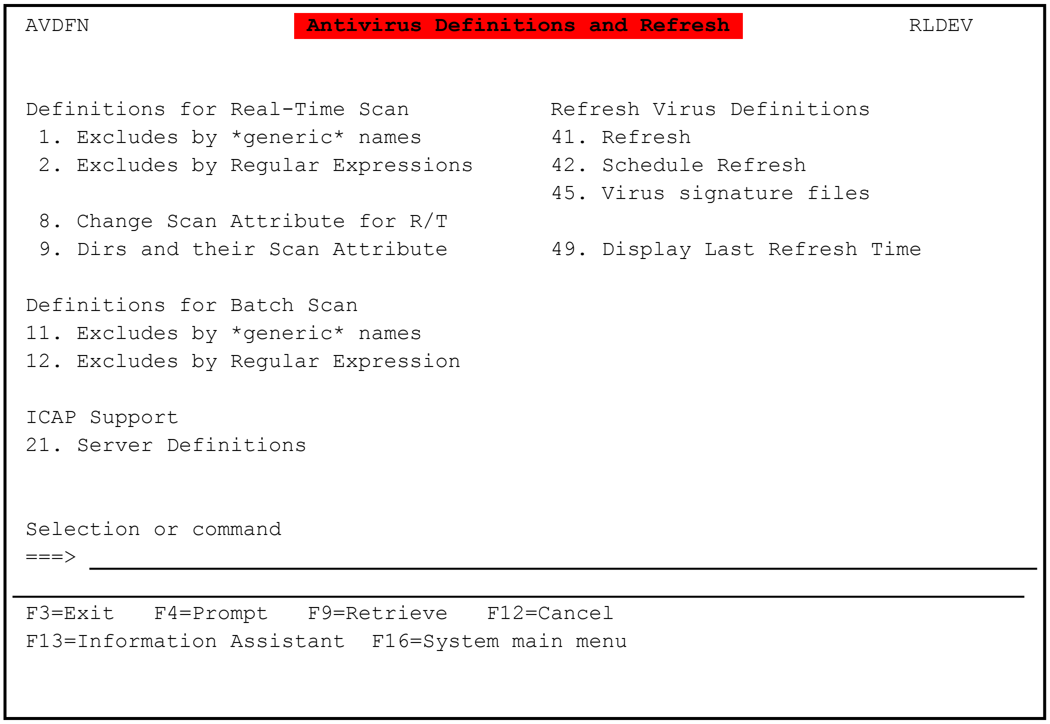
- **Y**: Send messages to SIEM
- **N**: Do not send messages to SIEM.

Send Email to

Send email to these addresses when a virus is detected.

Excluding Objects from Scans

You can create lists of objects for Antivirus to skip when scanning directories that contain them. These can be either full directories or files within them.

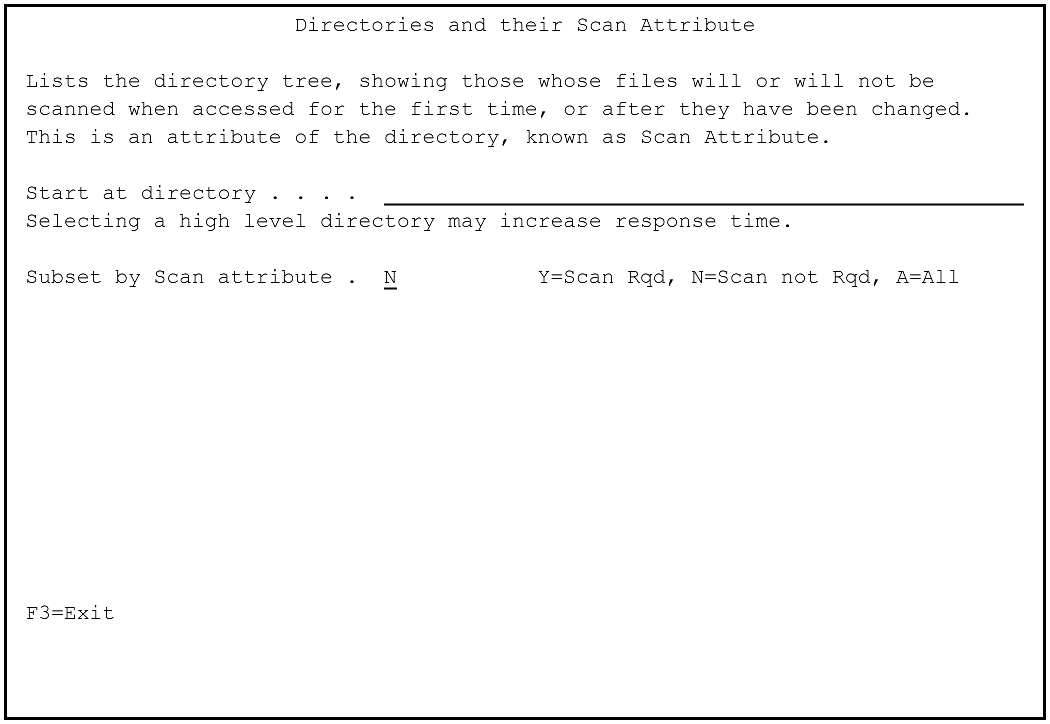


```
AVDFN                 Antivirus Definitions and Refresh                 RLDEV


Definitions for Real-Time Scan          Refresh Virus Definitions
 1. Excludes by *generic* names         41. Refresh
 2. Excludes by Regular Expressions     42. Schedule Refresh
                                        45. Virus signature files
 8. Change Scan Attribute for R/T
 9. Dirs and their Scan Attribute       49. Display Last Refresh Time

Definitions for Batch Scan
11. Excludes by *generic* names
12. Excludes by Regular Expression

ICAP Support
21. Server Definitions


Selection or command
===> ____________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

Excluding items from Real-Time Scans

To **exclude objects from real-time scans by editing a file**, select **`1. Exclude from Real-Time Scan`** from the **Refresh, Definitions, ICAP** menu (*STRAV>* **`21`**). An editor opens to edit the **`/SMZVDTA/conf/OA_exc.conf`** file.

To **exclude objects from real-time scans by selecting items**, select **`9. Dirs and their Scan Attribute`** from the **Refresh, Definitions, ICAP** menu (*STRAV>* **`21`**). The **Directories and their Scan Attribute** screen appears.



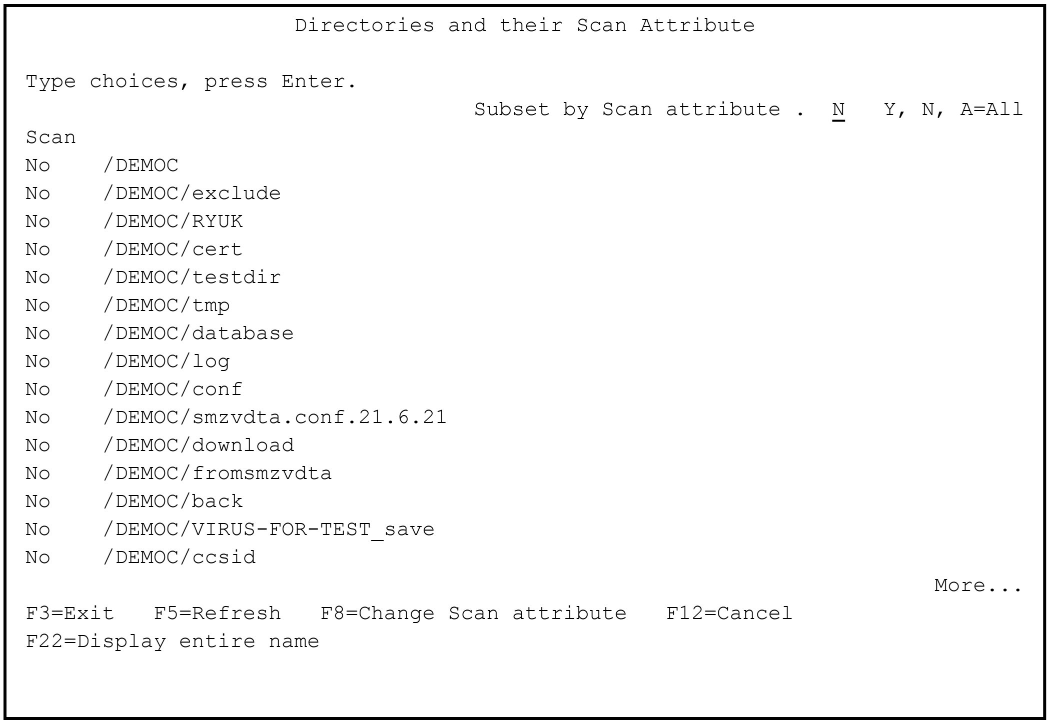
```
                      Directories and their Scan Attribute

 Lists the directory tree, showing those whose files will or will not be
 scanned when accessed for the first time, or after they have been changed.
 This is an attribute of the directory, known as Scan Attribute.

 Start at directory . . . .  __________________________________________________
 Selecting a high level directory may increase response time.

 Subset by Scan attribute .  N          Y=Scan Rqd, N=Scan not Rqd, A=All










 F3=Exit
```

In the **Start at directory** field, enter the absolute pathname of a directory, beginning with the slash ("**/**") character. To reduce scanning time, start relatively low in the directory tree.

The **Subset by Scan attribute** field indicates whether to display files and directories within that directory that will or will not be scanned. Possible values include:

- **Y**: Show items that will be scanned
- **N**: Show items that will not be scanned
- **A**: Show all items

Press **Enter** to see the selected items. A second **Directories and their Scan Attribute** screen appears.

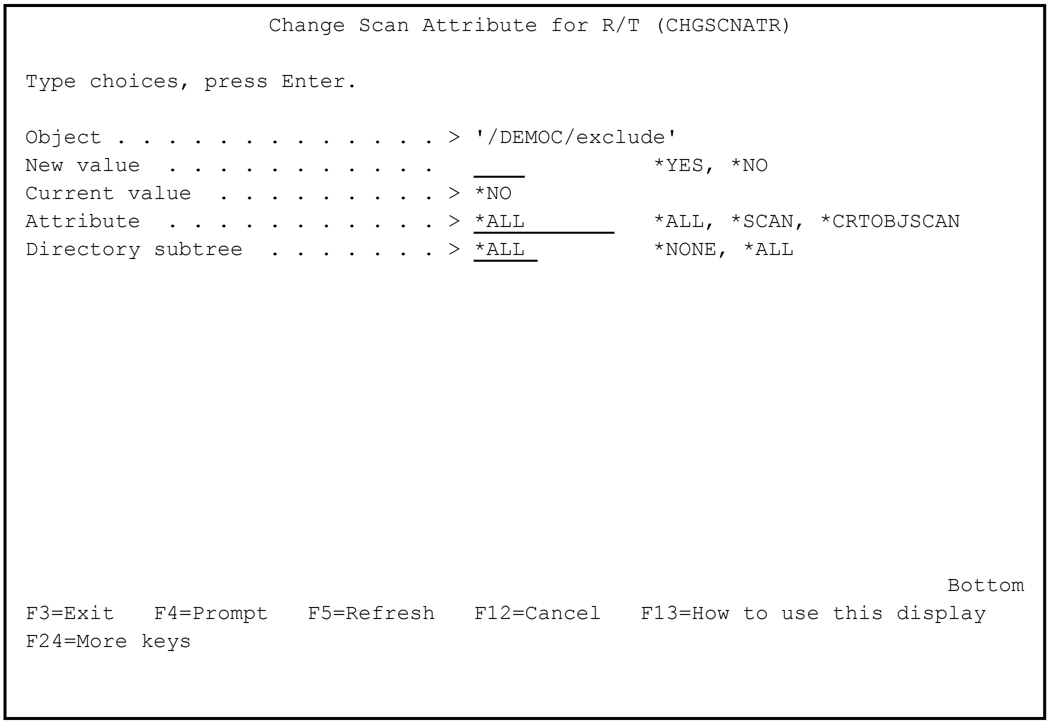


```
                     Directories and their Scan Attribute

Type choices, press Enter.
                                   Subset by Scan attribute .  N   Y, N, A=All
Scan
No    /DEMOC
No    /DEMOC/exclude
No    /DEMOC/RYUK
No    /DEMOC/cert
No    /DEMOC/testdir
No    /DEMOC/tmp
No    /DEMOC/database
No    /DEMOC/log
No    /DEMOC/conf
No    /DEMOC/smzvdta.conf.21.6.21
No    /DEMOC/download
No    /DEMOC/fromsmzvdta
No    /DEMOC/back
No    /DEMOC/VIRUS-FOR-TEST_save
No    /DEMOC/ccsid
                                                                       More...
F3=Exit   F5=Refresh   F8=Change Scan attribute   F12=Cancel
F22=Display entire name
```

The body of the screen lists the objects in the directory. For each, the Scan field shows whether Antivirus will scan it. As with the previous screen, you can set whether to list only objects that will be scanned, those that will not, or all objects by setting the **`Subset by scan attribute`** field to **`N`**, **`Y`**, or **`A`**, respectively.

To **display the full pathname** of an object if the name is truncated on the screen, press the **F22** (**Shift+F10**) key. The **Display Entire Name** window appears, showing the entire name of the object. To dismiss the window, press the **F12** key.

To **change the scan attribute** of an item, place the cursor on the line for that item and press the **F8** key. The **Change Scan Attribute for R/T (CHGSCNATR)** screen appears.



```
                     Change Scan Attribute for R/T (CHGSCNATR)

Type choices, press Enter.

Object . . . . . . . . . . . . . > '/DEMOC/exclude'
New value  . . . . . . . . . . .   ____           *YES, *NO
Current value  . . . . . . . . . > *NO
Attribute  . . . . . . . . . . . > *ALL           *ALL, *SCAN, *CRTOBJSCAN
Directory subtree  . . . . . . . > *ALL           *NONE, *ALL








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

The body of the screen contains these fields:

Object

(Read-only) The pathname of the object.

New value

The new value for the attribute. Valid values include ***YES** and ***NO**.

Current value

(Read-only) Whether the object is currently set to be scanned.

Attribute

The attribute to be changed. Possible values include:

- ***ALL**: For either scan files or directories: specifies whether the object or, for a directory, the objects created in the directory will be scanned when exit programs are registered with any of the integrated file system scan-related exit points
- ***SCAN**: For stream files: specifies whether the object will be scanned when exit programs are registered with any of the integrated file system scan-related exit points.

- ***CRTOBJSCAN**: For directories: specifies whether the objects created in the directory will be scanned when exit programs are registered with any of the integrated file system scan-related exit points

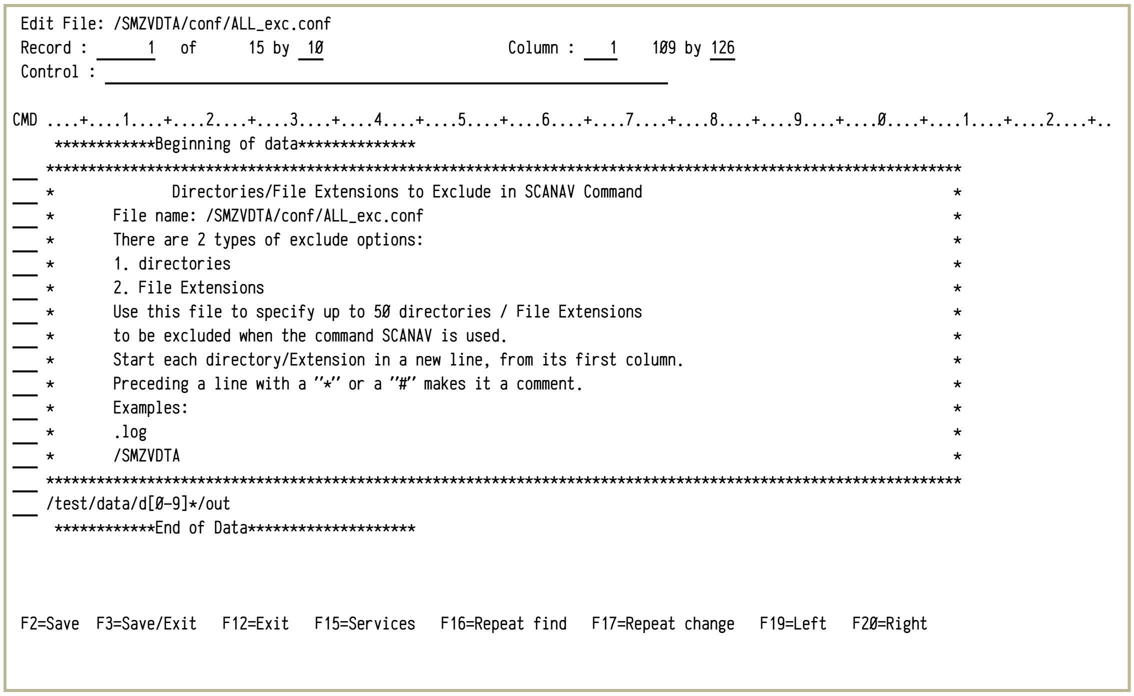
Directory subtree

The subtrees to be scanned.

NOTE: The most effective way to prevent Antivirus from scanning a file or directory is to set the ***SCAN** or ***CRTOBJSCAN** attribute, respecively, to ***NO**.

Excluding items from Batch Scans

To **exclude objects from batch scans**, select **2. Exclude from Batch Scan** from the **Antivirus Definitions and Refresh** menu (*STRAV>* **21**). An editor opens to edit the **/SMZVDTA/conf/ALL_exc.conf** file.



```
 Edit File: /SMZVDTA/conf/ALL_exc.conf
 Record :       1   of      15 by  1Ø                      Column :    1    1Ø9 by 126
 Control :

CMD ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....Ø....+....1....+....2....+..
     ************Beginning of data**************
___ *************************************************************************************************************
___ *              Directories/File Extensions to Exclude in SCANAV Command                                     *
___ *       File name: /SMZVDTA/conf/ALL_exc.conf                                                               *
___ *       There are 2 types of exclude options:                                                               *
___ *       1. directories                                                                                      *
___ *       2. File Extensions                                                                                  *
___ *       Use this file to specify up to 5Ø directories / File Extensions                                     *
___ *       to be excluded when the command SCANAV is used.                                                     *
___ *       Start each directory/Extension in a new line, from its first column.                                *
___ *       Preceding a line with a "*" or a "#" makes it a comment.                                            *
___ *       Examples:                                                                                           *
___ *       .log                                                                                                *
___ *       /SMZVDTA                                                                                            *
___ *************************************************************************************************************
___ /test/data/d[Ø-9]*/out
     ************End of Data********************



 F2=Save  F3=Save/Exit   F12=Exit   F15=Services   F16=Repeat find   F17=Repeat change   F19=Left   F2Ø=Right
```

You can specify wildcards for the names of the objects as either:

- IBM i extended notation, using *generic* names with multiple (up to 10) asterisks (*). You can specify whether the definition is case sensitive.
- Regular Expressions, as in Linux.

For example, the entry shown above, "**`[0-9]*/out`**" skips any file or directory named "**`out`**" within a directory whose name consists only of one or more digits.

Connecting to ICAP Servers

With the ICAP protocol, Antivirus scans your system's files for viruses using a remote system.

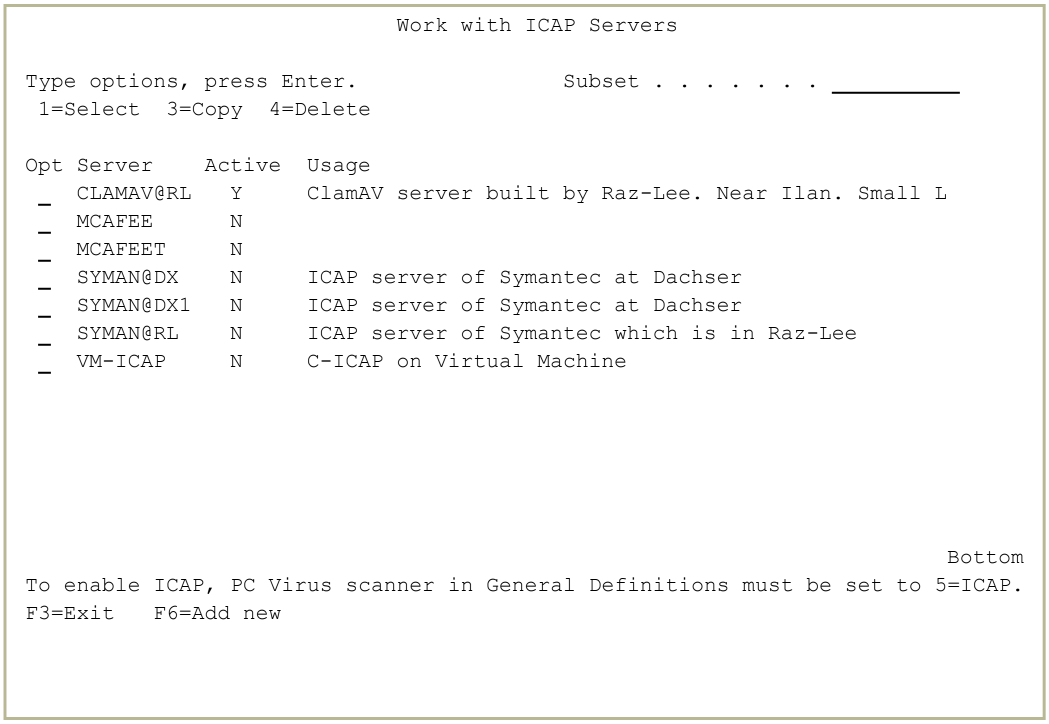
Virus scans tend to be CPU-intensive because they scan millions of possible virus signatures. Using ICAP reduces the load that virus scanning can demand from IBM i servers by distributing the CPU-intensive part of virus scanning onto separate external ICAP servers. When iSecurity Antivirus intends to scan an object, with the addition of the ICAP Client, it passes the file to the ICAP server for processing. The file can be simultaneously scanned by multiple ICAP servers. Those servers send responses back to the iSecurity ICAP client clearing the object for use or flagging it as infected. Using ICAP ensures that your IBM i is always protected without a performance drop. Scan time is faster – by twenty times in some tests. The portion of the IBM i CPU that would have been used for virus scanning becomes available for other purposes.

The ICAP Client can communicate with any ICAP server. When you use an external ICAP server, the main Antivirus subsystem, ZANTIVIRUS, only runs two or three monitoring jobs and one to four real time scanning jobs. The local IBM i CLAMAV engine remains in silent mode (effectively off) and uses a very limited percentage of CPU.

NOTE: The ICAP Client is an add-on to Antivirus and requires an additional license. To define ICAP servers, you must have licensed the ICAP client.

To **use an ICAP server**, the **`Type of virus scanner Local/ICAP`** field on the **Antivirus General Definitions** screen (*STRAV>* **`81`**) must be set to "**5**" (as shown in "Setting General Definitions" on page 17).

To **define ICAP servers**, select **`21. Server Definitions`** from the **Antivirus Definitions and Refresh** screen (*STRAV>* **`21`**). The **Work with ICAP Servers** screen appears:



```
                             Work with ICAP Servers

Type options, press Enter.                Subset . . . . . . . __________
 1=Select  3=Copy  4=Delete

Opt Server    Active  Usage
 _  CLAMAV@RL   Y     ClamAV server built by Raz-Lee. Near Ilan. Small L
 _  MCAFEE      N
 _  MCAFEET     N
 _  SYMAN@DX    N     ICAP server of Symantec at Dachser
 _  SYMAN@DX1   N     ICAP server of Symantec at Dachser
 _  SYMAN@RL    N     ICAP server of Symantec which is in Raz-Lee
 _  VM-ICAP     N     C-ICAP on Virtual Machine








                                                                    Bottom
To enable ICAP, PC Virus scanner in General Definitions must be set to 5=ICAP.
F3=Exit   F6=Add new
```

The body of the screen lists the servers known to the system. For each, it shows the fields

Server

The name of the server

Active

Whether Antivirus is using this server. Possible values are:

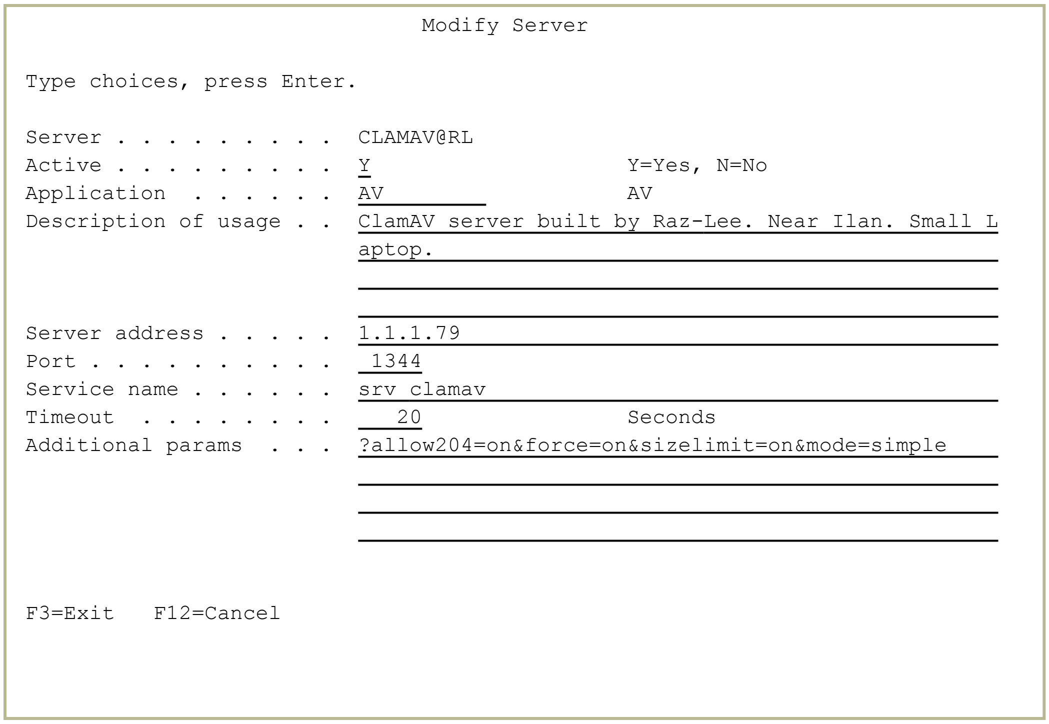
- **Y**: Antivirus is using this server
- **N**: Antivirus is not using this server

Usage

A free-form description of the server.

To **activate, deactivate, and change details** of a server, enter **1** in the **Opt** field for that server and press **Enter**. The **Modify Server** screen appears.

To **add a server**, press the **F6** key. The **Add New Server** screen appears, which has the same fields as the **Modify Server** screen.



```
                               Modify Server

 Type choices, press Enter.

 Server . . . . . . . . .  CLAMAV@RL
 Active . . . . . . . . .  Y                     Y=Yes, N=No
 Application  . . . . . .  AV                    AV
 Description of usage . .  ClamAV server built by Raz-Lee. Near Ilan. Small L
                           aptop.


 Server address . . . . .  1.1.1.79
 Port . . . . . . . . . .   1344
 Service name . . . . . .  srv_clamav
 Timeout  . . . . . . . .     20                 Seconds
 Additional params  . . .  ?allow204=on&force=on&sizelimit=on&mode=simple




 F3=Exit   F12=Cancel
```

The screen contains these fields:

Server

The name of the server. (Read only)

Active

Whether the system is actively using the server. Possible values are:

- **Y**: Active
- **N**: Inactive

Application

The type of application. This is always **AV**.

Description of usage

A free-from description of the server, also used for the **Usage** field on the **Work with ICP Server** screen.

Server address

The IP address of the server.

Port

The port on the server. **1344** is the default port for ICAP.

Service name

The name of the server.

- For ClamAV servers, this is **srv_clamav**
- For McAfee servers, this is **respmod**
- For Symantec servers, this is **avscan**

Timeout

The maximum number of seconds that a request to the server may take before timing out.

Additional params

Additional parameters to be passed to the server. These will differ, based on the server type and the requirements of your installation.

For McAfee and Symantec, set the field to **?allow204=on&force=on&sizelimit=on&mode=simple**

To check that the values for the client are correct, enter the commands

CALL QP2TERM
cat /SMZVDTA/conf/icapsf.stmf

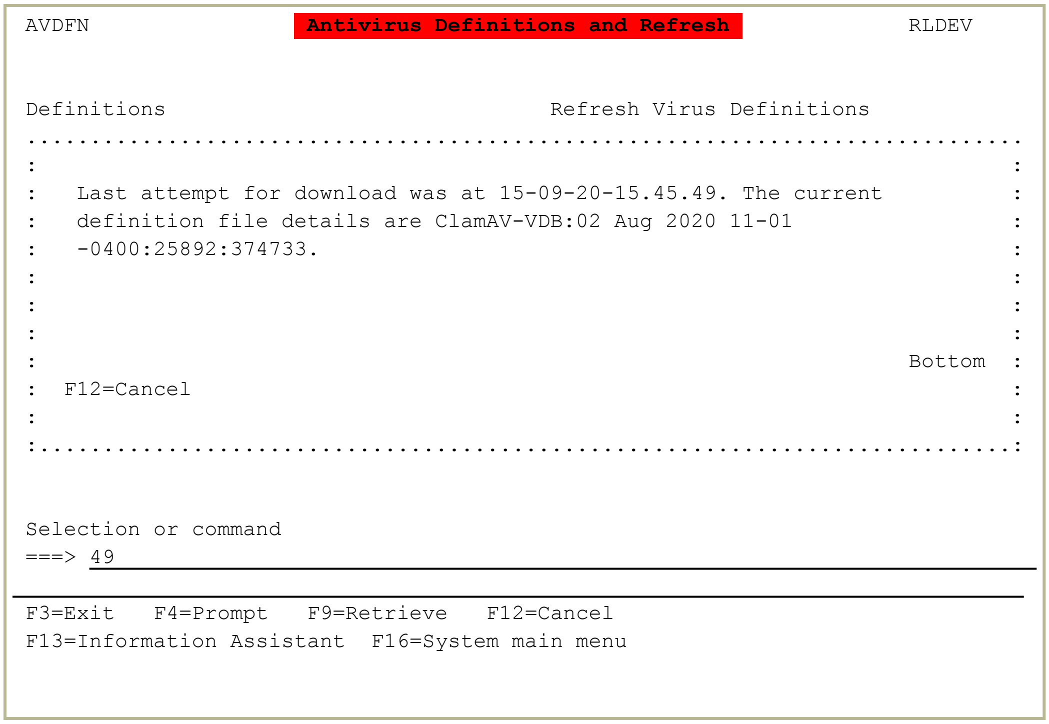
The output should resemble the following with values matching what has been entered:

```
--icap-host="1.1.1.122" --icap-port="01344" --
icap-Server="srv_clamav" --icap-timout="00020" -
-icap-Additional-
Parameters="?alw204=on&force=on&sizelimit=on&mod
e=simple"
```

Updating Virus Definitions

To **ensure that you have the most up-to-date virus definition files** available, update them frequently. Virus definitions are generally updated twice each day. If you are updating from a CD or the Internet, you must prepare your virus definition sources before updating for the first time. You can then update definitions in real-time or schedule a one-time or recurring update for later.

To **view the most recent update**, select **`49. Display Last Update Time`** from the **Antivirus Definitions and Refresh** menu (*STRAV>* **`21`**). The date appears together with the precise update time and file definition file details.



```
AVDFN                   Antivirus Definitions and Refresh            RLDEV


Definitions                                Refresh Virus Definitions
..............................................................................
:                                                                            :
:   Last attempt for download was at 15-09-20-15.45.49. The current          :
:   definition file details are ClamAV-VDB:02 Aug 2020 11-01                 :
:   -0400:25892:374733.                                                      :
:                                                                            :
:                                                                            :
:                                                                            :
:                                                                    Bottom  :
:  F12=Cancel                                                                :
:                                                                            :
:............................................................................:


Selection or command
===> 49

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

You can update virus definitions from several different sources:

- **`*CD`**: Refresh the Virus Signature Database from a CD which was burned on an internet-connected PC which has downloaded files **`main.cvd`** and **`daily.cvd`** from the ClamAV server.
- **`*CMD`**: Load the definitions via a command on the command line.
- **`*DIR`**: Specify a directory on the IBM i that contains the definitions.

- ***INTERNET**: Download the Virus Signature Database refresh directly from the internet to the IBM i. This option enables users to refresh virus definitions at their own computers. (If regulations prevent your IBM i system from connecting to the internet, updating from *CD might be more feasible.)
- ***LAN**: Download the Virus Signature Database refresh to a PC, then upload it to the IBM i via a LAN. This option enables only one user to download definitions, thereby providing greater security. All other users receive their updates from that user.
- ***RAZLEE**: Download from Raz-Lee website.

Preparing Virus Definition Sources

To update definitions from a **`*LAN`** or from the **`*INTERNET`**, you must first set up the data sources.

Updating Domain Information for Internet Updates

To **update your domain information** when you update virus definitions for the first time:

1. Enter the command ***CFGTCP*** into the command line and select option 12. The **Change TCP/IP Domain (CHGTCPDMN)** screen appears.
2. Check that your DNS (Domain Name Server) is defined. If not, update your ISP Domain details.

Setting Up a Proxy for LAN Updates

To set up the LAN proxy when you update virus definitions for the first time:

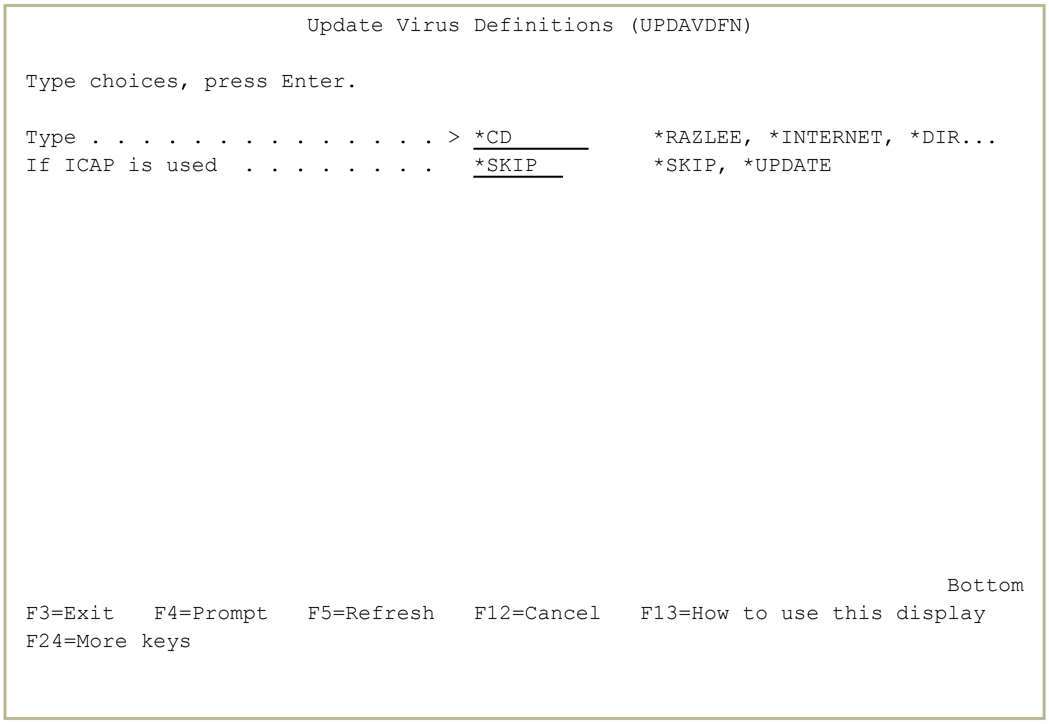
1. Enter the command *CFGTCP* into the command line and select option **10**. The Work with TCP/IP Host Table Entries screen appears.
2. Add your IP address with the host name **AVDBPC** by using option **1** next to the blank line at the top of the **Internet Address** column.
3. If you are installing the definitions from an installation disk, copy the **avpc** directory from the installation disk to **C:\**
4. If you are downloading the definition file:
    a. Download the zip file AVPC.zip from the link : **http://as400.razlee.com/downloads/PTF/AVPC.zip**
    b. Extract the **avpc** directory from the zip file to **C:\avpc**.
5. Open the **C:\avpc** folder and double-click Apache installation file: **C:\avpc\apache_2.0.43-win32-x86-no_ssl.exe** .
6. Enter domain, server name, and email when prompted (you can use any text you like).
7. Double-click batch file: **ScheduledUpdate.bat**. When the download is finished, files are ready for the IBM i update tool.
8. To update virus database on a daily basis, add **ScheduledUpdate.bat** to the scheduled tasks on the PC. Select **Start > Programs > Accessories > System Tools > Scheduled Tasks**, and click **Add Scheduled Task**.
9. Browse to folder **C:\avpc** and open **ScheduledUpdate.bat**.
10. Check daily option, fill in login password, choose your preferred time for the update, select Finish, and press Enter.
11. Return to native interface and enter *STRAV* to return to the Antivirus main screen.

Performing or Scheduling Virus Definition Updates

You can update virus definitions on demand or schedule them to run as one-time or recurring events.

Refreshing (Updating) Virus Definition Files on Demand

To **update virus definition files on demand** via any of these methods, Select **`41. Refresh`** from the **IFS Viruses, Worms and Trojans** menu (*STRAV* **`> 21`**). The **Update Virus Definitions (UPDAVDFN)** screen appears:



```
                      Update Virus Definitions (UPDAVDFN)

Type choices, press Enter.

Type . . . . . . . . . . . . . . > *CD            *RAZLEE, *INTERNET, *DIR...
If ICAP is used  . . . . . . . .   *SKIP          *SKIP, *UPDATE

















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

1. The screen, as it first appears, has two fields:

   `Type`

   The type of update. Possible values are **`*CD`**, **`*CMD`**, **`*DIR`**, **`*INTERNET`**, **`*LAN`**, and **`*DIR`** (as shown in "Updating Virus Definitions" on page 36).

   `If ICAP is used`

   If you are scanning via an ICAP server (as shown in "Connecting to ICAP Servers" on page 32), whether to update the definitions. (This parameter is useful if updating the definitions from a script that calls the *UPDAVFN* command.) Possible values are:

   - **`*SKIP`**: Do not perform the update.
   - **`*UPDATE`**: Perform the update.

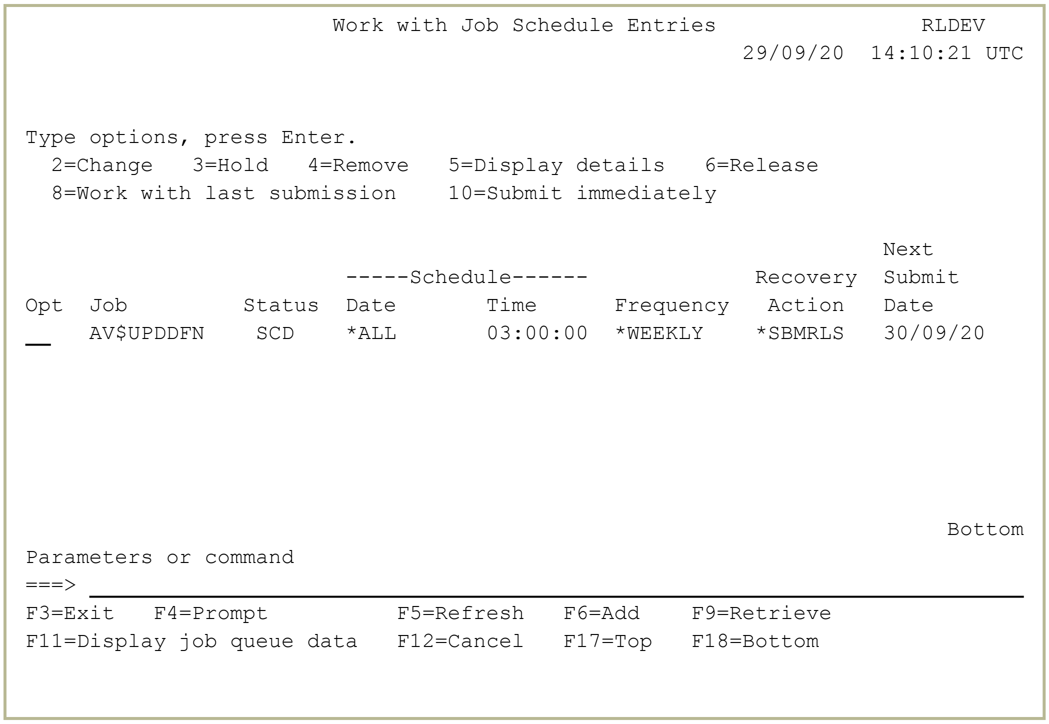
2. The next step depends on the value in the **`Type`** field:

- For ***CD** or ***INTERNET** updates: The **Incremental or Full update** field appears. Possible values are:
    - ***INCREMENTAL**: Only update definitions that have changed since the last update.
    - ***FULL**: Update the full set of definitions.
- For ***CMD** updates: The **Command to load definitions** field appears. Fill in the command to run. By default, the command is: '*/*Refresh /SMZVDTA/database/* */*'
- For ***DIR** updates: The **Directory ('/dir/')** field appears. Enter the path to the directory containing the definitions.
- For ***LAN** or ***RAZLEE** updates: There are no further fields.

3. Press **Enter**. Antivirus updates its definitions.

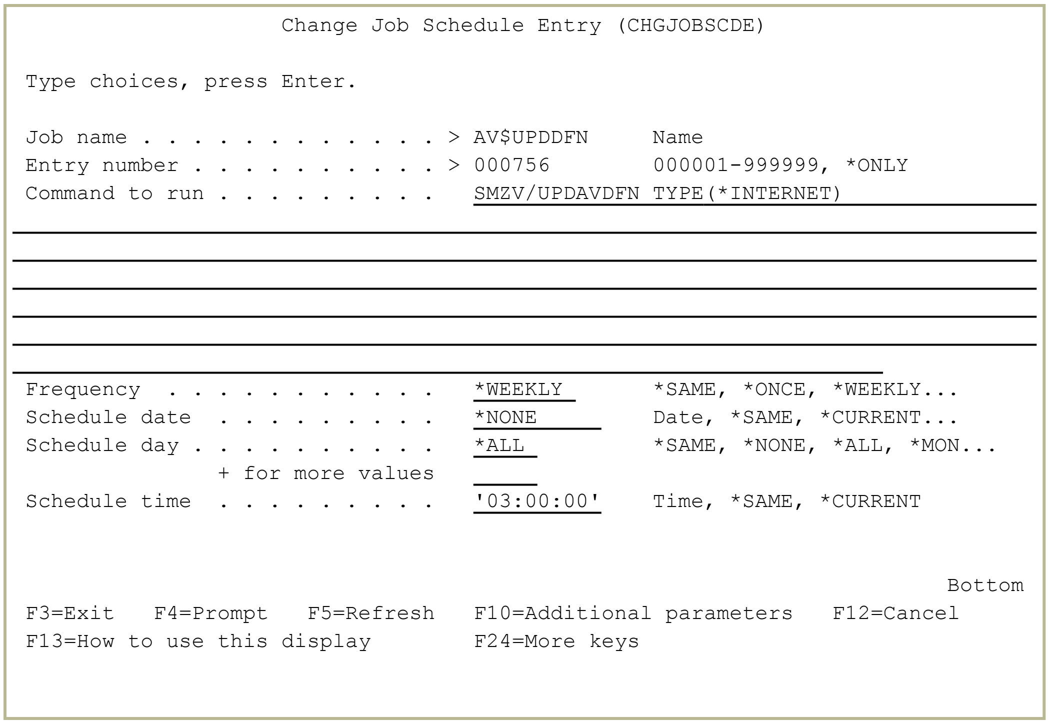
Scheduling Virus Definition Updates

To **schedule virus definition updates**, as either a one-time or recurring event, select **`42. Schedule Refresh`** from the **Antivirus Definitions and Refresh** screen (*STRAV>* `21`). The standard **Work with Job Schedule Entries** screen appears, with an entry for the job **`AV$UPDDFN`**.



```
                         Work with Job Schedule Entries                RLDEV
                                                           29/09/20  14:10:21 UTC


Type options, press Enter.
  2=Change   3=Hold   4=Remove   5=Display details   6=Release
  8=Work with last submission    10=Submit immediately

                                                                   Next
                          -----Schedule------            Recovery  Submit
Opt  Job         Status  Date       Time      Frequency   Action   Date
__   AV$UPDDFN    SCD    *ALL       03:00:00  *WEEKLY    *SBMRLS   30/09/20






                                                                        Bottom
Parameters or command
===> _________________________________________________________________________
F3=Exit   F4=Prompt          F5=Refresh   F6=Add     F9=Retrieve
F11=Display job queue data   F12=Cancel   F17=Top    F18=Bottom
```

To **see and change the parameters for the scheduled job**, type **2** in the **`Opt`** field for that line and press Enter. The **Change Job Schedule Entry (CHGJOBSCDE)** screen for that command appears, showing the values for the job.

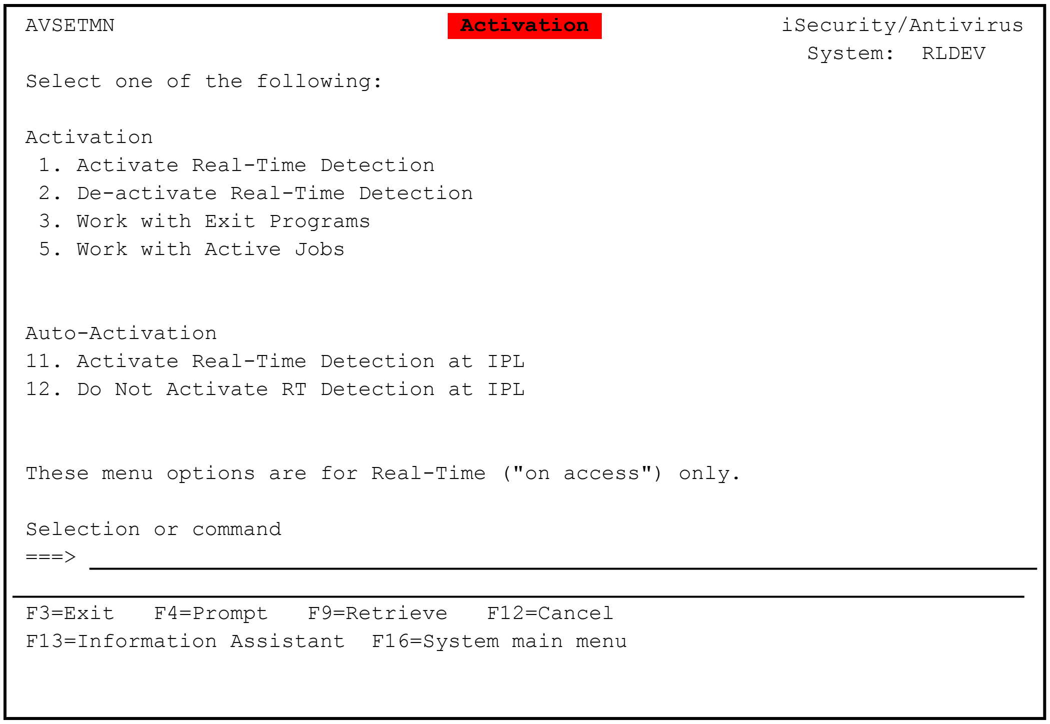


```
                    Change Job Schedule Entry (CHGJOBSCDE)

Type choices, press Enter.

Job name . . . . . . . . . . . . > AV$UPDDFN     Name
Entry number . . . . . . . . . . > 000756        000001-999999, *ONLY
Command to run . . . . . . . . .   SMZV/UPDAVDFN TYPE(*INTERNET)







Frequency  . . . . . . . . . . .   *WEEKLY       *SAME, *ONCE, *WEEKLY...
Schedule date  . . . . . . . . .   *NONE         Date, *SAME, *CURRENT...
Schedule day . . . . . . . . . .   *ALL          *SAME, *NONE, *ALL, *MON...
               + for more values
Schedule time  . . . . . . . . .   '03:00:00'    Time, *SAME, *CURRENT


                                                                       Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

Activating and De-Activating Real-Time Virus Detection

Once you have set up and run Antivirus for the first time, you can activate On-Access detection to monitor your system for viruses in real-time.

To **activate and de-activate On-Access detection**, select **1. Activation** from the Antivirus main menu. The **Activation** screen appears:



```
AVSETMN                          Activation                  iSecurity/Antivirus
                                                               System:   RLDEV
Select one of the following:

Activation
 1. Activate Real-Time Detection
 2. De-activate Real-Time Detection
 3. Work with Exit Programs
 5. Work with Active Jobs


Auto-Activation
11. Activate Real-Time Detection at IPL
12. Do Not Activate RT Detection at IPL


These menu options are for Real-Time ("on access") only.

Selection or command
===> ______________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

To **check whether real-time detection had already been activated**, select **`5. Work with Active Jobs`**. A message at the bottom of the screen shows whether the subsystem is active.

To **check the registration information for exit points**, select **`3. Work with Exit Programs`**. The standard **Work with Registration Information** screen appears, with information on system scans for exit points.

To **start real-time detection**, select **`1. Activate Real-Time Detection`**. The **Start Real-Time Antivirus (STRRTAV)** screen appears. Press **Enter** to start detection, or the **F3** key to exit without starting detection.

To end real-time detection, select **`2. De-activate Real-Time Detection`**. The End Real-Time Antivirus (ENDRTAV) screen appears. Press Enter to end detection, or the F3 key to exit without ending detection.

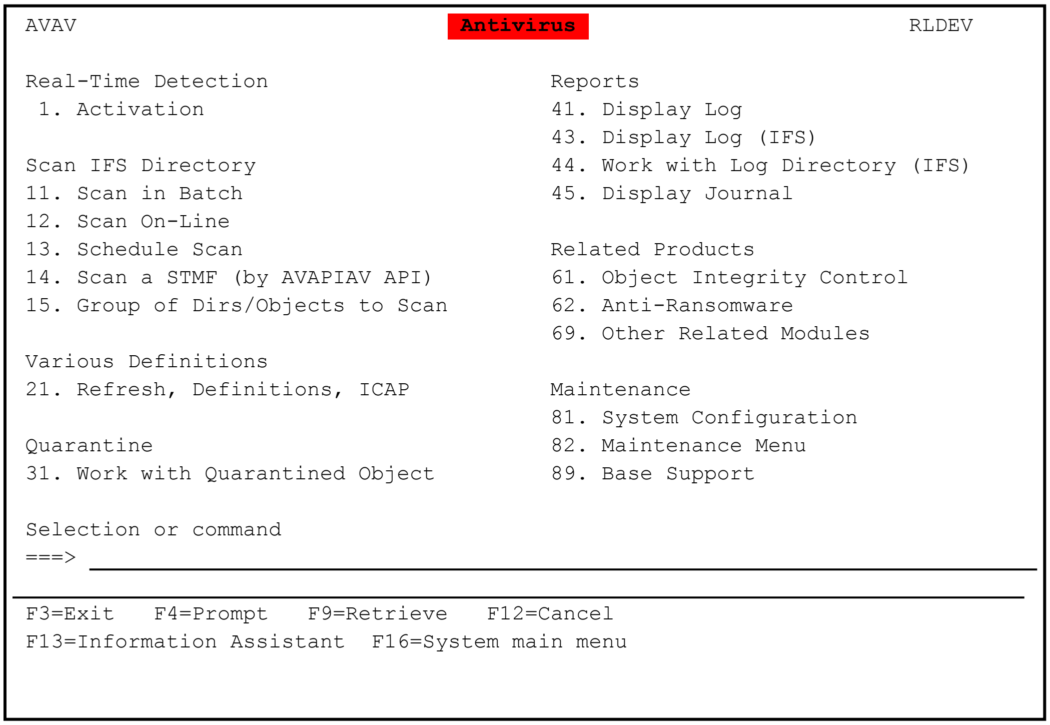
To activate real-time detection each time the system restarts, select **`11. Activate Real-Time Detection at IPL`**. The message "Change effective next time subsystem starts" appears on the bottom line of the screen.

To stop activating real-time detection each time the system restarts, select **`12. Do Not Activate RT Detection at IPL`**. The message "Change effective next time subsystem starts" appears on the bottom line of the screen.

Scanning for Viruses

Once you have set up Antivirus and updated the virus definitions, you can scan the IFS area of your IBM i system.

You can scan in three ways from the main Antivirus screen (***STRAV***):



```
AVAV                              Antivirus                           RLDEV

Real-Time Detection                       Reports
 1. Activation                            41. Display Log
                                          43. Display Log (IFS)
Scan IFS Directory                        44. Work with Log Directory (IFS)
11. Scan in Batch                         45. Display Journal
12. Scan On-Line
13. Schedule Scan                         Related Products
14. Scan a STMF (by AVAPIAV API)          61. Object Integrity Control
15. Group of Dirs/Objects to Scan         62. Anti-Ransomware
                                          69. Other Related Modules
Various Definitions
21. Refresh, Definitions, ICAP            Maintenance
                                          81. System Configuration
Quarantine                                82. Maintenance Menu
31. Work with Quarantined Object          89. Base Support

Selection or command
===> ____________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

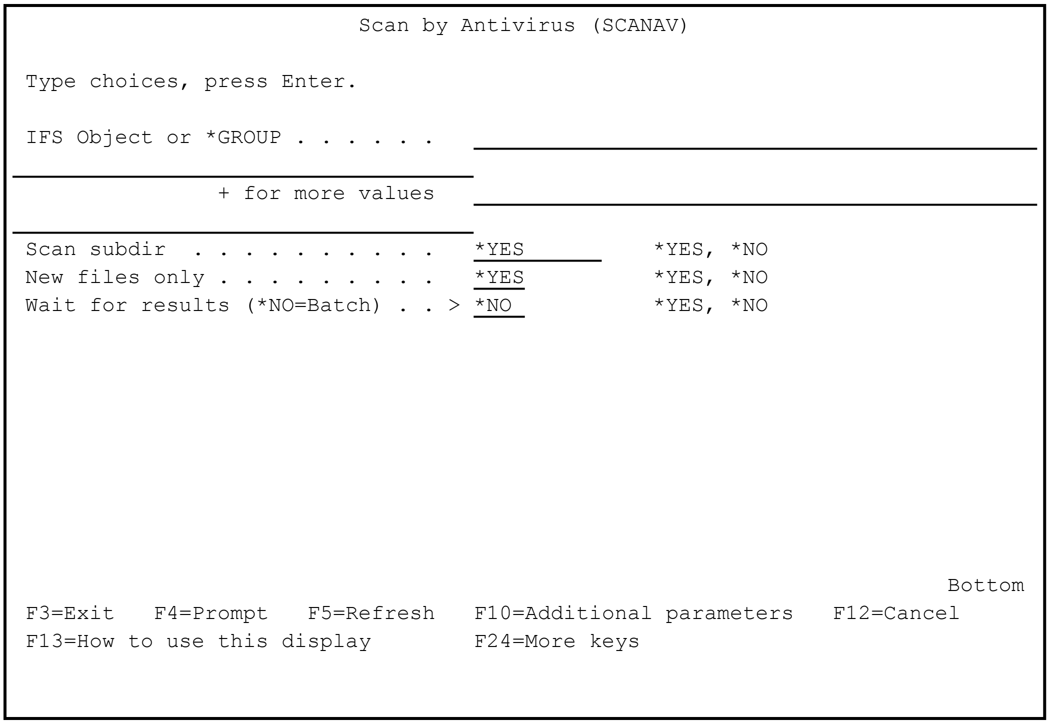
To **scan in batch mode**, running the scan in the background and generating a report when it is done, select **`11. Scan in Batch`**. The **Scan by AntiVirus (SCANAV)** screen appears with values for batch scans, as shown in "Scanning in Batch Mode" on page 53.

To **scan in real-time**, displaying the results of the scan onscreen as it progresses, select **`12. Scan On-Line`**. The **Scan by AntiVirus (SCANAV)** screen appears with values for real-time scans, as shown in "Scanning in Real-Time" on page 57.

To **schedule scans** to run, either as one-time or recurring events, select **`13. Schedule Scan`**. The **Work with Job Schedule Entries (WRKJOBSCDE)** screen appears with values for scheduling scans, as shown in "Scheduling Virus Scans" on page 59.

Scanning in Batch Mode

To **scan in batch mode**, running the scan in the background and generating a report when it is done, select **`11. Scan in Batch`** from the **Antivirus** main menu (*STRAV*). The **Scan by AntiVirus (SCANAV)** screen appears with values for batch scans.



```
                           Scan by Antivirus (SCANAV)

 Type choices, press Enter.

 IFS Object or *GROUP . . . . . .   ____________________________________________
____________________________________
                 + for more values  ____________________________________________
____________________________________
 Scan subdir  . . . . . . . . . .   *YES          *YES, *NO
 New files only . . . . . . . . .   *YES          *YES, *NO
 Wait for results (*NO=Batch) . . > *NO           *YES, *NO








                                                                          Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys
```

The body of the screen contains the following fields:

`IFS Object or *GROUP`

The file or directory to be scanned.

To scan multiple objects, enter a plus sign ("**+**") in the **`+ for more fields`** subfield. A secondary screen opens in which you can enter up to ten files or directories.

`Scan subdir (*BYDIR:n=Parallel)`

Whether to scan subdirectories of the IFS directory to be scanned. Possible values are:

- **`*YES`**: Scan subdirectories
- **`*NO`**: Do not scan subdirectories

- ***BYDIR#1** / ***BYDIR#2** / ***BYDIR#3**: Scan 1, 2, or 3 sub-directories in parallel

New files only

Whether to scan all files in the directory or only those that had been created or changed since the previous scan. Possible values are:

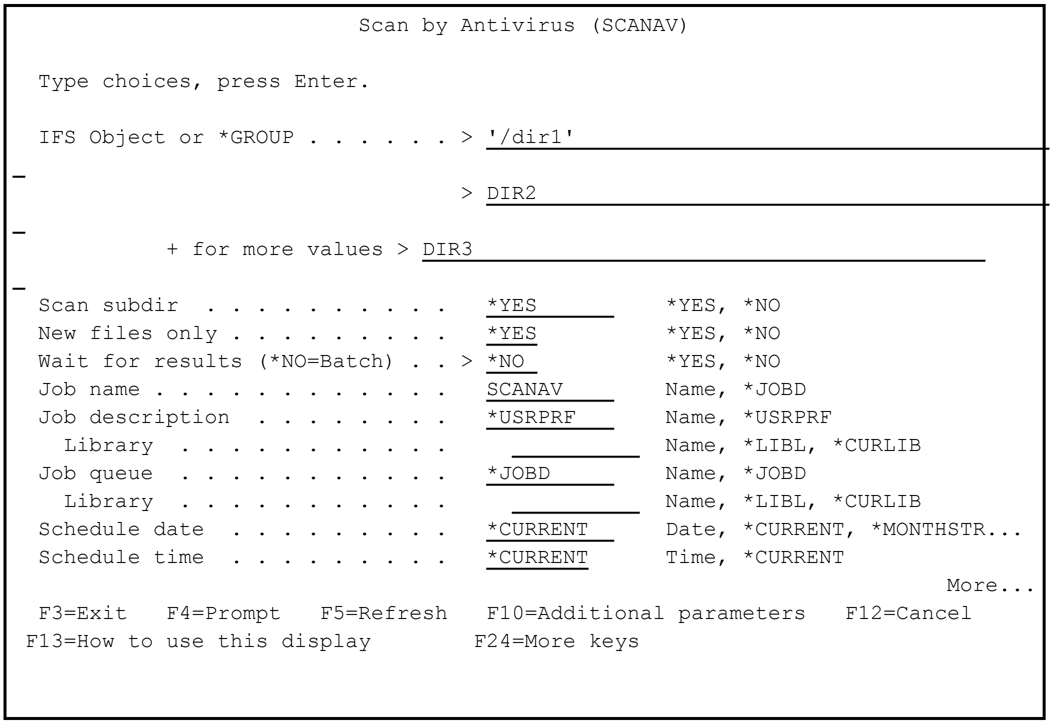
- ***YES**: Only scan new files
- ***NO**: Scan all files

Wait for results (*NO=Batch)

Whether to display results on the screen in real-time or to deliver them as a report when the scan is complete.

- ***YES**: Display results in real-time
- ***NO**: Display or print results as a report when the scan is complete (Batch mode)

Once you have entered these values, further fields appear on the screen:



```
                            Scan by Antivirus (SCANAV)

  Type choices, press Enter.

  IFS Object or *GROUP . . . . . . > '/dir1'
_
                                   > DIR2
_
            + for more values > DIR3
_
  Scan subdir  . . . . . . . . . .   *YES          *YES, *NO
  New files only . . . . . . . . .   *YES          *YES, *NO
  Wait for results (*NO=Batch) . . > *NO           *YES, *NO
  Job name . . . . . . . . . . . .   SCANAV        Name, *JOBD
  Job description  . . . . . . . .   *USRPRF       Name, *USRPRF
    Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
  Job queue  . . . . . . . . . . .   *JOBD         Name, *JOBD
    Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
  Schedule date  . . . . . . . . .   *CURRENT      Date, *CURRENT, *MONTHSTR...
  Schedule time  . . . . . . . . .   *CURRENT      Time, *CURRENT
                                                                        More...
  F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys
```

Job name

The name of the job. The default is **SCANAV**. Possible values are:

- Any string that is valid for job names
- ***JOBD**

Job description

The default is ***USPRF**. Possible values are:

- Any string that is valid for job descriptions
- ***USRPRF**

Library

Possible values are:

- The name of any library to which the user can write
- ***LIBL**
- ***CURLIB**

Job queue

The default is ***JOBD**. Possible values are:

- Any job queue available to the user
- ***JOBD**

Library

Possible values are:

- The name of any library to which the user can write
- ***LIBL**
- ***CURLIB**

Schedule date

The date on which the job is to run. The default is ***CURRENT**. Possible values are:

- Any valid date string
- ***CURRENT**: Today
- ***MONTHSTR**: The start of the next month
- ***MONTHEND**: The end of the current month
- ***MON**
- ***TUE**
- ***WED**
- ***THU**
- ***FRI**

- ***SAT**
- ***SUN**

Schedule time

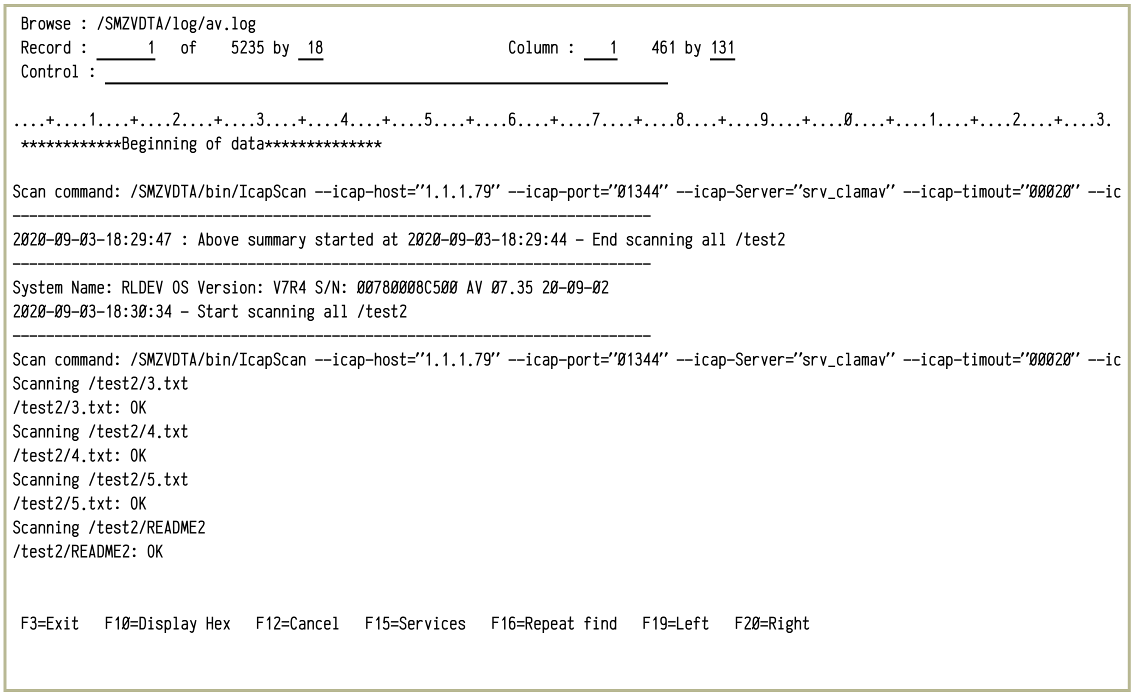
The time at which the job is to run. The default is ***CURRENT**. Possible values are:

- Any valid time string.
- ***CURRENT**: The current time.

Send Email To Recipient(s)

The email addresses of people to whom the job will send email when it is finished]. The default is ***NONE**.

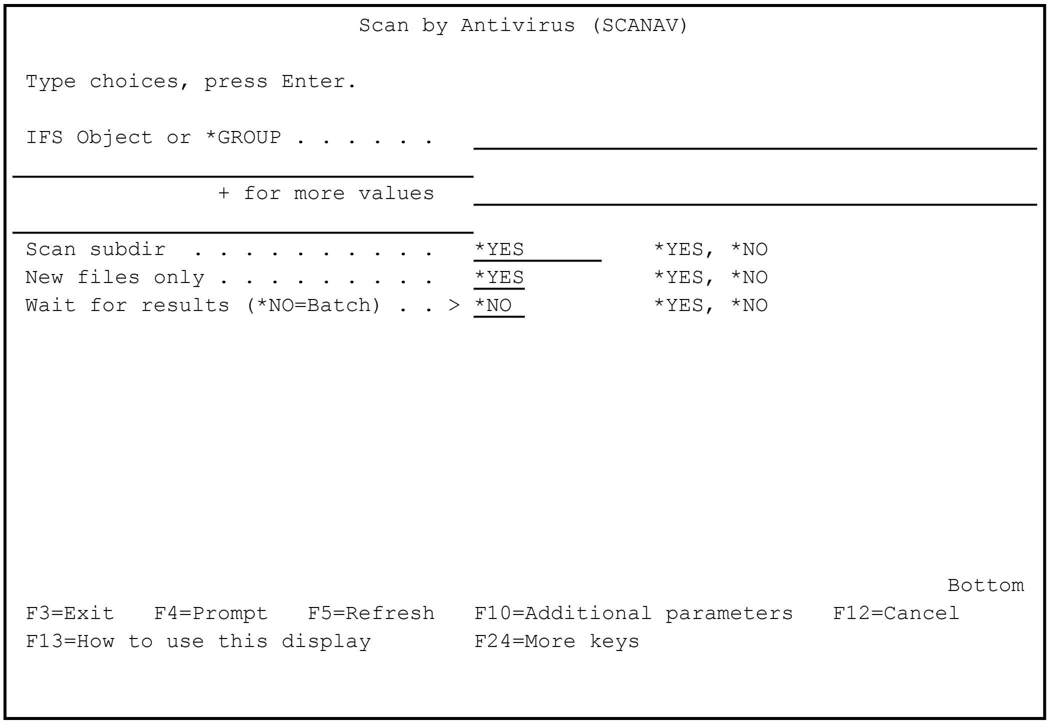
To **display the results** of a batch scan, select **41. Display Log** from the **Antivirus** main menu. The log file appears in a file display window:



```
 Browse : /SMZVDTA/log/av.log
 Record : ______1   of    5235 by  18                    Column : ___1    461 by 131
 Control : ___________________________________________________________________

....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3.
 ************Beginning of data**************

Scan command: /SMZVDTA/bin/IcapScan --icap-host="1.1.1.79" --icap-port="01344" --icap-Server="srv_clamav" --icap-timout="00020" --ic
----------------------------------------------------------------------------
2020-09-03-18:29:47 : Above summary started at 2020-09-03-18:29:44 - End scanning all /test2
----------------------------------------------------------------------------
System Name: RLDEV OS Version: V7R4 S/N: 00780008C500 AV 07.35 20-09-02
2020-09-03-18:30:34 - Start scanning all /test2
----------------------------------------------------------------------------
Scan command: /SMZVDTA/bin/IcapScan --icap-host="1.1.1.79" --icap-port="01344" --icap-Server="srv_clamav" --icap-timout="00020" --ic
Scanning /test2/3.txt
/test2/3.txt: OK
Scanning /test2/4.txt
/test2/4.txt: OK
Scanning /test2/5.txt
/test2/5.txt: OK
Scanning /test2/README2
/test2/README2: OK


 F3=Exit   F10=Display Hex   F12=Cancel   F15=Services   F16=Repeat find   F19=Left   F20=Right
```

Scanning in Batch Mode

To **scan in batch mode**, running the scan in the background and generating a report when it is done, select **`11. Scan in Batch`** from the **Antivirus** main menu (*STRAV*). The **Scan by AntiVirus (SCANAV)** screen appears with values for batch scans.



```
                          Scan by Antivirus (SCANAV)

 Type choices, press Enter.

 IFS Object or *GROUP . . . . . .   ____________________________________________
_____________________________________
                + for more values   ____________________________________________
_____________________________________
 Scan subdir  . . . . . . . . . .   *YES__        *YES, *NO
 New files only . . . . . . . . .   *YES          *YES, *NO
 Wait for results (*NO=Batch) . . > *NO           *YES, *NO










                                                                         Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys
```

The body of the screen contains the following fields:

`IFS Object or *GROUP`

The file or directory to be scanned.

To scan multiple objects, enter a plus sign ("**+**") in the **`+ for more fields`** subfield. A secondary screen opens in which you can enter up to ten files or directories.

`Scan subdir (*BYDIR:n=Parallel)`

Whether to scan subdirectories of the IFS directory to be scanned. Possible values are:

- **`*YES`**: Scan subdirectories
- **`*NO`**: Do not scan subdirectories
- **`*BYDIR#1`** / **`*BYDIR#2`** / **`*BYDIR#3`**: Scan 1, 2, or 3 sub-directories in parallel

New files only

Whether to scan all files in the directory or only those that had been created or changed since the previous scan. Possible values are:

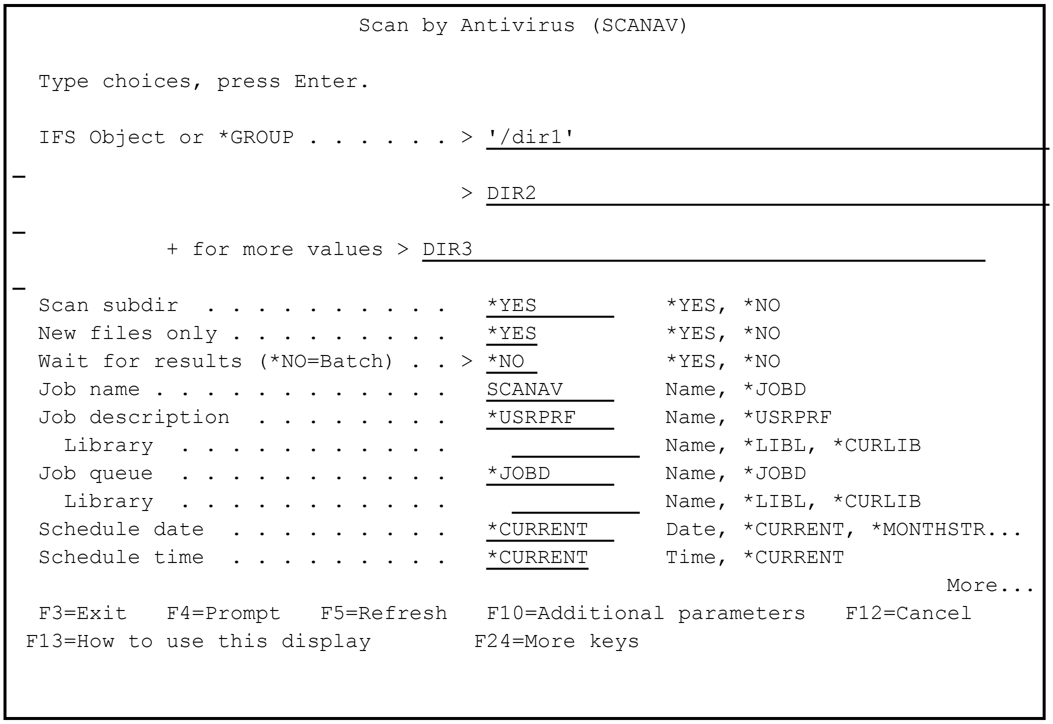
- ***YES**: Only scan new files
- ***NO**: Scan all files

Wait for results (*NO=Batch)

Whether to display results on the screen in real-time or to deliver them as a report when the scan is complete.

- ***YES**: Display results in real-time
- ***NO**: Display or print results as a report when the scan is complete (Batch mode)

Once you have entered these values, further fields appear on the screen:



```
                            Scan by Antivirus (SCANAV)

  Type choices, press Enter.

  IFS Object or *GROUP . . . . . . > '/dir1'
_
                                   > DIR2
_
            + for more values > DIR3
_
  Scan subdir  . . . . . . . . . .   *YES          *YES, *NO
  New files only . . . . . . . . .   *YES          *YES, *NO
  Wait for results (*NO=Batch) . . > *NO           *YES, *NO
  Job name . . . . . . . . . . . .   SCANAV        Name, *JOBD
  Job description  . . . . . . . .   *USRPRF       Name, *USRPRF
    Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
  Job queue  . . . . . . . . . . .   *JOBD         Name, *JOBD
    Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
  Schedule date  . . . . . . . . .   *CURRENT      Date, *CURRENT, *MONTHSTR...
  Schedule time  . . . . . . . . .   *CURRENT      Time, *CURRENT
                                                                        More...
  F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys
```

Job name

The name of the job. The default is **SCANAV**. Possible values are:

- Any string that is valid for job names
- ***JOBD**

Job description

The default is ***USPRF**. Possible values are:

- Any string that is valid for job descriptions
- ***USRPRF**

Library

Possible values are:

- The name of any library to which the user can write
- ***LIBL**
- ***CURLIB**

Job queue

The default is ***JOBD**. Possible values are:

- Any job queue available to the user
- ***JOBD**

Library

Possible values are:

- The name of any library to which the user can write
- ***LIBL**
- ***CURLIB**

Schedule date

The date on which the job is to run. The default is ***CURRENT**. Possible values are:

- Any valid date string
- ***CURRENT**: Today
- ***MONTHSTR**: The start of the next month
- ***MONTHEND**: The end of the current month
- ***MON**
- ***TUE**
- ***WED**
- ***THU**
- ***FRI**
- ***SAT**
- ***SUN**

Schedule time

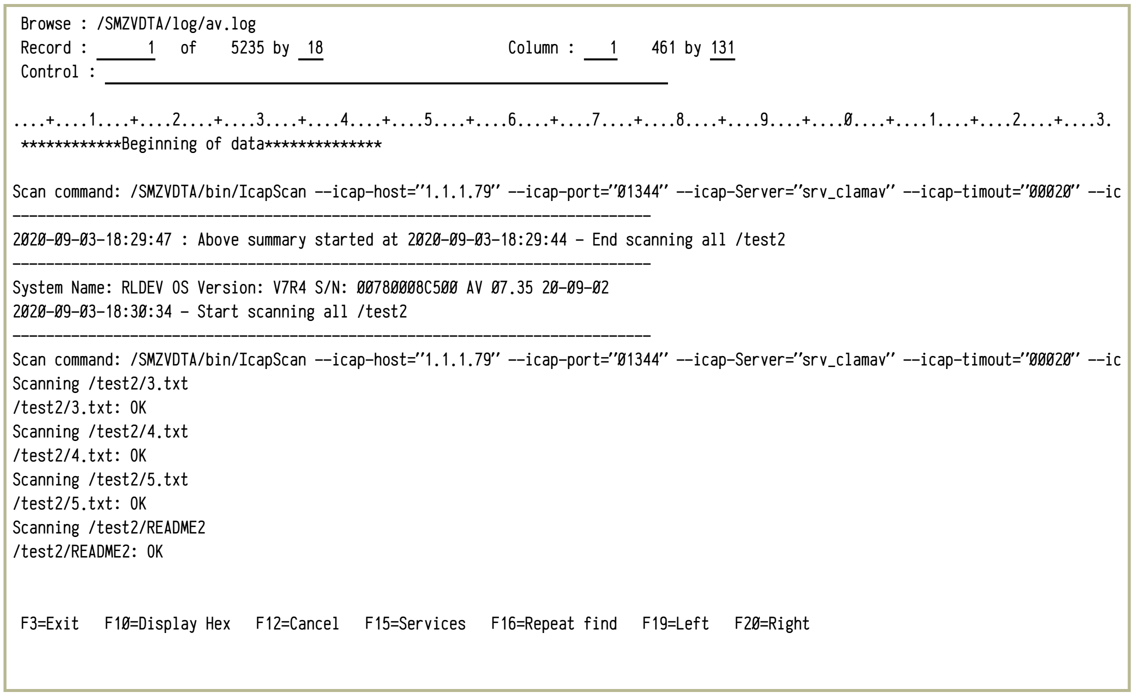
The time at which the job is to run. The default is ***CURRENT**. Possible values are:

- Any valid time string.
- ***CURRENT**: The current time.

Send Email To Recipient(s)

The email addresses of people to whom the job will send email when it is finished]. The default is ***NONE**.

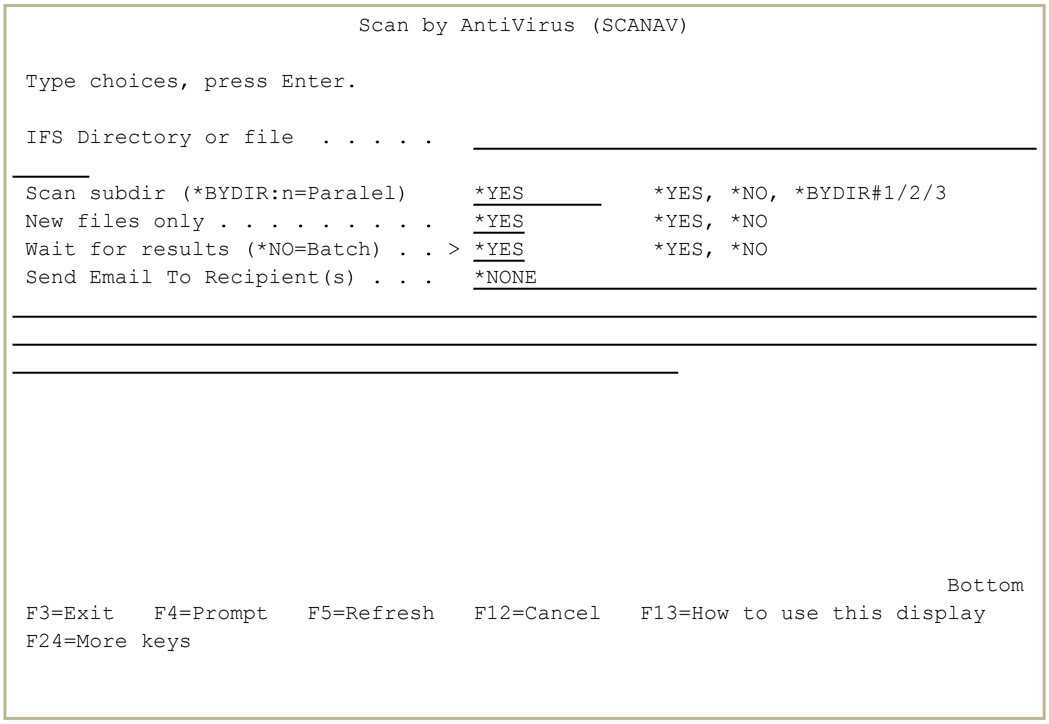
To **display the results** of a batch scan, select **41. Display Log** from the **Antivirus** main menu. The log file appears in a file display window:



```
 Browse : /SMZVDTA/log/av.log
 Record : _____1   of    5235 by  18                    Column : ___1    461 by 131
 Control : ____________________________________________________________

....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3.
 ************Beginning of data**************

Scan command: /SMZVDTA/bin/IcapScan --icap-host="1.1.1.79" --icap-port="01344" --icap-Server="srv_clamav" --icap-timout="00020" --ic
----------------------------------------------------------------------------
2020-09-03-18:29:47 : Above summary started at 2020-09-03-18:29:44 - End scanning all /test2
----------------------------------------------------------------------------
System Name: RLDEV OS Version: V7R4 S/N: 00780008C500 AV 07.35 20-09-02
2020-09-03-18:30:34 - Start scanning all /test2
----------------------------------------------------------------------------
Scan command: /SMZVDTA/bin/IcapScan --icap-host="1.1.1.79" --icap-port="01344" --icap-Server="srv_clamav" --icap-timout="00020" --ic
Scanning /test2/3.txt
/test2/3.txt: OK
Scanning /test2/4.txt
/test2/4.txt: OK
Scanning /test2/5.txt
/test2/5.txt: OK
Scanning /test2/README2
/test2/README2: OK


 F3=Exit   F10=Display Hex   F12=Cancel   F15=Services   F16=Repeat find   F19=Left   F20=Right
```

Scanning in Real-Time

To **scan in real-time**, running the scan in the foreground and displaying the results as they happen, select **`12. Scan On-Line`** from the **Antivirus** main menu (*STRAV*). The **Scan by AntiVirus (SCANAV)** screen appears with values for real-time scans.



```
                           Scan by AntiVirus (SCANAV)

 Type choices, press Enter.

 IFS Directory or file  . . . . .    ____________________________________________
______
 Scan subdir (*BYDIR:n=Paralel)     *YES______     *YES, *NO, *BYDIR#1/2/3
 New files only . . . . . . . . .   *YES           *YES, *NO
 Wait for results (*NO=Batch) . . > *YES           *YES, *NO
 Send Email To Recipient(s) . . .   *NONE________________________________________
________________________________________________________________________________
________________________________________________________________________________
_____________________________________________________











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

The body of the screen contains the following fields:

`IFS Directory or file`

The file or directory to be scanned

`Scan subdir (*BYDIR:n=Parallel)`

Whether to scan subdirectories of the IFS directory to be scanned. Possible values are:

- **`*YES`**: Scan subdirectories
- **`*NO`**: Do not scan subdirectories
- **`*BYDIR#1`** / **`*BYDIR#2`** / **`*BYDIR#3`**: Scan 1, 2, or 3 sub-directories in parallel

New files only

Whether to scan all files in the directory or only those that had been created or changed since the previous scan. Possible values are:

- ***YES**: Only scan new files
- ***NO**: Scan all files

Wait for results (*NO=Batch)

Whether to display results on the screen in real-time or to deliver them as a report when the scan is complete.

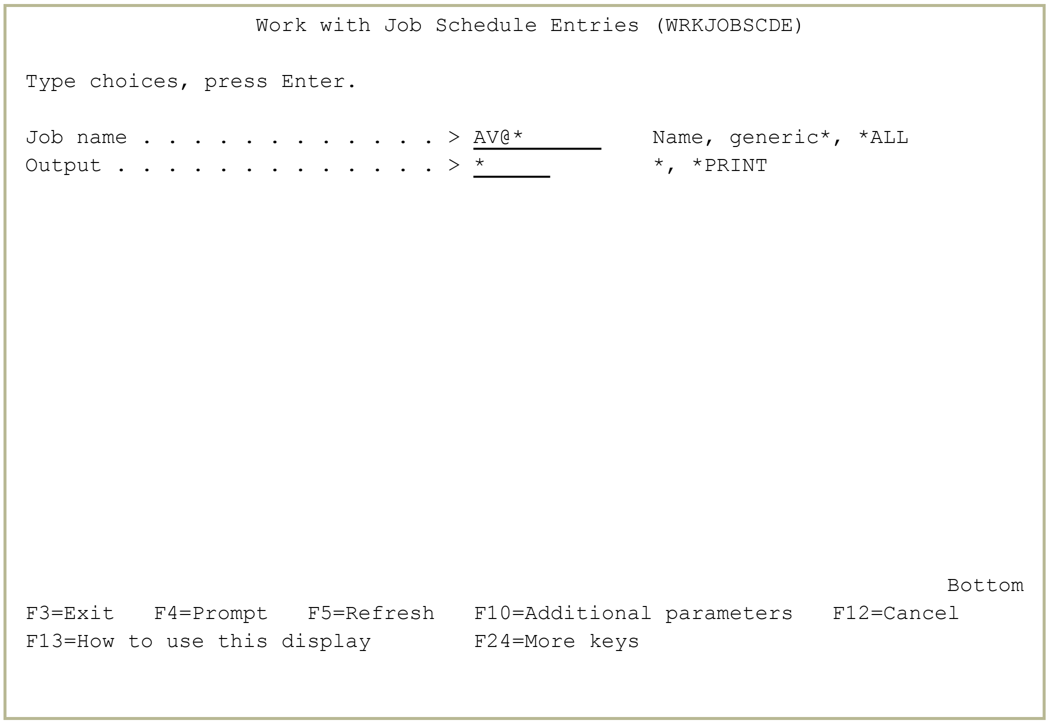
- ***YES**: Display results in real-time
- ***NO**: Display or print results as a report when the scan is complete (Batch mode)

Send Email To Recipient(s)

The email addresses of people to whom the job will send email when it is finished. The default is ***NONE**.

Scheduling Virus Scans

To schedule virus scans, as either a one-time or recurring event, select **13. Schedule Scan** from the **Antivirus** main menu(*STRAV*). The standard **Work with Job Schedule Entries (WRKJOBSCDE)** screen appears, with an entry for virus scanning.



```
                  Work with Job Schedule Entries (WRKJOBSCDE)

Type choices, press Enter.

Job name . . . . . . . . . . . . . > AV@*__________    Name, generic*, *ALL
Output . . . . . . . . . . . . . . > *______           *, *PRINT















                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

The screen contains two fields:

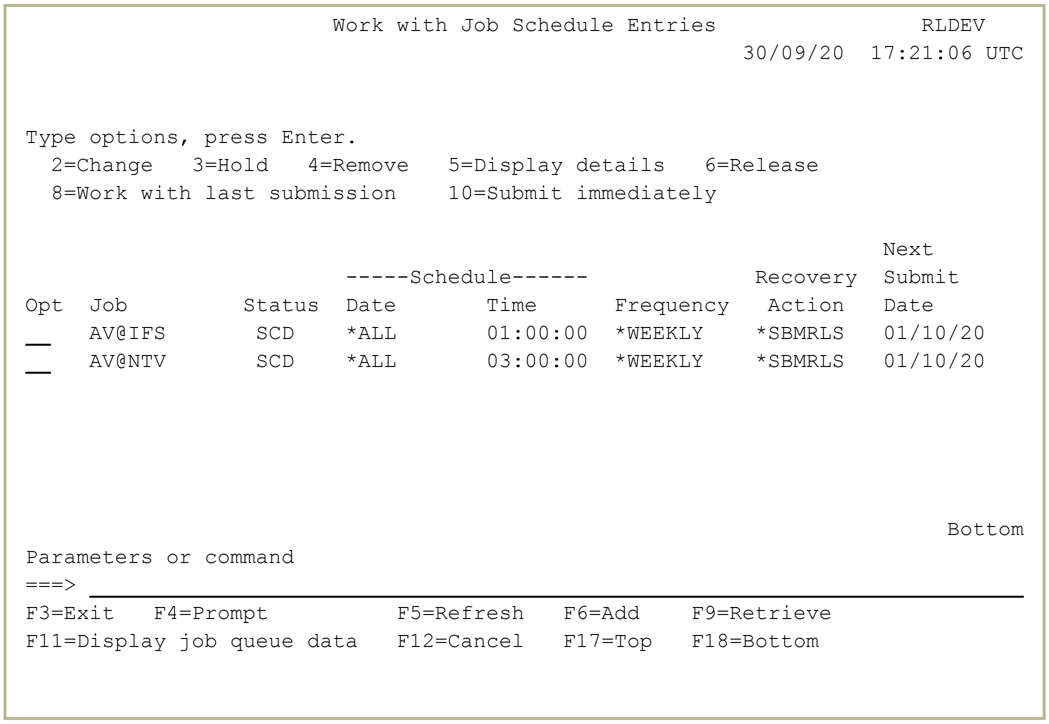
Job name

The name of the job being examined. For Antivirus scans, this is **AV@***.

Output

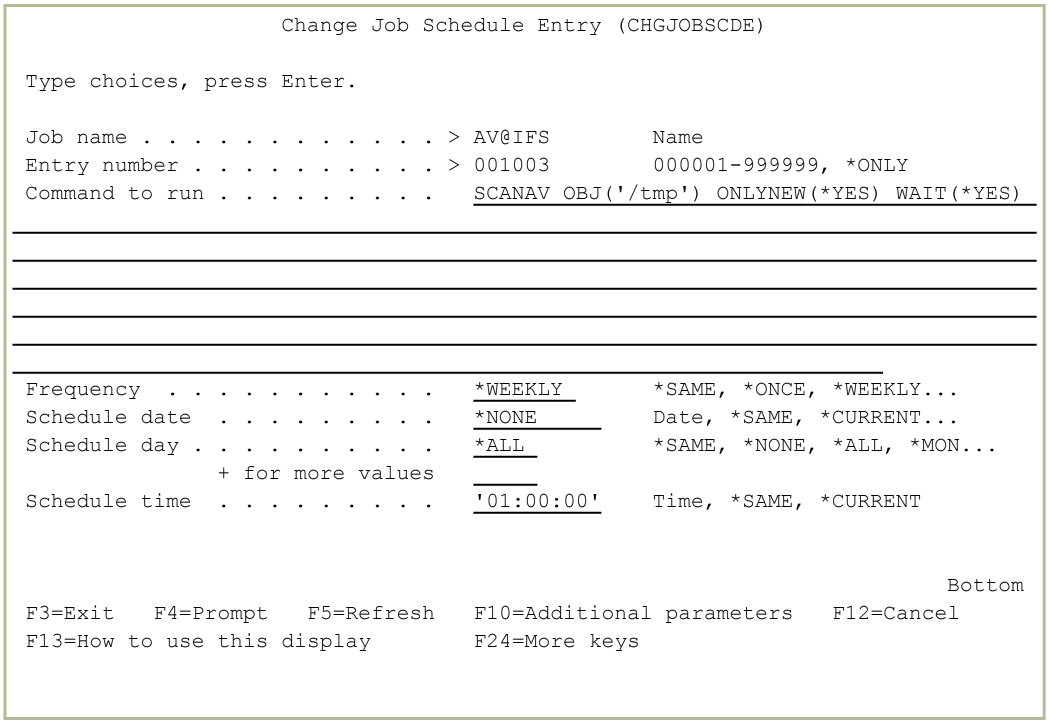
The destination of the listing. For the screen, this is ***** (an asterisk).

The screen displays scheduled entries:



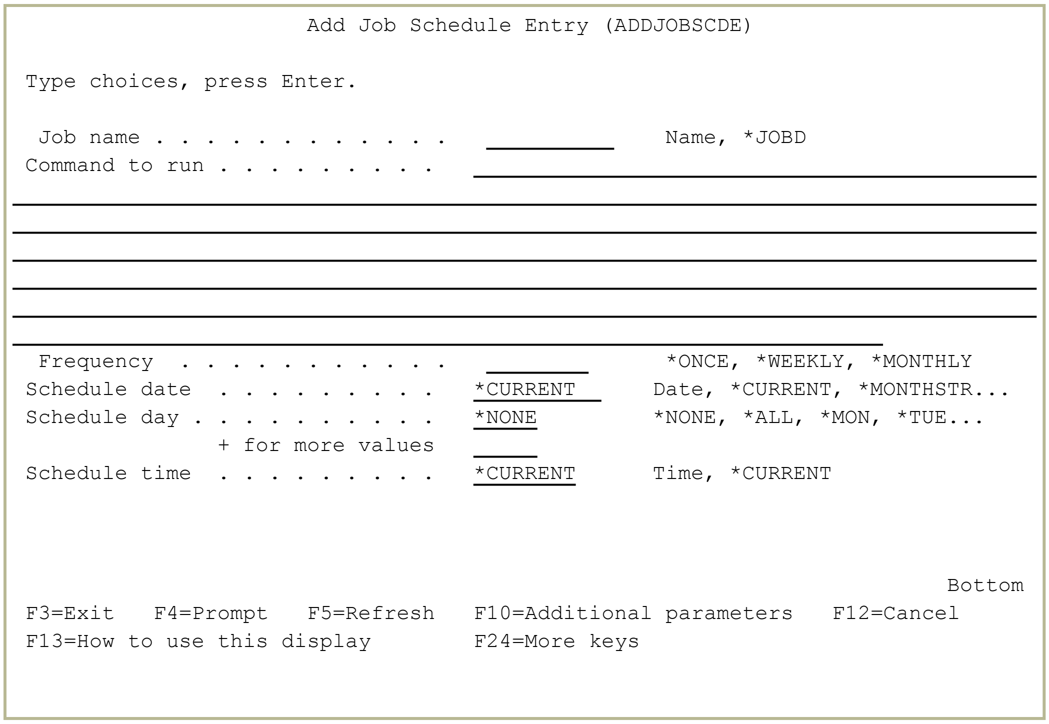
```
                         Work with Job Schedule Entries               RLDEV
                                                          30/09/20  17:21:06 UTC


Type options, press Enter.
  2=Change   3=Hold   4=Remove   5=Display details   6=Release
  8=Work with last submission    10=Submit immediately

                                                                    Next
                          -----Schedule------             Recovery  Submit
Opt  Job         Status  Date       Time       Frequency   Action   Date
__   AV@IFS       SCD    *ALL       01:00:00   *WEEKLY    *SBMRLS   01/10/20
__   AV@NTV       SCD    *ALL       03:00:00   *WEEKLY    *SBMRLS   01/10/20






                                                                         Bottom
Parameters or command
===> ________________________________________________________________________
F3=Exit   F4=Prompt          F5=Refresh   F6=Add    F9=Retrieve
F11=Display job queue data   F12=Cancel   F17=Top   F18=Bottom
```

To **see and change the parameters for a scheduled job**, type **2** in the **Opt** field for that line and press **Enter**. The **Change Job Schedule Entry (CHGJOBSCDE)** screen for that command appears, showing the values for the job.



```
                     Change Job Schedule Entry (CHGJOBSCDE)

Type choices, press Enter.

Job name . . . . . . . . . . . . > AV@IFS        Name
Entry number . . . . . . . . . . > 001003        000001-999999, *ONLY
Command to run . . . . . . . . .   SCANAV OBJ('/tmp') ONLYNEW(*YES) WAIT(*YES)






Frequency  . . . . . . . . . . .   *WEEKLY       *SAME, *ONCE, *WEEKLY...
Schedule date  . . . . . . . . .   *NONE         Date, *SAME, *CURRENT...
Schedule day . . . . . . . . . .   *ALL          *SAME, *NONE, *ALL, *MON...
               + for more values   
Schedule time  . . . . . . . . .   '01:00:00'    Time, *SAME, *CURRENT


                                                                         Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

To **add a scheduled job**, press the F6 key. The **Add Job Schedule Entry (ADDJOBSCDE)** screen for that command appears, showing the values for the job.



```
                      Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

 Job name . . . . . . . . . . . .   __________        Name, *JOBD
Command to run . . . . . . . . .   ____________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
____________________________________________________________________
 Frequency  . . . . . . . . . . .   ________         *ONCE, *WEEKLY, *MONTHLY
Schedule date  . . . . . . . . .   *CURRENT__      Date, *CURRENT, *MONTHSTR...
Schedule day . . . . . . . . . .   *NONE           *NONE, *ALL, *MON, *TUE...
               + for more values   _____
Schedule time  . . . . . . . . .   *CURRENT        Time, *CURRENT



                                                                         Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

The command depends on the server type.

The parameters depend our your installation's needs.

For example, as shown above, the command

`SCANAV OBJ('/tmp') ONLYNEW(*YES) WAIT(*YES)`

runs the **`SCANAV`** command for a ClamAV server, scanning the **`/tmp`** directory, looking only at new objects and displaying the results at the end of the run.

Viewing Scan Results

The results of real-time scans appear on your screen as they happen. You can also view and work with these results and those of batch and scheduled scans later.

To **display the most recent log** of scan results and alerts, select **`41. Display Log`** from the **Antivirus** main menu (*STRAV*. The log file appears in a file display window, as shown in "Displaying Recent Virus Scan and Alert Logs" on the facing page.

To **view files that Antivirus has quarantined** as possibly harboring viruses, select **`31. Work with Quarantined Object`** from the **Antivirus** main menu (*STRAV*. The **Work with Object Links** screen appears, as shown in "Viewing Quarantined Objects" on page 65.

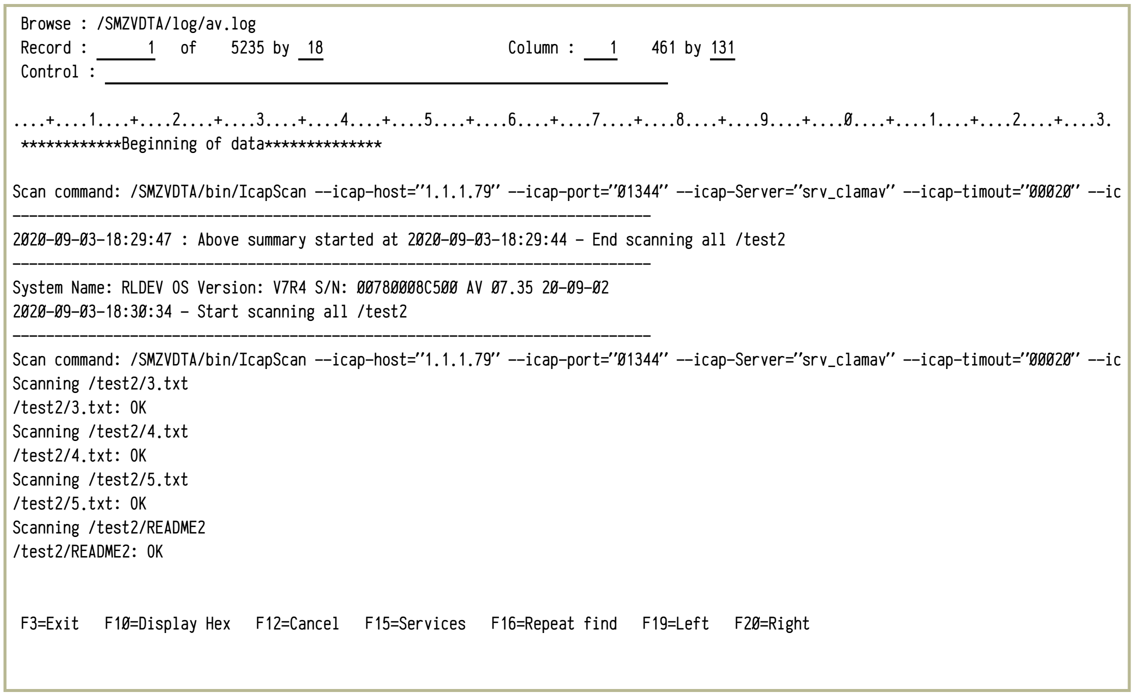
To **mark scanned objects as unscanned and vice versa**, select **`31. Reset Scan Status of a File`** from the **Maintenance Menu** (*STRAV>* **`82`**). The **Reset Scan Status (RSTSCNSTS)** screen appears, as shown in "Resetting the Scan Status of Objects" on page 66.

To **view older scan logs**, select **`42. Work with Log Directory`** from the **Antivirus** main menu (*STRAV*). The **Work with Scan Logs** screen appears, as shown in "Viewing Older Scan Logs" on page 67

To **close the current log file and start a new one**, select **`8. Start a New Log file`** from the **Maintenance Menu** (*STRAV>* **`82`**). The **Change Antivirus Log (CHGAVLOG)** screen appears, as shown in "Starting a New Log File" on page 68.

Displaying Recent Virus Scan and Alert Logs

To **display the most recent log** of scan results, select **`41. Display Log`** from the **Antivirus** main menu (***STRAV***. The log file appears in a file display window:



```
 Browse : /SMZVDTA/log/av.log
 Record : ______1   of    5235 by  18                    Column :  __1    461 by 131
 Control : ____________________________________________________________________

....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3.
 ************Beginning of data**************

Scan command: /SMZVDTA/bin/IcapScan --icap-host="1.1.1.79" --icap-port="01344" --icap-Server="srv_clamav" --icap-timout="00020" --ic
----------------------------------------------------------------------------
2020-09-03-18:29:47 : Above summary started at 2020-09-03-18:29:44 - End scanning all /test2
----------------------------------------------------------------------------
System Name: RLDEV OS Version: V7R4 S/N: 00780008C500 AV 07.35 20-09-02
2020-09-03-18:30:34 - Start scanning all /test2
----------------------------------------------------------------------------
Scan command: /SMZVDTA/bin/IcapScan --icap-host="1.1.1.79" --icap-port="01344" --icap-Server="srv_clamav" --icap-timout="00020" --ic
Scanning /test2/3.txt
/test2/3.txt: OK
Scanning /test2/4.txt
/test2/4.txt: OK
Scanning /test2/5.txt
/test2/5.txt: OK
Scanning /test2/README2
/test2/README2: OK


 F3=Exit   F10=Display Hex   F12=Cancel   F15=Services   F16=Repeat find   F19=Left   F20=Right
```

The summary log offers full information including:

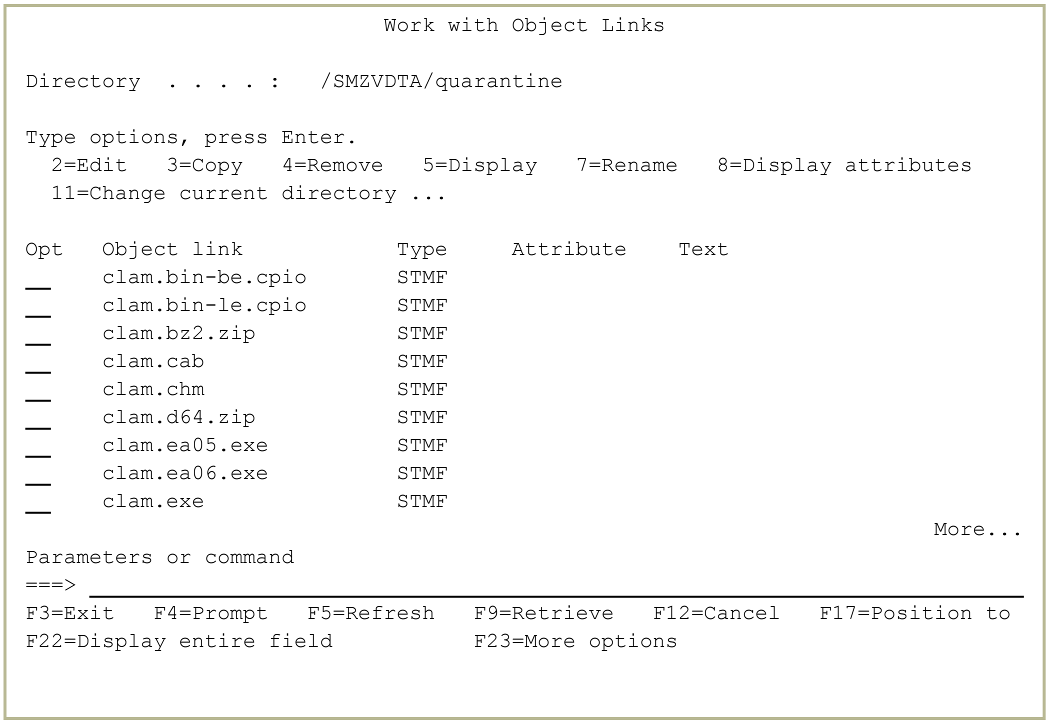
- Virus definition updates
- Virus scans, including:
  - The date, time, and duration of the scan
  - The scanned system
  - The full scan command used
  - Within the scan command
    - The top directory or file
    - Whether the scan was recursive
    - Excluded directories
    - If the scan used ICAP, the system and port used
  - Each file scanned and its status
  - A count of:
    - Known viruses
    - Scanned directories

        - Scanned files
        - Infected files
- On access scans
- On-Access Alarms, including:
    - The date and time of the alert
    - The name of the threat found
    - The infected object
    - The action taken

Viewing Quarantined Objects

When a virus scan identifies an infected object, it moves it into a quarantine directory.

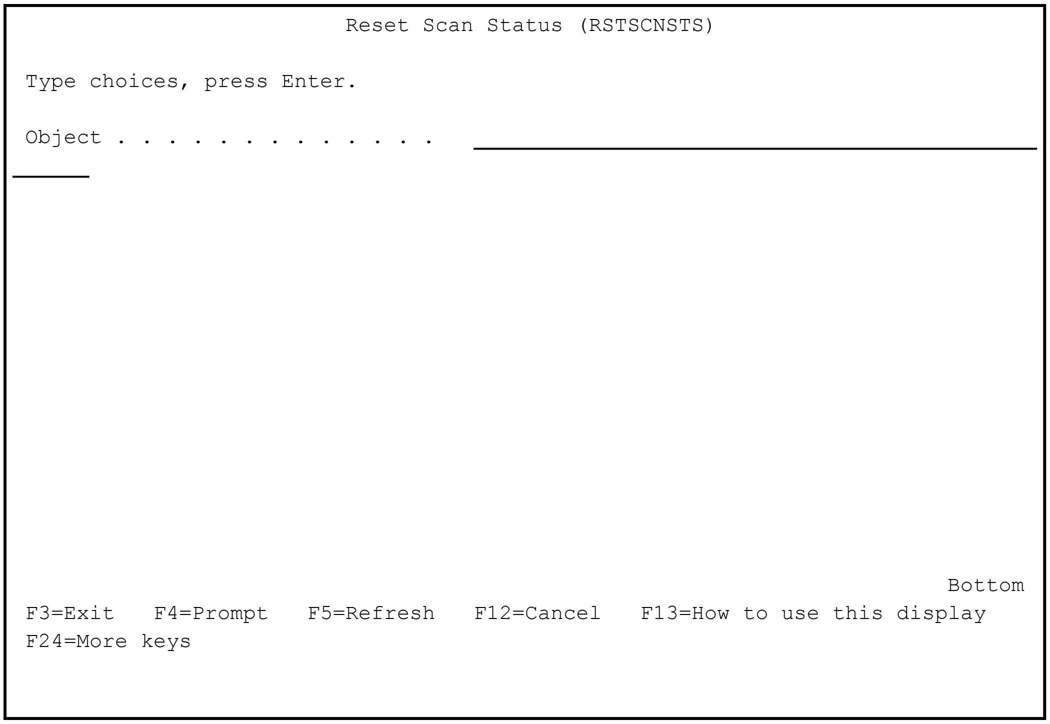
To **view and manage quarantined objects**, select **`31. Work with Quarantined Object`** from the **Antivirus** main menu (*STRAV*). The standard **Work with Object Links** screen appears:



```
                            Work with Object Links

Directory  . . . . :   /SMZVDTA/quarantine

Type options, press Enter.
  2=Edit   3=Copy   4=Remove   5=Display   7=Rename   8=Display attributes
  11=Change current directory ...

Opt   Object link            Type     Attribute    Text
__    clam.bin-be.cpio       STMF
__    clam.bin-le.cpio       STMF
__    clam.bz2.zip           STMF
__    clam.cab               STMF
__    clam.chm               STMF
__    clam.d64.zip           STMF
__    clam.ea05.exe          STMF
__    clam.ea06.exe          STMF
__    clam.exe               STMF
                                                                       More...
Parameters or command
===> _________________________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F12=Cancel   F17=Position to
F22=Display entire field           F23=More options
```

Resetting the Scan Status of Objects

To **mark scanned objects as unscanned and vice versa**, select **`31. Reset Scan Status of a File`** from the **Maintenance Menu** (*STRAV>* **`82`**). The **Reset Scan Status (RSTSCNSTS)** screen appears:

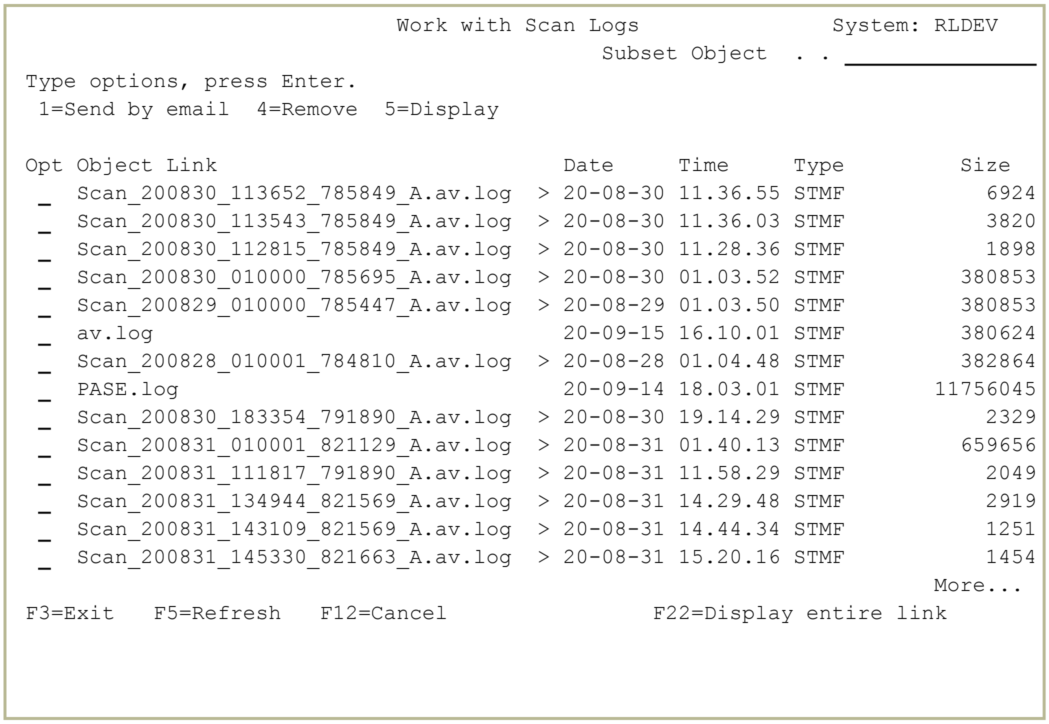


```
                          Reset Scan Status (RSTSCNSTS)

 Type choices, press Enter.

 Object . . . . . . . . . . . . .    ____________________________________________
______










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

Type the pathname of an object in the **`Object`** field and press Enter. The status of the object changes to unscanned.

Viewing Older Scan Logs

To **view older scan logs**, select **`44. Work with Log Directory`** from the **Antivirus** main menu (*STRAV*). The **Work with Scan Logs** screen appears:



```
                              Work with Scan Logs                System: RLDEV
                                              Subset Object  . . _______________
Type options, press Enter.
 1=Send by email  4=Remove  5=Display

Opt Object Link                           Date     Time     Type         Size
 _  Scan_200830_113652_785849_A.av.log  > 20-08-30 11.36.55 STMF           6924
 _  Scan_200830_113543_785849_A.av.log  > 20-08-30 11.36.03 STMF           3820
 _  Scan_200830_112815_785849_A.av.log  > 20-08-30 11.28.36 STMF           1898
 _  Scan_200830_010000_785695_A.av.log  > 20-08-30 01.03.52 STMF         380853
 _  Scan_200829_010000_785447_A.av.log  > 20-08-29 01.03.50 STMF         380853
 _  av.log                                20-09-15 16.10.01 STMF         380624
 _  Scan_200828_010001_784810_A.av.log  > 20-08-28 01.04.48 STMF         382864
 _  PASE.log                              20-09-14 18.03.01 STMF       11756045
 _  Scan_200830_183354_791890_A.av.log  > 20-08-30 19.14.29 STMF           2329
 _  Scan_200831_010001_821129_A.av.log  > 20-08-31 01.40.13 STMF         659656
 _  Scan_200831_111817_791890_A.av.log  > 20-08-31 11.58.29 STMF           2049
 _  Scan_200831_134944_821569_A.av.log  > 20-08-31 14.29.48 STMF           2919
 _  Scan_200831_143109_821569_A.av.log  > 20-08-31 14.44.34 STMF           1251
 _  Scan_200831_145330_821663_A.av.log  > 20-08-31 15.20.16 STMF           1454
                                                                        More...
F3=Exit   F5=Refresh   F12=Cancel               F22=Display entire link
```

The body of the screen lists existing scan logs. For each, it shows the log file's **`Object Link`**, the **`Date`** and **`Time`** that it was created, and its **`Type`** and **`Size`**.

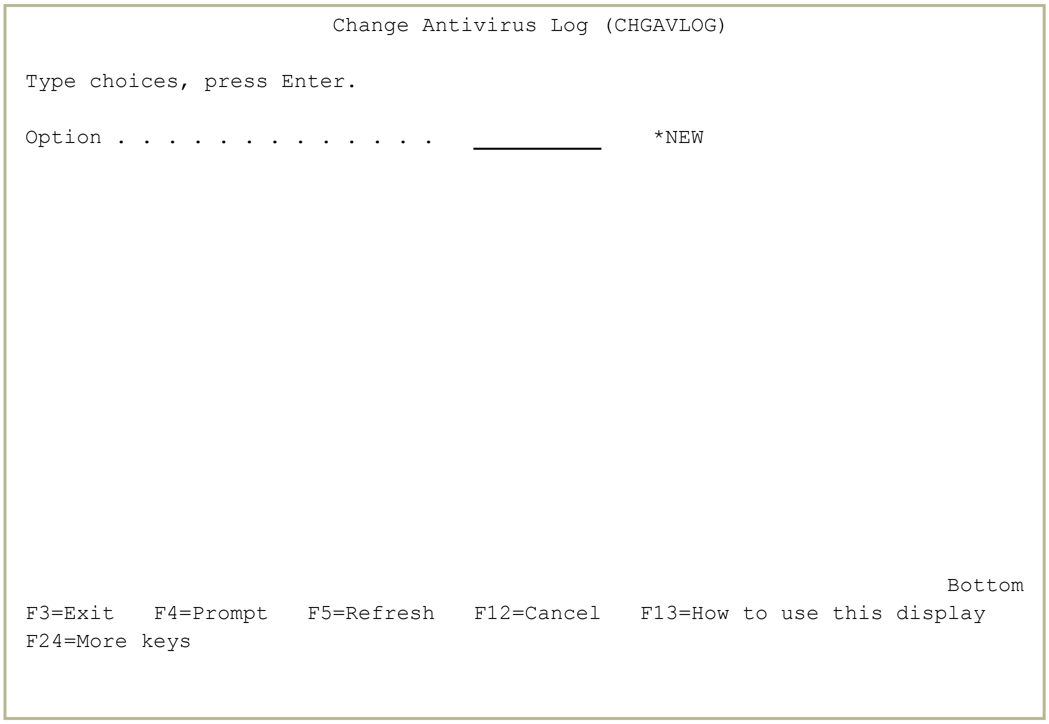
To **display the contents of a log file**, enter **5** in its **`Opt`** field. A file viewer screen displays the contents of the file.

To **remove a log file**, enter **`4`** in its **`Opt`** field. The **Remove Link (RMVLNK)** screen appears, in which you can confirm or cancel the file removal.

To **send a log file by email**, enter **`1`** in its **`Opt`** field. The **Send to Email Address** window appears, in which you can specify the email address to which the file is to be sent.

Starting a New Log File

To **close the current log file and start a new one**, select **`33. Start a New Log file`** from the **Maintenance Menu** (*STRAV>* **`82`**). The **Change Antivirus Log (CHGAVLOG)** screen appears:



```
                         Change Antivirus Log (CHGAVLOG)

Type choices, press Enter.

Option . . . . . . . . . . . . .   __________    *NEW

















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

To **start a new log**, enter **`*NEW`** in the **`Option`** field.

A new log file opens. The current file is closed and saved with the other older logs, as shown in "Viewing Older Scan Logs" on the previous page

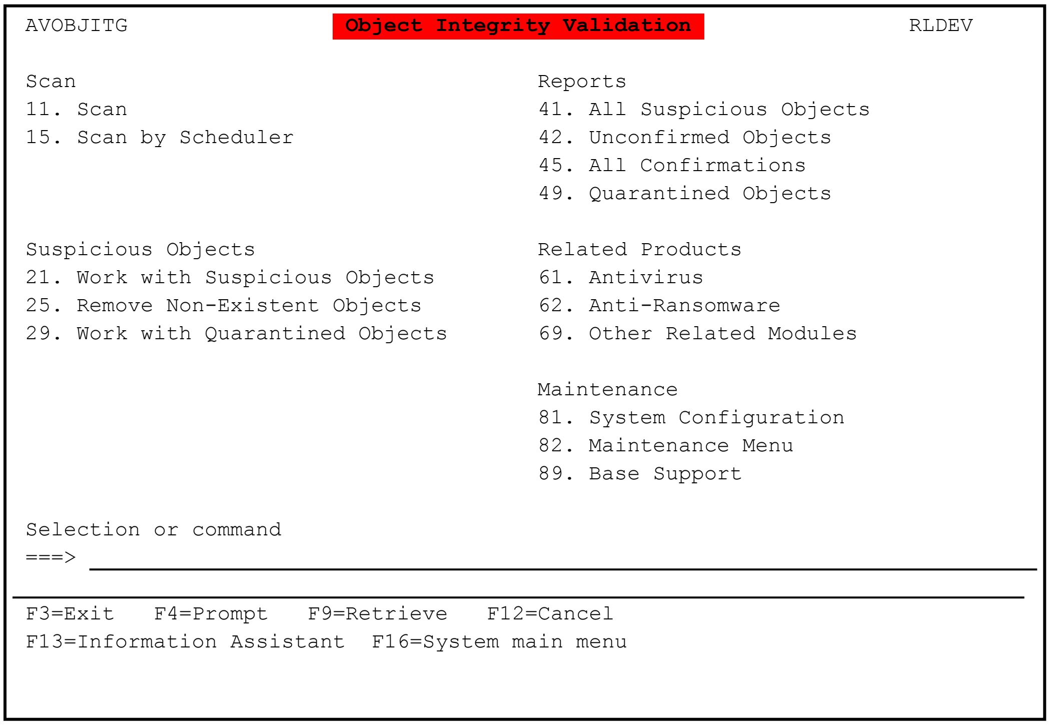
Validating Object Integrity

Native Object Integrity, which is packaged together with Antivirus, checks objects on both IFS and the Native IBM i filesystems and identifies suspicious objects that may or may not have integrity violations.

An integrity violation occurs if:

- a command has been tampered with
- an object has a digital signature that is not valid
- an object has an incorrect domain attribute for its object type
- a program or module object has been tampered with
- a library's attributes have been tampered with

To **run Native Object Integrity** tools, select **`61. Object Integrity Control`** from the **Antivirus** main menu (*STRAV*). The **Object Integrity Validation** screen appears:



```
AVOBJITG                  Object Integrity Validation                RLDEV

Scan                                        Reports
11. Scan                                    41. All Suspicious Objects
15. Scan by Scheduler                       42. Unconfirmed Objects
                                            45. All Confirmations
                                            49. Quarantined Objects

Suspicious Objects                          Related Products
21. Work with Suspicious Objects            61. Antivirus
25. Remove Non-Existent Objects             62. Anti-Ransomware
29. Work with Quarantined Objects           69. Other Related Modules

                                            Maintenance
                                            81. System Configuration
                                            82. Maintenance Menu
                                            89. Base Support

Selection or command
===> ____________________________________________________________________
_______________________________________________________________________________
F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel
F13=Information Assistant  F16=System main menu
```

To **scan your system** for suspicious objects, select **`11. Scan`**. A standard **Submit Job (SBMJOB)** screen appears, with parameters set for this scan.

To schedule a one-time or recurring scan, select **12. Scan by Scheduler**. A standard Work with Job Schedule Entries screen appears with information on the job **AV@NTV**, from which you can change its parameters.

To remove information on objects that no longer exist, select **25. Remove Non-Existent Objects**. The information on these objects is removed.

For reports on suspicious objects:

- To report on all suspicious objects, select **41. All Suspicious Objects**.
- To report on objects marked as suspicious but not confirmed as inoffensive, select **42. Unconfirmed Objects**.
- To report on objects confirmed as inoffensive, select **45. All Confirmations**.

For each of these reports, the Display AV Object Integrity (DSPAVITG) screen appears, as shown in "Reporting on Suspicious Objects" on the facing page.

To manage suspicious objects, select **21. Work with Suspicious Objects**. The Remove Non-existent Objects window appears. Enter **Y** to remove information on objects that no longer exist, or N to retain the information, then press Enter. The Work with Suspicious Objects screen appears, as shown in "Managing Suspicious Objects" on page 75.

To report on quarantined objects, select **49. Quarantined Objects**. The standard Display Library screen appears, showing the objects in the **SMZVQRN** quarantine library.

To manage quarantined objects, select **29. Work with Quarantined Objects**. The standard Work with Objects Using PDM screen appears, showing the objects in the **SMZVQRN** quarantine library.

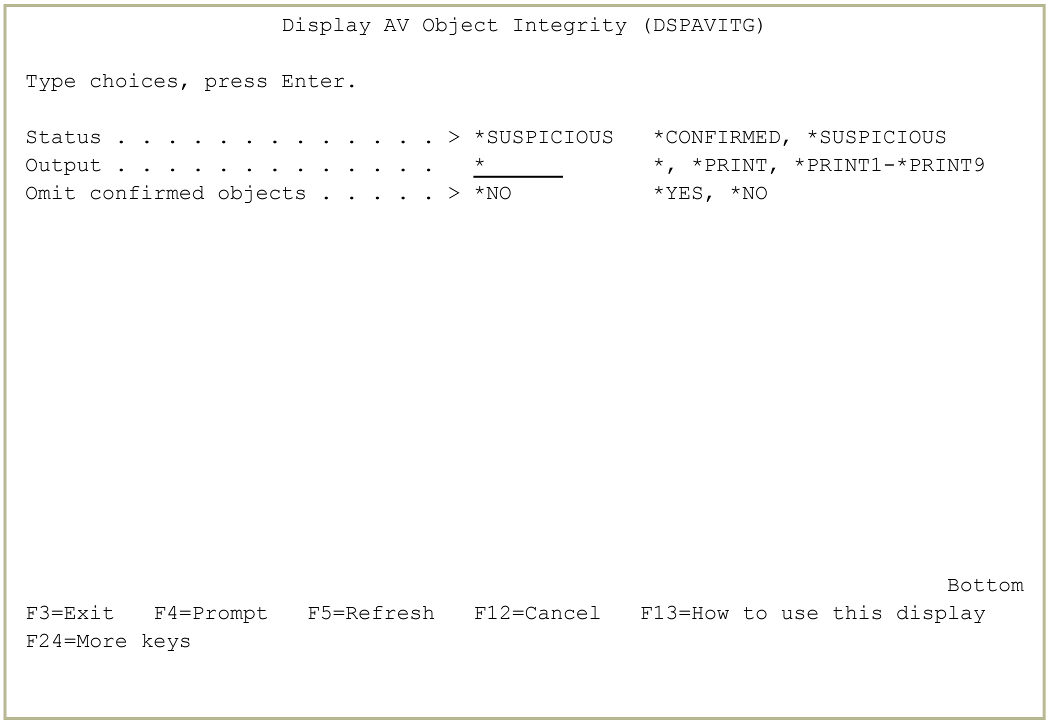
-

Reporting on Suspicious Objects

To **report on all suspicious objects**, select **`41. All Suspicious Objects`** from the **Object Integrity Validation** screen (*STRAV>* **`61`**). The **Display AV Object Integrity (DSPAVITG)** screen appears, with the **`Status`** field set to **`*SUSPICIOUS`** and the **`Omit confirmed objects`** field set to ***NO**.

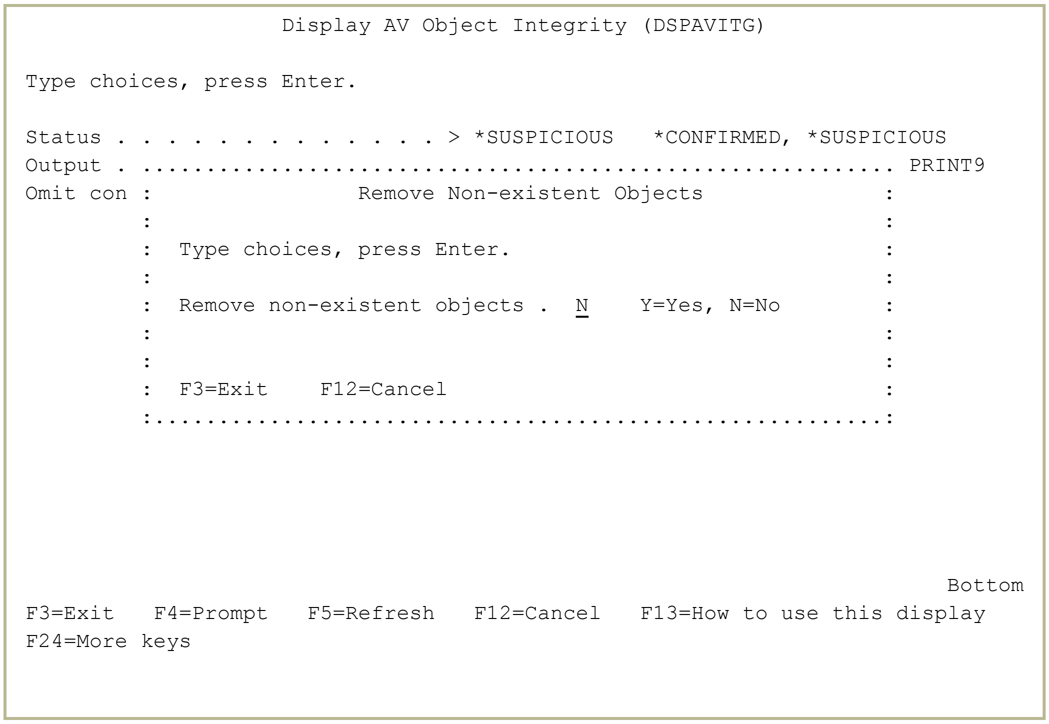
To **report on objects marked as suspicious but not confirmed as inoffensive**, select **`42. Unconfirmed Objects`** from the **Object Integrity Validation** screen (*STRAV>* **`61`**). The **Display AV Object Integrity (DSPAVITG)** screen appears, with the **`Status`** field set to **`*SUSPICIOUS`** and the **`Omit confirmed objects`** field set to ***YES**.

To **report on objects confirmed as inoffensive**, select **`45. All Confirmations`** from the **Object Integrity Validation** screen (*STRAV>* **`61`**). The **Display AV Object Integrity (DSPAVITG)** screen appears, with the **`Status`** field set to **`*CONFIRMED`** and the **`Omit confirmed objects`** omitted.



```
                     Display AV Object Integrity (DSPAVITG)

Type choices, press Enter.

Status . . . . . . . . . . . . . . > *SUSPICIOUS   *CONFIRMED, *SUSPICIOUS
Output . . . . . . . . . . . . . .   *             *, *PRINT, *PRINT1-*PRINT9
Omit confirmed objects . . . . . . > *NO           *YES, *NO

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

Press **Enter**. The **Remove Non-existent Objects** window appears.

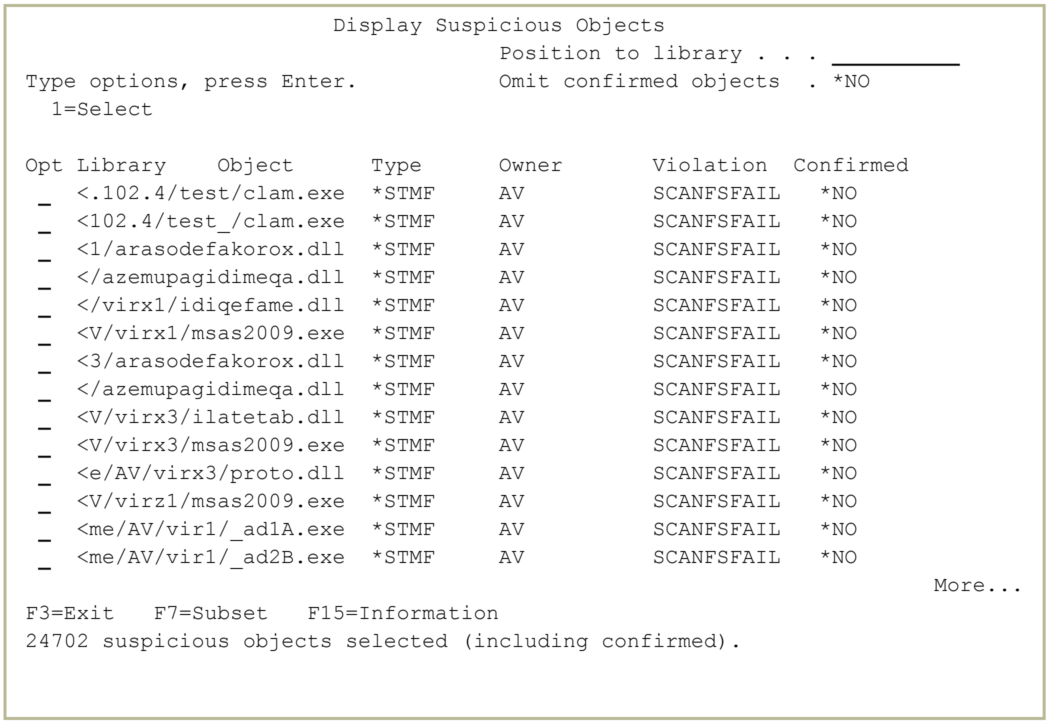


```
                    Display AV Object Integrity (DSPAVITG)

Type choices, press Enter.

Status . . . . . . . . . . . . . > *SUSPICIOUS   *CONFIRMED, *SUSPICIOUS
Output . ........................................................... PRINT9
Omit con :                Remove Non-existent Objects            :
         :                                                       :
         :  Type choices, press Enter.                           :
         :                                                       :
         :  Remove non-existent objects .  N    Y=Yes, N=No       :
         :                                                       :
         :                                                       :
         :  F3=Exit    F12=Cancel                                :
         :.......................................................:






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

To remove listings of objects that no longer exist, press **Y**. Otherwise, press **N**.

For **reports on all suspicious objects or unconfirmed suspicious objects**, the **Display Suspicious Objects** screen appears.

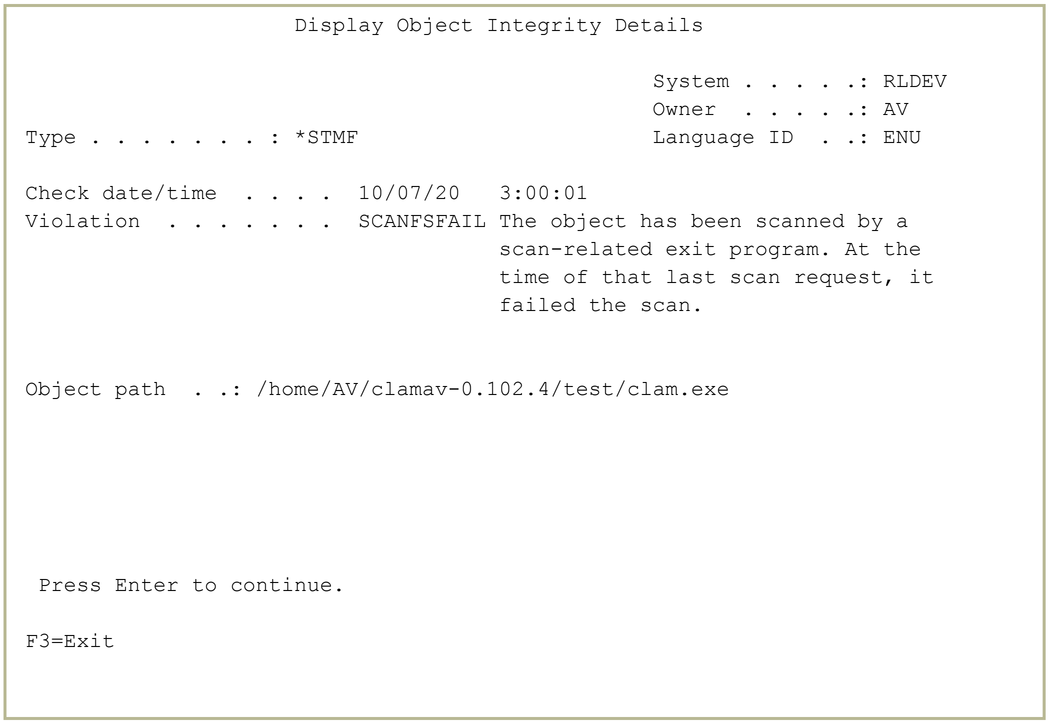
For **reports on confirmed objects**, the **Display Confirmed Violation** screen appears. It is identical to the **Display Suspicious Objects** screen except that the **`Confirmed`** field is not displayed.



```
                        Display Suspicious Objects
                                     Position to library . . . __________
Type options, press Enter.           Omit confirmed objects  . *NO
  1=Select

Opt Library    Object      Type      Owner       Violation  Confirmed
 _  <.102.4/test/clam.exe  *STMF     AV          SCANFSFAIL   *NO
 _  <102.4/test_/clam.exe  *STMF     AV          SCANFSFAIL   *NO
 _  <1/arasodefakorox.dll  *STMF     AV          SCANFSFAIL   *NO
 _  </azemupagidimeqa.dll  *STMF     AV          SCANFSFAIL   *NO
 _  </virx1/idiqefame.dll  *STMF     AV          SCANFSFAIL   *NO
 _  <V/virx1/msas2009.exe  *STMF     AV          SCANFSFAIL   *NO
 _  <3/arasodefakorox.dll  *STMF     AV          SCANFSFAIL   *NO
 _  </azemupagidimeqa.dll  *STMF     AV          SCANFSFAIL   *NO
 _  <V/virx3/ilatetab.dll  *STMF     AV          SCANFSFAIL   *NO
 _  <V/virx3/msas2009.exe  *STMF     AV          SCANFSFAIL   *NO
 _  <e/AV/virx3/proto.dll  *STMF     AV          SCANFSFAIL   *NO
 _  <V/virz1/msas2009.exe  *STMF     AV          SCANFSFAIL   *NO
 _  <me/AV/vir1/_ad1A.exe  *STMF     AV          SCANFSFAIL   *NO
 _  <me/AV/vir1/_ad2B.exe  *STMF     AV          SCANFSFAIL   *NO
                                                                      More...
F3=Exit   F7=Subset   F15=Information
24702 suspicious objects selected (including confirmed).
```

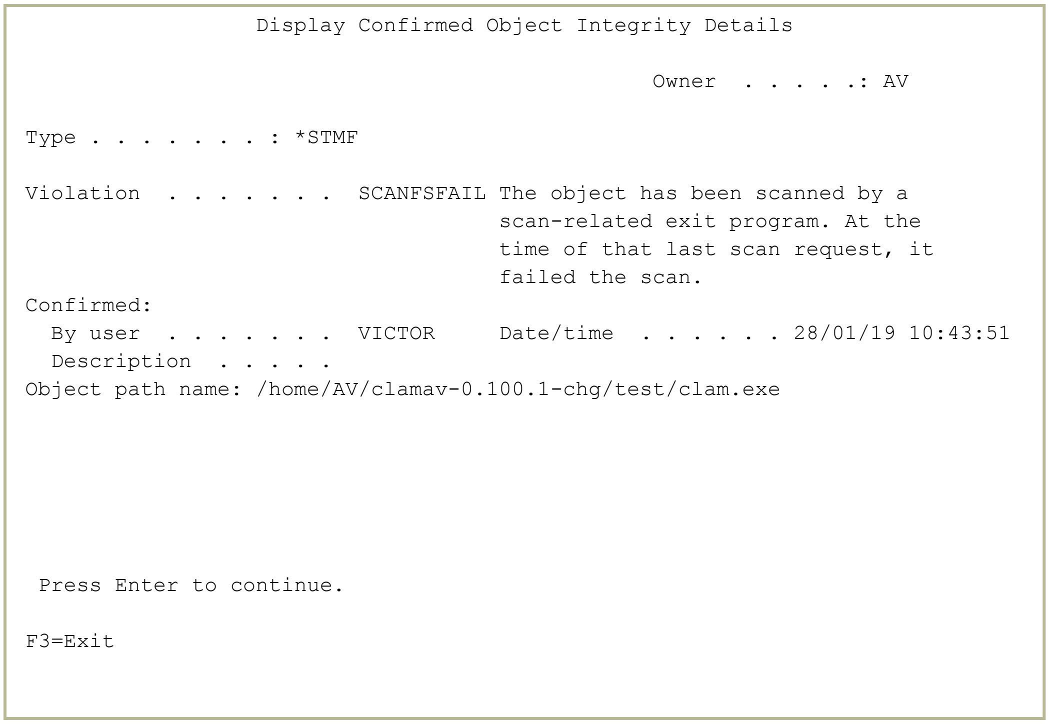
For more information on any of the objects, enter **1** in the **Opt** field for that object.

For **reports on all suspicious objects or unconfirmed suspicious objects**, the **Display Object Integrity Details** screen appears:



```
                     Display Object Integrity Details


                                                 System . . . . .: RLDEV
                                                 Owner  . . . . .: AV
Type . . . . . . . : *STMF                       Language ID  . .: ENU

Check date/time  . . . .  10/07/20   3:00:01
Violation  . . . . . . .  SCANFSFAIL The object has been scanned by a
                                     scan-related exit program. At the
                                     time of that last scan request, it
                                     failed the scan.


Object path  . .: /home/AV/clamav-0.102.4/test/clam.exe






 Press Enter to continue.

F3=Exit
```

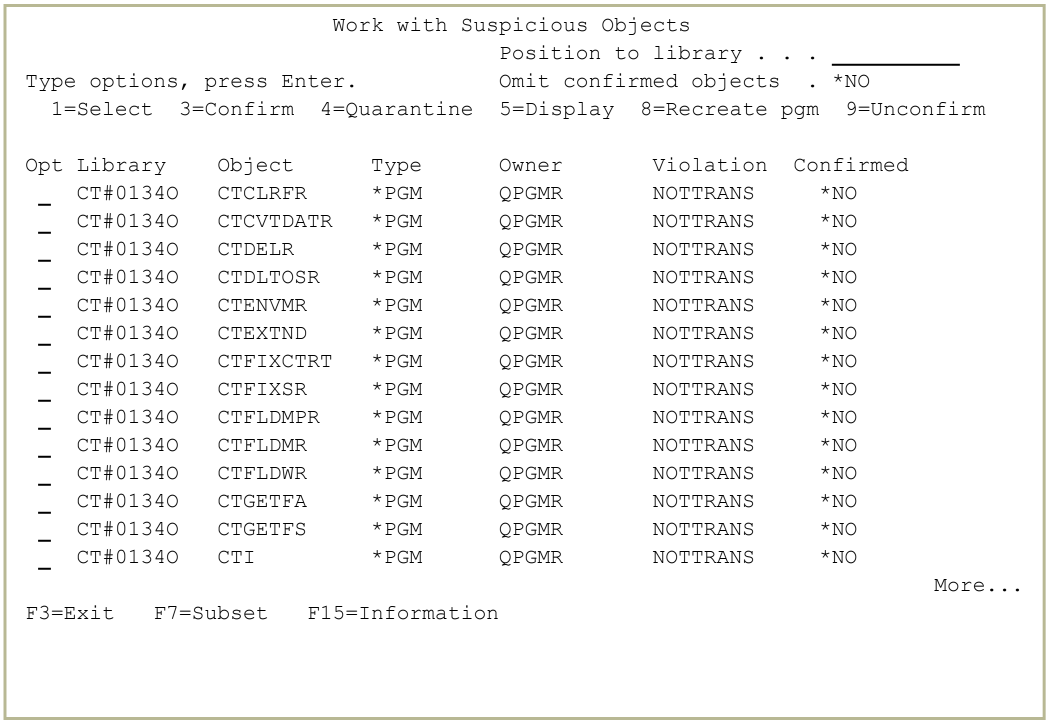
For **reports on confirmed objects**, the **Display Confirmed Object Integrity Details** screen appears:



```
                  Display Confirmed Object Integrity Details

                                                 Owner  . . . . .: AV

Type . . . . . . . . : *STMF

Violation  . . . . . . .  SCANFSFAIL The object has been scanned by a
                                     scan-related exit program. At the
                                     time of that last scan request, it
                                     failed the scan.
Confirmed:
  By user  . . . . . . .  VICTOR     Date/time  . . . . . . 28/01/19 10:43:51
  Description  . . . . .
Object path name: /home/AV/clamav-0.100.1-chg/test/clam.exe






 Press Enter to continue.

F3=Exit
```

Managing Suspicious Objects

To **manage suspicious objects**, select **`21. Work with Suspicious Objects`** from the **Object Integrity Validation** screen (*STRAV>* **`62`**). The **Remove Non-existent Objects** window appears. Enter **`Y`** to remove information on objects that no longer exist, or **N** to retain the information, then press **Enter**. The **Work with Suspicious Objects** screen appears:



```
                        Work with Suspicious Objects
                                     Position to library . . . __________
Type options, press Enter.           Omit confirmed objects  . *NO
  1=Select  3=Confirm  4=Quarantine  5=Display  8=Recreate pgm  9=Unconfirm

Opt Library    Object      Type      Owner       Violation  Confirmed
 _  CT#01340   CTCLRFR     *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTCVTDATR   *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTDELR      *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTDLTOSR    *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTENVMR     *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTEXTND     *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTFIXCTRT   *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTFIXSR     *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTFLDMPR    *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTFLDMR     *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTFLDWR     *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTGETFA     *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTGETFS     *PGM      QPGMR       NOTTRANS     *NO
 _  CT#01340   CTI         *PGM      QPGMR       NOTTRANS     *NO
                                                                        More...
F3=Exit   F7=Subset   F15=Information
```

For each object, the screen shows the **`Library`** containing the object and the **`Object`** name (or, for objects in IFS, the pathname), the **`Type`** of object, its **`Owner`**, the **`Violation`** that caused it to be marked as suspicious, and whether it has been **`Confirmed`** as inoffensive.

Possible values for **`Violation`** include:

ALTERED

The object has been tampered with.

BADLIBUPDA

The library protection attribute is set incorrectly.

BADSIG

The object has a digital signature that is not valid.

DMN

The domain is not correct for the object type.

NOTCHECKED

The object could not be checked. At the time of the scan the debug mode was on, or the object was saved with its storage freed or was compressed.

NOTTRANS

The object has not been converted to RISC format.

OSIG

The object can be signed but does not have a digital signature.

PGMMOD

The runnable object has been tampered with.

SCANFSFAIL

The object has been scanned by a scan-related exit program. At the time of that last scan request, it failed the scan.

To **see more information** about the violation, enter **1** in the **Opt** field for the object. The **Display Object Integrity Details** screen appears, showing the date and time of the check that spotted the violation and a description of the violation type.

To **see detailed information about the object**, enter **5** in the **Opt** field for the object. The standard **Display Program Information** screen appears, containing several pages of information about the object.

To **confirm that the object is inoffensive**, enter **2** in the **Opt** field for the object. The **Confirm Object as Inoffensive** window appears. Enter information about the confirmation in the **Description** field in the window. The **Confirmed** field changes from ***NO** to ***YES**.

To **remove the confirmation for an object**, enter **9** in the **Opt** field for the object. The **Confirmed** field changes from ***YES** to ***NO**.

To **quarantine an object**, enter **4** in the **Opt** field for the object. The **Quarantine Object** window appears. Press **Enter** to confirm that you want to quarantine the object or the **F12** key to cancel.

> NOTE: To remove an object from quarantine, select **29. Work with Quarantined Objects** from the **Object Integrity Validation** screen (*STRAV>* **61**). The standard **Work with Objects Using PDM** screen appears, showing the objects in the **SMZVQRN** quarantine library.

To **recreate a program** of the **Type *PGM** that has a Violation of **ALTERED**, enter **8** into the **Opt** field for the object. The program is recompiled. The new version replaces the suspicious object.

Message Codes for Anti-Virus

Message ID: Message Description
AVE0108: Threat %s found in file: %s. Job details
AVE1302: !! Antivirus detected virus &1
AVE0107: AV: No Authorization code. Exiting RT Detection.
AVE0109: Virus scan &1
AVE1234: No Virus Definitions found. Use…
AVE0110: Virus scan, Job: &1'
AVE1231: !! Antivirus configuration is not set
AVE1234: No Virus Definitions found. Use…
AVE0111: Scanav found infected files. Details in
AVE0112: Refresh Fail. Details in /SMZVDTA/log/av.log

Installing the iSecurity ICAP Server on a PC

While the iSecurity ICAP Client can communicate with any supported ICAP server, you can install the iSecurity ICAP server on a Windows PC within your organization's network. To download the daily virus definitions update, the PC must be able to check clamav.net on port 80.

1. Download the file **RazleeICAP.ova** to the PC from **http://as400.razlee.com/products/security/anti%20virus/rand_ksymcckz/RazleeICAP.ova**
2. On the PC and its firewall, open ports 1344 and 1345 that are used for ICAP.
3. Install the **Oracle Virtual machine** from **https://www.virtualbox.org/wiki/Downloads**
4. Within the virtual machine, select **File > Import appliance** and choose the **RazleeICAP.ova** file.
5. Start the installed appliance.
6. NOTE: If a message appears about USB 2.0, disable USB within the virtual machine settings, then restart the appliance.
7. In the virtual machine, which runs a form of Linux, log in with the username **smz** and the password **razlee**.
8. Change to the root user by entering the command ***su*** and the password **razlee**.
9. Enter the command ***cp /etc/network/interfaces /home/interfaces-bck***

10. Edit the **/etc/network/interfaces** file with the command ***vi /etc/network/interfaces*** or your favorite Linux text editor.
11. Edit the following lines to change them to the appropriate IP address, network mask, and gateway, respectively:
    - **address 1.1.1.122**
    - **netmask 255.255.255.0**
    - **gateway 1.1.1.254**
12. Save the file and exit the editor.
13. Restart Linux by entering the command ***reboot***.
14. Check the IP address of the ICAP server by entering the command ***ip a | grep global*** The IP address following the string **inet** in the response should match the value that you entered in the **address** line in the interfaces file.
15. Connect to the server from the Widows PC with the command
    ssh -o UserKnownHostsField=no smz@ADDRESS
    where ADDRESS is the value that you had entered in the **address** line of the interfaces file.
16. Enter the password **razlee**
17. Enter the command ***menu***
18. Wait for four or five minutes for the definitions to update.
19. Select option 1) ICAP State. The output should resemble these lines:

    ```
    root 459 1 17 10:23 ? 00:00:49
    /usr/local/sbin/clamd
    root 493 1 22 10:24 ? 00:00:47 /usr/local/c-
    icap/bin/c-icap -N -D -d 2
    root 503 493 0 10:25 ? 00:00:00 /usr/local/c-
    icap/bin/c-icap -N -D -d 2
    root 515 493 0 10:25 ? 00:00:00 /usr/local/c-
    icap/bin/c-icap -N -D -d 2
    root 527 493 0 10:25 ? 00:00:00 /usr/local/c-
    icap/bin/c-icap -N -D -d 2
    ```
20. Test whether ClamAV is running, passing it the name of a file to check. For example, to check the file /tmp/fn, run the command
    c-icap-client -i debian -s srv_clamav -f /tmp/fn
    The result should resemble:

    ```
    ICAP server:debian, ip:127.0.0.1, port:1344
    No modification needed (Allow 204 response)
    ```

21. On the IBM i, run these commands, replacing "1.1.1.122" in the last command with the IP address of the ICAP server:
    CALL QP2TERM
    export LIBPATH=/SMZVDTA/lib/ppc64:/SMZVDTA/lib
    /SMZVDTA/bin/c-icap-client -i 1.1.1.122 -s srv_clamav
22. The output contains sections on **`OPTIONS`** and **`ICAP HEADERS`**.
    NOTE: It should not end with the string "**`Connection: close`**".