SAV Dynamic Interface
SAVDI ICAP test guide

Product version: 2.0
Document date: March 2011
## Contents

1. Introduction ......................................................................................................................... 3
2. Pre-requisites .......................................................................................................................... 3
3. Installation ............................................................................................................................... 4
   3.1 Upgrading ............................................................................................................................. 4
       3.1.1 Non-Windows .................................................................................................................. 4
       3.1.2 Windows .......................................................................................................................... 4
   3.2 Clean Install ......................................................................................................................... 5
       3.2.1 Non-Windows .................................................................................................................. 5
       3.2.2 Windows ......................................................................................................................... 5
4. Functional Tests ...................................................................................................................... 5
   4.1 Starting SAVDI to log to the screen ..................................................................................... 5
   4.2 Sun Vscan Users ................................................................................................................... 6
   4.3 Basic ICAP test ..................................................................................................................... 6
   4.4 Changing the Port to scan on ............................................................................................... 6
   4.5 Turn on 204 Responses ....................................................................................................... 7
   4.6 Adding a Service to a Channel ............................................................................................. 7
   4.7 Adding a new ICAP Channel ................................................................................................. 7
   4.8 Changing the Thread Count and Queue ............................................................................... 8
5. Appendices .............................................................................................................................. 9
   5.1 Appendix A ........................................................................................................................... 9
   5.2 Appendix B ........................................................................................................................... 9
   5.3 Appendix C .......................................................................................................................... 11
6. Legal notices ........................................................................................................................... 14
1 Introduction

This guide will define test cases to validate correct usage of the ICAP functionality of SAVDI.

We recommend that these tests are carried out by anyone who wants to ensure a particular client correctly adheres to the ICAP standard and is thereby compatible with Sophos.

Note for 3rd parties seeking Sophos Compatibility Certification: one element of achieving this is that these tests need to be carried out and the results provided for review by Sophos.

SAVDI is available for Windows, Linux and some UNIX platforms. ICAP Testing has been carried out on the following platforms by Sophos, using an in-house ICAP client, Squid (http://www.squid-cache.org/) and C-ICAP (http://c-icap.sourceforge.net/)

Win 2003 32 bit – SP2
Win 2008 64 bit – SP2
Win 2008 (32 bit) – SP2
RHEL5 64 bit – 5.5
SUSE 11 (64 bit) – OpenSUSE 11.3
SLES 11 (64 bit) – Suse Linux Enterprise Server 11 SP1
SUSE 10 (32 bit) – OpenSUSE 10.2
TurboLinux 10 (32 bit) – 10.0
RHEL 6 (64 bit) – 6.0
RHEL 4 (32 bit) – 4.1.18
Solaris 10 on SPARC
FreeBSD 7 (32 bit) – 7.0
FreeBSD 7 (64 bit) – 7.0
FreeBSD 8 (32 bit) – 8.1
FreeBSD 8 (64 bit) – 8.1

2 Pre-requisites

Please read the SAVDI user guide before installing.

In order to install SAVDI you must first have a compatible version of Sophos Anti-Virus or SAVI installed on your machine. You must also have the correct version of the SAVDI installer for your platform.
SAVDI 2.0 ICAP test guide

If you have a firewall installed you may need to open up the port you wish to send ICAP requests to/from. The default is port 1344.

If you are using Squid, then you will need to build it with --enable-icap-client and then add the following lines to your squid.conf:

```
icap_enable on
adaptation_access sophosicap allow all
icap_service sophosicap respmod_preactice icap://<ICAP server IP>/<ICAP Service Name>
```

The squid service will need restarting after changes.

3 Installation

3.1 Upgrading

3.1.1 Non-Windows

1. Check that SAVDI isn’t running as a daemon using the command `ps -A | grep 'savdi'`
2. If it is, kill it using `kill <PID>`. Run the first command again to check that it is no longer running.
3. Change the directory to your SAVDI install location (`/usr/local/savdi` by default).
4. Make a backup copy of your savdid.conf configuration file to a safe location.
5. Copy the new installer to the `/tmp` directory and unpack it. `tar -xvf <package name>`
6. Change the directory to the `savdi` dir created by the unpacking SAVDI.
7. Run the installer script `/savdi_install.sh`
8. This will overwrite the previous install of SAVDI v1.0.
9. If required copy your backed up configuration file back to `/usr/local/savdi` and add any ICAP related configuration required to it (see SAVDI manual for this).
10. There is also an ICAP enabled configuration file (also called `savdid.conf`) created by the new install if you would prefer to use this.

3.1.2 Windows

1. Check if SAVDI is running on the command line. If it is then stop it.
2. Check if SAVDI is currently running as a process by opening up services.msc and seeing if the SAV Dynamic Interface is running. If it is then stop it.
3. Make a backup copy of your savdid.conf configuration file to a safe location.
4. Run the installer for the new SAVDI and follow the steps through to its completion.
5. If you chose to install to the default location then your previous SAVDI files (except the savdid.conf) will be overwritten.
6. If you chose a new install DIR then the previous DIR will be deleted and the new one created. The previous savdid.conf will be copied to the new DIR.

7. When the install has completed check through the savdid.conf and ensure that it hasn’t changed, if it has then restore from your backup.

8. Please note that when you install SAVDI V2.0 it will install itself as a service which will automatically start. This can be removed by running savdid.exe –uninstall

3.2 Clean Install

3.2.1 Non-Windows

1. Copy the new installer to the /tmp directory and unpack it. tar –xvf <package name>
2. Change the directory to the savdi dir created by the unpacking SAVDI.
3. Run the installer script /savdi_install.sh
4. This will install SAVDI to /usr/local/savdi and the executable to /usr/local/bin/
5. If required edit the savdid.conf file in /usr/local/savdi and add any extra configuration required to it (see SAVDI manual for this).

3.2.2 Windows

1. Double click the MSI to start the installer.
2. Click Next on the Welcome screen.
3. Read and accept the EULA.
4. Choose the install DIR for SAVDI. The default will add it to the same area as your other Sophos products
5. Click install and SAVDI will get installed to the directory specified.
6. A service called SAV Dynamic Interface will be installed and started using the default configuration file savdid.conf
7. If you wish to view the documentation leave the checkbox ticked and when you finish the installer the directory containing the documentation will be opened.

4 Functional Tests

4.1 Starting SAVDI to log to the screen

1. Open the savdid.conf in a text editor and search for loglevel. Set it to level 2.
2. Open a shell/CMD prompt to the savdid executable DIR.
SAVDI 2.0 ICAP test guide

3. Windows type savdid.exe –l or non-Windows type ./savdid –l
4. Provided that the configuration file is correct SAVDI should start by printing the version information and then a PID for SAVDI (PID may take a few seconds to appear).

4.2 Sun Vscan Users

There is a configuration file created on install that can be used by Sun Vscan users. This can be used either on the command line or when running SAVDI as a service.

1. In a command prompt change to the install directory.
2. If you have SAVDI running as a service (it will do it automatically on install) run savdid.exe – uninstall to remove the service.
3. To run using the Vscan config file on the command line type savdid.exe –c icap-sun-w32.conf
4. If you want to run as a service you will need to rename icap-sun-w32.conf to savdid.conf (will need to rename the original savdid.conf first). You can then reinstall the service using the command savdid.exe – install and then net start savdid

4.3 Basic ICAP test

1. Open your savdid.conf, and check that there is an ICAP channel.
2. Note the port number and the name of the service in the ICAP channel.
3. Save and close the savdid.conf and start SAVDI to log to the screen.
4. Using your ICAP client scan an Eicar AV test file (available from http://eicar.org)
5. Your client should report that a threat was found and not return the file.
6. On the SAVDI console it should report, Threat Found, <Name of Virus>, and Virus Found in Virus Scan (See Appendix A).

4.4 Changing the Port to scan on

1. Stop SAVDI from running.
2. Open your savdid.conf, and look for where your ICAP channel has been defined.
3. Change the port number (default of 1344) to the port you would like to use.
4. Ensure that the port has been opened on any firewalls.
5. Save and close the savdid.conf and start SAVDI to log to the screen.
6. Using you ICAP client scan an Eicar AV test file on the old port 1344.
7. You should get some sort of communications failure (client dependant).
8. Change the ICAP client to scan on the new port and re-scan Eicar.
9. Your client should report that a threat was found and not return the file.
10. On the SAVDI console it should report, *Threat Found, <Name of Virus>, and Virus Found in Virus Scan* (see image for basic ICAP test).

### 4.5 Turn on 204 Responses

1. Stop SAVDI from running.
2. Open your savdid.conf, and look for where your ICAP channel has been defined.
3. Search for the line `allow204:` and change the value to YES. Ensure there isn’t a # at the start of the line.
4. Save and close the savdid.conf and start SAVDI to log to the screen.
5. Using your ICAP client (that can accept a 204 response) scan a clean file and check that you get a 204 response header and that the file is not sent back to your client.

### 4.6 Adding a Service to a Channel

You may want to add another service to your ICAP channel if you need require different options to be used for different machines e.g. you may want some file types blocked for certain machines but not others. Or allow some machines to receive a 204 header rather than the file. See Appendix B for an example of an ICAP channel with two services

1. Stop SAVDI from running.
2. Open your savdid.conf, and look for where your ICAP channel has been defined.
3. Copy the service section from the ICAP channel down to the close bracket.
4. Paste the text under the current service close bracket, but inside the close channel bracket.
5. Change the name of the service (make sure that type stays as avscan).
6. Change another options for the service.
7. Save and close the savdid.conf and start SAVDI to log to the screen.
8. Use your ICAP client and relevant test files to check that the option you chose are working correctly.

### 4.7 Adding a new ICAP Channel

You may want to add another ICAP channel if you want different configurations to be given different port numbers. The different channels can have the same service name if they have different port numbers. You can also have multiple services within each channel.

See Appendix C for an example two ICAP channel config.

1. Stop SAVDI from running.
2. Open your savdid.conf, and look for where you ICAP channel has been defined.
3. Copy the entire channel down to its close bracket.
4. Paste the text under the current close channel bracket.
5. Change the port number and/or the name of the service (make sure that type stays as avscan).
6. Change another options for the channel.
7. Save and close the savdid.conf and start SAVDI to log to the screen.
8. Use your ICAP client and relevant test files to check that the option you chose are working correctly.

4.8 Changing the Thread Count and Queue

Changing the number of threads and queue will change the number of concurrent connections that can be made to SAVDI. The thread count is the number of connections that can be processed at the same time, and the queue is how many connections can be held waiting for processing before connections are refused.

1. Stop SAVDI from running.
2. Open your savdid.conf, and look for `threadcount:` change this to the number of threads you would like to spawn at startup.
3. Look for `maxqueuedsessions:` (or add if it doesn’t exist) and put the number of connections to queue.
4. Save and close the savdid.conf and start SAVDI to log to the screen.
5. Using multiple ICAP clients, either scanning single large files for groups of smaller files, send enough requests to exceed the thread count and ensure the requests get queued rather than rejected.
5 Appendices

5.1 Appendix A

```sh
C:\Program Files\Sophos\SAV Dynamic Interface>savdid.exe -l
11:02:00:22812 [4d429a33] 0003e403 New connection
To: 0.0.0.0:1344 From 127.0.0.1:1344
11:02:00:22812 [4d429a33] 0003e402 New session
11:02:00:22812 [4d429a33] 0003e403 Session ended
11:02:00:22812 [4d429a34] 0003e400 New connection
To: 0.0.0.0:1344 From 127.0.0.1:1344
11:02:00:22812 [4d429a33] 0003e401 Connection ended
To: 0.0.0.0:1344 From 127.0.0.1:1344
11:02:00:22812 [4d429a34] 0003e402 New session
11:02:00:22812 [4d429a34] 0003e405 Threat found
Identity: "ICAP-AU-Test" ""
11:02:00:22812 [4d429a34] 0003e403 Virus found during virus scan
11:02:00:22812 [4d429a34] 0003e403 Session ended
11:02:00:22812 [4d429a34] 0003e401 Connection ended
To: 0.0.0.0:1344 From 127.0.0.1:1344
```

5.2 Appendix B

A basic ICAP Channel with two services. One allowing 204 responses, and one not.

```plaintext
channel {
    commprotocol {
        type: IP
        port: 1344
        requesttimeout: 120
        sendtimeout: 2
        recvtimeout: 10
    }
    service {
        # uses the same name.
        name: sophosav
        # The type of service, for now can only be avscan
```
type: avscan
scanprotocol {
    # The type of protocol in use. Can only be ICAP.
    type: ICAP
    # Version of the configuration for this service.
    version: 1.01
    # 204 is the ICAP code indicating that the object
    # sent for processing is unmodified and OK and will
    # not be returned to the client. Default: NO

    # allow204: NO
    tmpfilestub: c:savdi\temp\icap_
}
scanner {
    type: SAVI
    inprocess: YES
    savists: enableautostop 1
    savigrp: grpsuper 1
}
}
service {
    # uses the same name.
    name: sophosallow

    # The type of service, for now can only be avscan
    type: avscan

    scanprotocol {
        # The type of protocol in use. Can only be ICAP.
        type: ICAP
        # Version of the configuration for this service.
        version: 1.01

        # 204 is the ICAP code indicating that the object
        # sent for processing is unmodified and OK and will
        # not be returned to the client. Default: NO
5.3 Appendix C

An example config section containing two ICAP channels on different ports but with the same service name. One channel allow 204 responses, logs requests and has a couple more scanning options than the other.

channel {
  commprotocol {
    type: IP
    port: 1344
    requesttimeout: 120
    sendtimeout: 2
    recvtimeout: 10
  }
  service {
    name: sophosav
    type: avscan
    scanprotocol {
      type: ICAP
      # Version of the configuration for this service.
      version: 1.01
      # allow204: NO
      tmpfilestub: c:\savdi\temp\icap_
    }
  }
}
SAVDI 2.0 ICAP test guide

```
scanner {
    type: SAVI
    inprocess: YES
    savists: enableautostop 1
    savigrp: grpsuper 1
    }
    }
}
channel {
    logrequests: YES
    }

commprotocol {
    type: IP
    port: 1346
    requesttimeout: 120
    sendtimeout: 2
    recvtimeout: 10
    }

service {
    name: sophosav
    type: avscan
    scanprotocol {
        type: ICAP
        # Version of the configuration for this service.
        version: 1.01
        allow204: YES
        tmpfilestub: c:\savdi\temp\icap_
        }
    }

scanner {
    type: SAVI
    inprocess: YES
    savists: enableautostop 1
    savigrp: grpsuper 1
```
savigrp: GrpArchiveUnpack 0
savigrp: GrpInternet 1
}
}
}
6 Legal notices

Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.