

INTEGRATING DOMINO WITH AN ICAP SERVER

Marianna Tomasatti - marianna.tomasatti@gttech.it

Roberto Boccadoro - roberto.boccadoro@eldeng.it



WELCOME TO THE YELLOW RESTAURANT!



THE SPECIAL OF TODAY IS....

Scan Config on domino

Open MailScan Log Edit Server New Server Enable Server Disable Server Delete Server

Server Name	Configuration	Health Errors/Warnings
domino/GTlab	mock server	

Servers Configurations

Roberto Boccadoro - Mail

New Reply Reply to All Forward More

Who	Subject	Date	Size
Today (total: 8)			
Marianna Tomasatti	icap test	15:11	2K
Roberto Boccadoro	Message blocketest	16:18	2K
Marianna Tomasatti	Message blockdtest D	16:21	2K
Marianna Tomasatti	Virus foundFw: test D —Forwarded by Marianna	16:28	3K
Marianna Tomasatti	Virus found: test virus 2	16:29	2K
Marianna Tomasatti	Message blocked: test 3	16:30	2K
Marianna Tomasatti	[Virus found]: test 17	16:55	2K
Marianna Tomasatti	[Message blocked]: new test some text	16:57	2K

[Virus found]: test 17
Marianna Tomasatti to Roberto Boccadoro 26/01/2024 16:55 [Show Details](#)

1 attachment

eicar.com



THE CHEFS

Roberto Boccadoro
Former Lotus / IBMer
Working with
Lotus/IBM/HCL
Collaboration since
1994
Many years of
experience with
Domino, Sametime,
Connections, Docs and
other HCL products
HCL Ambassador 
OpenNTF Director 



Marianna Tomasatti
Working with Domino
since 1997
Lots of experience as
System and Domino
Administrator



THE MASTER CHEF WHO HELPED US



Daniel Nashed

If you know him, you don't need his bio 😊
If you don't know him, too bad, we will need too many slides to tell you what he does



THE INGREDIENTS

1)



HCL Domino

Minimum version 12.0.2

2) **An ICAP server**



THE RECIPE

- Run mailscan for the first time to create cscancfg.nsf
- Create a configuration document in cscancfg.nsf
- Create a server document in cscancfg.nsf
- Run mailscan again

Official documentation

https://help.hcltechsw.com/domino/14.0.0/admin/conf_scanningattachments_forviruses.html?



RIN MAILSCAN THE FIRST TIME

- load mailscan.
- The mailscan task starts up, creates cscancfg.nsf on the administration server, creates a replica on the current server, and shuts down.



CSCANCFG.NSF

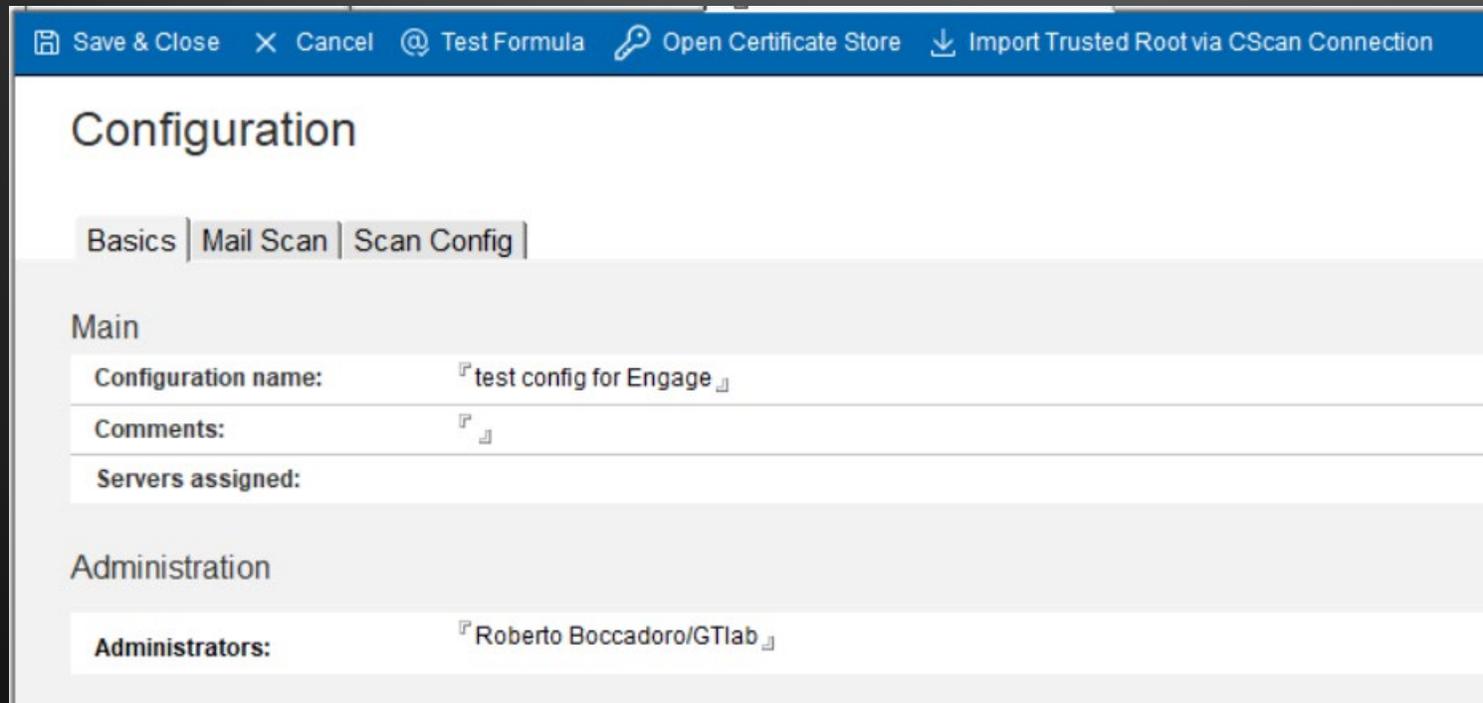
- Open it and create a configuration

The screenshot displays the 'Scan Config' interface within a Domino environment. The interface is titled 'Scan Config on domino' and features a sidebar with 'Servers' and 'Configurations' options. The main area shows a table with the following data:

Name	Type	Scan Server	Port	Service
ICAP-ClamAV	ICAP	dominolab.gttech.it	1344	clamav

CONFIGURATION

- In the basic tab type a name for the configuration.



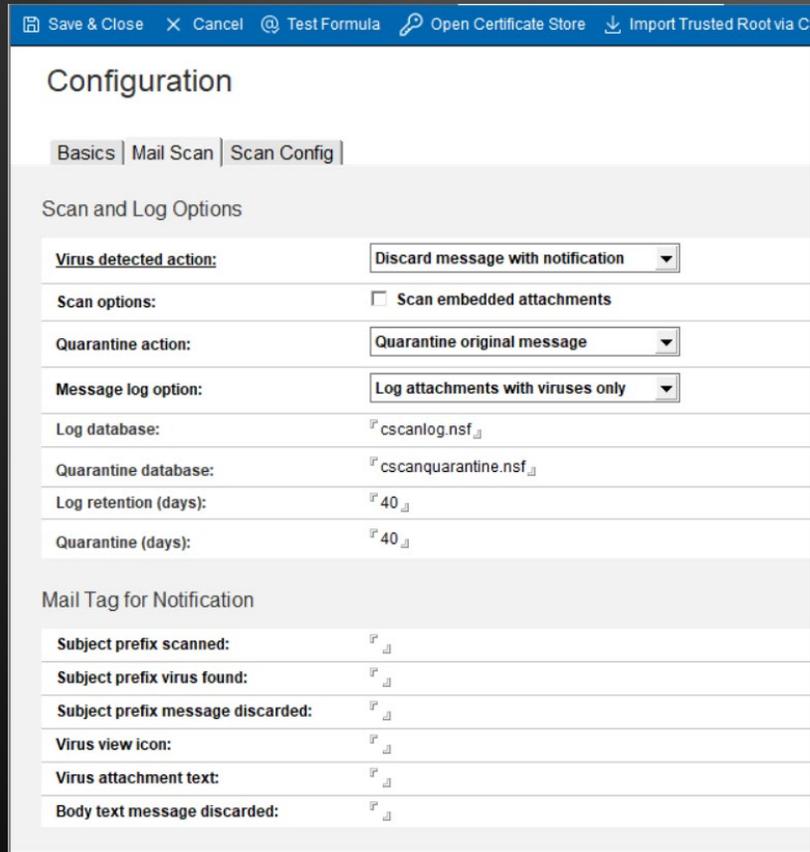
The screenshot shows a software application window titled "Configuration". The window has a blue header bar with menu items: "Save & Close", "Cancel", "Test Formula", "Open Certificate Store", and "Import Trusted Root via CScan Connection". Below the header, there are three tabs: "Basics", "Mail Scan", and "Scan Config". The "Basics" tab is selected. Under the "Main" section, there are three fields: "Configuration name:" with the value "test config for Engage", "Comments:" with an empty field, and "Servers assigned:" which is currently empty. Under the "Administration" section, there is one field: "Administrators:" with the value "Roberto Boccadoro/GTlab".

You can't assign it to any server yet, because you have not created one. It will be done in the next steps



CONFIGURATION

- In the mail scan tab you define the options



The screenshot shows a software configuration window titled "Configuration" with a blue header bar containing menu items: "Save & Close", "Cancel", "Test Formula", "Open Certificate Store", and "Import Trusted Root via C". Below the header, there are three tabs: "Basics", "Mail Scan", and "Scan Config". The "Mail Scan" tab is selected. The main area is divided into two sections: "Scan and Log Options" and "Mail Tag for Notification".

Scan and Log Options

Virus detected action:	Discard message with notification
Scan options:	<input type="checkbox"/> Scan embedded attachments
Quarantine action:	Quarantine original message
Message log option:	Log attachments with viruses only
Log database:	cscanlog.nsf
Quarantine database:	cscanquarantine.nsf
Log retention (days):	40
Quarantine (days):	40

Mail Tag for Notification

Subject prefix scanned:	
Subject prefix virus found:	
Subject prefix message discarded:	
Virus view icon:	
Virus attachment text:	
Body text message discarded:	



VIRUS DETECTED ACTION

Virus detected action:	Discard message with notification ▼
Scan options:	Discard message with notification Clean message and deliver Silently discard message

- Choose from the following options to specify what happens to a message when a virus is detected:
- Discard message with notification** - This option deletes the original message content. The message is sent with a Subject prefix that contains the text configured in the Subject prefix message discarded field and body text configured in the Body text message discarded field.
- Clean message and deliver** - This option deletes viruses from infected attachments. The message is sent with a Subject prefix that contains the text configured in the Subject prefix virus found field and the contents of any infected attachments are replaced with the text configured in the Virus attachment text field.
- Silently discard the message** - With this option, the recipient does not receive the message or any notification about a virus.



SCAN OPTIONS

Scan options:

Scan embedded attachments

Domino mail servers might rarely process a MIME message that contains unencoded content. Although such content is not technically an attachment, when the document is opened in Notes it is manifested as an attachment. We refer to such data as an embedded attachment. Starting in Domino 14.0 you can configure virus scanning to scan such attachments by checking Scan embedded attachments.



QUARANTINE ACTION

Quarantine action:	Quarantine original message
Message log option:	Quarantine original message Do not quarantine

- Quarantine original message Original messages with viruses are saved in Domino Content Scan Quarantine (cscanquarantine.nsf).
- Do not quarantine



MESSAGE LOG OPTION

Message log option:	Log attachments with viruses only ▼
Log database:	Log attachments with viruses only Log all attachments

Specify with attachments should be logged



LOG AND QUARANTINE OPTIONS

Log database:	『 cscanlog.nsf 』
Quarantine database:	『 cscanquarantine.nsf 』
Log retention (days):	『 40 』
Quarantine (days):	『 40 』



MAIL TAG FOR NOTIFICATIONS

Mail Tag for Notification	
Subject prefix scanned:	📧
Subject prefix virus found:	📧
Subject prefix message discarded:	📧
Virus view icon:	📧
Virus attachment text:	📧
Body text message discarded:	📧

The text to display before the subject in a sent message indicating that the message was scanned for viruses and none were found. For example, "Virus scanned."

The text to display before the subject in a sent message indicating that a virus was found. For example, "Virus found."

Applies when the virus detected action is "Clean message and deliver."

The text to display before the subject in a sent message indicating that the message was discarded because it contained a virus. For example, "Message blocked due to virus." Applies when the virus detected action is "Discard message with notification."

A number representing the icon to use in a mail view to indicate a message had a virus. (Hint, red envelope is 131)

The text to display inside an attachment that has been cleaned due to a virus. For example, "Virus found! Attachment text replaced." Applies when the virus detected action is "Clean message and deliver." If unable to double-click the attachment to open it, open it from a text editor to read the message.

The text to display in the body of sent message indicating that the message was discarded because it contained a virus. For example, "Virus found! Message discarded." Applies when the virus detected action is "Discard message with notification."

SCAN CONFIG

Basics | Mail Scan | Scan Config

Scan Configuration

Scan protocol:	ICAP
Maximum scan size (MB):	100.0
ICAP server name (DNS):	
ICAP TLS server port: (All connections require TLS)	1344
ICAP service name:	
ICAP preview:	<input type="checkbox"/> Enable ICAP Preview
Virus name formula:	

TLS Connection Security

Trusted roots:	
TLS options:	<input type="checkbox"/> Accept expired TLS certificates <input type="checkbox"/> Allow partial certificate chains
Certificate subject:	
Certificate expiration warning period:	21

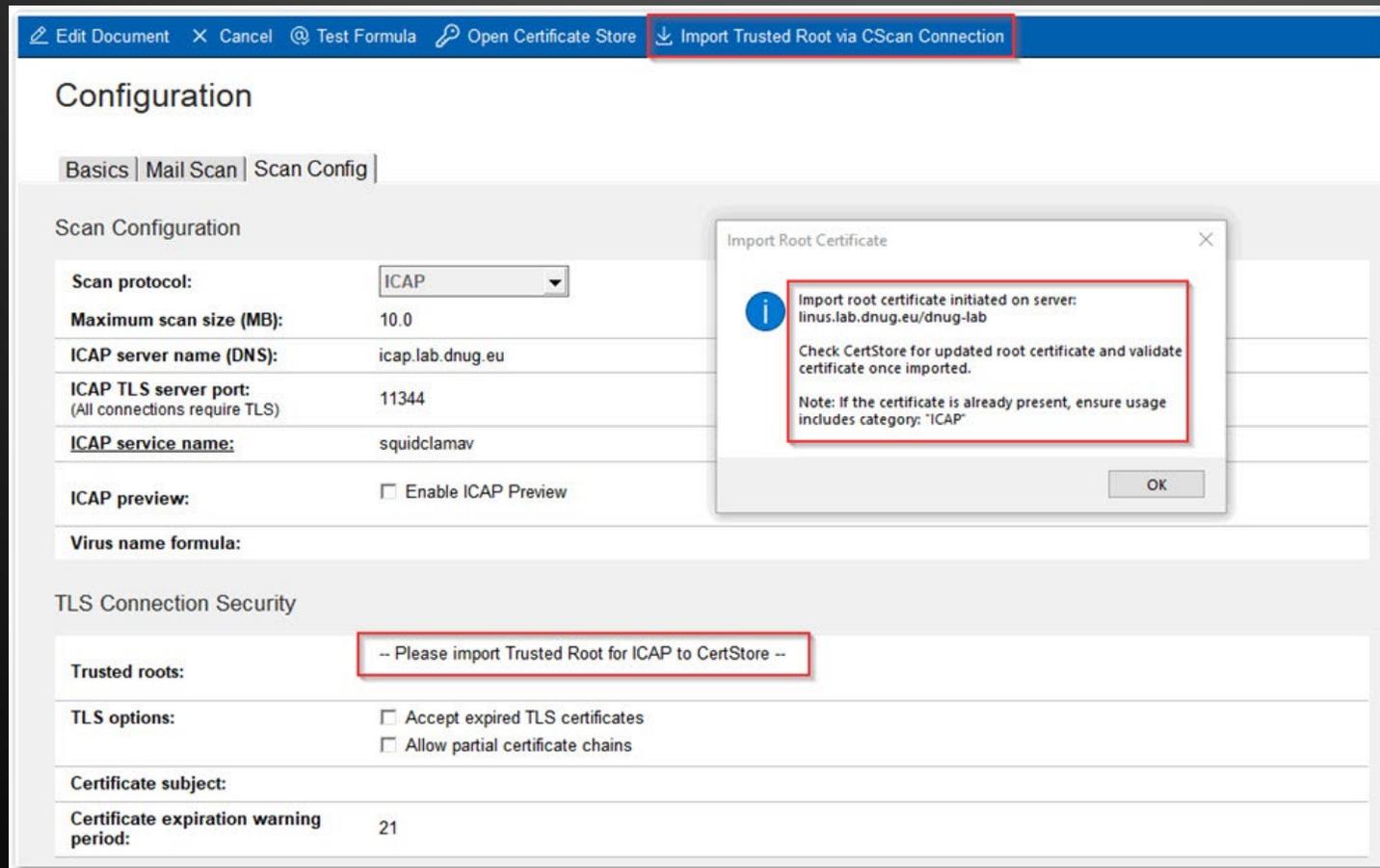
You must know the port the ICAP server uses, default for ICAP is 1344 but it may be different

You must know the name of the service your vendor uses.
E.g. Trend Micro is "interscan"
The demo server I use is "clamav"

Now is empty, we have to import the trusted root via Cscan connection

IMPORTING TRUSTED ROOTS

- This process requires that certstore.nsf is present on the server

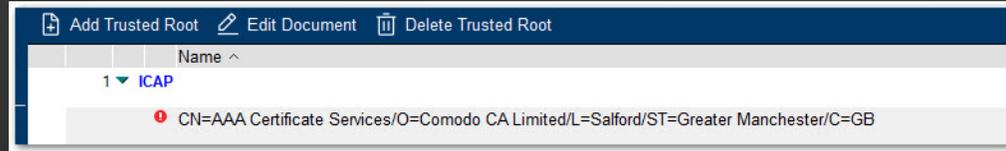


The screenshot shows a software configuration window with a menu bar at the top containing 'Edit Document', 'Cancel', 'Test Formula', 'Open Certificate Store', and 'Import Trusted Root via CScan Connection'. The main window is titled 'Configuration' and has tabs for 'Basics', 'Mail Scan', and 'Scan Config'. The 'Scan Configuration' section includes fields for 'Scan protocol' (set to ICAP), 'Maximum scan size (MB)' (10.0), 'ICAP server name (DNS)' (icap.lab.dnug.eu), 'ICAP TLS server port' (11344), 'ICAP service name' (squidclamav), and 'ICAP preview' (unchecked). Below this is the 'TLS Connection Security' section, where the 'Trusted roots' field contains the text '-- Please import Trusted Root for ICAP to CertStore --'. An 'Import Root Certificate' dialog box is overlaid on the configuration window, displaying an information icon and the following text: 'Import root certificate initiated on server: linus.lab.dnug.eu/dnug-lab', 'Check CertStore for updated root certificate and validate certificate once imported.', and 'Note: If the certificate is already present, ensure usage includes category: "ICAP"'. An 'OK' button is visible at the bottom right of the dialog box.

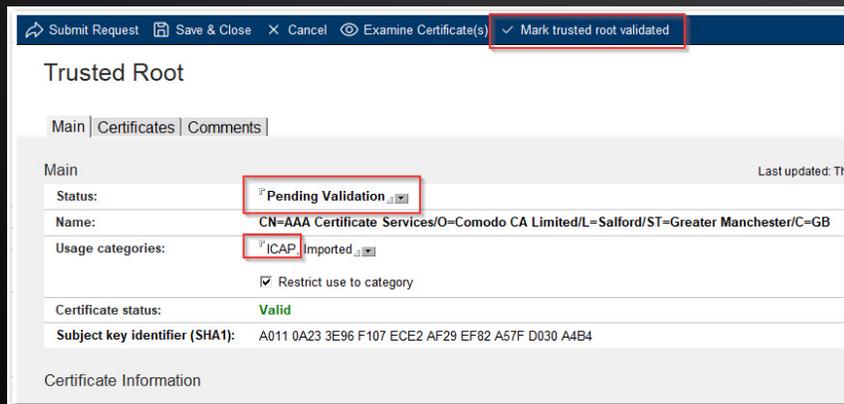


IMPORTING TRUSTED ROOTS

- open cerstore.nsf on the same server on which you opened cscancfg.nsf, and open the Trusted Roots view.
- validate the trusted root as follows:
- Expand the ICAP category. Any new trusted roots added by the preceding steps have been added under that category, in a pending state.

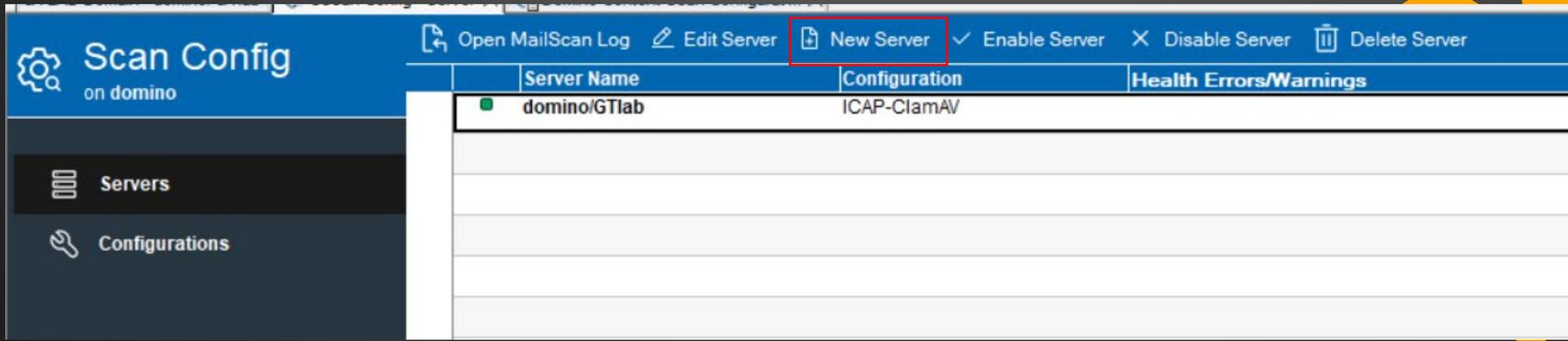


- Open the document for a root certificate that you want to examine. Verify that the Status is Pending Validation and the Certificate status is Valid
- Use the action Mark trusted root validated to validate the trusted root.



CREATE A SERVER

- Open cscancfg.nsf and go in the Servers view



The screenshot shows the 'Scan Config' interface on a Domino server. The top navigation bar includes 'Open MailScan Log', 'Edit Server', 'New Server' (highlighted with a red box), 'Enable Server', 'Disable Server', and 'Delete Server'. The left sidebar shows 'Servers' and 'Configurations' options. The main content area displays a table with the following data:

Server Name	Configuration	Health Errors/Warnings
domino/GTlab	ICAP-ClamAV	

- Click on New Server

NEW SERVER

Server

Main

Server name: [Server Selection Icon]

Configuration name: ICAP-ClamAV

Health status: Pending validation

Status: Enabled

Log options: normal

Log to file

Comments: [Text Area]

Administration

Administrators: Roberto Boccadoro/GTlab

Select your Domino server

Select the configuration you have just created

normal

minimal

normal

verbose

When you first create a server document, the Health status field displays as Pending validation. It remains that way until the mailscan task runs with a valid configuration and connects to the ICAP server. At that point, the status should be updated to Service Validated

Server name: domino/GTlab

Configuration name: ICAP-ClamAV

Health status: Service validated

TEST THE SOLUTION

- Go to the EICAR web site and download the test virus <https://www.eicar.org/download-anti-malware-testfile/>
- Send an email with the virus

	Marianna Tomasatti	[Message blocked]: new test
✉	Marianna Tomasatti	[Message discarded]test new icap
✉	Marianna Tomasatti	[Message discarded]Fw: test new icap

What is the eicar test file?

The EICAR Anti-Virus Test File or EICAR test file is a computer file that was developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO), to test the response of computer antivirus programs. Instead of using real malware, which could cause real damage, this test file allows people to test anti-virus software without having to use a real computer virus.