Use ICAP Antivirus Scanning

ICAP antivirus integration is available in FileCloud Server version 18.2.

ICAP scans are noted in audit logs beginning with version 19.3.

FileCloud uses Internet Content Adaption Protocol (ICAP) to integrate with any antivirus product currently supporting ICAP.

On this page

What is ICAP?

ICAP is a generic protocol that allows web servers to offload specialized tasks to custom-built servers. Examples of such specialized tasks include DLP (data loss prevention) based content scanning, URL filtering and antivirus scanning.

FileCloud's ICAP integration feature:

- Works on both Linux and Windows servers
- Triggers virus scanning only for uploaded files, that is - when files are uploaded to a FileCloud server instance
- Scanning is scheduled "inline" as soon as the file upload is completed
- Is part of FileCloud server itself
- Provides flexibility and scalability - the ICAP antivirus server does not have to be deployed on the same server as the one running the FileCloud server instance.

If you have already purchased your own antivirus solution and want to use it, or if you do not want to use ClamAV for various reasons, we highly recommended using this feature.

We also recommend that the ICAP Antivirus server administrator consult the antivirus product documentation to understand the operational and configuration parameters, capabilities and limitations. As virus scanning is a critical feature for maintaining water-tight security and smooth functioning of any workplace, consulting the documentation is important before configuring FileCloud's ICAP integration settings, it would also help in troubleshooting and maintenance.

When ICAP detects a virus

Similar to the case of ClamAV, if FileCloud's ICAP Client has been configured correctly with a properly deployed ICAP AV server, when a virus is detected in an uploaded file, the following actions occur:

1. The incoming file is deleted.
2. An alert will be displayed in the Admin Portal.
3. A toast will be displayed in the User Portal.
4. An entry will be added in the audit log about virus detection in the file and subsequent deletion of the file.

Integrating ICAP with FileCloud

Using ICAP to integrate Antivirus capabilities into FileCloud requires customers to:

1. Set up an ICAP antivirus server.
2. Configure FileCloud's inbuilt ICAP client to access your antivirus server.

FileCloud has made it easy for administrators to connect a FileCloud server to your antivirus server by including an inbuilt ICAP Client.

The easy configuration steps apply to both Windows and Linux servers.

To configure FileCloud to use your antivirus server:

1. Open a browser and log on to the *Admin Portal*.
2. On the left navigation panel, click *Settings*.
3. Select the *Third Party Integrations* tab.

4. In the *Anti-Virus* tab, from the Anti-Virus type drop down list, select *ICAP AV*.
5. Configure the various parameters for the ICAP Client as described in the Table 1.
6. To save your changes, click *Save*.
7. To confirm if the configuration has been done correctly, click the ICAP Test button.
8. A positive reply will confirm proper connectivity with the ICAP AV Server.

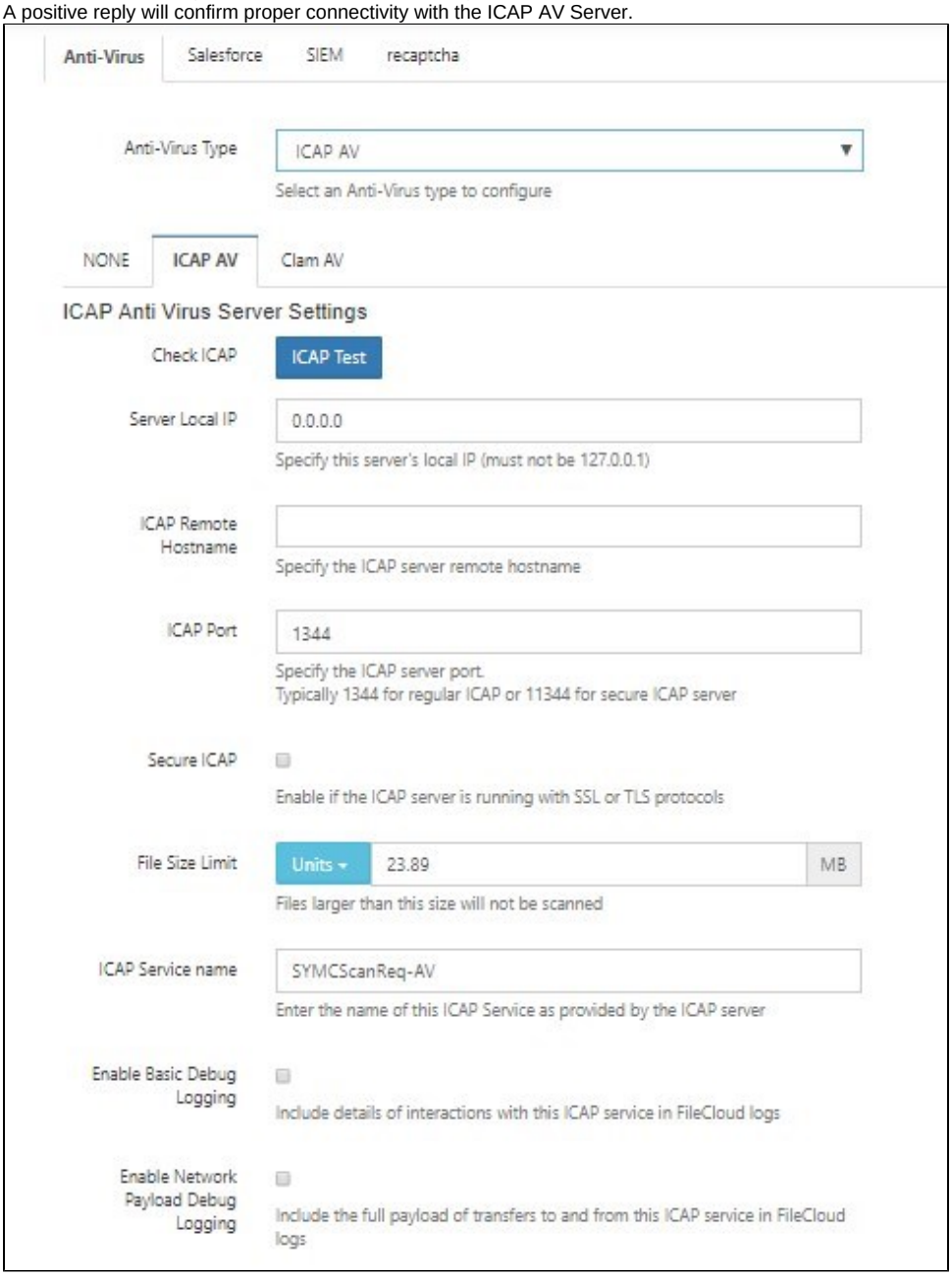


Table 1. ICAP Client Parameters

Setting	Description
Server Local IP	In most cases, leave the default value of 0.0.0.0. If you are using a separate FileCloud policy with ICAP, enter the Private (LAN) IP of the FileCloud server.
ICAP Remote Hostname	Enter the hostname or IP of the system where the ICAP AV is deployed.
ICAP Port	Leave the default value of 1344 as it is. In rare cases, this might need to be changed to whatever port the ICAP AV server is listening on.
Secure ICAP	Enable if the ICAP server is running with SSL or TLS protocols.
File Size Limit	This is the file limit in bytes that will be scanned. For example, very large files can be excluded from scanning. Default value is 25MB

ICAP Service Name	Consult the ICAP AV server product documentation to know this value. It must be set correctly otherwise integration wont work.
Enable Basic Debug Logging	Check this to enable logging of detailed operational debug messages in the (error) logs.
Enable Network Payload Debug Logging	Check this to enable logging of detailed network communication related debug messages in the (error) logs.

User details sent with scan requests

To help the ICAP server determine if a scan is required, the following headers are sent with every scan request:

Header X-FILECLOUD-USER-NAME - name of user performing the upload.
Header X-FILECLOUD-USER-EMAIL - email of user performing the upload.
Header X-FILECLOUD-USER-TYPE - type of user performing the upload. Possible values are "full", "guest", and "limited".

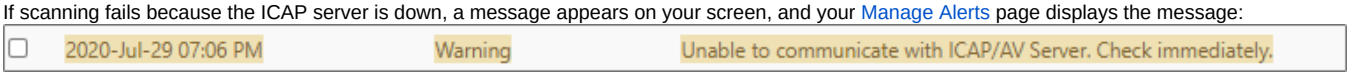
To disable sending of these headers:

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. Add the line:

```
define("TONIDOCLOUD_ICAPAV_DISABLE_ADDITIONALHEADERS", "1");
```

If scanning fails

If scanning fails because the ICAP server is down, a message appears on your screen, and your Manage Alerts page displays the message:



By default, if ICAP fails to scan a file because the ICAP server is down, the file is not deleted.

To automatically delete files if ICAP scan fails because the ICAP server is unavailable:

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. Add the line:

```
define("TONIDOCLOUD_ICAP_DELETE_ON_SCAN_FAIL",1);
```

Now, when scan fails, the file is deleted, and the audit log displays the message: *ICAP removed [FILE_PATH] due to scan fail.*

⚠ If TONIDOCLOUD_ICAP_DELETE_ON_SCAN_FAIL is enabled and the ICAP server is not available, FileCloud does not allow files to be uploaded.