

## Maximum oversize threshold

### Article

Description	This article describes the maximum file size for virus scanning (called the maximum oversize threshold) on FortiGate units.															
Components	All FortiGate units. FortiOS v2.80 and v3.0															
	<p>On mid- to low-end FortiGate models, the maximum oversize threshold is 10% of total RAM. The remaining RAM is reserved for system use.</p> <p>FortiGate units automatically calculate the maximum oversize threshold for virus scanning.</p> <p>To display the maximum oversize threshold from the FortiOS v3.0 web-based manager, edit any protection profile and view the Antivirus settings. You can also display the maximum oversize threshold from the FortiOS v3.0 CLI when configuring http, ftp, imap, pop3, smtp, im, or nntp settings in a protection profile.</p> <p>To display the maximum oversize threshold from the FortiOS v2.80 web-based manager go to <b>Antivirus&gt; Config&gt; Config</b>. You can also display the maximum oversize threshold from the FortiOS v3.0 CLI using the command <code>config antivirus service &lt;service&gt; by entering set memfilesizelimit ?</code>.</p> <p>The maximum oversize threshold approximately represents the 10% of RAM reserved for virus scanning plus 40% of the additional memory available.</p> <p>The table below displays the RAM available for virus scanning depending on the total RAM provided on the FortiGate unit.</p> <table border="1" data-bbox="427 1227 1114 1989"> <thead> <tr> <th>FortiGate Model</th> <th>RAM</th> <th>Maximum Oversize Threshold</th> </tr> </thead> <tbody> <tr> <td>50A 60 60M 60WiFi 60ADSL</td> <td>128MB</td> <td>12MB</td> </tr> <tr> <td>50B 60B 60WiFi 100A 100, 200, 300, 400, 500</td> <td>256MB</td> <td>25MB</td> </tr> <tr> <td>200A 224B 300A 400A FB1000</td> <td>512MB</td> <td>50MB</td> </tr> <tr> <td>310B 500A 800 800F 1000</td> <td>1GB</td> <td>139MB</td> </tr> </tbody> </table>	FortiGate Model	RAM	Maximum Oversize Threshold	50A 60 60M 60WiFi 60ADSL	128MB	12MB	50B 60B 60WiFi 100A 100, 200, 300, 400, 500	256MB	25MB	200A 224B 300A 400A FB1000	512MB	50MB	310B 500A 800 800F 1000	1GB	139MB
FortiGate Model	RAM	Maximum Oversize Threshold														
50A 60 60M 60WiFi 60ADSL	128MB	12MB														
50B 60B 60WiFi 100A 100, 200, 300, 400, 500	256MB	25MB														
200A 224B 300A 400A FB1000	512MB	50MB														
310B 500A 800 800F 1000	1GB	139MB														

1000A/AFA2 3000 4000		
3016B 3600 3600A 5001 5005	2GB	547MB
3810A	4GB	852MB

Changing the uncompressed file size limit (new for FortiOS v3.0 and AV Engine 2.002)

From the FortiOS v3.0 CLI you can use the `config antivirus service` command to control the size of uncompressed files that can be virus scanned. You can set this limit for each service.

```
config antivirus service <service>
  set uncompsizelimit <MB_integer>
end
```

Where:

<service> is ftp, http, https, im, imap, nntp, pop3 or smtp.

<MB\_integer> can be from 0 to the maximum oversize threshold. For example, for a FortiGate-5100SX the range is 1-547. For a FortiGate-100A the range is 1-25. The default <MB\_integer> is 10MB. You can set <MB\_integer> to 0 for no limit, but this configuration is not recommended. If an uncompressed file is larger than the <MB\_integer> limit, the compressed file is passed through without being virus scanned.

Changing compressed file nesting levels (new for FortiOS v3.0 and AV Engine 2.002)

From the FortiOS v3.0 CLI you can use the `config antivirus service` command to control the number of compression levels that FortiOS will open before virus scanning the resulting uncompressed file. You can set the number of levels for each service.

```
config antivirus service <service>
  set uncompnestlimit <depth_integer>
end
```

Where:

<service> is ftp, http, https, im, imap, nntp, pop3 or smtp.

<depth\_integer> can be from 2 to 100. The default <depth\_integer> is 12. A file with more compression levels than <depth\_integer> is passed through without being virus scanned.