IceWarp Unified Communications

AntiVirus Reference

Version 11.4

Published on 2/9/2016

Contents

AntiVirus

The IceWarp Anti-Virus engine can scan incoming and outgoing messages for viruses during SMTP transmission.

Up to version 10.1.2 the award-winning anti-virus engine from Avast is used.

For later versions, either Avast or Kaspersky anti-virus engines are used – depending on a license type purchased.

Various actions can be performed on messages found to contain a virus.

Legend

Icon	Description
	Warning – very important!
	*Note or tip – good to know.*
NOTE: Areas ...	*Note within a table.*
▸ Figure 4	Figure link – click the link to reveal the figure. Click it again to close it. (Works only in the ***CHM*** format.)

Registered Trademarks

About

Latest Avast! Engine

Built-in anti-virus upgraded to the latest version.

Kaspersky Anti-Virus Support

Support for KAVCOM instead of DKAV library implemented (external Kaspersky Anti-Virus).

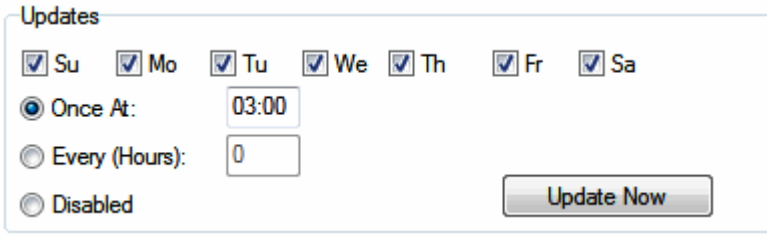
Support for LB Environments

Support for load-balanced environments added, new API variable which gets changed every update trigger, auto load feature and auto update is issued.

Reference

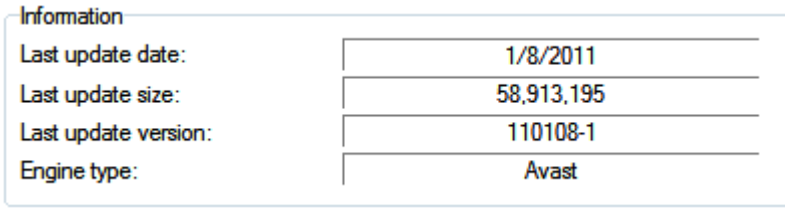
General

BE AWARE: Access mode to the service can be set on both domain and user levels. See the appropriate places (**[domain] – Policies**, **[user] – Policies**).



Field	Description
Su – Sa	Check these boxes to specify which day(s) to check for an AntiVirus update.
Once At:	Select this option and specify time when a check is to be done.
Every (Hours)	Select this option and enter a check interval.
Disabled	Select this option to disable checks for an AntiVirus update.
Update Now	Click the button to update AntiVirus now.

BE AWARE: The Control service must be running for AntiVirus updates to work.



The **Information** section shows information on the status of your IceWarp Anti-Virus definitions.

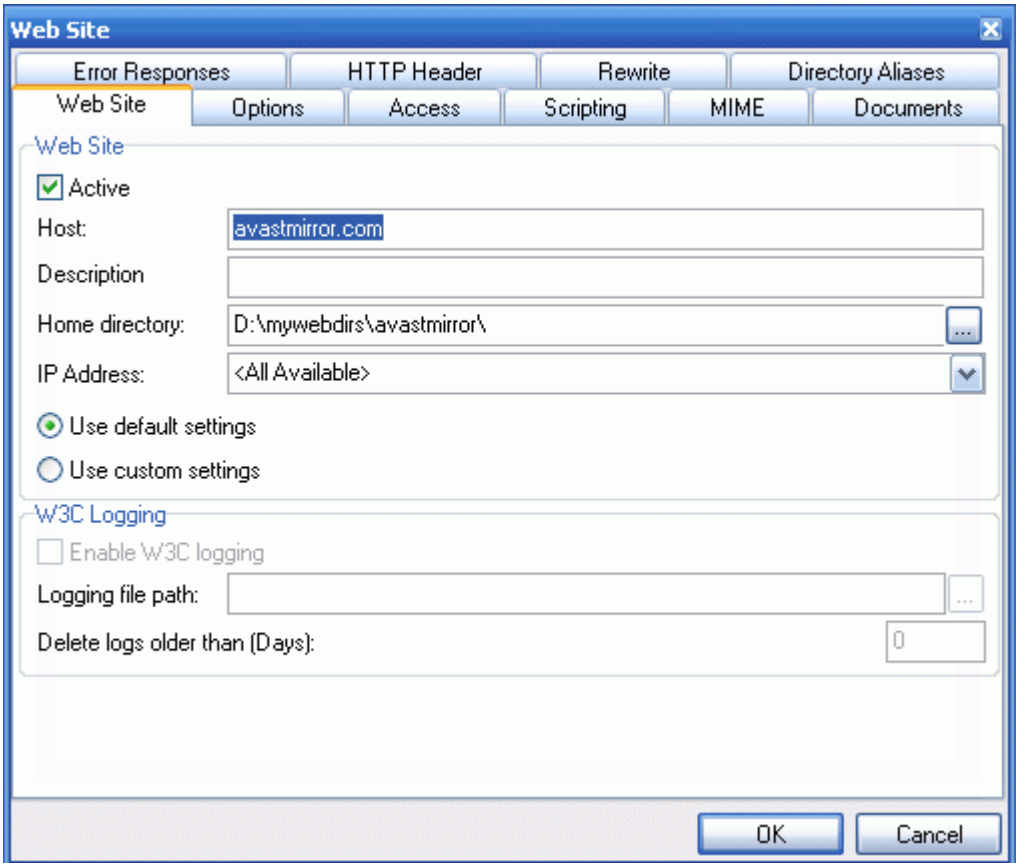
- The date the definitions file was last updated.
- The size of the last definitions update database.
- The version of the current definitions file.
- The engine type currently used.

This information can be useful for support issues.

Avast Mirror URL Setup

Define Web Site

- Create a home directory for the mirror site, for example: ***D:\mywebdirs\avastmirror***.
- Setup a new web site in IceWarp Server's Web Service node pointing to the previously defined home directory, with a suitable virtual host name e.g. ***avastmirror.com***.



Remember to set up a **DNS A** record for your new host.

Test Web Site

- Create a file test.txt in ***D:\mywebdirs\avastmirror***.
- Download it with any browser from ***http://avastmirror.com:32000/test.txt*** (using your hostname and port as required).

If it works, the web site is ready.

Setup Mirror

- Create a directory for the Avast mirroring program, e.g. ***D:\mirrorbase***, and extract the content of **mirror.zip** to it.
  mirror.zip is available from ***http://files.avast.com/files/eng/mirror.zip***

- Modify file **mirror.ini** in ***D:\mirrorbase\config***:

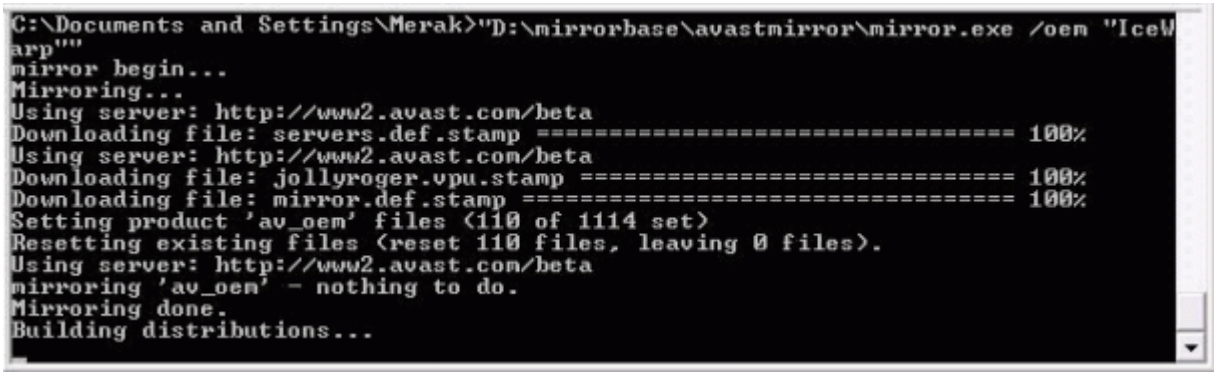
  Change two lines under [server0_0].

  Change "url" to WebSite host name, in this case ***url= http://avastmirror.com/***

  Change "upload_dest_directory" to the home directory of the Web Site, in this case ***upload_dest_directory=d:\mywebdirs\avastmirror***

- Run the first mirror update: ***D:\mirrorbase\avastmirror\mirror.exe /oem "IceWarp"***

  The program should run and produce output similar to the following:



This populates the home directory of your website with the current Avast files.

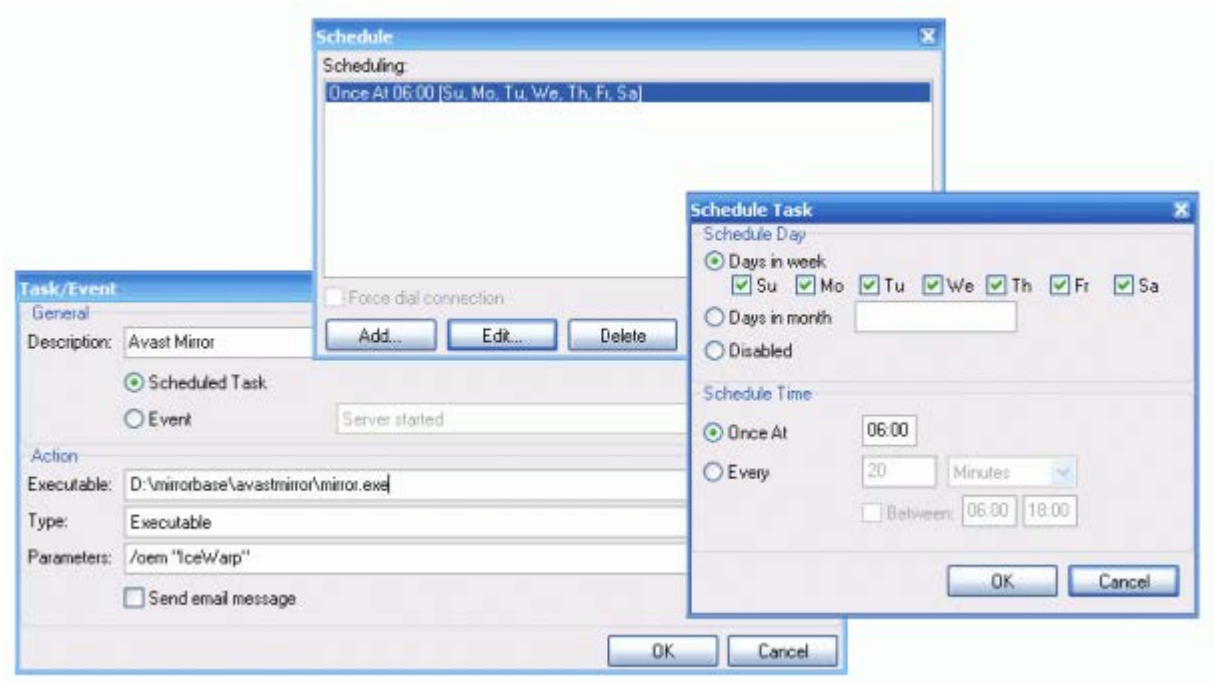
Test Mirror Site

- Download the definitions file with any browser from ***http://avastmirror.com:32000/servers_mirror.def***

If it is downloads successfully, the mirror is working.

Schedule Mirror Updates

- Add a new task to **IceWarp Server GUI – System – Tools – Tasks and Events** with the settings shown below (you may want to change the scheduling times).

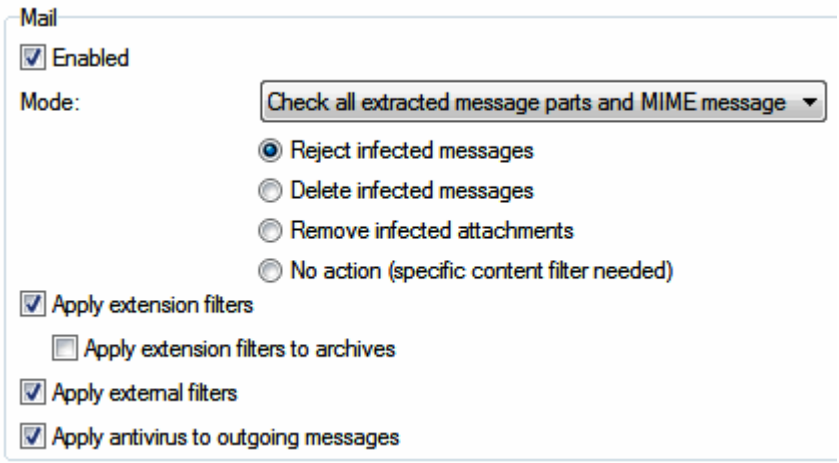


- Click the ***Run Now*** button in **IceWarp Server GUI – System – Tools – Tasks and Events**
- Wait a few minutes and check the log in ***D:\mirrorbase\avastmirror\logs\mirrors.log***.

If all is OK, it will show that the update was performed.

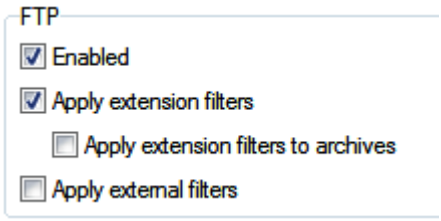
Action

Upon the **Action** tab you specify the actions to be taken when a message is found to contain a virus.

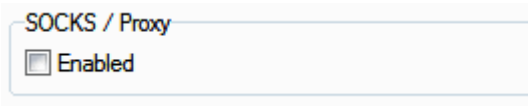


Field	Description
Enabled	Tick the box if you want to have this feature enabled.
Mode	Choose one of these options: **Check all extracted message attachments** Only message attachments are scanned. **Check all extracted message parts and MIME message** The complete messages, including attachments, are scanned. **Check MIME Message** Only the message is scanned (not attachments).
Reject infected messages	Infected messages will be immediately rejected by the server.
Delete infected messages	Infected messages will be accepted and deleted by the server. This option is useful if you want to further process the message even though it contains a virus. For example, you could use content filters to forward the message to an AntiVirus team.
Remove infected attachments	Any attachments containing a virus will be removed from the message. If an infected attachment cannot be removed, the message is rejected. *NOTE: This option will not function properly if the **Check all extracted message parts and MIME message** option is selected.*
No action (specific content filter needed)	The message is flagged as spam, but no other action is performed. BE AWARE: Use this option only if you have a content filter set properly! The appropriate condition is ***Where Scanned by Antivirus***. This option is suitable e.g. for viruses analyses.

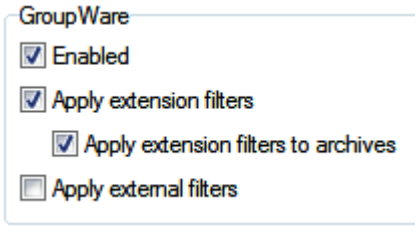
Apply extension filters	Tick the box if you want to use the extension filters defined upon the **Extension Filters** tab.
Apply extension filters to archives	Tick the box if you want to use the extension filters defined upon the **Extension Filters** tab also to archive folders.
Apply external filters	Tick the box if you want to use the external filters defined upon the **External Filters** tab.
Apply antivirus to outgoing messages	Tick the box if you want to have also outgoing messages checked by antivirus.



Field	Description
Enabled	Tick the box if you want to have uploaded files checked by antivirus.
Apply extension filters	Tick the box if you want to use the extension filters defined upon the **Extension Filters** tab.
Apply extension filters to archives	Tick the box if you want to use the extension filters defined upon the **Extension Filters** tab also to archives.
Apply external filters	Tick the box if you want to use the external filters defined upon the **External Filters** tab.



Field	Description
Enabled	Tick the box if you want to have enabled antivirus for SOCKS/Proxy.

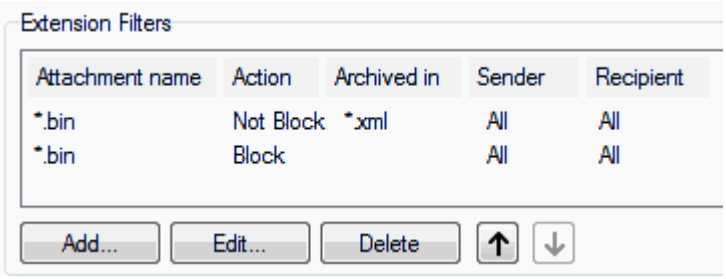


Field	Description
Enabled	Tick the box if you want to have groupware items checked by antivirus.
Apply extension filters	Tick the box if you want to use the extension filters defined upon the **Extension Filters** tab.
Apply extension filters to archives	Tick the box if you want to use the extension filters defined upon the **Extension Filters** tab also to archives.
Apply external filters	Tick the box if you want to use the external filters defined upon the **External Filters** tab.

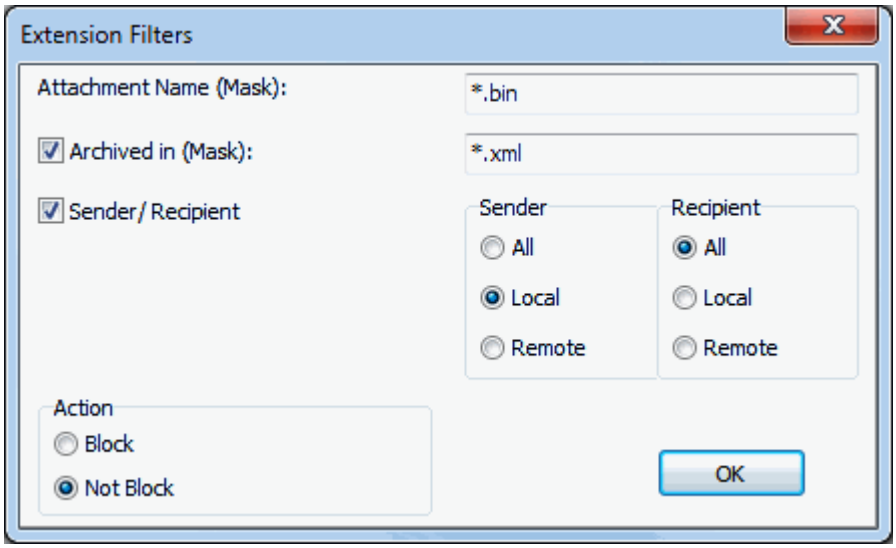
Extension Filters

The **Extension Filters** tab allows you to define a list of file extensions which will be considered a virus – file name masks are used.

If IceWarp Server finds an attached file with a listed extension then the message is processed as if it contained a virus.



Field	Description
Add	Click the button to add a new extension. The **Extension** dialog opens.
Edit	Select an extension and click the button to edit this extension. The **Extension** dialog opens.
Delete	Select an extension and click the button to remove this extension.



Field	Description
Attachment Name (Mask)	Enter the filename mask – e. g. ***.exe***.
Archived in (Mask)	Tick the box if you want to deal with files "inside" other files. For example, *xml* files can contain *bin* files. If you want to allow this combination , enter the ***.bin*** mask into the *Attachment Name* field, tick the box here and enter the ***.xml*** mask. Select the *Not Block* option lower. *NOTE: The first matching rule is applied, other rules are not processed. E. g. in the situation shown in the first figure, the bin files included into the xml files will not be blocked, but simple bin files will be blocked. Use the arrows to set the right rules order.*
Sender/Recipient	Select whether you want to apply the rule to *All*, *Local* or *Remote* users.
Action	Select whether you want either to *Block* or *Not Block* the specified filename mask.

BE AWARE: You must specify the ***** (asterisk) and **.** (dot) before the extension.

ALSO: You should not block the ***.TMP*** extension as this will cause IceWarp Server to categorize all messages as containing a virus.

External Filters

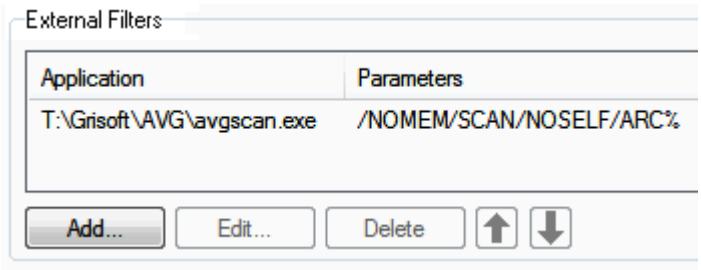
The **External Filters** tab allows you to configure IceWarp Server to use any external anti-virus filter(s) that support command-line scanning.

BE AWARE: This feature is provided for backwards compatibility and we strongly recommend that you use the built in AntiVirus engine provided with IceWarp Server. This section shows an example of using the AVGscan command line scanner. The information shown may be incorrect and we do not support these scanners directly. However, you may find information and help on our user-to-user forum at ***http://forum.icewarp.com/***, where you can search for previous posts or interact with a group of very helpful IceWarp Server users.

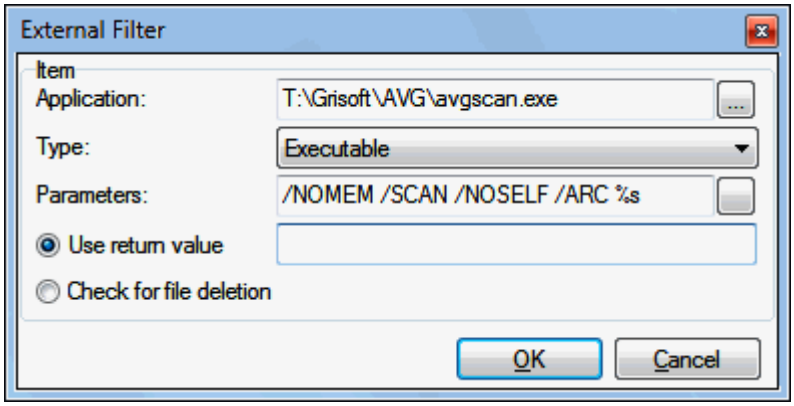
IceWarp Anti-Virus allows two ways of external AntiVirus usage:

- executable applications
- libraries

NOTE: If you choose to use any external on-access AntiVirus scanner you should exclude the ***<InstallDirectory>\Temp*** *folder from the scanning as this could cause severe server slowdown and problems with IceWarp Server itself.*

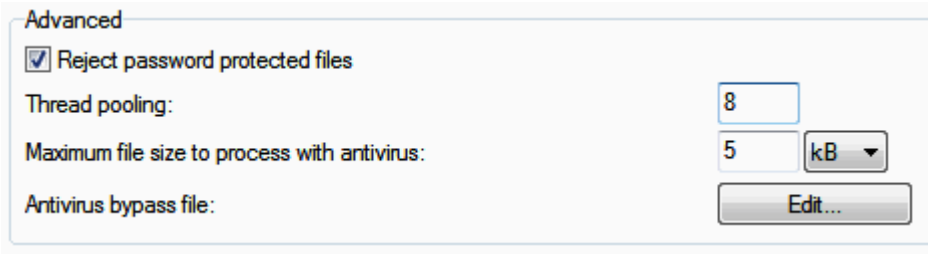


Field	Description
Add	Click the button to add a new external filter. The **External Filter** dialog opens.
Edit	Select an external filter and click the button to edit this filter. The **External Filter** dialog opens.
Delete	Select an external filter and click the button to remove this filter.
Arrows	Select an external filter and use the buttons to move this filter up or down within the list. You can change the order in what filters will be performed.

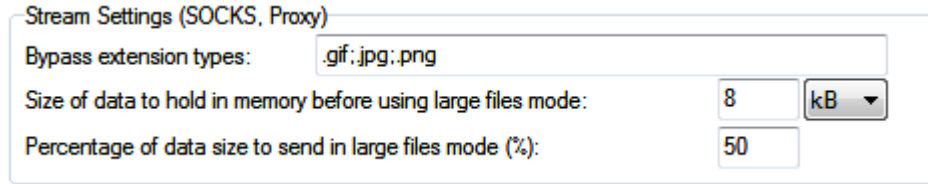


Field	Description
Application	Specify the fully qualified path to the external filter. Use the '...' button to open a standard file browser dialog.
Type	Select the type of module you are calling: **Executable** Choose this for a standard executable module. **StdCall Library, Cdecl Library** Choose this to call the filter from a library.
Parameters	Here specify parameters required by the external filter. Refer to documentation of your filter for further information.
Use return value	Enter values that your external filter returns if a virus is found. Refer to your filters documentation for this information. Multiple values should be separated by commas. For example, AVGscan issues the following codes: 0 – Everything is OK 1 – User cancelled/interrupted test 2 – Any error during the test – cannot open a file etc. 3 – Change identified 4 – Suspicion detected by heuristic analysis 5 – Virus found by heuristic analysis 6 – Specific virus detected 7 – Active virus in memory detected 8 – AVG corrupted 9 – Double extension 10 – Archive contains password protected files Codes 4, 5, and 6 indicate a virus (7 is discounted as this virus would not be within a message!) So we would enter 4,5,6 in this field.
Check for file deletion	Some filters do not return a value, but simply delete the file. If your filter behaves in this manner, select this option. After the filter is run, IceWarp Server will check whether the file has been deleted and, if it has, will treat the message as it contains a virus.

Advanced

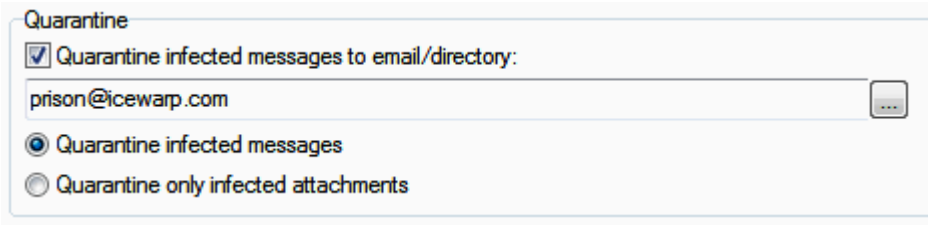


Field	Description
Reject password protected files	The IceWarp Anti-Virus engine must unpack attachments to check them for a virus. If an attached file is password protected then IceWarp Server cannot check the file contents. By default, the message would be forwarded to the recipient. This scenario could be exploited to get viruses into your system. Check this option to categorize any messages containing password protected files as containing a virus. *NOTE: This option applies to compressed files like ZIP and RAR ones or to encrypted .docx and .xlsx files (internally packed), not to previous versions of Word or Excel documents with password protection.* *ALSO: This functionality could also be done using filters, giving you more control over the actions.*
Thread pooling	The IceWarp Anti-Virus engine is multi-threading, this can sometimes cause problems on slower servers if the engine takes up too many resources, like 100% CPU. Entering a non-zero value here limits the number of IceWarp Anti-Virus threads that will be run concurrently.
Maximum message size to proceed with antivirus	Enter a non-zero value to have IceWarp Anti-Virus processing bypassed for messages exceeding the given size. *NOTE: If you do not have message size generally restricted, this could be risky as bigger messages containing viruses would bypass processing too.*
AntiVirus bypass file	Click the ***Edit*** button to edit a bypass file for the IceWarp Anti-Virus engine. This is a standard IceWarp Server bypass file. Examples of usage are given within the editor. Messages from email addresses, domains, and IP ranges specified within this file will not be processed by the IceWarp Anti-Virus engine.



Field	Description
Bypass extension types	Here you can define file (extension) types that are to be bypassed by antivirus engine. Separate extensions by semicolons. Define extensions with dots (e.g. ***.jpg***).
Size of data to hold in memory before using large files mode	There are two ways how to examine files: ▪ The checked file is in a memory – this is faster for small files.

	▪ The checked file is saved to a disk and examined here (large files mode) – a huge file would block too big part of memory. Define a large file size limit here.
Percentage of data size to send in large files mode (%)	Define a file size percentage that is examined before the examined file part is sent. E.g.: You define 50%, a half of a large file is examined and sent. Meanwhile, the second half of the file is examined (and sent consequently).



Field	Description
Quarantine infected message to email/directory	Check this option to create an archive of infected messages. Specify a fully qualified directory name where the messages will be stored, or an email address where the messages will be forwarded.
Quarantine infected messages	The whole message will be quarantined.
Quarantine only infected attachments	Only the infected attachments will be quarantined.

BE AWARE: This is NOT the same quarantine function as used by the AntiSpam engine.

These notifications are sent when:

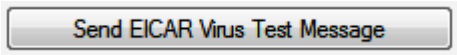
- attachment contains a virus
- attachment is rejected because of an extension filter
- attachment is an archive which contains a file with a blocked extension
- attachment is rejected by an external filter
- attachment is a password protected archive and the *Reject password protected files* option is enabled.

Field	Description
Administrator/Recipient/Sender	You can opt to send notification messages to a domain administrator(s), another recipient(s) and/or sender(s). Tick the appropriate one(s).
Customize	You can customize the message content and use IceWarp Server system variables within the message. Click the ***Customize*** button next to the person (that is to be notified) to open the message editor dialog. It is possible to use the *%%VirusName%%* variable within the message. For more infornation, refer to the **manual.chm – Shared Topics – Server Variables** section. Also, refer to the **<install_dir>/examples/variables.dat.html** file – find an example at the very end of the file.

"B" button	You can also define a bypass file for each person. Click the ***B*** button next to the person to define any bypass criteria you wish to impose. Examples are given within the editor (the ***Text File*** button).

EICAR Test

You can test your IceWarp Anti-Virus setup by pressing the ***Send EICAR Virus Test Message*** button.



EICAR (European Institute for Computer Antivirus Research) is a consortium of independent experts in the antivirus industry.

Obviously, you should not send out real viruses for testing purposes, so EICAR provides a file that can safely be sent, is non-viral, but which should trigger your IceWarp Anti-Virus software as though it were a virus.

If your IceWarp Anti-Virus is correctly set up you will obtain a warning message like the one below after pressing the button ***Send EICAR Test Message***.

If this warning does not appear, there is some problem with your setup and you should investigate further.

NOTE: If you are using remote console, sending a test message can bring different results (than this warning) because you are an eternal IP connected to IceWarp Server and not authenticated.

You may get several errors such as:

- *Access not allowed (due to the **Reject if sender local and not authenticated** option)*
- *Greylisting*
- *DNSBL*

Access Mode – Policies

Access mode for individual services is set on both domain and user levels:

- Upon the **[domain] – Policies** tab (**Domains and Accounts – Management**) for domains.
- Upon the **[user] – Policies** tab (**Domains and Accounts – Management – [domain]**) for users.

Firewall Settings

Some servers (systems) block the outgoing HTTP. AntiVirus service (using either Avast or Kaspersky) needs to have Firewall opened for outgoing HTTP. It can be done in the **<install_dir> /avast/setup/servers.def** file for Avast and **<install_dir>\kaspersky\kaspersky\bin\Bases\updcfg.xml** for Kaspersky.

Just make sure the hosts in the files mentioned above can be reached via port 80 outbound (you can do a telnet to test it).