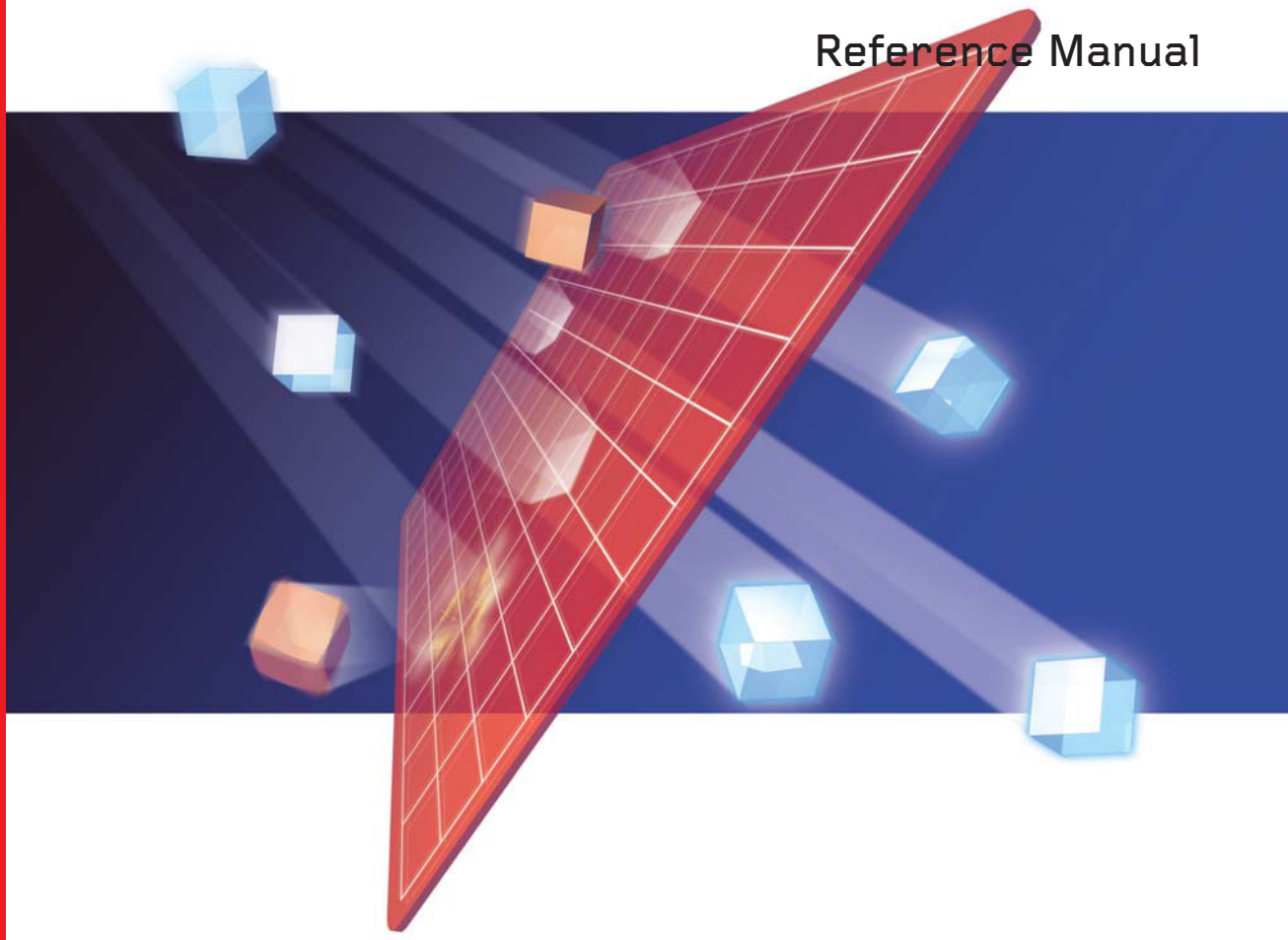
TREND MICRO™
InterScan™ VirusWall™ 6

Integrated virus and spam protection for your Internet gateway

for Linux™

Reference Manual



TREND MICRO™

Before installing and using the software, please review the readme files, release notes and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Document Part No. IVEM62664/60224
Release Date: July 2006
Protected by U.S. Patent Nos. 5,623,600; 5,889,943; 5,951,698 and 6,119,165

The Reference Manual for Trend Micro™ InterScan VirusWall™ is intended as a quick reference for administrators managing an InterScan VirusWall installation.

Detailed information about how to use specific features within the software is available in the online help file and online Knowledge Base at the Trend Micro Web site.

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com.

Your feedback is always welcome.

Please evaluate this documentation on the following site:
http://www.trendmicro.com/download/documentation/rating.asp.

Contents

Chapter 1

Outbreak Prevention Services

Outbreak Prevention Services (OPS) allows you to receive updates directly from TrendLabs[SM] as interim protection from virus/malware outbreaks while a solution is being developed. OPS has automatic deployment options available to the administrator, including when to activate an outbreak policy and how long to keep the policy in effect.

An OPS policy is activated depending on the issue date and expiration period set within the policy. If OPS is activated, and the OPS policy that Trend Micro has issued has an expiration date that occurs after the current system time, then that policy is activated. Trend Micro specifies the duration of the policy but you can manually override it if desired.

To receive OPS policies for POP3, SMTP, HTTP, and FTP services, you must have these services enabled to enable corresponding OPS policies.

Enabling OPS

To enable OPS and view detailed status information:

1. On the main menu, select **Outbreak Defense > Current Status**.
2. Select the **Enable Outbreak Prevention Services (OPS)** check box as shown in Figure 1-1.

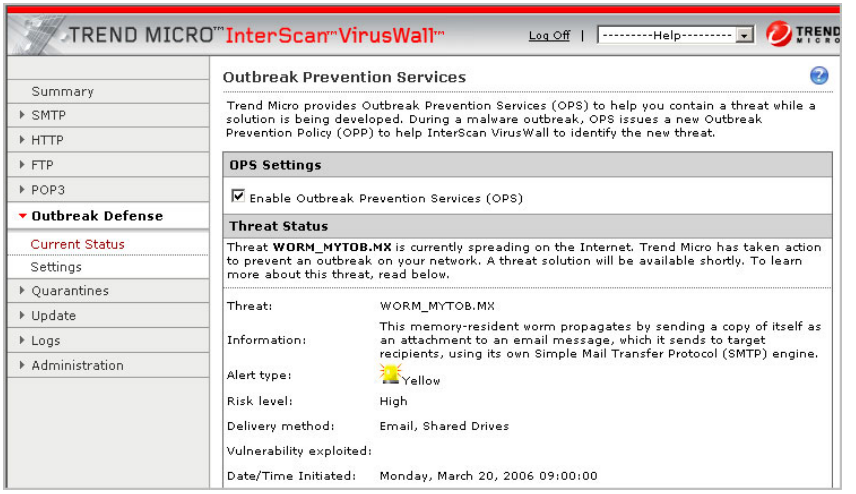


FIGURE 1-1. Outbreak Prevention Services Current Status screen, upper half

3. Click **Save**.

To see whether Outbreak Prevention Services (OPS) is enabled and active:

1. On the main menu, select **Summary** and then click the **Status** tab.
2. If necessary, click the icon on the right to expand the Outbreak Prevention Services information so that you can check the status of the services.

   Figure 1-2 shows a sample Summary Status tab with information about Outbreak Prevention Services.

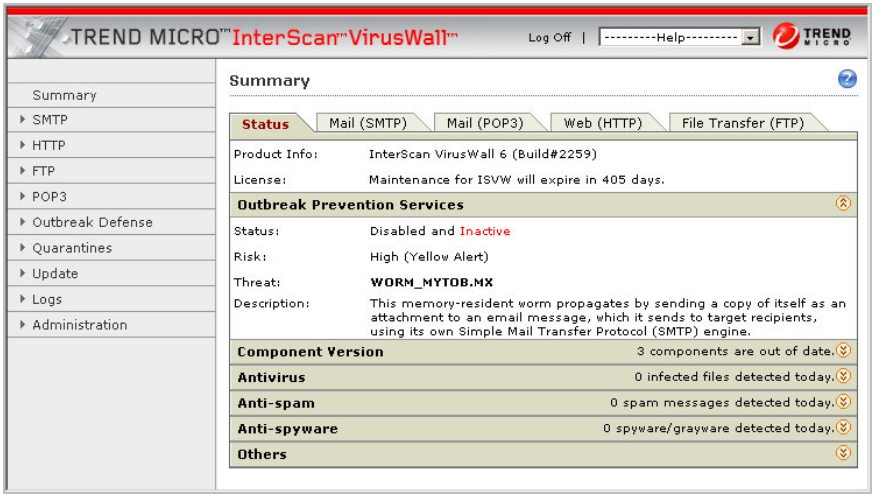


FIGURE 1-2. Summary screen, Status tab

Available Current Status

Since Trend Micro issues and manages the OPS policies, you can view but not modify the rest of the information on the Outbreak Prevention Services Current Status screen.

- The **Threat Status** section provides status of the current threat.
- The **Attachment Filter** section lists the types of files in email messages (through POP3/SMTP services) that are blocked.
  - File names being blocked solely matches file extensions (the "*" wildcard can be used in the name only, not the extension).
  - File types being blocked detects the true file type from actual file content and blocks by type. The numbers that appear here are internal file type representations for InterScan VirusWall.
- The **Content Filter** section shows the email message contents (through POP3/SMTP services) OPS is blocking. This is a regular-expression filter for mail subject/body/attachment name. The wildcard characters "*" and "?" can be used in the expression.
- The **URL Blocking** section lists the URLs (through HTTP service) that OPS is blocking. URLs are represented with regular expressions; "*" denotes any character.
- The **File Blocking** section shows the type of files (through HTTP and FTP services) that OPS is blocking.

Configuring OPS Settings

Trend Micro specifies the expiration time of OPS policies, but you can manually change the time.

To configure OPS settings:

1. On the left side menu, select **Outbreak Defense > Settings**.
2. Under **Outbreak Alert Expiration**, specify when you want the alert for the Outbreak Prevention Policy (OPP) to expire. The expiration date is based on when the OPP is issued.
3. To schedule policy download settings, select the **Enable scheduled policy download** check box and select a download frequency (expressed in minutes) for OPS policies.
4. Click **Save**.

   Figure 1-3 shows the default settings for Outbreak Prevention Services.

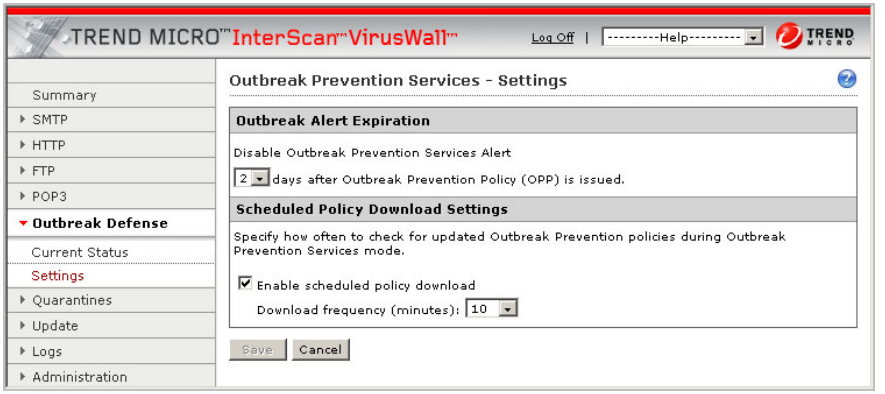


FIGURE 1-3. Outbreak Prevention Services - Settings screen

Note: If InterScan VirusWall 6 downloads and activates a new OPS policy, the expiration setting will be overwritten. To manually manage the effective duration of the OPS policies, modify the expiration period for each individual OPS policy.

Chapter 2

System Checklists

Use the checklists in this chapter to record relevant system information.

Server Address Checklist

You must provide the following server address information during installation, as well as during the configuration of InterScan VirusWall 6 to work with your network. Record them here for easy reference.

Required Information	Sample	Your Value
Trend Micro InterScan VirusWall 6 server information		
IP address	10.1.104.255	
Fully Qualified Domain Name (FQDN)	server.company.com	
Proxy server information		
IP address	10.1.174.225	
Fully Qualified Domain Name (FQDN)	proxy.company.com	

Required Information	Sample	Your Value
Notification server information		
IP address	10.1.123.225	
Fully Qualified Domain Name (FQDN)	mail.company.com	

Port Checklist

InterScan VirusWall 6 uses the following ports:

Port	Sample	Your Value
SMTP	25	
POP3	110	
HTTP	8080	
FTP	21	
Web console	9240	
Web console (SSL)	9241	

Supported Commands

SMTP

The InterScan VirusWall 6 SMTP module supports ESMTP commands but not SMTP SSL.

Command Name	Explanation
HELO	helo: be polite
EHLO	extended SMTP hello command
MAIL	mail: designate sender
RCPT	rcpt: designate recipient
DATA	data: send message text
RSET	rset: reset state
HELP	help: give usage info
NOOP	noop: do nothing
QUIT	quit: close connection and die
SAML	saml: send AND mail
SOML	soml: send OR mail
AUTH	encrypted authentication
VRFY	verify the user name
EXPN	expand a mailing list
TURN	change role to receiver or sender

FTP

InterScan VirusWall 6 supports most FTP commands supported in popular FTP servers and clients. Known unsupported commands include REST, APPE, and STOU. When Store unique is on, the FTP "put" command is not implemented. Kerberos authentication is also not supported.

POP3

POP3 supported commands include CAPA, AUTH, and all commands specified in RFC 1939. POP3 SSL is not supported.

Command Name	Explanation	RFC
CAPA	List support features	RFC 2449
APOP	Log on with MD5	RFC 1939
AUTH	For Exchange servers	RFC 1734/3206
USER	Send user name	RFC 1939
PASS	Send password	RFC 1939
QUIT	Quit sessions	RFC 1939
STAT	List status of mailbox	RFC 1939
LIST	List info of mails	RFC 1939
UIDL	List UID of mails	RFC 1939
TOP	Get header of mails	RFC 1939
RETR	Get mails	RFC 1939
DELE	Mark mails as deleted	RFC 1939
RSET	Unmark deleted mails	RFC 1939
NOOP	Do nothing	RFC 1939

Chapter 3

Migration Reference

This chapter provides a reference when migrating settings from InterScan VirusWall for Unix 3.8x with eManager 3.8 to InterScan VirusWall 6.

The following settings can be migrated:

SMTP Virus Scan

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Define the files to scan	level= scanext	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/ScanTypePolicy=3 root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/ScanTypePolicy=3	E-Mail Scan Configuration > Files to Scan > Scan all files with the following file extensions	SMTP Scanning > Files to Scan > Specified file extensions…
Scanning according to file extension	extensions= .aaa .bbb	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/UserExtensions= aaa;bbb root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/UserExtensions= aaa;bbb	E-Mail Scan Configuration > Files to Scan > Scan all files with the following file extensions	SMTP Scanning > Files to Scan > Specified file extensions… > Scan Specified Files by Extension
Action on infected files	action=pass/ delete/ move/clean	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/VirusAction=0/4/2/3 root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/VirusAction=0/4/2/3	E-Mail Scan Configuration > Action on Viruses	SMTP Scanning > Action on Messages with Infected Items
Action on uncleanable files	ucaction= pass/delete/ move	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/VirusAction2nd= 0/4/2 root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/VirusAction2nd= 0/4/2	E-Mail Scan Configuration > Action on Non-Cleanable Files	SMTP Scanning > Action on Messages with Infected Items > If cannot be cleaned, specify an action

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Whether to send notification to the administrator	notify_admin =yes/no	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Admin/Enable=1/0 root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Admin/Enable=1/0	E-Mail Scan Configuration > Notifications > E-mail to administrator	SMTP Scanning > Email Notifications > Administrator
Content of the notification to the administrator	admin_msg (string)	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Admin/Body(string) root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Admin/Body(string)	E-Mail Scan Configuration > Notifications > Message	SMTP Scanning > Email Notifications > Administrator
Whether to send notification to the recipient	notify_user= yes/no	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Recipient/Enable=1/0 root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Recipient/Enable=1/0	E-Mail Scan Configuration > Notifications > Warning to recipients	SMTP Scanning > Email Notifications > recipient
Content of the notification to the recipient	user_msg (string)	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Recipient/Body(string) root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Recipient/Body(string)	E-Mail Scan Configuration > Notifications > Warning to recipients	SMTP Scanning > Email Notifications > recipient

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Whether to send notification to the sender	notify_ sender=yes/ no	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Sender/Enable=1/0 root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Sender/Enable=1/0	E-Mail Scan Configuration > Notifications > Warning to sender	SMTP Scanning > Email Notifications > sender
Content of the notification to the sender	sender_msg (string)	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Sender/Body(string) root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/Outcomes/Outcome Virus/Actions/Notification Sender/Body(string)	E-Mail Scan Configuration > Notifications > Warning to sender	SMTP Scanning > Email Notifications > sender
Additional message	addtl=yes/no /replace	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/Additional=1/0/1 root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/Additional=1/0/1	E-Mail Scan Configuration > Virus Warning Message > Additional message	The feature migrates to config.ini
Content of the additional message	addtl_ message (string)	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/AdditionalMsg (string) root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/AdditionalMsg (string)	E-Mail Scan Configuration > Virus Warning Message > Additional message	The feature migrates to config.ini

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Whether to insert a 'safe' stamp into the users' email with a message	safe_stamp =yes/no	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/SafeStamp=1/0 root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/SafeStamp=1/0	E-Mail Scan Configuration > Notifications > Stamp	SMTP Scanning > Inline Notification Stamp > Virus free
Content of the “safe” stamp	safe_ message (string)	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/SafeStampMsg (string) root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/SafeStampMsg (string)	E-Mail Scan Configuration > Notifications > Stamp	SMTP Scanning > Inline Notification Stamp > Virus free
Specify where virus and disclaimer messages are inserted	rlocation= top/bottom/ none	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/AddInfoInBottom= 0/1/? root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/AddInfoInBottom= 0/1/?	E-Mail Scan Configuration > Miscellaneous > Specify where virus and disclaimer messages are inserted	The feature only migrates to config.ini
Configure SMTP-Return Code Message	unaccept_ err_msg (string)	root/Smtp/MessageWhen Reject	Additional Email Options > Return Message	The feature only migrates to config.ini
Enable SMTP virus scanning	mailscan (yes/no)	root/Smtp/Policies/ Incoming/Rule1/MailVirus Scan/Enable=1/0 root/Smtp/Policies/ Outgoing/Rule1/MailVirus Scan/Enable=1/0	Scan Configuration > E-Mail Scan	SMTP Scanning > Enable SMTP Scanning

SMTP Configuration

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Send virus warning message to external sender	incom_ notify=yes out_check= yes	root/Smtp/Policies/ Outgoing/Rule1/ MailVirusScan/ Outcomes/ OutcomeVirus/ Actions/ NotificationSender /Enable=1	Additional Email Options > Send virus warning message to external sender	SMTP Configuration > outgoing > Email Notifications > Sender
Whether to log the message ID	save_msgid =yes/no	root/Smtp/Policies/ Incoming/Rule1/ LogMessageID=1/ 0	E-Mail Scan Configuration > Miscellaneous > Log incoming Message-ID	SMTP Configuration > SMTP Scan Log > Log incoming Message-ID
Send the "NOOP" command to the original server to prevent timeout every X number of seconds	data_intval_ time(int)	root/Smtp/ SendNoopIntval (int)	E-Mail Scan Configuration > Miscellaneous > Send the "NOOP" command to the original server	SMTP Configuration > Send the "NOOP" command to the original server to prevent timeout
Limit email size to 5MB	msg_size= 5M	root/Smtp/ MaxDataSize= 5*1024	E-Mail Scan Configuration >Miscellaneous >Maximum size	SMTP Configuration > Message size >Maximum size
Limit email size to 5KB	msg_size= 5K	root/Smtp/ MaxData Size=5	E-Mail Scan Configuration > Miscellaneous > Maximum size	SMTP Configuration > Message size > Maximum size
Limit email size to 5GB	msg_size= 5G	root/Smtp/ MaxDataSize= 5*1024*1024	E-Mail Scan Configuration > Miscellaneous > Maximum size	SMTP Configuration > Message size > Maximum size
No limitation on email size	msg_size=0	root/Smtp/ MaxDateSize=0	E-Mail Scan Configuration > Miscellaneous > Maximum size	SMTP Configuration > Message size > Maximum size

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Specify local domains to support outbound mail processing	local_ domain= localhost #127.0.0.1	root/Smtp/ LocalDomain	Additional Email Options > Local domain	SMTP Configuration > Outbound Processing > To support outbound mail processing, specify your local domains
Local domain list file	local_ domain=/opt /trend/local_ domain_list	root/Smtp/ LocalDomain	Not available in the Web console	SMTP Configuration > Outbound Processing > To support outbound mail processing, specify your local domains
For outbound email, accept recipient address only if specified	accept_rcpt (string)	root/Smtp/ AcceptAddress	Additional Email Options > Local domain > Enable Anti-Relay > Accept RCPT address	SMTP Configuration > Anti-Relay
Enable Anti-Relay	anti_relay= yes/no	root/Smtp/ AntiRelay=1/0	Additional Email Options > Local domain > Enable Anti-Relay	SMTP Configuration > Anti-Relay
Whether to add a customized disclaimer text	out_ disclaimer= yes/no	root/Smtp/Policies/ Outgoing/Rule1/ AddDisclaimer= 1/0	Additional Email Options > Local domain > Disclaimer	SMTP Configuration > Outbound Processing > Add customized disclaimer text to every outbound mail message
Whether to select source relay check	src_relay_ check= yes/no	root/Smtp/ SrcRelay=1/0	E-Mail Scan Configuration > Miscellaneous > Source relay check	SMTP Configuration > Source relay

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Specify typical character for source relay	src_relay_ meta(string)	root/Smtp/ SrcRelayMeta (string)	E-Mail Scan Configuration > Miscellaneous > Source relay check	SMTP Configuration > Source relay > Specify typical character for source relay
Main SMTP listening service port	svcport (1-65535)	root/Smtp/ ServicePort (1-65535)	E-Mail Scan Configuration > Main Service Port	SMTP Configuration > Main SMTP listening service port
Original SMTP server location: Remote server	local_mode= no remote_ daemon_ host=IP/host remote_ daemon_ port=port	root/Smtp/Original CommondMode=0 root/Smtp/Original ProxyAddress=IP/ host root/Smtp/Original ProxyPort=port	E-Mail Scan Configuration > Remote server	SMTP Configuration > Forward mail to SMTP server at #
Original SMTP server location: Local server	local_mode= yes command_ mode=no local_ daemon_ port=port	root/Smtp/Original CommondMode=0 root/Smtp/Original ProxyAddress= 127.0.0.1 root/Smtp/Original ProxyPort=port	E-Mail Scan Configuration > Local server	SMTP Configuration > Use sendmail
Local mail program command	local_mode= yes command_ mode=yes command_ param=/usr/ lib/sendmail -bs	root/Smtp/Original CommondMode=1 root/Smtp/Original Commond=/usr/ lib/sendmail -bs	E-Mail Scan Configuration > Local server > Command mode	SMTP Configuration > Local mail program command

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Whether to enable message redirection	multi_relay= yes/no	root/Smtp/ AddrMapping/ Enable=1/0	Additional Email Options > Forward Messages for Final Processing > Enable message redirection	SMTP Configuration > Forward Messages for Final Processing > Enable message redirection
Message direction file	multi_relay_ ini=/etc/ iscan/ direction.ini	root/Smtp/Addr Mapping/Addr.n/* root/Smtp/Addr Mapping/Count	Not available in the Web console	The feature migrates to config.ini
Receive a greeting when connection is established	greeting= yes/no	root/Smtp/Enable Greeting=1/0	E-Mail Scan Advanced Configuration > Receive greeting when connection is established	SMTP Configuration > Advanced Configuration > Receive greeting when connection is established

FTP Virus Scan

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Define the files to scan	level = scanall	/root/Ftp/Policies/ Rule1/FileVirus ScanScan/ TypePolicy = 1	FTP Scan Configuration > Scan all files	FTP Scanning > All scannable files
Define the files to scan	level = scanext	/root/Ftp/Policies/ Rule1/FileVirus ScanScan/ TypePolicy = 3	FTP Scan Configuration > Scan all files with the following file extensions	FTP Scanning > Specified file extensions
Scanning according to file extension	extensions= .aaa .bbb	/root/Ftp/Policies/ Rule1/FileVirus Scan/ UserExtensions= aaa;bbb	FTP Scan Configuration > Scan all files with the following file extensions > .aaa,.bbb	FTP Scanning > Specified file extensions > Scan Specified Files by Extension
Action on infected files	action=pass/delete/move/clean	/root/Ftp/Policies/ Rule1/FileVirus Scan/VirusAction= 0/5/2/3	FTP Scan Configuration > Action on Viruses:	FTP Scanning > Action on Infected Files
Action on uncleanable files	uaction= pass/delete/move	/root/Ftp/Policies/ Rule1/FileVirus Scan/VirusAction= 0/5/2	FTP Scan Configuration > Action on Non-Cleanable Files	FTP Scanning > Action on Infected Files > If cannot be cleaned, specify an action
Whether to send notification to the administrator	notify_admin= yes/no	/root/Ftp/Policies/ Rule1/FileVirus Scan/Outcomes/ OutcomeVirus Deliver/Actions/ NotificationAdmin/ Enable=1/0	FTP Scan Configuration > Notification >E-mail to administrator	FTP Scanning > Notification > Administrator Notification
Content of the notification to the administrator	admin_msg	/root/Ftp/Policies/ Rule1/FileVirus Scan/Outcomes/ OutcomeVirus Deliver/Actions/ NotificationAdmin/ Body=string	FTP Scan Configuration > Notification > Message	FTP Scanning > Notification > Administrator Notification

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Whether to block the selected file type	block = no	/root/Webui/FTP/AntiVirus/BlockType_Media = 0 /root/Webui/FTP/AntiVirus/BlockType_Img = 0 /root/Webui/FTP/AntiVirus/BlockType_Comp = 0 /root/Webui/FTP/AntiVirus/BlockType_Java = 0 /root/Webui/FTP/AntiVirus/BlockType_Exec = 0 /root/Webui/FTP/AntiVirus/BlockType_MsDoc = 0 /root/Webui/FTP/AntiVirus/BlockType_Other = 0	FTP Scan Configuration > File Types to Block > Block the following file types	FTP Scanning > Block Selected File Types
Block Java files	block = yes oblock_types = java	/root/Webui/FTP/AntiVirus/BlockType_Java = 1	FTP Scan Configuration > File Types to Block > Block the following file types > Java applets	FTP Scanning > Block Selected File Types > Java (.class)
Block executable files	block = yes oblock_types = exec	/root/Webui/FTP/AntiVirus/BlockType_Exec = 1	FTP Scan Configuration > File Types to Block > Block the following file types > Executables	FTP Scanning > Block Selected File Types > Executable (.exe, .dll, etc.)

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Block Microsoft Word documents	block = yes oblock_types = office	/root/Webui/FTP/AntiVirus/BlockType_MsDoc = 1	FTP Scan Configuration > File Types to Block > Block the following file types > Office documents	FTP Scanning > Block Selected File Types > Microsoft documents (.doc, .xls, etc.)
Block compressed file types	block = yes oblock_types = archiv	/root/Webui/FTP/AntiVirus/BlockType_Comp = 1	FTP Scan Configuration> File Types to Block > Block the following file types > Compressed archives	FTP Scanning > Block Selected File Types > Compressed (.zip, .tar, .jar, etc.)
Block audio/video file types	block = yes oblock_types = audiovideo	/root/Webui/FTP/AntiVirus/BlockType_Media = 1	FTP Scan Configuration > File Types to Block > Block the following file types > Audio/video files	FTP Scanning > Block Selected File Types > Audio/Video (.mp3, .wav, etc.)
Block image files	block = yes oblock_types = picture	/root/Webui/FTP/AntiVirus/BlockType_Img = 1	FTP Scan Configuration> File Types to Block > Block the following file types > Pictures	FTP Scanning > Block Selected File Types > Images (.gif, .jpg, etc.)
Block unknown file types	block = yes oblock_types = unknown	/root/Webui/FTP/AntiVirus/BlockType_Other = 1	FTP Scan Configuration > File Types to Block > Block the following file types > Unknown types	FTP Scanning > Block Selected File Types > Other file types
Block other file types	block = yes oblock_types = unknown aaa	/root/Webui/FTP/AntiVirus/BlockType_Other = 1 /root/Webui/FTP/AntiVirus/BlockType_OtherTypes = aaa	FTP Scan Configuration > File Types to Block > Block the following file types > Other types	FTP Scanning > Block Selected File Types > Other file types

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Send notification to user	addtl_virus_ message	/root/Ftp/Policies/ Rule1/FileVirus Scan/UserNotif Virus=string	FTP Scan Configuration> Virus Warning Message > Additional message	FTP Scanning > Block Selected File Types > User Notification
Enable FTP virus scanning	intscan.ini [Scan-Configuration] ftpscan= yes/no	Root/FTP/Policies/ Rule1/FileVirusScan/EnableVirusScan=yes/no	Scan Configuration > FTP Scan	FTP Scanning > Enable FTP Scanning

FTP Configuration

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
FTP VirusWall listening port	svcport	/root/Ftp/svcport	FTP Scan Configuration > Main service port	FTP Configuration > FTP service port
FTP virus wall transfer data port	dataport	/root/Ftp/ dataport	Not available in the Web console	Not available in the Web console
Original FTP server location: Use user@host	self_proxy= yes/no	/root/Ftp/ self_proxy= yes/no	FTP Scan Configuration > Use user@host	FTP Configuration > Use user@host
Original FTP server location: Server location	original	/root/Ftp/original	FTP Scan Configuration > Server location	FTP Configuration > Server location
Receive a greeting when connection is established	greeting=yes/no	/root/Ftp/ greeting=yes/no	FTP Scan Advanced Configuration > Receive greeting when connection is established	FTP Configuration > Receive greeting when connection is established
Receive log transaction history	log_trans= yes/no	/root/Ftp/ log_trans= yes/no	FTP Scan Advanced Configuration > Receive log transaction history	FTP Configuration > Receive log transaction history

HTTP Virus Scan

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Define the files to scan	level= scanall	Root/Http/Plugin/ScanVsapi/http/level=scanall	HTTP Scan Configuration > Files to Scan	HTTP Scanning > Files to scan > All scannable files
Define the files to scan	level= scanext	Root/Http/Plugin/ScanVsapi/http/level=scanext	HTTP Scan Configuration > Scan all files with the following extensions	HTTP Scanning > Files to scan > Specified file extensions
Scanning according to file extension	extensions (string)	Root/Http/Plugin/ScanVsapi/http/extensions	Scan all files with the following extensions	HTTP Scanning > Files to scan > Specified file extensions > Scan Specified Files by Extension
Define MIME type not to scan	skip=yes skiptype (string)	Root/Http/Main/http/skiptype=string	HTTP Scan Configuration > MIME Content-type to skip:	HTTP Scanning > MIME Type Exceptions

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Whether to block the selected file type	block=no oblock_ types(string)	Root\Http\main\scan_ configuration\enable_ true_file_type_block=no Root\Http\main\scan_ configuration\block_ types=Null WebUI\HTTP\AntiVirus\ BlockType_Media=0 WebUI\HTTP\AntiVirus\ BlockType_Comp=0 WebUI\HTTP\AntiVirus\ BlockType_Img=0 WebUI\HTTP\AntiVirus\ BlockType_Java=0 WebUI\HTTP\AntiVirus\ BlockType_Exec=0 WebUI\HTTP\AntiVirus\ BlockType_Msdoc=0 WebUI\HTTP\AntiVirus\ BlockType_Other=0 WebUI\HTTP\AntiVirus\ BlockType_OtherTypes =Null	HTTP Scan Configuration > File Types to Block:	HTTP Scanning > Block Selected File Types

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Block Java files	block = yes oblock_ types = java	Root\Http\main\scan_ configuration\enable_ true_file_type_block= yes Root\Http\main\scan_ configuration\block_ types=(int values in vsapi) WebUI\HTTP\AntiVirus\ BlockType_Java=1	HTTP Scan Configuration > File Types to Block: > Java applets	HTTP Scanning > Block Selected File Types > Java (.class)
Block executable files	block = yes oblock_ types = exec	Root\Http\main\scan_ configuration\enable_ true_file_type_block= yes Root\Http\main\scan_ configuration\block_ types=(int values in vsapi) WebUI\HTTP\AntiVirus\ BlockType_Exec=1	HTTP Scan Configuration > File Types to Block: > Executables	HTTP Scanning > Block Selected File Types > Executable (.exe, .dll, etc.)
Block Microsoft Word documents	block = yes oblock_ types = office	Root\Http\main\scan_ configuration\enable_ true_file_type_block= yes Root\Http\main\scan_ configuration\block_ types=(int values in vsapi) WebUI\HTTP\AntiVirus\ BlockType_Msdoc=1	HTTP Scan Configuration > File Types to Block: > Office documents	HTTP Scanning > Block Selected File Types > Microsoft documents (.doc, .xls, etc.)

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Block compressed file types	block = yes oblock_ types = archiv	Root\Http\main\scan_ configuration\enable_ true_file_type_block= yes Root\Http\main\scan_ configuration\block_ types=(int values in vsapi) WebUI\HTTP\AntiVirus\ BlockType_Comp=1	HTTP Scan Configuration > File Types to Block: > Compressed archives	HTTP Scanning > Block Selected File Types > Compressed (.zip, .tar, .jar, etc.)
Block audio/video file types	block = yes oblock_ types = audiovideo	Root\Http\main\scan_ configuration\enable_ true_file_type_block= yes Root\Http\main\scan_ configuration\block_ types=(int values in vsapi) WebUI\HTTP\AntiVirus\ BlockType_Media=1	HTTP Scan Configuration > File Types to Block: > Audio/video files	HTTP Scanning > Block Selected File Types >Audio/Video (.mp3, .wav, etc.)
Block image files	block = yes oblock_ types = picture	Root\Http\main\scan_ configuration\enable_ true_file_type_block= yes Root\Http\main\scan_ configuration\block_ types=(int values in vsapi) WebUI\HTTP\AntiVirus\ BlockType_Img=1	HTTP Scan Configuration > File Types to Block: > Pictures	HTTP Scanning > Block Selected File Types > Images (.gif, .jpg, etc.)

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Block other file types	block = yes oblock_ types = unknown	Root\Http\main\scan_ configuration\enable_ true_file_type_block= yes Root\Http\main\scan_ configuration\block_ types=(int values in vsapi) WebUI\HTTP\AntiVirus\ BlockType_Other=1 WebUI\HTTP\AntiVirus\ BlockType_OtherTypes =string types	HTTP Scan Configuration > File Types to Block: > Unknown types	HTTP Scanning > Block Selected File Types > Other file types
Block other file types	block = yes oblock_ types = aaa	Root\Http\main\scan_ configuration\enable_ true_file_type_block= yes Root\Http\main\scan_ configuration\block_ types=(int values in vsapi) WebUI\HTTP\AntiVirus\ BlockType_Other=1 WebUI\HTTP\AntiVirus\ BlockType_OtherTypes =aaa	HTTP Scan Configuration > File Types to Block: > Other types	HTTP Scanning > Block Selected File Types > Other file types
Enable/ Disable macroscan	macroscan= yes/no	Root/Http/Main/Scan-configuration/ macroscan=yes/no	HTTP Scan Configuration > Macro Scan:	Migrates to config.xml
Action on macroscan	macro_act= quarantine/ clean	Root/Http/Main/Scan-configuration/macro_ act=quarantine/clean	HTTP Scan Configuration > Quarantine/Clean	Migrates to config.xml

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Notification displayed in the user's browser	addtl_virus_ message (string)	Root/Http/Main/http/ virus_notification=string	HTTP Scan Configuration > Virus Warning Message: > Additional message:	HTTP Scanning > Notification > User Notification
Header line displayed in the browser	msg_body (string)	Root/HTTP/Main/http/ Security_event_ headline	HTTP Scan Configuration > Virus Warning Message: > Header line:	Not available in the Web console
Action on infected files	action= pass/delete/ move/clean	Root/Http/Main/http/ action=pass/delete/ move/clean	HTTP Scan Configuration > Action on Viruses:	HTTP Scanning > Action > Action on Infected Files
Action on uncleanable files	uaction= pass/move/ delete	Root/Http/Main/http/ uaction=pass/move/ delete	HTTP Scan Configuration > Action on Non-Cleanable Files	HTTP Scanning > Action > Action on Infected Files > clean
Enable HTTP virus scanning	intscan.ini [Scan-Configuration] httpscan= yes/no	Root/HTTP/Main/http/ virus_scan_enabled= yes/no Root/HTTP/Plugin/ScanVsapi/plug-in/enabled= yes/no	Scan Configuration > HTTP Scan	HTTP Scanning > Enable HTTP Scanning

HTTP Configuration

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
HTTP VirusWall listening port	svcport (1-65535)	Root/Http/ Protocol/ HttpProxy/main/ port	HTTP Scan Configuration > InterScan HTTP Proxy port	HTTP Configuration > HTTP listening port
Use standalone mode	self_proxy=yes/ no	Root/Http/ Protocol/ HttpProxy/http/ self_proxy=yes/ no	HTTP Scan Configuration > InterScan acts as proxy itself	HTTP Configuration > Use standalone mode
Use standalone mode	self_proxy=yes	Root/Webui/ HTTP/ ProxyMode= StandAlone	HTTP Scan Configuration > InterScan acts as proxy itself	HTTP Configuration > Use standalone mode
Use dependent mode	self_proxy=no	Root/Webui/ HTTP/ ProxyMode= Dependent	HTTP Scan Configuration > Other (server and port):	HTTP Configuration > Dependent mode
Dependent mode proxy and port	Original=IP Port	Root/Http/ Protocol/ HttpProxy/http/ original_server= IP Root/Http/ Protocol/ HttpProxy/http/ original_server_ port= Port	HTTP Scan Configuration > Other (server and port):	HTTP Configuration > Proxy: Port:

ActiveUpdate Pattern Update

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Schedule update (weekly)	Frequency = Weekly	root/Common/ ActiveUpdate/ ScheduleUpdate/ VirusUpdate/Type = 4	Set Automatic Update Time > Update Time > Update weekly	Scheduled Update > Update Schedule > Week, on
Schedule update (hourly)	Frequency = Hourly	root/Common/ ActiveUpdate/ ScheduleUpdate/ VirusUpdate/Hours = 1 root/Common/ ActiveUpdate/ ScheduleUpdate/ VirusUpdate/Type = 4 root/Webui/Update/ Schedule/hour = 1	Set Automatic Update Time > Update Time > Update hourly	Scheduled Update > Update Schedule > Hour(s)
Schedule update (daily)	Frequency = Daily	root/Common/ ActiveUpdate/ ScheduleUpdate/ VirusUpdate/Type = 3	Set Automatic Update Time > Update Time > Update daily	Scheduled Update > Update Schedule > Day(s)
Days of week	DayOfWeek1= Sunday… Monday	root/Common/ ActiveUpdate/ ScheduleUpdate/ VirusUpdate/Days = 0…6 root/Webui/Update/ Schedule/weekday = 0…6	Set Automatic Update Time > Update Time	Scheduled Update > Update Schedule

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Hours of weekday	Hour = n APM = PM	root/Common/ ActiveUpdate/ ScheduleUpdate/ VirusUpdate/hours = n+12 root/Webui/Update/ Schedule/hour_of_ weekday = n+12 root/Webui/Update/ Schedule/hour_of_day = n+12	Set Automatic Update Time > Update Time	Scheduled Update > Update Schedule
Hours of weekday	Hour = n APM = AM	root/Common/ ActiveUpdate/ ScheduleUpdate/ VirusUpdate/hours = n root/Webui/Update/ Schedule/hour_of_ weekday = n root/Webui/Update/ Schedule/hour_of_day = n	Set Automatic Update Time > Update Time	Scheduled Update > Update Schedule
AU server and product registration information	intscan.ini [Registration]	Config.xml /root/Common/ ActiveUpdate/ UpdateServers/ Server.x/ /root/Common/ ProductRegistration/ UpdateServers/ Server.x/ /root/Webui/Update/ TestConnection	Update Virus Pattern From Internet > Register for Products	Migrates to config.xml

Item	intscan.ini Location		Web Console Location	
	3.8x intscan.ini	6.0 config.xml	3.8x	6.0
Whether to use proxy server for pattern download	use_proxy = yes/no	UseProxy = 1/0	Set Proxy for Update Virus Pattern From Internet	Proxy Settings > Use a proxy server for pattern, engine, and license updates
Proxy	reg_proxy (string)	Proxy	Use proxy server for pattern download > proxy	Proxy Settings > Use a proxy server for pattern, engine, and license updates > Server name or IP address
Proxy Port	reg_port (int)	ProxyPort	Use proxy server for pattern download > port	Proxy Settings > Use a proxy server for pattern, engine, and license updates > Port:

eManager Key Config File Values

<table>
<tr><th>Feature</th><th colspan="5">3.8x</th><th colspan="3">6.0</th></tr>
<tr><td rowspan="9">Global Setting</td><td colspan="5"><install_path>/Plug-Ins/EM/ contscan.ini</td><td colspan="3">Config.xml</td></tr>
<tr><td colspan="5">[Content Filter]</td><td colspan="3">Keyword Filter (RuleType = 1), set in every filter property</td></tr>
<tr><td rowspan="2">Case Sensitive</td><td colspan="4">no</td><td rowspan="2">CaseSensitive (in each filter)</td><td>0</td></tr>
<tr><td colspan="4">yes</td><td>1</td></tr>
<tr><td rowspan="2">Exact Match</td><td colspan="4">no</td><td rowspan="2">Keyword (in each filter)</td><td>For Example, “.REG. “testKeyword””</td></tr>
<tr><td colspan="4">yes</td><td>For Example, “testKeyword”</td></tr>
<tr><td colspan="5">[Specialized Filter]</td><td colspan="3">Attachment Filter (RuleType = 2), set in every filter property</td></tr>
<tr><td rowspan="4">Remove Attachment</td><td rowspan="2">no</td><td rowspan="4">Check every attachment policy rule enable property</td><td>yes</td><td rowspan="4">Enable Rule</td><td rowspan="4">Result is decided by the two value “AND” operator result.</td><td><Value Name="EnableRule" string="" type="int" int="0" /></td></tr>
<tr><td>no</td><td><Value Name="EnableRule" string="" type="int" int="0" /></td></tr>
<tr><td rowspan="2">yes</td><td>yes</td><td><Value Name="EnableRule" string="" type="int" int="1" /></td></tr>
<tr><td>no</td><td><Value Name="EnableRule" string="" type="int" int="0" /></td></tr>
<tr><td rowspan="2">Quarantine</td><td colspan="4">no</td><td rowspan="2">Action</td><td rowspan="2"><Value Name="Action" string="Remove" type="string" int="0" /></td></tr>
<tr><td colspan="4">yes</td></tr>
<tr><td>Content filter</td><td colspan="5"><install_path>/Plug-Ins/EM/ Csconfig.dat</td><td colspan="3">Config.xml</td></tr>
<tr><td>Attach-ment filter</td><td colspan="5"><install_path>/Plug-Ins/EM/ spamrule/SFRule.txt</td><td colspan="3">Config.xml</td></tr>
<tr><td>Notifica-tion</td><td colspan="5"><intall_path>/Plug-Ins/EM/ contscan.ini</td><td colspan="3">Config.xml</td></tr>
</table>

eManager Content Filter

3.8x	6.0	3.8x Value	6.0 Value
shRuleName	RuleName	Copy the value	
	RuleType		1 - Keyword filter type
Action (sectionname= **rulename** in contscan.ini file)	Action	Delete	Delete
		Archive	Quarantine
		Quarantine	Quarantine
Inbound mailscan (sectionname= **rulename** in contscan.ini file)	InBound	Yes	1
		No	0
Outboundmail scan (sectionname= **rulename** in contscan.ini file)	OutBound	Yes	2
		No	0
Notification (sectionname= **rulename** in contscan.ini file)	InBoundNotify	Copy the value	
Notification (sectionname= **rulename** in contscan.ini file)	OutBound Notify	Copy the value	
seSynEnabled	Enable Synonyms	seSynEnabled=t	1
		seSynEnabled=f	0
peProfEnabled	EnableRule	peProfEnabled=t	1
		peProfEnabled=f	0
(Hidden attribute from global setting)	CaseSensitive	Yes	1
		No	0
(Hidden attribute from global setting)	ExactMatch	Yes	1
		No	0

3.8x	6.0	3.8x Value	6.0 Value
sf	File name	sf./spamrule/Bg_ AntiSpam.466 One Content Filter (see filter config definition) One line corresponding to one “KeyWord” “Trigger” = 1, Key Name	Compose one content filter; one word is one expression of the content filter
wh	One **keyword**	wh8 ALL LIVE - ALL NUDE SHOWSwh80 Million Addresses	<key Name=" KeywordFilter"> <key Name="word head_0"> … <key> </key>
wd	Multiple keywords separated by comma	wh<html> wd<script wd</script wd</html>	<key Name=" KeywordFilter"> <key Name="word head_0"> <Value Name="KeyWord" string="<html>,<script,</script,</html " type="string" int="0" /> <Value Name="IncludeSyn" string="" type="string" int="0" /> <Value Name="CaseSensitive" string="" type="int" int="0" /> <Value Name="ExactMatch" string="" type="int" int="0" /> </key> <key>

3.8x	6.0	3.8x Value	6.0 Value
sy	One synonym for one keyword. If **3.8** has more than one “sy”, use \t( ) to separate them	whshit sycrap sydirt	<Key Name="KeywordFilter"> <Key Name="word head_0"> <Value Name="KeyWord" string="shit" type="string" int="0" /> <Value Name="IncludeSyn" string="crap dirt " type="string" int="0" /> <Value Name="CaseSensitive" string="" type="int" int="0" /> <Value Name="ExactMatch" string="" type="int" int="0" /> </key> </key>
sn	One excluded synonym for one keyword	snturd sndump	Not migrated
ew	exclusive word	ewex_1 ewex_2	<Key Name="ExceptionFilter"> <Value Name="Trigger" string="" type="int" int="0" /> <Key Name=”Item 0”> <Value Name="KeyWord" string="ex_1" type="string" int="0" /> … </Key> <Key Name=”Item 1”> <Value Name="KeyWord" string="ex_2" **type="string" int="0" />** </Key> </key>

eManager Attachment Filter

3.8x	6.0	3.8x Value	6.0 Value
ENABLE	EnableRule	Yes	1
		No	0
RULE NAME	RuleName	Copy the value	
	RuleType		2 – Attachment type
Action	Action	Remove (Default value)	Remove
		Quarantine (From global setting is not migrated)	Quarantine
			Delete
MAIL TYPE	InBound, OutBound	A	A(InBound=1,OutBound=0)
		B	B(InBound=0,OutBound=2)
		C	C(InBound=1,OutBound=2)
AttachmentFilter Condition Description		In the configuration file, there are 4 conditions to enable/disable the rule	There are 4 content filters inside the attachment filter, which decide the attachment rule to enable/disable.
<ATTR><NAME> INCLUDE </NAME> </ATTR>	INCLUDE, EXCLUDE	INCLUDE	<Value Name="Trigger" string="" type="int" int="1" />
		EXCLUDE	<Value Name="Trigger" string="" type="int" int="0" />

3.8x	6.0	3.8x Value	6.0 Value
Condition1 From address	Name Case sensitive Exact match	<FROM> <NAME> jing_gao@isvw.com </NAME> <I>yes</I> <S>yes</S> </FROM>	Compose one content filter inside the filter <key name=”AttachmentFilenameFilter”> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name="AttachType" string="" type="int" int="1" /> <Value Name="AttachExp" string="*.txt" type="string" int="0" /> <Key Name="Filters"> <Key Name="From"> <Value Name="FilterType" string="" type="int" int="0" /> <Value Name="Trigger" string="" type="int" int="1" /> <Value Name="FilterScope" string="" type="int" int="4" /> <Key Name="word head_0"> <Value Name="KeyWord" string=" jing_gao@isvw.com " type="string" int="0" /> <Value Name="CaseSensitive" string="" type="int" int="1" /> <Value Name="ExactMatch" string="" type="int" int="1" /> </Key> …

3.8x	6.0	3.8x Value	6.0 Value
Condition2 To address	Name Case sensitive Exact match	<TO> <NAME> jing_gao@isvw.com </NAME> <I>yes</I> <S>yes</S> </TO>	Compose one content filter inside the filter <Key Name="AttachmentFilenameFilter"> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name="AttachType" string="" type="int" int="1" /> <Value Name="AttachExp" string="*.txt" type="string" int="0" /> <Key Name="Filters"> <Key Name="To"> <Value Name="FilterType" string="" type="int" int="0" /> <Value Name="Trigger" string="" type="int" int="1" /> <Value Name="FilterScope" string="" type="int" int="8" /> <Key Name="word head_0"> <Value Name="KeyWord" string=" jing_gao@isvw.com " type="string" int="0" /> <Value Name="CaseSensitive" string="" type="int" int="1" /> <Value Name="ExactMatch" string="" type="int" int="1" /> </Key> …

3.8x	6.0	3.8x Value	6.0 Value
Condition3 ReplyTo address	Name Case sensitive Exact match	<RTO> <NAME> jing_gao@isvw.com </NAME> <I>yes</I> <S>yes</S> </RTO>	Compose one content filter inside the filter <Key Name="AttachmentFilenameFilter"> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name="AttachType" string="" type="int" int="1" /> <Value Name="AttachExp" string="*.txt" type="string" int="0" /> <Key Name="Filters"> <Key Name="Others"> <Value Name="FilterType" string="" type="int" int="0" /> <Value Name="Trigger" string="" type="int" int="1" /> <Value Name="FilterScope" string="" type="int" int="128" /> <Key Name="word head_0"> <Value Name="KeyWord" string=" jing_gao@isvw.com " type="string" int="0" /> <Value Name="CaseSensitive" string="" type="int" int="1" /> <Value Name="ExactMatch" string="" type="int" int="1" /> </Key>

3.8x	6.0	3.8x Value	6.0 Value
Condition4 CC address	Name Case sensitive Exact match	<CC> <NAME> jing_gao@isvw.com </NAME> <I>yes</I> <S>yes</S> </CC>	Compose one content filter inside the filter <Key Name="AttachmentFilenameFilter"> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name="AttachType" string="" type="int" int="1" /> <Value Name="AttachExp" string="*.txt" type="string" int="0" /> <Key Name="Filters"> <Key Name="CC"> <Value Name="FilterType" string="" type="int" int="0" /> <Value Name="Trigger" string="" type="int" int="1" /> <Value Name="FilterScope" string="" type="int" int="16" /> <Key Name="word head_0"> <Value Name="KeyWord" string=" jing_gao@isvw.com " type="string" int="0" /> <Value Name="CaseSensitive" string="" type="int" int="1" /> <Value Name="ExactMatch" string="" type="int" int="1" /> </Key> …
Attachment removal MIME option	One Attachment Filter	<MIME> <NAME>text/plain </NAME> </MIME>	<Key Name="AttachmentFilenameFilter"> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name="AttachType" string="" type="int" int="2" /> <Value Name="AttachExp" string="text/plain" type="string" int="0" /> </Key>

3.8x	6.0	3.8x Value	6.0 Value
Attachment removal True file types	One Attachment Filter	<ATTACH> <NAME>exe </NAME> </ATTACH>	<Key Name="AttachmentFilenameFilter"> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name="AttachType" string="" type="int" int="1" /> <Value Name="AttachExp" string="exe;txt" type="string" int="0" /> </Key>
replacetext (in [specialized filtering] in the contscan.ini file)	Insert disclaimer	replacetext= The attachment file in the message has been removed by eManager.	<Key Name=”Remove”> <Value Name="EnableDisclaimer" string="" type="int" int="1" /> <Value Name="Disclaimer" string="The attachment file in the message has been removed by eManager." type="int" int="1" /> </Key>
Notification setting in [specialized filtering] in the contscan.ini file	InBoundNotify	Copy the value	
Notification setting in [specialized filtering] in the contscan.ini file	OutBoundNotify	Copy the value	

eManager Content Filter Notification

3.8x	6.0	3.8 Value	6.0 Value
Notification located in the section name which is the name in the policy; no distinction between inbound and outbound notifications			
warninguser warningsender warningrecipient	Enable/ Disable notification to administrator/ sender/ recipient	warninguser=yes warningsender=yes warningrecipient=yes	<key name=”Administrator”> <value name=”enable” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”enable” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”enable” string=”” type=”int” int=”1”/> … </key>
		warninguser=no warningsender=no warningrecipient=no	<key name=”Administrator”> <value name=”enable” string=”” type=”int” int=”0”/> … </key> <key name=”Sender”> <value name=”enable” string=”” type=”int” int=”0”/> … </key> <key name=”Recipient”> <value name=”enable” string=”” type=”int” int=”0”/> … </key>

3.8x	6.0	3.8 Value	6.0 Value
messageuser messagesender message recipient	Body	messageuser= Content filter has detected a sensitive email messagesenderr= Content filter has detected a sensitive email messagerecipient= Content filter has detected a sensitive email	<key name=”Administrator”> <value name=”Body” string=”Content filter has detected a sensitive e-mail” type=”string” int=”0”/> … </key> <key name=”Sender”> <value name=”Body” string=”Content filter has detected a sensitive e-mail” type=”string” int=”0”/> … </key> <key name=”Recipient”> <value name=”Body” string=”Content filter has detected a sensitive e-mail” type=”string” int=”0”/> … </key>
user subject (In [Content filter] in the “contscan. ini” file)	Subject	usersubject=Spam mail warning notification!	<key name=”Administrator”> <value name=”Subject” string=”Spam mail warning notification” type=”string” int=”0”/> … </key> <key name=”Sender”> <value name=”Subject” string=”Spam mail warning notification” type=”string” int=”0”/> … </key> <key name=”Recipient”> <value name=”Subject” string=”Spam mail warning notification” type=”string” int=”0”/> … </key>

3.8x	6.0	3.8 Value	6.0 Value
	ToUserType		<key name=”Administrator”> <value name=”ToUserType” string=”” type=”int” int=”0”/> … </key> <key name=”Sender”> <value name=”ToUserType” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”ToUserType” string=”” type=”int” int=”2”/> … </key>
	ShowFrom		<key name=”Administrator”> <value name=”ShowFrom” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”ShowFrom” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”ShowFrom” string=”” type=”int” int=”1”/> … </key>

3.8x	6.0	3.8 Value	6.0 Value
	ShowTo		<key name=”Administrator”> <value name=”ShowTo” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”ShowTo” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”ShowTo” string=”” type=”int” int=”1”/> … </key>
	ShowPolicy		<key name=”Administrator”> <value name=”ShowPolicy” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”ShowPolicy” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”ShowPolicy” string=”” type=”int” int=”1”/> … </key>

3.8x	6.0	3.8 Value	6.0 Value
	ShowAction		<key name=”Administrator”> <value name=”ShowAction” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”ShowAction” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”ShowAction” string=”” type=”int” int=”1”/> … </key>
	ToUserType		<key name=”Administrator”> <value name=”ToUserType” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=” ToUserType” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=” ToUserType” string=”” type=”int” int=”1”/> … </key>

3.8x	6.0	3.8 Value	6.0 Value
notification attachment (In [advanced options] in the “contscan.ini” file)	NotifyType	None	<value name=” NotifyType” string=”” type=”int” int=”0”/>
		Header	<value name=” NotifyType” string=”” type=”int” int=”1”/>
		All	<value name=” NotifyType” string=”” type=”int” int=”2”/>
		AllText	<value name=” NotifyType” string=”” type=”int” int=”3”/>

eManager Attachment Filter Notification

3.8x	6.0	3.8 Value	6.0 Value
Notification located in [specialized filtering], distinction is made between inbound and outbound notifications			
Warnadmin warnsender warnrecipient	Enable/ Disable administrator/ sender/ recipient notification	warnadmin=yes warnsender=yes warnrecipient=yes	<key name=”Administrator”> <value name=”enable” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”enable” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”enable” string=”” type=”int” int=”1”/> … </key>
		warnuser=no warnsender=no warnrecipient=no	<key name=”Administrator”> <value name=”enable” string=”” type=”int” int=”0”/> … </key> <key name=”Sender”> <value name=”enable” string=”” type=”int” int=”0”/> … </key> <key name=”Recipient”> <value name=”enable” string=”” type=”int” int=”0”/> … </key>

3.8x	6.0	3.8 Value	6.0 Value
messageuser messagesender message recipient	Body	messageuser= Content filter has detected a sensitive email messagesenderr= Content filter has detected a sensitive email messagerecipient= Content filter has detected a sensitive email	<key name=”Administrator”> <value name=”Body” string=”Content filter has detected a sensitive e-mail” type=”string” int=”0”/> … </key> <key name=”Sender”> <value name=”Body” string=”Content filter has detected a sensitive e-mail” type=”string” int=”0”/> … </key> <key name=”Recipient”> <value name=”Body” string=”Content filter has detected a sensitive e-mail” type=”string” int=”0”/> … </key>

3.8x	6.0	3.8 Value	6.0 Value
ioadmin iosender iorecipient	InBoundNotify OutBound Notify	ioadmin=both iosender=inbound iorecipient=outbound	<key name=”InBoundNotify”> <key name=”Administrator”> <value name=”Enable” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”Enable” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”Enable” string=”” type=”int” int=”0”/> … </key> </key> <key name=”OutBoundNotify”> <key name=”Administrator”> <value name=”Enable” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”Enable” string=”” type=”int” int=”0”/> … </key> <key name=”Recipient”> <value name=”Enable” string=”” type=”int” int=”1”/> … </key> </key>

3.8x	6.0	3.8 Value	6.0 Value
usersubject (In [Content filter] of the “contscan.ini” file)	Subject	usersubject=Spam mail warning notification!	<key name=”Administrator”> <value name=”Subject” string=”Spam mail warning notification” type=”string” int=”0”/> … </key> <key name=”Sender”> <value name=”Subject” string=”Spam mail warning notification” type=”string” int=”0”/> … </key> <key name=”Recipient”> <value name=”Subject” string=”Spam mail warning notification” type=”string” int=”0”/> … </key>
	ToUserType		<key name=”Administrator”> <value name=”ToUserType” string=”” type=”int” int=”0”/> … </key> <key name=”Sender”> <value name=”ToUserType” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”ToUserType” string=”” type=”int” int=”2”/> … </key>

3.8x	6.0	3.8 Value	6.0 Value
	ShowFrom		<key name=”Administrator”> <value name=”ShowFrom” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”ShowFrom” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”ShowFrom” string=”” type=”int” int=”1”/> … </key>
	ShowTo		<key name=”Administrator”> <value name=”ShowTo” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”ShowTo” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”ShowTo” string=”” type=”int” int=”1”/> … </key>

3.8x	6.0	3.8 Value	6.0 Value
	ShowPolicy		<key name=”Administrator”> <value name=”ShowPolicy” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”ShowPolicy” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”ShowPolicy” string=”” type=”int” int=”1”/> … </key>
	ShowAction		<key name=”Administrator”> <value name=”ShowAction” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=”ShowAction” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=”ShowAction” string=”” type=”int” int=”1”/> … </key>

3.8x	6.0	3.8 Value	6.0 Value
	ToUserType		<key name=”Administrator”> <value name=”ToUserType” string=”” type=”int” int=”1”/> … </key> <key name=”Sender”> <value name=” ToUserType” string=”” type=”int” int=”1”/> … </key> <key name=”Recipient”> <value name=” ToUserType” string=”” type=”int” int=”1”/> … </key>
notification attachment (In [advanced options] of the “contscan.ini” file)	NotifyType	None	<value name=” NotifyType” string=”” type=”int” int=”0”/>
		Header	<value name=” NotifyType” string=”” type=”int” int=”1”/>
		All	<value name=” NotifyType” string=”” type=”int” int=”2”/>
		AllText	<value name=” NotifyType” string=”” type=”int” int=”3”/>

Chapter 4

Default Values

The InterScan VirusWall 6 Web console provides different options to help you configure your ISVW installation according to your specifications.

This chapter is provided as a reference when there is an absolute need to modify certain configurations using the configuration files (intscan.ini and config.xml). Please note that certain default values should never be changed directly because they are derived from, or dependent upon, corresponding values. Changing these values, independent of their related contexts can result in invalid configurations and unexpected results.

Note: It is always good practice to back up the configuration files before you edit them.

This chapter contains a list of the InterScan VirusWall 6 configuration options. Each parameter is accompanied by an explanation, its default value, a list of any other possible values, and an explanation of the other possible values.

SMTP Anti-Spam

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\Enable	1	0, 1	Enable/Disable the SMTP anti-spam feature
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\WhiteList	N/A	String	SMTP anti-spam approved senders list
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\BlackList	N/A	String	SMTP anti-spam blocked senders list
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\WhiteKeyword	N/A	String	SMTP anti-spam exception keyword list
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\MostConfident Action	Stamp	Stamp, Delete, Quarantine, Deliver	SMTP anti-spam action for high confidence level messages
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\ConfidentAction	Stamp	Stamp, Delete, Quarantine, Deliver	SMTP anti-spam action for medium confidence level messages
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\LeastConfident Action	Stamp	Stamp, Delete, Quarantine, Deliver	SMTP anti-spam action for low confidence level messages
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\MostConfident Action\Stamp\StampText	Spam:	String	Stamp inserted into high confidence level mail subjects
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\ConfidentAction\ Stamp\StampText	Spam:	String	Stamp inserted into medium confidence level mail subjects
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\LeastConfident Action\Stamp\StampText	Spam:	String	Stamp inserted into low confidence level mail subjects

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\Notifications\ Administrator\Enable	0	0, 1	Enable/Disable SMTP notification sent to the administrator
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\Notifications\ Administrator\Body	A message sent from %SENDER% to %RCPTS% has been identified as spam. The message subject is "%SUBJECT%". InterScan VirusWall 6 has taken the action: %FINALACTION%	String	Body of the SMTP anti-spam notification email sent to the administrator
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\Notifications\ Recipient\Enable	0	0, 1	Enable/Disable SMTP notification sent to the recipient
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiSpam\Notifications\ Recipient\Body	Warning: InterScan VirusWall 6 has identified a message sent to you from %SENDER% as spam. The message subject is "%SUBJECT%". The message may not be delivered.	String	Body of the SMTP anti-spam notification email sent to the recipient

SMTP Virus/Spyware/IntelliTrap

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Enable	1	0, 1	Enable/Disable virus scan. If disabled, all VirusScan, IntelliTrap, and Anti-spyware filters will be disabled.
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ EnableVirusScan	1	0, 1	Enable/Disable virus scan
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ AddAlert	0	0, 1	Insert a virus alert in the message
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ AddInfo	1	0, 1	If enabled, inserts a disclaimer message in the user's mail
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Additional	1	0, 1	IF enabled, inserts an additional message in the user's mail
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ AdditionalMsg	Please contact the administrator for further information.	String	Shown as the last sentence of the warning message when 'Additional' is enabled and there are other messages inserted. This is inserted only once in the email.
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ CleanLayerExceedMsg	Warning: Your file, %CONTAINERNAME %, is infected with too many viruses. ISVW stopped attempting to clean them, and it still may contains some viruses	String	Related to MultipleCleanLayer. When the number of cleaning is beyond MultipleCleanLayer, the infected files may not be scanned entirely. This message will be inserted in the user's email.
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ CompressScan	1	0, 1	Enable/Disable scanning of compressed file/ attachment
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ EnableMailTrap	1	0, 1	Enable/Disable IntelliTrap

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ EnableSpywareScan	1	0, 1	Enable/Disable spyware scanning
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ EnableTrendExt	1	0, 1	If enabled and file/ attachment extension matches the scan engine's recommended extensions, the file/ attachment will be scanned
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ EnableUserExcludeExt	1	0, 1	If enabled and file/ attachment extension matches UserExcludeExtensions, the file/attachment will not be scanned. See also CheckExtension.
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ EnableUserExt	1	0, 1	If enabled and file/ attachment extension matches UserExtensions, the file/attachment will be scanned. See also CheckExtension.
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ IntelliScan	1	0, 1	If enabled, ISVW will try to scan file/attachment by true type, but not by extension
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ MailTrapAction	2	0, 2, 4	Select an IntelliTrap action: 0 (pass), 2 (quarantine), 4 (delete).
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ MaxDecompressCount	0	0~ 2148473647	ISVW will scan compressed files that do not exceed the value specified here
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ MaxDecompressDepth	20	1~20	ISVW will scan compressed files that do not exceed the value specified here
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ MaxDecompressRatio	0	0~100	ISVW will scan compressed files that do not exceed the value specified here

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ MaxDecompressSize	10485760	0~ 2148473647	ISVW will scan compressed files that do not exceed the value specified here
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ MaxEntityCount	50	10~ 2148473647	Limits the number of attachments to scan
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ MaxScanSize	0	0~ 2148473647	The maximum size of file/attachment VirusScan will process
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ MaxVirusCount	20	0~50	Number of viruses to display
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ MultipleClean	1	0, 1	If enabled, circularly checks and cleans virus in file/attachment
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ MultipleCleanLayer	5	2~ 2148473647	When a user sets the MultipleClean option, virus filter will loop clean the infected file until no more viruses can be cleaned. This option limits the loop count.
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ NoVirusAlert	0	0, 1	If enabled, inserts NoVirusMsg in the user's message when attachment contains no virus
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ NoVirusMsg	The file attachment, (%CONTAINER NAME%), has been scanned using antivirus software. No viruses were detected.	String	Displays if NoVirusAlert is enabled and the attachment has no virus. This is inserted for each email attachment.
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ ReplaceWarning	1	0, 1	If enabled, replaces the deleted attachment with the warning message

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ ReplaceWarningMsg	A file attached to this message, (%CONTAINER NAME%), was removed because it was infected with the %VIRUSNAME% computer virus.	String	If an attachment has been deleted, and ReplaceWarning is set to 1 (non-zero means enable), the attachment will be inserted in the user's message to replace the removed attachment
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ SafeStamp	0	0, 1	If enabled, inserts SafeStampMsg in the user's message
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ SafeStampMsg	InterScan VirusWall 6 has scanned this message and found it to be free of known viruses.	String	Displays when SafeStamp is enabled and a message is regarded as safe by virus filter. This is inserted once on the entire email.
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ ScanAll	1	0, 1	If enabled, every file/ attachment will be passed to the scan engine for scanning
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ ScanTypePolicy	1	1, 2, 3	Choose a scan policy: 1 (all scannable files), 2 (IntelliScan), 3 (scan based on file extensions)
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ SpywareAction	4	0, 2, 4	Spyware action: 0 (pass), 2 (quarantine), 4 (delete)
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ SpywareExcludeList	N/A	String	The file/attachment name that matches this setting will not be considered as spyware
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ SpywareTypes	255		Types of spyware to scan
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ UserExtensions	N/A		Extension list. Extension name is delimited by semicolon (for example, exe;zip;r??), and supports wildcards (* and ?). Do not insert any redundant space.

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ VirusAction	3	0, 2, 3, 4	Defines how to handle a file/attachment when virus is detected: 0 (pass), 2 (quarantine), 3 (clean), 4 (delete)
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ VirusAction2nd	4	0, 2, 4	Defines how to handle a file/attachment when cleaning failed: 0 (pass), 2 (quarantine), 4 (delete)
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ VirusAlert	InterScan VirusWall 6 has detected an item that contains a virus in this message.	String	Contained in the scan result and inserted in all attachments in the users' message
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Virus\Actions\Notification Admin\Enable	1	0, 1	If enabled, sends a notification email to the administrator
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Virus\Actions\Notification Admin\Body	Virus/malware was detected in a message sent from %SENDER% to %RCPTS% . The message subject is "%SUBJECT%". InterScan VirusWall 6 has taken the action: %FINALACTION%	String	Body of the notification email
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Virus\Actions\Notification Sender\Enable	0	0, 1	If enabled, sends a notification email to the sender
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Virus\Actions\Notification Sender\Body	Warning: InterScan VirusWall 6 has detected a virus in a message sent from your computer to %RCPTS%. The message subject is "%SUBJECT%". The message may not have been delivered.	String	Body of the notification email

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Virus\Actions\Notification Recipient\Enable	0	0, 1	If enabled, sends a notification email to the recipient
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Virus\Actions\Notification Recipient\Body	Warning: InterScan VirusWall has detected a virus in a message sent to you from %SENDER%. The message subject is %SUBJECT%. The message may not be delivered.	String	Body of the notification email
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\OutcomeMail Trap\Actions\Notification Admin\Enable	1	0, 1	If enabled, sends a notification email to the administrator
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\OutcomeMail Trap\Actions\Notification Admin\Body	IntelliTrap detected a potentially malicious application in a message sent from %SENDER% to %RCPTS%. The message subject is "%SUBJECT%". InterScan VirusWall 6 has taken the action: %FINALACTION%	String	Body of the notification email
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\OutcomeMail Trap\Actions\Notification Sender\Enable	0	0, 1	If enabled, sends a notification email to the sender
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\OutcomeMail Trap\Actions\Notification Sender\Body	Warning: IntelliTrap has detected a compressed file containing a malicious application in a message sent from your computer to %RCPTS%. The message subject is "%SUBJECT%". The message may not have been delivered.	String	Body of the notification email

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\OutcomeMail Trap\Actions\Notification Recipient\Enable	0	0, 1	If enabled, sends a notification email to the recipient
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\OutcomeMail Trap\Actions\Notification Recipient\Body	Warning: IntelliTrap has detected a compressed file containing a malicious application in a message sent to you from %SENDER%. The message subject is "%SUBJECT%". The message may not be delivered.	String	Body of the notification email
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Spyware\Actions\ NotificationAdmin\ Enable	1	0, 1	If enabled, sends a notification email to the administrator
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Spyware\Actions\ NotificationAdmin\Body	Spyware/grayware was detected in a message sent from %SENDER% to %RCPTS%. The message subject is "%SUBJECT%". InterScan VirusWall 6 has taken the action: %FINALACTION%	String	Body of the notification email
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Spyware\Actions\ NotificationSender\ Enable	0	0, 1	If enabled, sends a notification email to the sender

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Spyware\Actions\ NotificationSender\Body	Warning: InterScan VirusWall 6 has detected a spyware/ grayware application in a message sent from your computer to %RCPTS%. The message subject is "%SUBJECT%". The message may not have been delivered. Trend Micro suggests that you scan your computer for security risks.	String	Body of the notification email
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Spyware\Actions\ NotificationRecipient\ Enable	0	0, 1	If enabled, sends a notification email to the recipient
Smtp\Policies\Incoming\ Rule1\MailVirusScan\ Outcomes\Outcome Spyware\Actions\ NotificationRecipient\ Body	Warning: InterScan VirusWall 6 has detected a spyware/ grayware application in a message sent to you from %SENDER%. The message subject is "%SUBJECT%". The message may not be delivered.	String	Body of the notification email
Note: The Outgoing setting is the same as Incoming setting; the related key is under Smtp\Policies\Outcoming\.			

SMTP Content Filtering

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\Rule1\ MailContentScan\Enable	1	0, 1	Enable/Disable content filter

SMTP Anti-Phishing

Parameter	Default Value	Possible Values	Explanation
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiPhish\Enable	1	0, 1	Enable/Disable SMTP anti-phishing
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiPhish\AntiPhishAction	Quarantine	Quarantine, Deliver, Delete	SMTP anti-phishing action
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiPhish\Notifications\ Administrator\Enable	1	0, 1	Enable/Disable SMTP notification to the administrator
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiPhish\Notifications\ Administrator\Body	A phishing site was detected in a message sent from %SENDER% to %RCPTS% . The message subject is "%SUBJECT%". InterScan VirusWall 6 has taken the action: %FINALACTION%.	String	Body of the SMTP anti-phishing notification email sent to the administrator
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiPhish\Notifications\ Recipient\Enable	0	0, 1	Enable/Disable SMTP notification to the recipient
Smtp\Policies\Incoming\ Rule1\MailTMASEScan\ AntiPhish\Notifications\ Recipient\Body	Warning: InterScan VirusWall 6 has detected a phishing threat in a message sent to you from %SENDER%. The message subject is "%SUBJECT%". The message may not be delivered.	string	Body of the SMTP anti-phishing notification email sent to the recipient

SMTP Configuration

Parameter	Default Value	Possible Values	Explanation
Config.xml root/Smtp/AcceptAddress	Entered by user during installation	Domain names	Destination domains accepted by ISVW SMTP proxy
Config.xml root/Smtp/AntiRelay	1	0, 1	Enable/Disable the anti-relay function
Config.xml root/Smtp/ClientTimeout	120	60~180	Timeout for clients in network IO operations
Config.xml root/Smtp/EnableGreeting	1	0, 1	If enabled, sends the remote SMTP server's greeting message
Config.xml root/Smtp/IPAddressToBind	INADDR_ANY	Valid local addresses	Listening IP addresses
Config.xml root/Smtp/GetClientName WhenConnecting	0	0, 1	Performs DNS reverse lookup
Config.xml root/Smtp/LocalDomain	Null	Domain names	All local domain names
Config.xml root/Smtp/MaxDataSize	10240	0~102400	Maximum email size
Config.xml root/Smtp/MaxSimultaneous ClientConnections	500	0, 50~1000	Maximum simultaneous client connections
Config.xml root/Smtp/OriginalCommand	/usr/lib/ sendmail -bs	Valid program path	The sendmail program path
Config.xml root/Smtp/OriginalCommand Mode	0	0, 1	Enable/Disable command mode
Config.xml root/Smtp/OriginalProxy Address	Null	Valid SMTP server name or address	The SMTP server that will receive emails from ISVW
Config.xml root/Smtp/OriginalProxyPort	25	Valid port number	The SMTP server's service port

Parameter	Default Value	Possible Values	Explanation
Config.xml root/Smtp/SendNoopIntval	300	0~600	The interval for sending NOOP command to keep connections
Config.xml root/Smtp/ServerTimeout	180	60~180	Timeout for servers in network IO operations
Config.xml root/Smtp/ServicePort	25	Valid port number	Service port for the ISVW SMTP proxy
Config.xml root/Smtp/SessionTimeout	600	60~900	Timeout for client session
Config.xml root/Smtp/ShutdownTimeout	120	60~180	Timeout for servers in shutdown operation
Config.xml root/Smtp/SrcRelay	0	0, 1	Enable/Disable source relay
Config.xml root/Smtp/SrcRelayMeta	Null	ASCII characters	The characters set for the source relay
Config.xml root/Smtp/TempPath	Temp	Valid folder path	Path for the temp folder
Config.xml root/Smtp/ThreadPoolSize	20	1~200	Number of threads
Config.xml root/Smtp/WriteConnectionMsg	0	0, 1	Writes a connection message
Config.xml root/Smtp/MessageWhenReject	Unacceptable content	Valid messages for clients	Error messages sent to clients when message content is rejected
Config.xml root/Smtp/UseMemoryForScan	1	0, 1	Enable/Disable memory scan
Config.xml root/Smtp/Enable	1	0, 1	Enable/Disable ISVW SMTP proxy
Config.xml root/Smtp/AddrMapping/Enable	0	0, 1	Enable/Disable address mapping

Parameter	Default Value	Possible Values	Explanation
Config.xml root/Smtp/AddrMapping/ Count	5	1~5	Number of mapping items
Config.xml root/Smtp/AddrMapping/ Addr.1/Enable	0	0, 1	Enable/Disable mapping
Config.xml root/Smtp/AddrMapping/ Addr.1/SourceAddress	Null	Valid address or domain	Source address in mapping
Config.xml root/Smtp/AddrMapping/ Addr.1/ProxyAddress	Null	Valid address or domain	SMTP server in mapping
Config.xml root/Smtp/AddrMapping/ Addr.1/ProxyPort	25	Valid port number	Service port of the SMTP server in mapping

POP3 Virus/Spyware/IntelliTrap

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\ MainVirusScan\ Enable	1	0, 1	Enable/Disable virus scan. If disabled, all MacroScan, MailTrap, Anti-spyware, and Virus filters will be disabled.
Pop3\Policies\Rule1\ MailVirusScan\ AddAlert	1	0, 1	If enabled, inserts a VirusAlert or MacroStripAlert in the user's message
Pop3\Policies\Rule1\ MailVirusScan\ AddInfo	1	0, 1	If enabled, inserts a disclaimer message in the user's email
Pop3\Policies\Rule1\ MailVirusScan\ Additional	1	0, 1	If enabled, inserts an additional message in the user's message
Pop3\Policies\Rule1\ MailVirusScan\ AdditionalMsg	"Please contact the administrator for further information."	String	Shown as the last sentence of the warning message when 'Additional' is enabled and there are other messages inserted. This is inserted only once in the email.
Pop3\Policies\Rule1\ MailVirusScan\ CleanLayerExceed Msg	"Warning: Your file, %CONTAINER NAME%, is infected with too many viruses. ISVW-SE stopped attempting to clean them, and it still may contains some viruses"	String	Related to MultipleCleanLayer. When the number of cleaning is beyond MultipleCleanLayer, the infected files may not be scanned entirely. This message will be inserted in the user's email.
Pop3\Policies\Rule1\ MailVirusScan\ CompressScan	1	0, 1	Enable/Disable scanning of compressed file/attachment
Pop3\Policies\Rule1\ MailVirusScan\ EnableMailTrap	1	0, 1	If enabled, performs MailTrap scan
Pop3\Policies\Rule1\ MailVirusScan\ EnableSpywareScan	1	0, 1	If enabled, performs spyware scan
Pop3\Policies\Rule1\ MailVirusScan\ EnableTrendExt	1	0, 1	If enabled and file/attachment extension matches the scan engine recommended extensions, the file/ attachment will be scanned

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\ MailVirusScan\ EnableUserExclude Ext	1	0, 1	If enabled and file/attachment extension matches UserExcludeExtensions, the file/attachment will not be scanned. See also CheckExtension.
Pop3\Policies\Rule1\ MailVirusScan\ EnableUserExt	1	0, 1	If enabled and file/attachment extension matches UserExtensions, the file/ attachment will be scanned. See also CheckExtension.
Pop3\Policies\Rule1\ MailVirusScan\ EnableVirusScan	1	0, 1	If enabled, performs virus scan
Pop3\Policies\Rule1\ MailVirusScan\ IntelliScan	1	0, 1	If enabled, ISVW will try to scan file/attachment by true type, but not by extension
Pop3\Policies\Rule1\ MailVirusScan\Max DecompressCount	0	0~ 2148473647	ISVW will scan compressed files that do not exceed the value specified here
Pop3\Policies\Rule1\ MailVirusScan\ MaxDecompress Depth	20	1~20	ISVW will scan compressed files that do not exceed the value specified here
Pop3\Policies\Rule1\ MailVirusScan\ MaxDecompressSize	0	0~0x7fffffff	ISVW will scan compressed files that do not exceed the value specified here
Pop3\Policies\Rule1\ MailVirusScan\ MaxEntityCount	50	10~ 2148473647	ISVW will scan compressed files that do not exceed the value specified here
Pop3\Policies\Rule1\ MailVirusScan\ MaxScanSize	0	0~ 2148473647	The maximum size of file/attachment VirusScan will process
Pop3\Policies\Rule1\ MailVirusScan\ MaxVirusCount	20	0~50	The maximum number of viruses displayed; virus names beyond the limit will not display
Pop3\Policies\Rule1\ MailVirusScan\ MultipleClean	1	0, 1	If enabled, circularly checks and cleans file/attachment infected with virus

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\ MailVirusScan\ MultipleCleanLayer	2	0~ 2148473647	When a user sets the MultipleClean option, virus filter will loop clean the infected file until no more viruses can be cleaned. This option limits the loop count.
Pop3\Policies\Rule1\ MailVirusScan\ NoVirusAlert	1	0, 1	If enabled, inserts NoVirusMsg in the user's message when attachment contains no virus
Pop3\Policies\Rule1\ MailVirusScan\ NoVirusMsg	"The file attachment, (%CONTAINER NAME%) has been scanned using antivirus software. No viruses were detected"	string	Displays if NoVirusAlert is enabled and the attachment has no virus. This is inserted for each email attachment.
Pop3\Policies\Rule1\ MailVirusScan\ ReplaceWarning	1	0, 1	If enabled, replaces the deleted attachment with the warning message
Pop3\Policies\Rule1\ MailVirusScan\ ReplaceWarningMsg	"A file attached to this message, (%CONTAINER NAME%), was removed because it was infected with the %VIRUSNAME% computer virus."	String	If attachment has been deleted and ReplaceWarning is set to 1 (non-zero=enable), the message will be inserted in the user's message to replace the removed attachment
Pop3\Policies\Rule1\ MailVirusScan\ SafeStamp	1	0, 1	If enabled, inserts the SafeStampMsg in the user's message
Pop3\Policies\Rule1\ MailVirusScan\ SafeStampMsg	"This message was scanned for computer viruses using Trend Micro's ISVW-SE and is believed to not contain any viruses or malicious content."	string	Displays when SafeStamp is enabled and virus filter regards the email as safe. This is inserted only once in the email.
Pop3\Policies\Rule1\ MailVirusScan\ ScanAll	1	0, 1	If enabled, every file/ attachment will be passed to the scan engine for scanning. See also CheckExtension.

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\ MailVirusScan\ UserExclude Extensions	None	String	Extension list. Extension name is delimited by semicolon (for example, exe;zip;r??), and supports wildcards (* and ?). Do not insert any redundant space. See EnableUserExcludeExt.
Pop3\Policies\Rule1\ MailVirusScan\ UserExtensions	None	String	Extension list. Extension name is delimited by semicolon (for example, exe;zip;r??), and supports wildcards (* and ?). Do not insert any redundant space. See EnableUserExt.
Pop3\Policies\Rule1\ MailVirusScan\ VirusAlert	"The file, (%FILENAME%), was infected with the %VIRUSNAME% computer virus. The following action has been taken: %ACTION%."	String	Contained in the scan result and inserted in all attachments in the users' message

POP3 Configuration

Parameter	Default Value	Possible Values	Explanation
root/Pop3/IPAddressToBind	INADDR_ANY		Listening IP addresses
root/Pop3/MaxSimultaneous ClientConnections	100	1~100	Concurrent clients
root/Pop3/AllowLoginParameter	1	0, 1	Enable/Disable proxy mode
root/Pop3/InboundPort	110		Proxy mode listening port
root/Pop3/AllowServerPortMapping	0	0, 1	Enable/Disable port mapping
root/Pop3/ServerPortMappingCount	0		Number of mapped ports

POP3 Content Filtering

Parameter	Default Value	Possible Values	Explanation
config.xml Pop3/Policies/Rule1/ MailContentScan/Enable	1	1, 0	Enable POP3 content filtering

POP3 Anti-Phishing

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\ MailTMASEScan\ AntiPhish\Enable	1	0, 1	Enable/Disable POP3 anti-phishing
Pop3\Policies\Rule1\ MailTMASEScan\ AntiPhish\AntiPhishAction	Quarantine	Quarantine, Deliver, Delete	POP3 anti-phishing action
Pop3\Policies\Rule1\ MailTMASEScan\ AntiPhish\Notifications\ Administrator\Enable	1	0, 1	Enable/Disable POP3 notification to the administrator
Pop3\Policies\Rule1\ MailTMASEScan\ AntiPhish\Notifications\ Administrator\FromUser	Scanner@ISVW	String	Sender’s address for the notification email sent to the administrator
Pop3\Policies\Rule1\ MailTMASEScan\ AntiPhish\Notifications\ Administrator\Body	The message addressed to you, "%SUBJECT%" from "%SENDER%", has been identified as spam and quarantined. Contact the administrator to release it.	String	Body of the notification email sent to the administrator
Pop3\Policies\Rule1\ MailTMASEScan\ AntiPhish\Notifications\ Administrator\Charset	UTF-8	String	Character set of the notification email sent to the administrator

POP3 Anti-Spam

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\MailTMASEScan\AntiSpam\Enable	1	0, 1	Enable/Disable POP3 anti-spam
Pop3\Policies\Rule1\MailTMASEScan\AntiSpam\Blacklist	None	String	POP3 anti-spam blocked senders list
Pop3\Policies\Rule1\MailTMASEScan\AntiSpam\Whitelist	None	String	POP3 anti-spam approved senders list
Pop3\Policies\Rule1\MailTMASEScan\AntiSpam\WhiteKeyword	None	String	POP3 anti-spam exception list
Pop3\Policies\Rule1\MailTMASEScan\AntiSpam\MostConfidentAction	Stamp	Stamp, Delete, Deliver, Quarantine	POP3 anti-spam action for most confident spam
Pop3\Policies\Rule1\MailTMASEScan\AntiSpam\ConfidentAction	Stamp	Stamp, Delete, Deliver, Quarantine	POP3 anti-spam action for confident spam
Pop3\Policies\Rule1\MailTMASEScan\AntiSpam\LeastConfidentAction	Stamp	Stamp, Delete, Deliver, Quarantine	POP3 anti-spam action for least confident spam
Pop3\Policies\Rule1\MailTMASEScan\AntiSpam\Notifications\Administrator\Enable	1	0, 1	Enable/Disable POP3 notification to the administrator
Pop3\Policies\Rule1\MailTMASEScan\AntiSpam\Notifications\Administrator\FromUser	Scanner@ISVW	String	Sender's address for the notification email sent to the administrator
Pop3\Policies\Rule1\MailTMASEScan\AntiSpam\Notifications\Administrator\Body	The message addressed to you, "%SUBJECT%" from "%SENDER%", has been identified as spam and quarantined. Contact the administrator to release it.	String	Body of the notification email sent to the administrator

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\Mail TMASEScan\AntiSpam\ Notifications\ Administrator\Charset	UTF-8	String	Character set of the notification email sent to the administrator
Pop3\Policies\Rule1\Mail TMASEScan\AntiSpam\ Notifications\ Administrator\Subject	Spam email was identified.	String	Subject of the notification email sent to the administrator

FTP Virus Scanning

Parameter	Default Value	Possible Values	Explanation
root\Ftp\Policies\ Rule1\FileVirusScan\ EnableVirusScan	1	1, 0	Enable/Disable FTP virus scanning
root\Ftp\Policies\ Rule1\FileVirusScan\ EnableMailTrap	1	1, 0	Enable/Disable FTP virus scanning
root\Ftp\Policies\ Rule1\FileVirusScan\ EnableFileTypeBlock	0	1, 0	Enable/Disable FTP file type blocking
root\Ftp\Policies\ Rule1\FileVirusScan\ FileTypeBlockinglist	[Empty]	4004, 4020, 4028, 4031, 6014, 6, 10, 4021, 4022, 22, 2001, 4002, 4024, 4026, 4027, 6005, 9, 11, 13, 14, 20, 25, 2000, 2003, 4003, 4030, 4005, 4005, 5, 4006, 4007, 4008, 4009, 4010, 4014, 4015, 4016, 4017, 4018, 7, 24, 2005, 6002, 1, 4029, 2, 4, 16, 17, 26, 30, 4025, 1, 4029, 4033, 6001, 6004, 6007, 6008, 6015	File types to block; each number represents a file type
root\Ftp\Policies\ Rule1\FileVirusScan\ ScanTypePolicy	1	1, 2, 3	Defines how ISVW will scan files: 1 (All scannable files), 2 (IntelliScan), 3 (Specified file extensions...)
root\Ftp\Policies\ Rule1\FileVirusScan\ UserExtensions	[Empty]	File extensions separated by a semicolon (;). For example, lll;kkk;vvv	User defined extensions; only works when the value of ScanTypePolicy is 3

Parameter	Default Value	Possible Values	Explanation
root\Ftp\Policies\ Rule1\FileVirusScan\ Compresscan	1	1, 0	Defines how compressed files are handled: 1 (Scan all compressed files or Do not scan compressed files if), 0 (Do not scan compressed files)
root\Webui\Ftp\ BlockMethod	BlockNone	BlockNone, BlockAll, BlockIf	Defines how compressed files are handled: BlockNone (Scan all compressed files), BlockAll (Do not scan compressed files), BlockIf (Do not scan compressed file if)
root\Ftp\Policies\ Rule1\FileVirusScan\ MaxDecompressCount	0	0 to 2147483647	ISVW will scan compressed files that do not exceed the value specified here
root\Ftp\Policies\ Rule1\FileVirusScan\ MaxDecompressDepth	20	2 to 20	ISVW will scan compressed files that do not exceed the value specified here
root\Ftp\Policies\ Rule1\FileVirusScan\ MaxDecompressRatio	0	0 to 100	ISVW will scan compressed files that do not exceed the value specified here
root\Ftp\Policies\ Rule1\FileVirusScan\ MaxDecompressSize	2147483647	0 to 2147483647	ISVW will scan compressed files that do not exceed the value specified here
root\Ftp\Policies\ Rule1\FileVirusScan\ VirusAction	3	2, 3, 5, 0	The first action on files infected with a virus: 3 (Clean), 2 (Quarantine), 5 (Block), 0 (Pass)
root\Ftp\Policies\ Rule1\FileVirusScan\ VirusAction2nd	5	2, 5, 0	The second action on files infected with a virus (only works when "virusAction=3"): 2 (Quarantine), 5 (Block), 0 (Pass)

Parameter	Default Value	Possible Values	Explanation
root\Ftp\Policies\ Rule1\FileVirusScan\ UserNotifSpyware	Trend Micro InterScan VirusWall 6 has determined that the file you are attempting to transfer contains spyware/grayware. It has taken action on the file.	Spyware notification message on the FTP client	Spyware notification message on the FTP client
root\Ftp\Policies\ Rule1\FileVirusScan\ UserNotifVirus	Trend Micro InterScan VirusWall 6 has determined that the file you are attempting to transfer is infected. It has taken action on the file.	Virus notification message on the FTP client	Virus notification message on the FTP client
root\Ftp\Policies\ Rule1\FileVirusScan\ UserNotifFileType Block	Trend Micro InterScan VirusWall 6 has determined that the file you are attempting to transfer triggered file type blocking policy. It has taken action on the file.	File type blocking notification message on the FTP client	File type blocking notification message on the FTP client

FTP Anti-Spyware

Parameter	Default Value	Possible Values	Explanation
root\Ftp\Policies\ Rule1\FileVirusScan\ EnableSpywareScan	1	1, 0	Enable/Disable FTP anti-spyware
root\Ftp\Policies\ Rule1\FileVirusScan\ SpywareExcludeList	[empty]	String, for example, file1/ file2/*.exe1/ *.exe2/etc	The file/attachment name that matches this setting will not be considered as spyware
root\Ftp\Policies\ Rule1\FileVirusScan\ SpywareTypes	255	0 to 255	Types of spyware to scan: 1 (spyware), 2 (adware), 4 (dialers), 16 (joke programs), 8 (hacker tools), 32 (remote access tools), 64 (password), 128 (others), 0 (none selected), 255 (all types of spyware)
root\Ftp\Policies\ Rule1\FileVirusScan\ SpywareAction	2	0, 2, 5	Spyware action: 2 (Quarantine), 5 (Block), 0 (Pass)

FTP Configuration

Parameter	Default Value	Possible Values	Explanation
root/Ftp/svcport	21	1 to 65535	FTP listening port for ISVW
root/Ftp/self_proxy	No	Yes, No	If yes, ISVW will act as a direct FTP proxy. If no, ISVW will act as a sentry, standing guard in front of a specific server within the LAN.
root/Ftp/FTPlocation	[Empty]	FTP server's IP and port or local daemon FTP program path (for example, "192.168.5.161 21" or "/usr/bin/vsftpd")	FTP server location; only applicable if "self_proxy=yes"
root/Ftp/greeting	Yes	Yes, No	If yes, sends a greeting message to the FTP client when FTP connection is established
root/Ftp/log_trans	Yes	Yes, No	If yes, logs transaction history
root/Ftp/addr_to_host	Yes	Yes, No	If yes, reverses the FTP client's IP address to the host name. Information is recorded in the connection log.
root/Ftp/Cli_timeout	120	60 to 180	Client connection timeout
root/Ftp/srv_timeout	180	60 to 180	Server connection timeout
root/Ftp/write_timeout	600	60 to 900	Write data timeout
root/Ftp/idle_kill	3600	0, 30 to 7200	Child process will terminate after being idle for X seconds. '0' means child processes will never terminate.
root/Ftp/max_proc	25	0 to 100	The maximum number of child processes. '0' means no limitation.
root/Ftp/thr_per_proc	5	1 to 20	The maximum number of threads for each child process

Parameter	Default Value	Possible Values	Explanation
root/Ftp/pro_max_reqs	500	0 to 9999	The child processes will restart after X number of connections. '0' means never restart.
root/Ftp/dead_time	8	1 to 20	The child processes will die if there are no responses within X minutes.

HTTP

Parameter	Default Value	Possible Values	Explanation
Http\Main\http\ virus_scan_ enabled=yes\no	Yes	Yes, No	Enable/Disable virus scan
Http\Main\ scan_configuration\ enable_true_file_ type_block=no \Http\main\ scan_configuration\ block_types=Null	No Null	Yes, No Null\int type value according to the file types set in the Web console	Defines file types to block
Http\Plugin\Scan Vsapi\http\level	scanall	scanall, scanintelli, scanext	scanall: scans all HTTP traffic scanintelli: the scan engine decides which files to scan based on TrueFileType scanext: scans only files with certain extensions
Http\Plugin\ ScanVsapi\http\ extensions		Extension list	The default list of extensions to scan if level is set to "scanext". Items should be separated with a semicolon (;).
Http\Main\ scan_configuration\ compress_flag	Yes	Yes, No	If yes, scans all compressed files
Http\main\http\ skiptype		A list of MIME types	Provides better performance but less security since the content-type header may not truly represent the type of the content
Http\Main\scan\ scan_huge_file	Yes	Yes, No	Enable/Disable scanning of large files. If set to 'Yes' then no files larger than max_scan_size will be scanned.
Http\Main\scan\ max_scan_size	1048576	Large file size	The file size limitation of scanned files, in KB
Http\Main\scan\ special_handling	Yes	Yes, No	Enable/Disable “deferred” or “scan-behind” scan when a file is larger than the file size limitation

Parameter	Default Value	Possible Values	Explanation
Http\Main\scan\ deferred_scanning	Yes	Yes, No	Setting for deferred scanning
Http\Main\scan\ max_synchronous_ scan_size	524288	File size for deferred scan setting	File size for deferred scanning
Http\Main\http\action	Clean	Clean, Move, Delete, Pass	Clean: cleans the file then continue the transfer, if it is cleanable. If uncleanable, 'ucaction' must be set. 'ucaction' can be pass, move or delete. The default value is delete. Move: moves the data into a temporary file on proxy host Delete: blocks the transfer Pass: sends data to the user
Http\Main\http\ ucaction	Delete	Move, Delete, Pass	'ucaction' can be pass, move or delete. The default value is delete.
Http\Main\http\ movedir	\opt\trend\isvw6\ quarantine\http	Directory path	The quarantine directory
Http\Main\http\ virus_notification	Trend Micro InterScan VirusWall 6 has determined that the file you are attempting to transfer is infected. It has taken action on the file.	String	Notification displayed when virus is detected
Webui\HTTP\ Antiphish\Enable	Yes	Yes, No	Enable/Disable HTTP anti-phishing

Parameter	Default Value	Possible Values	Explanation
Http\Main\http\ phish_notification	The URL you are attempting to access may redirect you to a site to collect your confidential and personal data. Access to this URL has been blocked for security reasons. If you have any questions, contact your administrator.	String	Notification displayed when URL access is blocked by PhishTrap
Webui\HTTP\ Antiphish\ BlockAccess	Yes	Yes, No	If yes, blocks access to phishing sites
Http\Main\http\ spyware_scan_ enabled	Yes	Yes, No	Enable/Disable spyware scan
Http\Main\http\ spyware_scan_type	255	The number corresponding to the selected spyware scan type	Spyware type to scan
Http\Main\http\ spyaction	Delete	Move, Pass, Delete	Actions on detected spyware
Http\Main\http\ spyware_notification	Trend Micro InterScan VirusWall 6 has determined that the file you are attempting to transfer contains spyware\graywar e. It has taken action on the file.	String	Notification displayed when spyware is detected
Http\Main\http\url_ blocking_enabled	Yes	Yes, No	Enable/Disable URL blocking

Parameter	Default Value	Possible Values	Explanation
Http\Main\http\ reject_notification	The URL you are attempting to access has been blocked. Organization policy prohibits accessing this type of site. If you have any questions, contact your administrator.	String	Notification displayed when attempting to access a blocked URL
Http\Plugin\URL Filter\plug-in\enable	No	Yes, No	Enable/Disable HTTP URL filtering
Http\Main\Policy\ WorkTime_Day	value=0111110		Work time settings
Http\Main\Policy\ WorkTime_AM_Start	0900 (start time is 9:00 am)	0600, 0630, 0700, 0730, 0800, 0830, 0900, 0930, 1000	Work time start, A.M.
Http\Main\Policy\ WorkTime_AM_End	1200 (end time is 12:00 am)		Work time end, A.M.
Http\Main\Policy\ WorkTime_PM_Start	1300		Work time start, P.M.
Http\Main\Policy\ WorkTime_PM_End	1800		Work time end, P.M.
Http\Main\http\ urlf_notification	The URL you are attempting to access has been blocked. Organization policy prohibits accessing this type of site. If you have any questions, contact your administrator.	String	Notification displayed when attempting to access a blocked URL

Parameter	Default Value	Possible Values	Explanation
\Http\Protocol\ HttpProxy\http\ self_proxy	Yes	Yes, No	If yes, ISVW will act as a direct HTTP proxy (Browser > ISVW > Web server). If no, ISVW will act as a dependent proxy (Browser > ISVW > Upstream HTTP proxy > Web server). If set to "No" you must specify the upstream proxy's name and port number in original_server and original_server_port, respectively.
\Http\Protocol\ HttpProxy\http\ original_server		IP address or host name	original_server indicates the name of the upstream HTTP proxy server that ISVW will pass traffic through if it is installed in dependent mode
\Http\Protocol\ HttpProxy\http\ original_server_port	Null	Port number	original_server_port contains the port number that the upstream HTTP proxy server is listening to for HTTP traffic
\Http\Protocol\ HttpProxy\http\ reverse_proxy	No	Yes, No	Checked when self_proxy value is no. If yes, reverse proxy mode is activated, the original server/port will be used as an ordinary HTTP server, not an upstream proxy.
\Http\Protocol\ HttpProxy\http\ anonymous_ftp_ mail_address		Anonymous FTP mail address	anonymous_ftp_mail_address indicates the email address ISVW should supply when connecting anonymously to an FTP server for FTP-over-HTTP requests
\Http\Protocol\ HttpProxy\main\port	8080	1~65535	HTTP service port of ISVW
\Http\Main\internet-accessmonitoring\ enable	No	Yes, No	Enable/Disable access log

Outbreak Prevention Services

Parameter	Default Value	Possible Values	Explanation
Config.xml root/Common/ActiveUpdate/ Server.3/Source	http://oc.activeupdate. trendmicro.com/ activeupdate/isvw	Real TrendLabs OPS update URL	OPS ActiveUpdate server
Config.xml root/Common/Schedule Update/OPSUpdate/ EnableUpdate	1	0, 1	Enable/Disable ScheduleUpdate
Config.xml root/Common/Schedule Update/OPSUpdate/Minutes	10	1, 5, 10, 30, 60, 120	Scheduled update interval
Config.xml root/Scan/OPP/Enable	0	0, 1	Enable/Disable OPS filter
Config.xml root/Scan/OPP/ActiveOPPID		OPPID from OPS policy	Generated by TrendLabs
Config.xml root/Scan/OPP/IssueDuration	2880	1440 * (1, 2, 3, 4, 5)	OPS expiration

Logs

Parameter	Default Value	Possible Values	Explanation
Common\Logging\LogDir	log		The relative path of log files; cannot be modified from the Web console
Common\Logging\ EnableMaintenance	1	0, 1	Enable/Disable automatic log maintenance
Common\Logging\ WhatMaintenance	63 (All types of logs)	Options on the Web console	Logs > Maintenance > Automatic > Target
Common\Logging\ ExpiredDays	30	0~360	Logs > Maintenance > Automatic > Action
Common\Logging\ DebugEnable	0	0, 1	Enable/Disable debug log
Webui\Log\Query\protocol	1 (SMTP)	Options on the Web console	Logs > Query > Protocol
Webui\Log\Query\logtype	1 (Virus/Malware)	Options on the Web console	Logs > Query > Log type
Webui\Log\Query\ timeperiod	1 (All)	Options on the Web console	Logs > Query > Time period
Webui\Log\Query\ ItemPerPage	25	10, 25, 50, 00	Logs > Query > Entries per page
Webui\Log\Maintenance\ Manual\Action	1 (Delete all logs older than X days)	Options on the Web console	Logs > Maintenance > Manual > Action
Webui\Log\Maintenance\ Manual\LogTypes	63 (All types of logs)	Options on the Web console	Logs > Maintenance > Manual > Target
Webui\Log\Maintenance\ Manual\LogChoice	All (All types of logs)	Options on the Web console	Logs > Maintenance > Manual > Target
Webui\Log\Maintenance\ Manual\ExpiredDays	30	0~360	Logs > Maintenance > Manual > Action
Webui\Log\Maintenance\ Auto\Enable	1	0, 1	Enable/Disable automatic log maintenance
Webui\Log\Maintenance\ Auto\Action	1 (Delete all logs older than X days)	Options on the Web console	Logs > Maintenance > Automatic > Action
Webui\Log\Maintenance\ Auto\LogTypes	63 (All types of logs)	Options on the Web console	Logs > Maintenance > Automatic > Target

Parameter	Default Value	Possible Values	Explanation
Webui\Log\Maintenance\ Auto\ExpiredDays	30	0~360	Logs > Maintenance > Automatic > Action
Webui\Log\Maintenance\ Auto\LogChoice	All (All types of logs)		Logs > Maintenance > Automatic > Target

Quarantine

Parameter	Default Value	Possible Values	Explanation
Webui\Quarantine\ Maintenance\ ManualDelete	7	0~360	Quarantines > Maintenance > Manual > Action
Webui\Quarantine\ Move\MoveDirectory	/tmp	Can be assigned from the Web console	Quarantines > Query > Move

ActiveUpdate

Parameter	Default Value	Possible Values	Explanation
Root\Common\ActiveUpdate\UpdateServers\Server.1\Source	http://isvw-av.activeupdate.trendmicro.com/activeupdate/	AU Server URL	AU server for updating the virus/spyware patterns and engines
Root\Common\ActiveUpdate\UpdateServers\Server.1\UseProxy	0	0, 1	Enable/Disable update through proxy
Root\Common\ActiveUpdate\UpdateServers\Server.2\Source	http://isvw-as.activeupdate.trendmicro.com/activeupdate/	AU server URL	AU server for updating the spam pattern and engine
Root\Common\ActiveUpdate\UpdateServers\Server.2\UseProxy	0	0, 1	Enable/Disable update through proxy
Root\Common\ActiveUpdate\UpdateServers\Server.3\Source	http://oc.activeupdate.trendmicro.com/activeupdate/	AU Server URL	AU server for updating the OPP pattern
Root\Common\ActiveUpdate\UpdateServers\Server.3\Source	0	0, 1	Enable/Disable update through proxy
Root\common\ActiveUpdate\ScheduleUpdate\virusUpdate\EnableUpdate	1	0, 1	Enable/Disable scheduled update
Root\common\ActiveUpdate\ScheduleUpdate\virusUpdate\EnableItems	2047	1, 2, 4, 8, 48, 192, 1792, or the sum of all or several of these numbers	Enable scheduled update for selected items
Root\common\ActiveUpdate\ScheduleUpdate\virusUpdate\Type	3	1~3	Virus type