



Virtual AutumnTECH Appliance



Use and Administration Guide v1.5.1

Updated September 7, 2012

COPYRIGHT

Copyright 2012 AutumnTECH, LLC

All rights reserved. Printed in the U.S.A.

This manual and any associated artwork, software and product designs are copyrighted with all rights reserved. Under the copyright laws such materials may not be copied, in whole or part, without the prior written consent of AutumnTECH, LLC. Under the law, copying includes translation to another language or format.

AutumnTECH, LLC

www.AutumnTECH.com

Support@AutumnTECH.com

Part Number

For additional copies of this electronic manual, order AutumnTECH part number SFH/ManPDF. E-mail your request to Sales@AutumnTECH.com

Printed copies

For printed copies of this manual, order part number SFH/ManDoc (P/N 9980-0001) E-mail requests for printed copies to Sales@AutumnTECH.com. A \$15 shipping and handling fee payable to AutumnTECH, LLC is required.

GPL License Information

AutumnTECH appliances are distributed with GPL licensed software. To request copies of the current GPL source code, send an e-mail request to Support@AutumnTECH.com

CONTENTS

Welcome to the Virtual AutumnTECH *User's Reference Guide*. This guide is designed to be your single source for information about your Virtual appliance. It is intended to be viewed on-line, using Adobe Acrobat Reader. The information displayed has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you're performing.

Disclaimer

END-USER LICENSE AGREEMENT FOR AUTUMNTECH SOFTWARE

IMPORTANT-READ CAREFULLY: This AUTUMNTECH End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and AUTUMNTECH LLC for the AUTUMNTECH software product identified above, which includes computer software and associated media and printed materials, and may include "online" or electronic documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA; promptly return the unused SOFTWARE PRODUCT to the place from which you obtained it for a full refund; or if you received the SOFTWARE PRODUCT as part of a subscription or other service from AUTUMNTECH, you may cancel the subscription and receive a pro rata portion of the subscription price.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. This EULA grants you the following limited, non-exclusive rights: Software Product. You may install and use one running instance of the SOFTWARE PRODUCT on one computer. Each concurrent instance of SOFTWARE PRODUCT requires a separate license available for purchase at <http://www.AutumnTECH.com>. You may not copy the SOFTWARE PRODUCT. You may redistribute the SOFTWARE PRODUCT if you are an Authorized AutumnTECH Reseller and the reseller contract is valid and in full compliance at the time of the distribution.

2. COPYRIGHT. All rights, title, and copyrights in and to the SOFTWARE PRODUCT (including, but not limited to, any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT) and any copies of the SOFTWARE PRODUCT are owned by AUTUMNTECH or its suppliers. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material, except that you may either (a) make one copy of the SOFTWARE PRODUCT solely for backup or archival purposes or (b) install the SOFTWARE PRODUCT on a single computer, provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying the SOFTWARE PRODUCT.

3. PRERELEASE CODE. The SOFTWARE PRODUCT may contain PRERELEASE CODE that is not at the level of performance and compatibility of the final, generally available, product offering. These portions of the SOFTWARE PRODUCT may not operate correctly and may be substantially modified prior to first commercial shipment. AUTUMNTECH is not obligated to make this or any later version of the SOFTWARE PRODUCT commercially available.

4. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Limitations on Reverse-Engineering, Decompilation, and Disassembly. You may not reverse-engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

Rental. You may not rent or lease the SOFTWARE PRODUCT.

Software Transfer. You may not transfer any right under this EULA unless you are an Authorized AutumnTECH Reseller and the reseller contract is valid and in full compliance at the time of the transfer.

Termination. Without prejudice to any other rights, AUTUMNTECH may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

5. EXPORT RESTRICTIONS. You agree that neither you nor your customers intend to or will, directly or indirectly, export or transmit (a) the SOFTWARE PRODUCT or related documentation and technical data, or (b) your Application as described in Section 1 of this EULA (or any part thereof), or process, or service that is the direct product of the SOFTWARE PRODUCT to any country to which such export or transmission is restricted by any applicable U.S. regulation or statute, without the prior written consent, if required, of the Bureau of Export Administration of the U.S. Department of Commerce, or such other governmental entity as may have jurisdiction over such export or transmission.

6. U.S. GOVERNMENT RESTRICTED RIGHTS. The SOFTWARE PRODUCT and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is AUTUMNTECH™ LLC

7. AUTUMNTECH appliances are distributed with GPL licensed software. To request copies of the current GPL source code, send a e-mail request to Support@AutumnTECH.com AUTUMNTECH makes no claim of ownership for included GPL licensed software which is excluded from copyright notices posted for SOFTWARE PRODUCT. You are free to distribute GPL licensed software in accordance with the licensing terms found at <http://www.gnu.org/licenses/licenses.html>

MISCELLANEOUS

This EULA is governed by the laws of the State of Maryland.

Should you have any questions concerning this EULA, or if you desire to contact AUTUMNTECH for any reason? Please contact the AUTUMNTECH subsidiary serving your country, or e-mail Support@AutumnTECH.com

NO WARRANTIES. To the maximum extent permitted by applicable law, AUTUMNTECH expressly disclaims any warranty for the SOFTWARE PRODUCT. The SOFTWARE PRODUCT and any related documentation are provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties of merchantability or fitness for a particular purpose. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you.

LIMITATION OF LIABILITY. AUTUMNTECH's entire liability and your exclusive remedy under this EULA shall not exceed five dollars (US\$5.00).

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. To the maximum extent permitted by applicable law, in no event shall AUTUMNTECH or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profit, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of, or inability to use, this AUTUMNTECH product, even if AUTUMNTECH has been advised of the possibility of such damages. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

Table of Contents

Chapter 1: Introduction

Welcome

Installing Virtual AutumnTECH

Starting Virtual AutumnTECH for the First Time

Chapter 2: Configuring

Quick Start Configuration Wizard

Webtivity the Web-Based Management Utility

- Home
- General
- Advanced
- Updates
- Help

Chapter 3: Filtering

Chapter 4: Backup and Recovery

Chapter 5: Support

Chapter 1: Introduction

Welcome

Thank you for choosing the Virtual AutumnTECH appliance. This solution provides your network with a highly effective way to filter spam and stop most e-mail viruses while saving expensive bandwidth. How is this done? Inside this Virtual appliance you have powerful applications specifically designed to perform these duties. But what does all of this mean? At the core of this virtual appliance is a UNIX-like operating system security-hardened by a team of Certified Information Systems Security Professionals (CISSP).

Operating System

When choosing a hardware appliance that performs activities such as spam fighting and e-mail virus blocking, one of the most important aspects to consider is the underlying operating system. AutumnTECH appliances run the OpenBSD UNIX-like operating system. OpenBSD is widely known for its unparalleled attention to security. In eight years, OpenBSD has only seen one remote security hole in the default install.

E-Mail Server

AutumnTECH integrates the open-source project Postfix into our appliances. Postfix is a fully scalable and highly secure email system. We've included tools to block dangerous attachments at the MTA level, block e-mail sent from any number of block lists, absolutely deny any relay of e-mail other than to specified domains, and more.

Spam Identification

AutumnTECH integrates the open-source project Spamassassin™ into our appliances. Spamassassin is an extensible email filter which is used to identify spam. Using its rule base, it uses a wide range of advanced heuristic and statistical analysis tests on mail headers and body text to identify "spam", also known as unsolicited bulk email. The spam-identification tactics used include:

- **header analysis:** spammers use a number of tricks to mask their identities, fool you into thinking they've sent a valid mail, or fool you into thinking you must have subscribed at some stage. Spamassassin tries to spot these.
- **text analysis:** again, spam mails often have a characteristic style (to put it politely), and some characteristic disclaimers and CYA text. Spamassassin can spot these, too.
- **blacklists:** Spamassassin supports many useful existing blacklists, such as mail-abuse.org, ordb.org, SURBL, and others.
- **learning classifier:** Spamassassin uses a Bayesian-like form of probability-analysis classification, so that a user can train it to recognize mails similar to a training set.

In addition to Spamassassin, AutumnTECH integrates the open-source spam-fighting project **Greylisting**. Greylisting is a new method of blocking significant amounts of spam at the mailserver level, but without resorting to heavyweight statistical analysis or other heuristical approaches. Consequently, implementations are fairly lightweight, and may even decrease network traffic and processor load on your mailserver. Greylisting relies on the fact that most spam sources do not behave in the same way as "normal" mail systems.

Virus Blocker

AutumnTECH integrates the open-source project ClamAV into our appliances. ClamAV detects hundreds of thousands of viruses, worms, and Trojans. ClamAV supports archives and compressed files, detects Microsoft Office and MacOffice macro viruses, built-in support for RAR (2.0), Zip, Gzip, Bzip2 and others, built-in protection against archive bombs, and includes a database updater with support for digital signatures. Virtual AutumnTECH appliances perform hourly updates to the local ClamAV antivirus database file. When a virus is detected, the message is dropped and an e-mail alert is sent to the original recipient.

Webtility Management

In order to simplify the management of the projects described above, AutumnTECH has built a simple, web-based application that we call "Webtility". Webtility allows you to control services, modify messaging handling rules, update spam thresholds, reboot the appliance, backup/restore/update and more. Access to Webtility is done through a standard web browser and is secured by a username and password.

OPTIONAL SOFTWARE: To get the most out of your new virtual appliance, you'll need a SYSLOG Service running in your network.

Recommended:

- Syslog Daemon: www.kiwisyslog.com

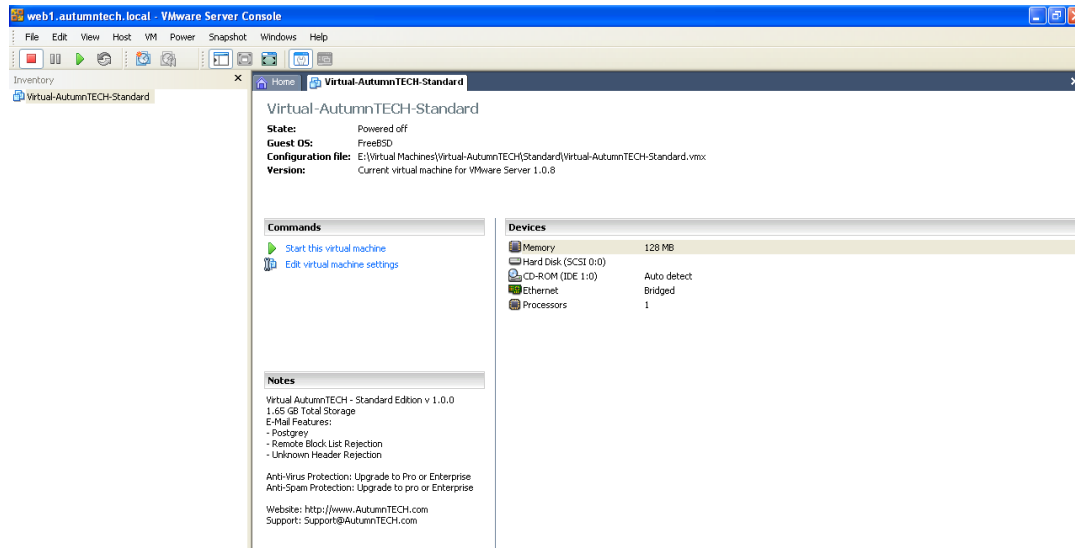
Installing Virtual AutumnTECH

Installing Virtual AutumnTECH could not be easier. Your order will include a download link that will point you to a .zip file for extracting the Virtual AutumnTECH VMware® files in UNIX and PC environments.

Once your download is installed and/or extracted, open your VMware® console. Virtual AutumnTECH was compiled on VMware® Server v 1.0.8 and was tested to work inside of all of the VMware® products including Player, Workstation, Server, and ESXi.

To get started quickly, we recommend VMware® player which at the time of publication was free and available for download at:

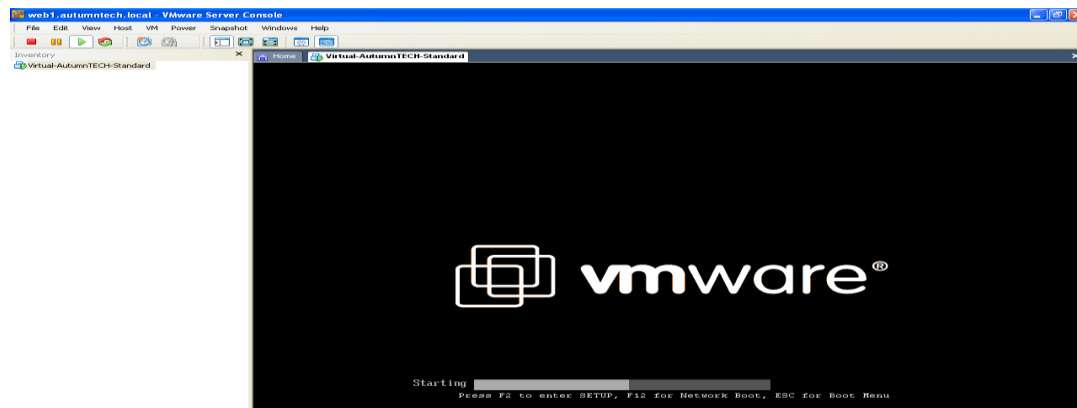
- <http://www.vmware.com/products/player/>



Starting Virtual AutumnTECH for the First Time

Open and select the Virtual AutumnTECH vmx file that was included in the download. This file contains the configuration instructions for VMware®. You may edit the configuration; supported editing includes increasing or decreasing the physical memory allocated to Virtual AutumnTECH.

Click “Start the Virtual Machine” to get Virtual AutumnTECH running.



The Virtual AutumnTECH startup screen

Webtivity the Web-Based Management Utility

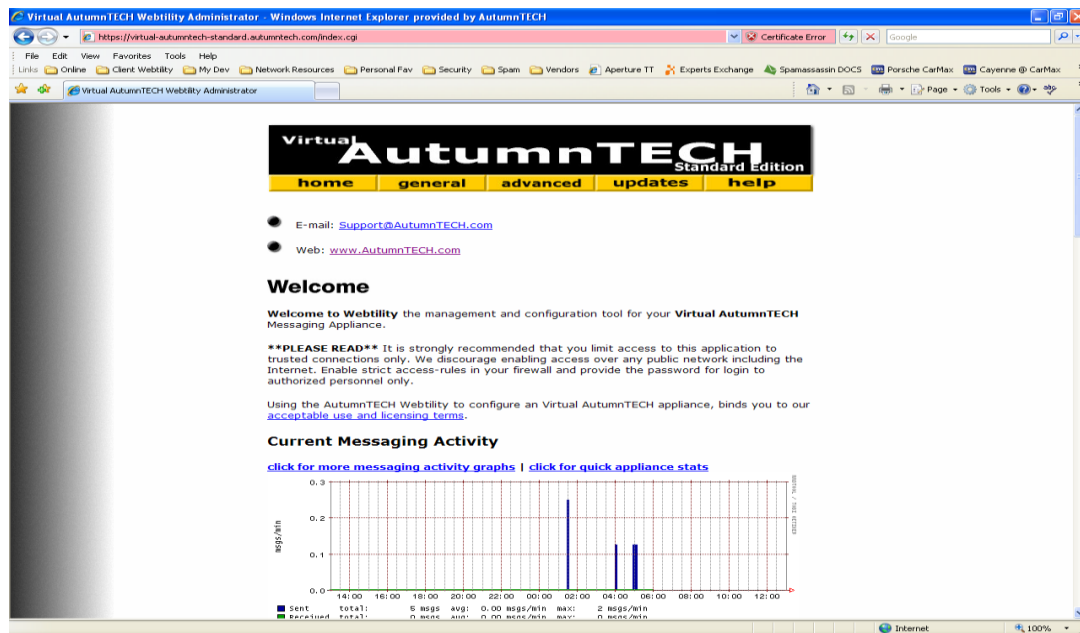
Webtivity can be accessed via any popular web browser. The URL is the same as the network IP address assigned, i.e. <https://theipaddressassigned>

The default Webtivity username is: **admin**
The default Webtivity password is: **password**

Webtivity contains five tabs; home, general, advanced, updates, and help

Home

The home tab contains useful information regarding the operating status of your Virtual Appliance. The information includes graphs that will update as e-mail traffic passes through the appliance.



General

The General area contains utilities to modify the appliance's date and time, networking information, passwords for Webtivity login, syslog settings, and rebooting to powering off the appliance.

Depending on the operating version, the quick stats reports will show a variety of information. The following is an example of the Enterprise version:

Quick Appliance Stats

Accepted E-mails Processed:

6

Latest Spam Activity:

[View High Limit Spam Traffic](#)

Tagged Spam	Not Tagged Spam	Tagged Spam Quarantined	Large Message Skipped
0	1	0	5

Number of Virus Infected E-mails:

0

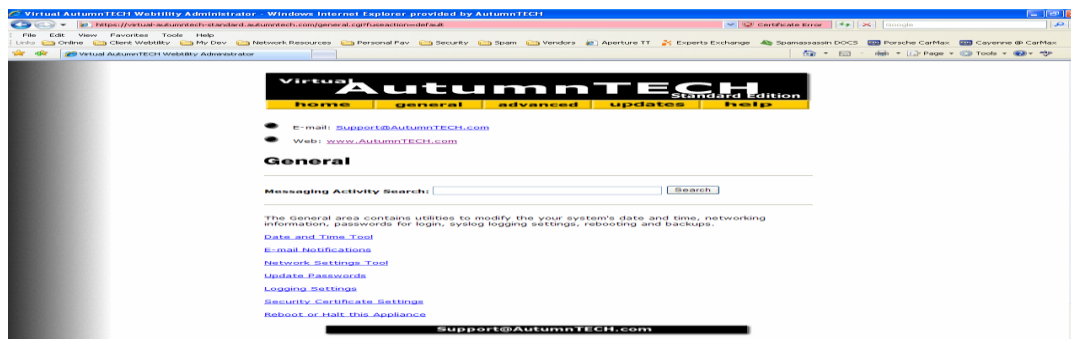
ClamAV 0.94.2/9057/Sat Feb 28 08:56:20 2009

Latest Virus Activity:

[View the Anti-virus Capture Report](#)

Date/Time:	None
Sender:	None
Recipient:	None
Subject:	None
Sender Network:	None
Virus Info:	None

Enterprise Edition - Quick Appliance Stats



Date and Time Tool

Use this tool to configure the network time server addresses, select your location time zone, and to manually set the appliances date and time.

E-mail Notifications

Use this tool to specify e-mail addresses that should receive appliance information including daily reports, status, and monitoring results.

Network Settings Tool

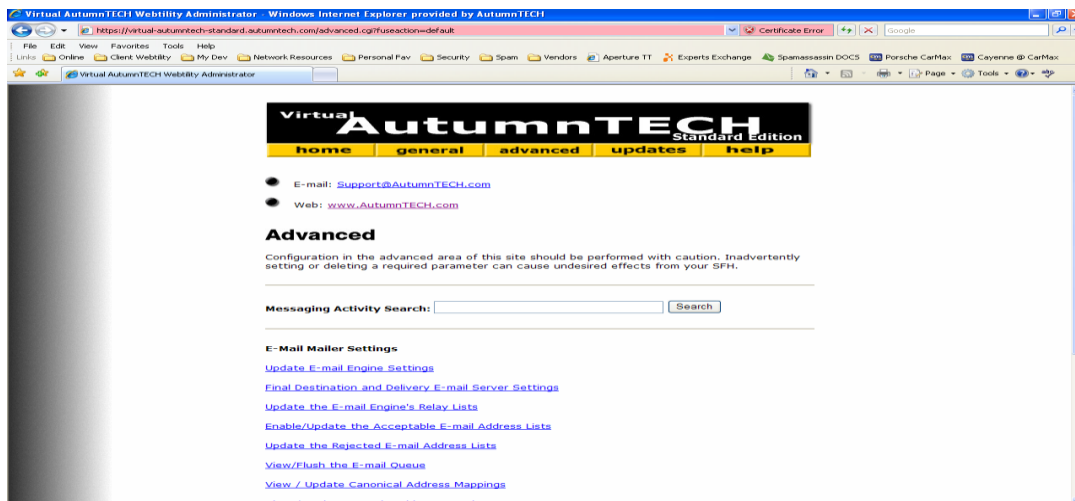
Use this tool to configure the network settings including the IP address, DNS servers, and default gateway. In addition, a network test utility is included for “pinging” and “trace routing” for diagnostic purposes.

Update Passwords

Use this tool to update the Webtility admin access password.

Use this tool to specify the Syslog server that real time output should be sent to. The Syslog output is an invaluable tool for diagnosing and is a highly recommended configuration.





Update Spam Flag and Tag Settings

This tool allows for the configuration and selection of common anti-spam fighting techniques. Settings include the minimum threshold score that a message will be considered as spam and a maximum threshold spam score limit that will delete and not deliver a message that's score exceeds.

In addition, you can configure the alteration of the subject line to include text if a message is detected as spam. Attaching suspected spam will generate a new message body for the e-mail that scored higher than the minimum threshold attaching the original message to that new message body.

The Bayesian learning system when set to auto-learn will extract and tokenize spam messages saving the result in a local database file. These tokens will then be used on future messages seeking similarities and scoring based on those similarities. The minimum and maximum setting is useful if your desire is to learn a maximum amount of e-mail first BEFORE scoring messages. Set this value to a higher number than the 200 default to train more and scoreless.

Use the "Allowed Senders" text area to specify e-mail addresses and entire domains that should always pass through the anti-spam check as not spam.

Use the "Blacklisted Senders" text area to specify e-mail addresses and entire domains that should always fail the anti-spam check. Depending on the maximum threshold defined above, blacklisting will most likely block e-mail entirely, deleting and removing the message off of the appliance.

Update the Anti-Spam Engine Settings

Use this tool to enable or disable the anti-spam check, set a maximum message size to send through the anti-spam engine, whether or not to quarantine e-mail tagged as spam, and finally whether or not to enable the e-mail message footer text that appends to all incoming e-mail and what that text should be.

Update LDAP Search Before Delivery Settings

**** Version 1.0.3+ only ****

Updates

Results of update:

1.0.3

Currently running the latest release

as of Apr 12 2009 09:39:15

Use this tool to authenticate sender and recipients before mail delivery. Authentication is validated by making a LDAP query call into an active and compliant directory. The LDAP authentication query includes FROM, TO, and CC e-mail addresses. BCC recipients **CAN NOT** be used for authentication. If any of the submitted addresses match a corresponding object in the directory, mail is allowed to pass to the next processing rule. If no match can be made, the "failed" option switch is activated.

The advantages of this tool included reduced failure reports generated by your mail delivery system and faster mail handling and processing. In addition, enabling this tool allows Administrators greater control over handling "spoofed" e-mail addresses and their delivery. Results from the lookup can be reviewed in the e-mail message header. Look for the value associated with the message header: "Virtual-AutumnTECH-ldapsearch"

This module is added after subscribing to the annual firmware update program. Once subscribed, operator applies for and downloads the latest firmware updates. Firmware version 1.0.3 will install the LDAP search module automatically. Subscribe to the annual update by linking to <https://www.autumntech.com/xcart/product.php?productid=51>

Update E-mail Engine Settings

Use this tool to update the primary e-mail server settings. Description of each of the features should be self-explanatory.

Final Destination and Delivery E-mail Server Settings

Virtual AutumnTECH uses split horizon DNS addressing to determine the final destination for e-mail delivery. The public will believe that the Virtual AutumnTECH appliance is the final destination for your e-mail, the Virtual AutumnTECH through configuration of this tool will understand that your internal e-mail server is the final destination.

If you used the Quick Start Configuration Wizard described in a Chapter 2, your domain will already be listed here. You must always configure here when adding additional e-mail domains that will filter through your Virtual AutumnTECH appliance.

Update the E-mail Engine's Relay List

This tool will allow you to specify the e-mail domains that are allowed to relay through and filter inside of your Virtual AutumnTECH appliance. Domains listed in the first text area and NOT in the second will only relay through the appliance and will not be passed to the filtering engine. Normally, the top two text areas contain the exact same domain information.

The final text area allows you to specify domains to send through the filter engine that are relaying out to the Internet. In order for outbound relaying to work, you must set "Permit relay mail out of my local area network?" to Enabled and then specify by IP address the servers actually allowed to relay out in the "Permitted these my local area relay network subnets" text field. These settings are found in Update E-mail Engine Settings.

IMPOTANT – Make sure that you create a mapping in "Final Destination and Delivery E-mail Server Settings" for ALL new incoming filtering domains created with this tool.

Enable/Update the Acceptable E-mail Address List

Set Current Status to "Enabled" and provide a list of acceptable e-mail address that your Virtual AutumnTECH will accept. Any recipient e-mail address not listed here will be rejected.

Update the Rejected E-mail Address Lists

Reject sender and recipient e-mail addresses and entire domains can be specified in this tool.

View/Flush the E-mail Queue

Check the status of the Virtual AutumnTECH e-mail queue. Search the queue and force re-queuing or deletion of e-mail.

View / Update Canonical Address Mappings

Use this tool to redirect e-mail and/or to masquerade the sender e-mail address before final delivery.

View / Update Generic Address Mappings

Address mapping tool that applies to the sender portion of outbound messages.

Update the Anti-Virus Engine Settings

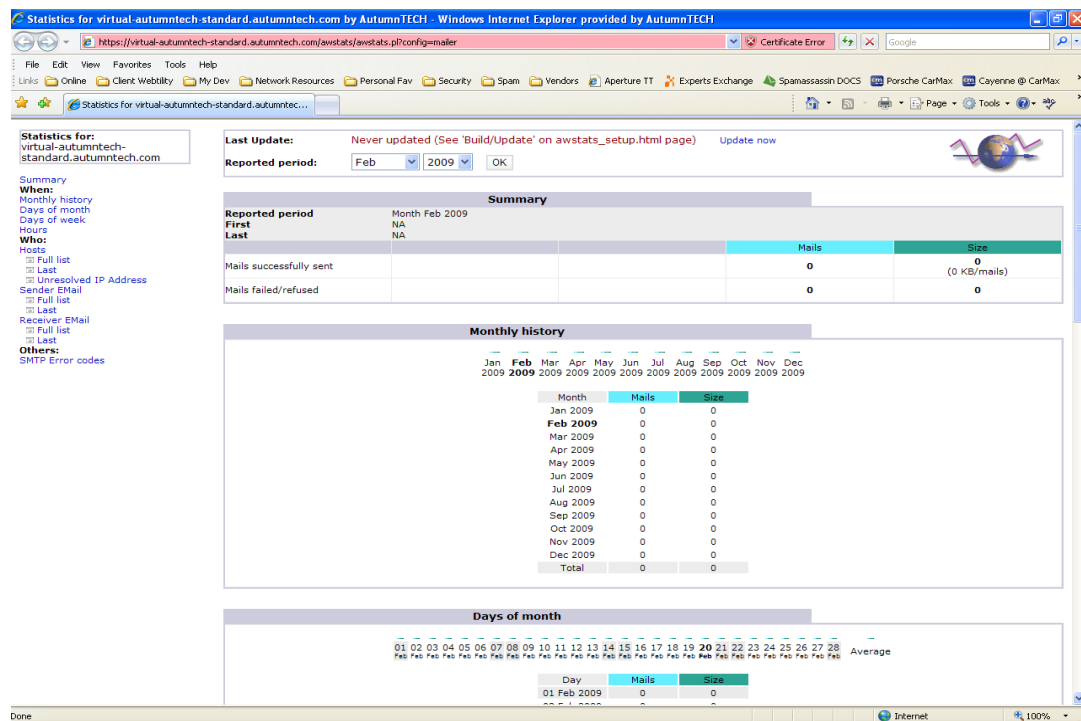
Use this tool to manage the whether the anti-virus engine should check e-mail as it filters through the Virtual appliance. In addition, set whether or not to notify the original recipient and/or appliance Administrators is a virus is detected.

Update Firewall Configuration and Ruleset

Use this tool to restrict access to the network services running on this appliance to specific network addresses.

E-mail Traffic Reports (graphics version)

This is a graphical tool for displaying current and archived e-mail traffic.



E-mail Traffic Reports (text only version)

Display current e-mail traffic and hourly statistics occurring today and over the past four days.

Anti-Virus Capture Report

This tool will report on the number of viruses detected, sender's public IP addresses, subjects of those viruses, and finally the top recipients of virus infected e-mail.

Anti-Virus Traffic Report

This tool will redirect to the search page using "virus-infected" as the search string. In here you'll be able to sort and filter the detected virus traffic.

Anti-Spam Traffic Report (top 100)

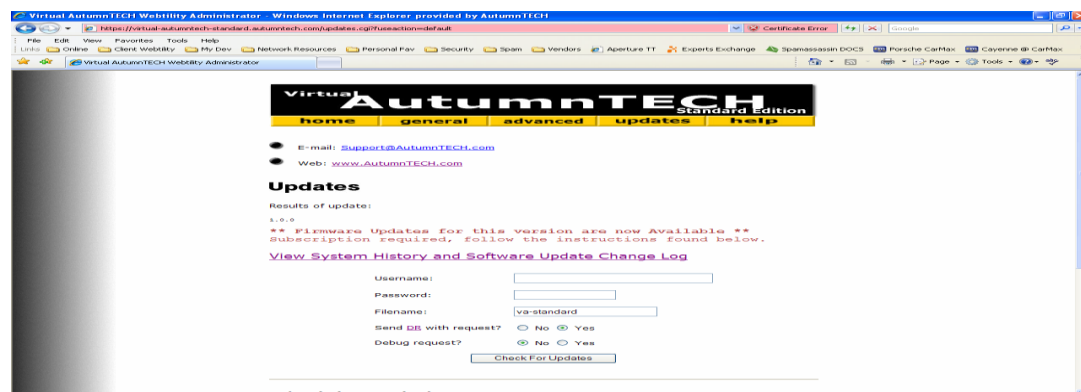
This tool allows you to view filtering statistics related to the filtering of e-mail inside of the anti-spam engine. Use the drop down menu to select today's history, or yesterdays, or report on traffic for the past four days.

Show Appliance Information

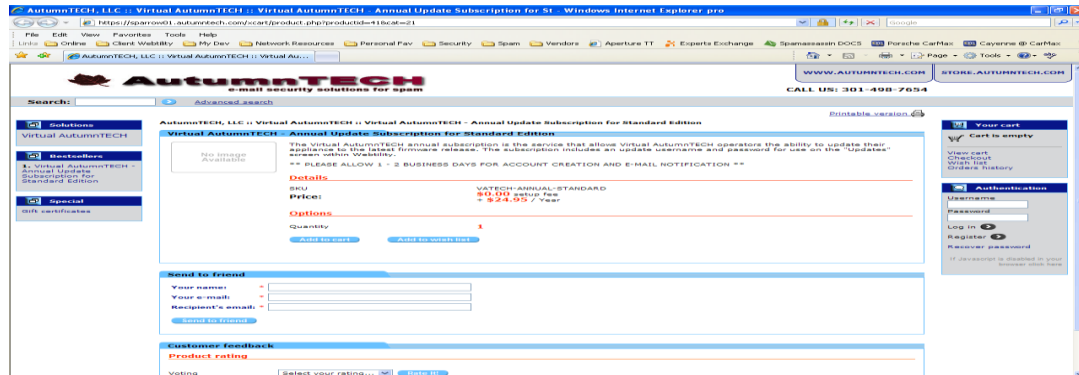
Display useful operational information regarding the uptime, processor load, and startup output.

Updates

The Updates tab will allow subscribers to apply the latest Virtual AutumnTECH firmware releases.



If you are not an update subscriber, use the link found on the updates tab to locate the secure online sign-up form. Subscription is charged in full annually on January 1st. Your charge for signing up will be pro-rated from today's date through December 31st.



Help

This page provides links and the ability to submit a diagnostic report to AutumnTECH support for troubleshooting assistance.

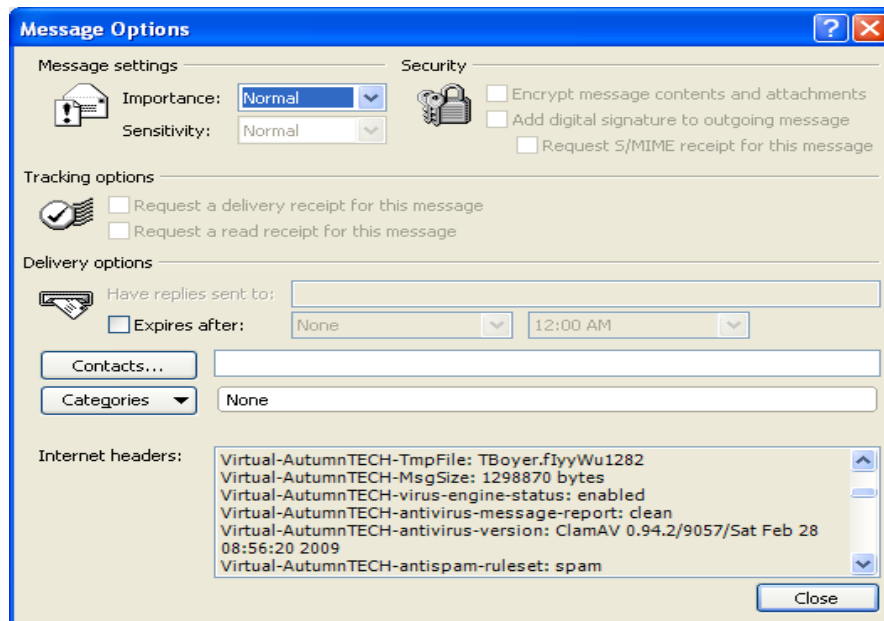


Chapter 3: Filtering

Virtual AutumnTECH should be placed in-between your firewall and your e-mail server. To enable Virtual AutumnTECH (typically) you must update the access control rule inside of your firewall so that incoming network traffic on TCP port 25 (SMTP) is mapped to the IP address of the Virtual AutumnTECH appliance.

**** IMPORTANT **** The Postgrey Greylisting service enabled in Update E-mail Engine Settings will cause minor delays in the delivery of e-mail from first time senders. Do not be alarmed if incoming e-mail begins to arrive shortly after enabling and not immediately.

All e-mail that passes through the filtering engine will contain useful information in the header of each e-mail message. Use this information for identifying what happened to the message as it passed through the Virtual Appliance.



Chapter 4: Backup and Recovery

We recommend backing up your Virtual Appliance weekly. To backup your virtual appliance, simply power down and zip or the Virtual-AutumnTECH-xxx.vmdx and Virtual-AutumnTECH-xxx.vmx files to location that your backup software will reach. To recovery, unzip or copy the backed up files to the original installation location.

Chapter 5: Support

You may e-mail Support@AutumnTECH.com or visit the AutumnTECH.com website for assistance and tips.