

Version

1.7

EMAIL SECURITY VIRTUAL APPLIANCE (ESVA)

Global-Domination.org

Installation and Administration Guide

Table of Contents

Getting Started.....	1
Introduction:	1
Prerequisites:	2
Software Prerequisites (one of the following):.....	2
Hardware Prerequisites:.....	2
Additional Prerequisites:	2
Default Usernames and Passwords	2
What's new?	3
Where has everything gone and what's changed?	3
Item Location in MailWatch URL	3
Postgrey	3
FuzzyOCR	3
ESVA Setup	5
VMware Host Setup	5
Initial ESVA Setup.....	6
MailWatch Setup.....	7
Securing the admin account.....	7
Creating Domain Administrator accounts.....	7
Creating User Accounts	7
Whitelisting and Blacklisting within MailWatch	8
Greylist options	10
Configuring ESVA to relay to additional domains.....	13
ESVA Upgrade/Migration	15
Which Procedure do I use?.....	15
Upgrade Migration from ESVA 1.6 to ESVA 1.7.....	16
Migration from ESVA 1.7 to ESVA 1.7.....	17
Extending the ESVA Quarantine Partition.....	19
Prerequisites	19
Extending the Partition	20
Customizing your ESVA.....	23
What's to customize?	23
Disabling "Report as SPAM" footer	23
Report as SPAM footer for Multiple Domains.....	24
Report as HAM footer	24
Destination Address Verification on Incoming Mail	25

Credits and Acknowledgements

A big thank you to all the clever people that have contributed to the success of ESVA over the last year – especially over the last six months since v 1.6 was released. As is the nature of online forums the population tends to be transient, however that doesn't mean that the quality of advice, fixes and general discussion has suffered. Because of the sheer amount of useful suggestions that have made their way into this release I can't thank everyone personally, however special thanks has to go to the guys who made it all possible with the excellent software upon which ESVA is based:

Julian Field – MailScanner

Steve Freegard – MailWatch for MailScanner

For their efforts in assisting with the documentation the following get a special mention:

Dave Waldron – (Waldronmct) – The author of sizable portions of this document

Angelo McComis – (amccomis) – White/Blacklisting and filters

GD forum members that get a special mention are:

abartlett	dave99	Gal_Z	LogIQ	Jasper
doggy101	danfulton	Webhopper	Catrinisn	robhostager

Also a mention to everyone on the MailScanner and Mailwatch mailing lists.

Any comments or suggestions should be posted to the official ESVA forum at:

<http://www.global-domination.org/forum>



Getting Started

E SVA is a pre-built VMware Virtual Appliance that is free to download and use - even the VMware software used to run it is free!

Introduction:

ESVA was born out of a need for organizations to have a cost-effective email virus & spam scanning solution. There are other commercial products out there, but these are often too expensive for small organizations to justify, or the existing free products are beyond the abilities of these organizations.

ESVA is simply a pre-built and semi-configured email scanning (security) Virtual Appliance (ESVA) that will run on VMware Workstation, Server, Player or ESX Server.

The idea is for the appliance to be pretty much set & forget with an easy to use interface so that users don't really need to know how to use the underlying GNU/Linux.

You are encouraged to join the online community forums at <http://www.global-domination.org/forum/>.

To download the latest version of ESVA, please visit <http://www.global-domination.org/ESVA.php>.

Prerequisites:

Software Prerequisites (one of the following):

- VMware Server 1.0.2 for Windows or Linux
 - Available for free at <http://www.vmware.com/products/server/>
- VMware Workstation 6.0
 - Trial available at <http://www.vmware.com/download/ws/eval.html>
- VMware Player
 - Available for free at <http://www.vmware.com/download/player>
- VMware Fusion for Mac OS X
 - See <http://www.vmware.com/products/desktop/fusion.html> for details
- ESX V3 (VI3)
 - Trial available at <http://www.vmware.com/download/vi/eval.html>

Hardware Prerequisites:

Minimum for Testing

- 5GB free disk space
- 512 MB unreserved memory

Recommended for Production

- 10-40 GB free disk space
- 512-1024 MB unreserved memory

Additional Prerequisites:

- A basic grasp of VMware principles and terminology
- Internet DNS MX records configured for your domain(s) pointing toward ESVA (or the public interface of your firewall, with appropriate port forwarding configured)
- A static IP Address for the ESVA appliance
- A DNS server for ESVA to resolve Internet addresses.

Default Usernames and Passwords

Resource	Username	Password
Console/Webmin	root	password
MailWatch Web Portal	admin	password

Important

All passwords should be changed from the defaults before ESVA is exposed to un-trusted networks (e.g. Internet).

What's new?

Most existing packages have been updated to more recent versions, including MailScanner, ClamAV and SpamAssassin.

Where has everything gone and what's changed?

A lot has changed in the interface since Version 1.6 with everything accessed from the modified MailWatch interface, so here's a quick guide to where certain things have moved to (although URLs generally haven't changed).

Item Location in MailWatch URL

Resource	Location
Webmin Tools/Links	<a href="https://<esvaname>">https://<esvaname>
Mailgraph Reports – MTA Statistics (Postfix)	/cgi-bin/mailgraph.cgi

Postgrey

Has been replaced by SQLGrey

<http://sqlgrey.sourceforge.net/>

The SQLGrey Web Interface implementation in ESVA is based on SGWI (albeit heavily modified), found here:

<http://www.vanheusden.com/sgwi/>

FuzzyOCR

FuzzyOCR has been implemented to catch the picture spam that makes it through the initial filters.

<http://fuzzyocr.own-hero.net/>

**EMAIL SECURITY VIRTUAL APPLIANCE (ESVA)
INSTALL AND ADMINISTRATION GUIDE**

ESVA Setup

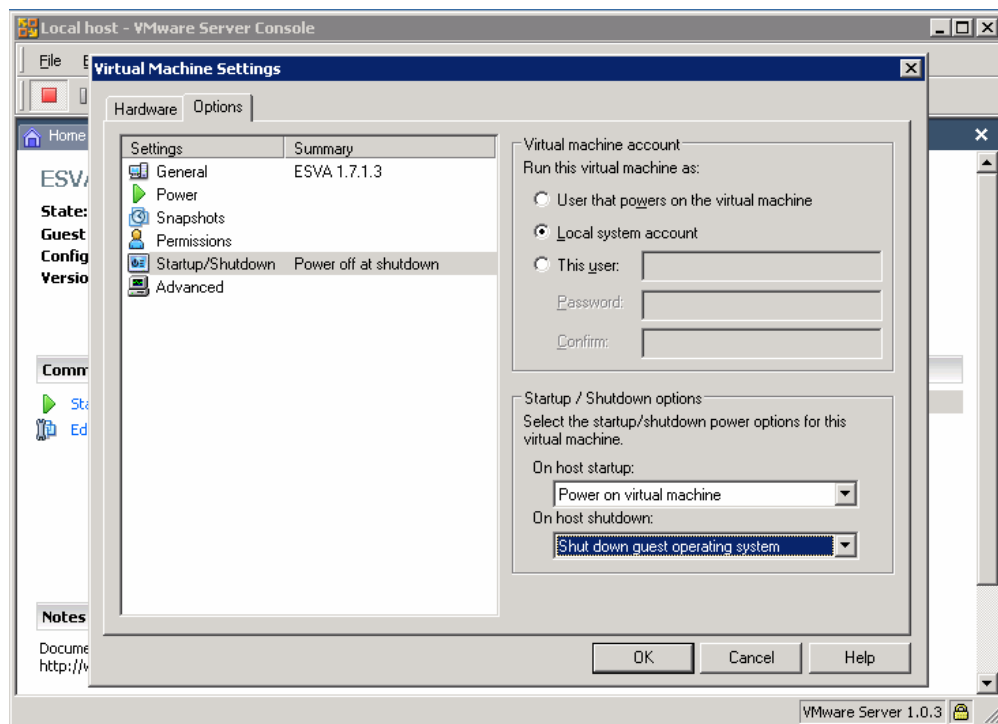
Unlike previous versions of ESVA, this version doesn't have its network interface configured to use DHCP out of the box. The initial setup is all done through the ESVA Console directly via VMware.

VMware Host Setup

Once you have downloaded, unzipped and registered ESVA with your VMware software, you should configure ESVA to start automatically at host start-up and to shut down gracefully at system shut down.

In VMware Server 1.x (For Windows) you will find these options by navigating through VM > Settings, then choosing the options tab.

Select Startup/Shutdown and configure the options as displayed below. Once this is configured, click OK and power ESVA on.



Initial ESVA Setup

- Click on the console and press alt-f2
- Login as root
- Type esva-configure to enter the quick setup program and answer the questions. For clarification of what some of the questions mean, and sample answers, please see the table below.

Prompt	Description
Keyboard (GUI)	The correct keyboard layout for your location
Timezone (menu)	The correct Timezone for your location
Host set to UTC time?	Is the VMware host set to use UTC time?
IP Address	The IP Address you want your ESVA to use
Netmask	The netmask in dotted format – e.g 255.255.255.0
Gateway	Gateway Default gateway
Hostname	The name of your ESVA – use a fully qualified name. e.g. mailgw.yourdomain.com. This should be the same as the Internet DNS A record.
DNS Domain	The domain part of your ESVA name. The default entry is usually OK (derived from the hostname)
DNS Search	A space delimited list of DNS domains for your ESVA to search through when it's trying to resolve a non-fully qualified name.
Primary DNS Server	The first DNS server to try. All the DNS servers should be able to resolve the names of internal servers – including your mail server. These DNS servers will also need to be able to resolve fully qualified internet addresses. If you are using Exchange as your mail server these should be the addresses of your AD DNS servers.
Secondary DNS Server	Second DNS server to try
Tertiary DNS Server	Third DNS server to try
Organization Name	A short name without spaces, e.g. your-domain
Organization Long Name	A longer name. Spaces are OK, e.g. Your Domain PLC
Organization Mail Server	The mail server that ESVA forwards scanned (clean) mail to. This can be either a name or IP address.
Email address for system messages	ESVA sends regular messages to keep you informed of any problems and log summaries etc. This should be a real monitored mailbox.
Regular user account	A username that can login to ESVA remotely via SSH session. Defaults to the username portion of the email address supplied for system messages.
Regular user password (x2)	The password for the regular user account – this must be typed twice – BEWARE: This is displayed on screen
Root password (x2)	Your new root password – this must be typed twice – BEWARE: This is displayed on screen. Avoid using the '@' symbol in the password as Webmin doesn't like it.

After the last question is answered the changes are committed and your ESVA will reboot. As soon as the Virtual Machine has rebooted it is ready to start processing mail. If you make any mistakes during the initial setup, press <ctrl>-C to exit the setup program and start again by typing esva-configure. Do NOT run esva-configure multiple times to completion as this will result in a non-functioning ESVA server.

MailWatch Setup

Point your browser at <http://the-ip-address-or-name-you-configured-esva-to-use>.

Securing the admin account

Sign in using username 'admin' and the default password (listed on page 2 of Getting Started)

1. Click on 'Tools/Links'
2. Click on 'User Management'
3. Edit the admin user
4. Change the password for admin, and for extra safety change the username as well.

Click update when done. You will need to login with the new details.

Creating Domain Administrator accounts

Domain Administrator accounts can manage the messages for a given email domain (e.g. global-domination.org). This means that the Domain Administrator can create new user accounts for that domain as well as manage spam, white/black lists and create reports for all users in the domain.

1. Login to MailWatch as the 'admin' account secured in above.
2. Click on 'Tools/Links'
3. Click on 'User Management'
4. Click on 'New User'
5. Complete the form, supplying real names and email addresses (This is where MailWatch decides which domain the user will be administrator of). Make sure that Domain Administrator is the 'User' Type.

Click on the 'Create' button when the fields have been filled in correctly.

Creating User Accounts

User accounts have the ability to manage only their own spam, whitelists and blacklists.

1. Login to MailWatch as the admin account secured under **Securing the admin account** or as the appropriate Domain Administrator account created in the previous step.
2. Click on 'Tools/Links'
3. Click on 'User Management'
4. Click on 'New User'.
5. Complete the form, supplying real names and email addresses (This is how MailWatch decides which messages belong to a particular user). Make sure that User is the User Type.

Click on the Create button when the fields have been filled in correctly.

Whitelisting and Blacklisting within MailWatch

There are many types of circumstances where you would need to use Whitelisting and Blacklisting.

It is important to understand the precedence of how these are processed: If a message matches both the whitelist and blacklist, the whitelist wins and the message will be delivered. Additionally, the options you see on the 'Lists' screen will vary depending on the type of logged-in user (User, Domain Admin, or System Admin)

To modify your whitelists and blacklists, use the 'Lists' text link in the upper left portion of the MailWatch interface.

It's best to illustrate how this works by examples.

Example 1:

Always accept mail from bob@example.co.uk illustrated at various user privilege levels.

Add to Whitelist/Blacklist	
From:	bob@example.co.uk
To:	<input type="text"/> @ <input type="text"/>
List:	<input checked="" type="radio"/> Whitelist <input type="radio"/> Blacklist
Action:	<input type="button" value="Reset"/> <input type="button" value="Add"/>

As a normal user, the To: fields are grayed out.

Add to Whitelist/Blacklist	
From:	bob@example.co.uk
To:	<input type="text"/> @ <input type="text"/>
List:	<input type="radio"/> Whitelist <input type="radio"/> Blacklist
Action:	<input type="button" value="Reset"/> <input type="button" value="Add"/>

As a Domain Administrator, you may choose to always whitelist bob@example.co.uk to everyone in your domain by adding this to the whitelist.

Add to Whitelist/Blacklist	
From:	bob@example.co.uk
To:	default @ <input type="text"/>
List:	<input checked="" type="radio"/> Whitelist <input type="radio"/> Blacklist
Action:	<input type="button" value="Reset"/> <input type="button" value="Add"/>

Finally, you can whitelist bob@example.co.uk system-wide.

Note that in many cases you wouldn't see this, but understanding that the use of the word "default" as the To: field allows this type of system-wide rule.

Example 2:

Always reject mail from spammy@badhost.net, illustrated at various user privilege levels.

**EMAIL SECURITY VIRTUAL APPLIANCE (ESVA)
INSTALL AND ADMINISTRATION GUIDE**

Add to Whitelist/Blacklist	
From:	spammy@badhost.net
To:	example.com
List:	<input type="radio"/> Whitelist <input checked="" type="radio"/> Blacklist
Action:	<input type="button" value="Reset"/> <input type="button" value="Add"/>

As a user, note again that the To: field cannot be modified. Mail from this address will be blocked, but only blocked when sending to this user.

Add to Whitelist/Blacklist	
From:	spammy@badhost.net
To:	
List:	<input type="radio"/> Whitelist <input checked="" type="radio"/> Blacklist
Action:	<input type="button" value="Reset"/> <input type="button" value="Add"/>

A Domain Administrator can block mail from this user across the entire domain.

Add to Whitelist/Blacklist	
From:	spammy@badhost.net
To:	default
List:	<input type="radio"/> Whitelist <input checked="" type="radio"/> Blacklist
Action:	<input type="button" value="Reset"/> <input type="button" value="Add"/>

Similar to Example 1, this might not be of much actual use in practice, but the system will block an email address system-wide by putting in a blacklist entry at the System Administrator user level.

Understanding MailWatch Lists when used with Filters.

Filters in MailWatch allow a MailWatch user to have access via MailWatch to mail messages that might be to an alias which they control. For example, user joe@company.com has an alias of info@company.com. MailWatch needs to know this so that Joe can actually manipulate (release from quarantine) mail that was sent to the info@ address. In MailWatch, the System Administrator can set up a “filter” for joe@company.com allowing him to also see info@company.com. It is important to understand that the current version of MailWatch does not automatically apply whitelist and blacklist rules against addresses that you specify via a filter. For example, joe@company.com has filter info@company.com. Joe’s business advertising advisor at advert@example.co.uk. Because of the nature of what they’re sending back and forth, they decide it’s best to whitelist each other to avoid false positives. So Joe@company.com has a whitelist entry of advert@example.co.uk. However, a message was sent to info@company.com, and was caught as spam because the joe@company.com whitelist did not apply. This is a known issue and there are some hacks in the forums to work around this issue.

Greylist options

When you click on the Greylist menu, a sub-menu opens below the main menu bar:

Recent Messages	Lists	Quarantine	Reports	Tools/Links	Greylist	Logout
Greylisted	AWL Addresses	AWL Domains	White Domains	White Addresses	Grey Domains	Grey Addresses
Greylisted	- Messages that are waiting to pass greylisting					
AWL	- Auto White List. These addresses or domains have passed greylisting tests and are now trusted, so won't be affected by greylisting again.					
White	- Manually Whitelisted. These addresses or domains will never be affected by greylist tests.					
Grey	- Manually Greylisted. These addresses or domains will always be subjected to greylist tests.					

A brief explanation of the terminology is included in the main screen (above).

All details displayed in the following lists can be sorted by clicking on the relevant column heading.

Greylisted

This screen lists all addresses that are awaiting verification. If an address isn't validated within 24hours it will be automatically removed from this list. You should keep an eye on this list to capture any addresses or domains that are valid but don't resend (common with website forum notifications – notably the VMware VMTN forums). Addresses in this list can be manually whitelisted or deleted by clicking on the appropriate link. It is also possible to delete all entries before a specific time via the form at the bottom of the page.

AWL Addresses

Once an address has been validated, it is automatically whitelisted and appears in this list. Addresses in this list can be deleted by clicking the delete link to the right of each address. At the bottom of the screen, there is a form to manually add individual addresses to the AWL. For the fields, follow the example below. The Source field is for the source IP address in either class c notation (first 3 octets - xxx.xxx.xxx – this will allow messages to be sent from any host within that class c address range) or class d notation (full IP address – xxx.xxx.xxx.xxx)

It is important to note that some of the AWL addresses are class c and some are class d – this is determined by SQLGrey and is a sign of how “trustworthy” an address is – A class d is less trusted, and probably comes from dynamic address space or doesn't have a matching reverse lookup.

Also note that any spam that survives greylisting will be added to the AWL. In the screenshot below the bottom address was a spam which was detected by and dealt with by MailScanner. If successful spam comes from a particular host or domain regularly, you should consider adding them to the Grey Domains or Grey Addresses lists to force a retry on every message sent, doubling the effort required for them to send to your domains.

**EMAIL SECURITY VIRTUAL APPLIANCE (ESVA)
INSTALL AND ADMINISTRATION GUIDE**

Recent Messages	Lists	Quarantine	Reports	Tools/Links	Greylist	Logout
Greylisted	AWL Addresses	AWL Domains	White Domains	White Addresses	Grey Domains	Grey Addresses
Auto Whitelist Addresses						
Sender name	Sender domain	Source	First seen	Last seen		
customer_service	vmware.com	66.35.234	2007-05-19 21:07:47	2007-05-19 21:08:14	Delete	
jiveadmin	vmware.com	66.35.226	2007-05-19 22:04:31	2007-05-19 22:04:31	Delete	
wouu	frontiernet.net	68.155.245.254	2007-05-19 21:23:17	2007-05-19 21:33:09	Delete	

[Delete '-undef-' entries](#)

Add to whitelist

Sender name:

Sender domain:

Source (class c or d):

AWL Domains

Once a domain has sent messages from multiple source addresses to multiple destination addresses, it will be auto whitelisted (and will appear in this list) – all senders from that domain will be trusted to send to all recipients, as long as the source remains the same (class c or d).

As for the AWL Addresses list, any domain can be deleted manually and entries can be manually added as long as you have the correct source address and class.

White Domains

The domain that is referred to here is the domain in the FQDN determined by reverse lookup, not the senders domain name. For example, company yyy sends all their mail through their ISPs (zzz) smarthost. The mail ‘from address’ will be yyy.com, but the reverse lookup on the mail server sending the message is zzz.com.

If you decide to trust all hosts that resolve to zzz.com hostnames, you can manually add zzz.com to the white domain list.

As with additions, domains can be deleted as well.

Recent Messages	Lists	Quarantine	Reports	Tools/Links	Greylist	Logout
Greylisted	AWL Addresses	AWL Domains	White Domains	White Addresses	Grey Domains	Grey Addresses
White Domains						
Add a domain						
gmail.com	delete					
googlemail	delete					
mailcontrol.com	delete					
vmware.com	delete					
yahoo.com	delete					
<input type="text"/>	<input type="button" value="Add"/>					

White Addresses

This is similar to the White Domains list, however is for specific servers rather than entire domains.

Grey Domains

If you get a lot of spam from a particular domain or sub-domain, you can force all hosts on that domain to be permanently greylisted, meaning they won’t be automatically whitelisted.

**EMAIL SECURITY VIRTUAL APPLIANCE (ESVA)
INSTALL AND ADMINISTRATION GUIDE**

Recent Messages	Lists	Quarantine	Reports	Tools/Links	Greylist	Logout
Greylisted	AWL Addresses	AWL Domains	White Domains	White Addresses	Grey Domains	Grey Addresses
Grey Domains						
Add a domain						
int.bellsouth.net delete						
<input type="text"/>						<input type="button" value="Add"/>

Grey Addresses

This is similar to the Grey Domains list, however is for specific servers rather than entire domains.

Configuring ESVA to relay to additional domains

In its default configuration, ESVA will only relay messages to the domain defined during the initial configuration process. To relay for additional domains, perform the following steps:

1. In the ESVA web interface, click on Tools/Links
2. Click on Edit Transport File.

Recent Messages Lists Quarantine Reports Tools/Links Greylist Logout

- User Management
- MySQL Database Status
- View Maillog
- Edit Transport file
- Webmin
- Update GeoIP Database
- View MailScanner Configuration
- SpamAssassin Bayes Database Info
- SpamAssassin Lint (Test)
- Update SpamAssassin Rule Descriptions

This will open up the page shown below. If you like, you can read through the file, but the all configuration is done at the bottom.

Recent Messages Lists Quarantine Reports Tools/Links Greylist Logout

```
/etc/postfix/transport
# TRANSPORT(5)                                TRANSPORT(5)
#
# NAME
#       transport - Postfix transport table format
#
# SYNOPSIS
#       postmap /etc/postfix/transport
#       postmap -q \\\"string\\\" /etc/postfix/transport
#       postmap -q - /etc/postfix/transport <inputfile
#
# DESCRIPTION
#       The optional transport(5) table specifies a mapping from
#       email addresses to message delivery transports and/or
#       relay hosts. The mapping is used by the trivial-rewrite(8)
#       daemon.
#
#       This mapping overrides the default routing that is built
#       into Postfix:
#
#       mydestination
#           A list of domains that is by default delivered via
#           $local_transport. This also includes domains that
#           match $inet_interfaces or $proxy_interfaces.
#
Update
```

The format is as follows:

domain.tld smtp:where_to_send_to

There are some additional options as well.

In the config shown above (indeed in the default config) you will notice the first line is:

*** :**

This will cause Postfix to deliver all messages from allowed hosts to domains that don't have a transport mapping (i.e. outbound messages to external domains) directly. To change this so that ESVA will forward all these messages to a smarthost (e.g. your ISP's smarthost) you should replace the default entry to read like this:

*** smtp:isp-smarthost.isp.net**

**EMAIL SECURITY VIRTUAL APPLIANCE (ESVA)
INSTALL AND ADMINISTRATION GUIDE**

To route messages for your own domains, use a similar format to the next line in the file (below):

global-domination.org smtp:[192.168.169.98]

This line translates to English as

Forward all scanned mail addressed to global-domination.org to the MTA (Mail Server) at 192.168.169.98 and don't use DNS to resolve MX.

The square brackets [] mean don't resolve MX records – this is probably a good idea to avoid mail-loops, especially if you have your external MX record pointing to your ESVA and your ESVA would resolve itself via DNS.

In order to forward/relay email for another domain, global-domination.co.uk, by name, the configuration line would read:

global-domination.co.uk smtp:[exchange01.global-domination.org]

Repeat this process for all the domains you wish to relay to/for and click the update button. The changes will be made effective instantly.

A much more detailed explanation is in the transport file if you require more information.

ESVA Upgrade/Migration

E SVA is built to be upgraded in future releases. Additionally, you can migrate from previous versions (1.6) to the current version (1.7) to ease upgrades in the future. Depending on how large your quarantine is, you might need to follow the procedure to extend your /var filesystem (documented both at <http://www.global-domination.org/ESVA/howto/howto-esvabigdisk.pdf> and later in this manual) first. If you followed that procedure for the 1.6 ESVA you will also need to extend your new 1.7 ESVA by following the same procedure.

Important

Before you do ANYTHING ELSE, backup your ESVAs by shutting them down and tarring or zipping them. This will be your rollback if it all goes wrong!
Please read this full procedure before proceeding with any of the steps!
This procedure requires use of the command line interface.
All databases on the destination server will be over-written by the imported databases.

Which Procedure do I use?

Depending on the version of ESVA you are currently using, you will either be performing an upgrade migration from ESVA 1.6 to ESVA 1.7, or a migration of your settings from one ESVA 1.7 to another ESVA 1.7.

DO NOT DO BOTH OF THE FOLLOWING PROCEDURES!

Upgrade Migration from ESVA 1.6 to ESVA 1.7

DO NOT USE THIS PROCEDURE IF YOU ARE MIGRATING FROM ANOTHER ESVA 1.7!!!

On the SOURCE ESVA (1.6)

1. Log in using an SSH client (putty or similar) as root
2. Enter the following commands:

```
service MailScanner stop
cd /var/spool/MailScanner
mkdir /var/tmp/export
tar -cvzf /var/tmp/export/quarantine.tgz ./quarantine/
cd /var/tmp/export
sa-learn --backup>bayes.txt
mysqldump mailscanner>mailscanner.sql
cd /var/tmp
tar -cvzf export.tgz ./export/
```
3. Using WinSCP or similar, copy export.tgz to your desktop or somewhere else temporarily.
4. Shutdown the source ESVA (1.6)

On the destination ESVA (1.7)

1. Power on your configured ESVA 1.7
2. Log in using an SSH client (putty or similar) as the username created during the setup process, then switch to the root account (type su-l and enter the root password when prompted)
3. Run the following command:

```
esva-import-1
```
4. Using WinSCP or similar, copy export.tgz to /var/tmp
5. Run the following command (**this might take a long time, and will overwrite all the information already in the mailwatch database on your new ESVA...**)

```
esva-import-2
```
6. Your ESVA should now have all the MailScanner database information and quarantined messages from your old ESVA, as well as your old Bayes database migrated to the mySQL database used in ESVA 1.7
7. You should now log out of the puTTY and WinSCP clients.

Migration from ESVA 1.7 to ESVA 1.7

**DO NOT USE THIS PROCEDURE IF YOU ARE PERFORMING AN UPGRADE
MIGRATION FROM ESVA 1.6!!!**

On the SOURCE ESVA (1.7)

1. Log in using an SSH client (putty or similar) as root
2. Enter the following commands:

```
service MailScanner stop
cd /var/spool/MailScanner
mkdir /var/tmp/export
tar cvzf /var/tmp/export/quarantine.tgz ./quarantine/
cd /var/tmp/export
mysqldump mailscanner>mailscanner.sql
mysqldump FuzzyOcr>FuzzyOcr.sql
mysqldump sa_bayes>sa_bayes.sql
mysqldump sqlgrey>sqlgrey.sql
cd /var/tmp
tar cvzf export.tgz ./export/
```
3. Using WinSCP or similar, copy export.tgz to your desktop or somewhere else temporarily.
4. Shutdown the source ESVA (1.6)

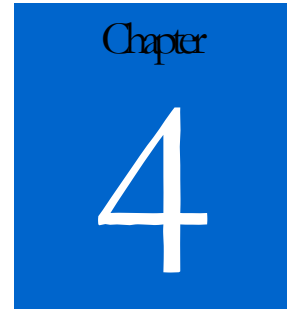
On the destination ESVA (1.7)

1. Power on your configured ESVA 1.7
2. Log in using an SSH client (putty or similar) as the username created during the setup process, then switch to the root account (type su-l and enter the root password when prompted)
3. Run the following command:

```
esva-import-1
```
4. Using WinSCP or similar, copy export.tgz to /var/tmp
5. Run the following commands

```
cd /var/tmp
tar -xvzf export.tgz
rm -f export.tgz
cd export
mysql mailscanner<mailscanner.sql
mysql FuzzyOcr<FuzzyOcr.sql
mysql sa_bayes<sa_bayes.sql
mysql sqlgrey<sqlgrey.sql
cd /var/spool/MailScanner
tar -xvzf /var/tmp/export/quarantine.tgz
sed -i 's/#PermitRootLogin/PermitRootLogin/g' /etc/ssh/sshd_config
service sshd restart
service MailScanner start
```
6. Your ESVA should now have all the MailScanner database information and quarantined messages from your original ESVA 1.7.
7. You should now log out of the puTTY and WinSCP clients.

**EMAIL SECURITY VIRTUAL APPLIANCE (ESVA)
INSTALL AND ADMINISTRATION GUIDE**



Extending the ESVA Quarantine Partition

This guide will help you to create an extended quarantine disk in order to store more messages on busy sites.

Thanks to all those who complained (so nicely!) about the appalling inaccuracies in the predecessor to this document – especially to those who came back with suggestions on how to improve the document!

Any comments or suggestions should be posted to the official ESVA forum at:
<http://www.global-domination.org/forum/>.

Prerequisites

- Sufficient free space for the new quarantine disk
- A basic grasp of VMware principles and terminology (for VMware Server)
- If using ESX server you really should be qualified to do so (VCP level)

Extending the Partition

Important

Before you do ANYTHING ELSE, backup your ESVAs by shutting them down and tarring or zipping them. This will be your rollback if it all goes wrong!
Please read this full procedure before proceeding with any of the steps!
This procedure requires use of the command line interface.

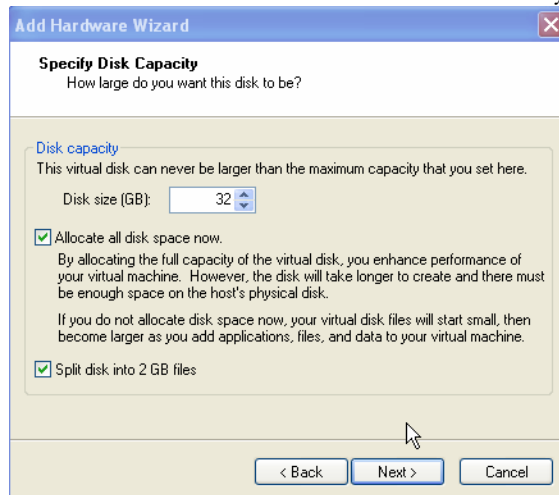
Important

This procedure will require some downtime for your ESVA and will require 2 reboots of the Virtual Machine.

Read through the ENTIRE procedure before you do anything else!

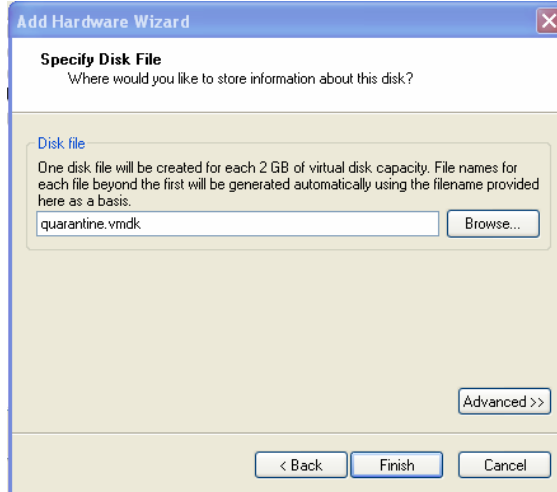
1. Shut down your ESVA and backup appropriately (don't use a snapshot).
2. In the settings of your ESVA, add a new virtual disk. The remaining steps in this procedure are based on VMware Server 1.0.3. **If you are using ESX server and don't know how to add a new disk, you shouldn't be attempting this procedure!**
3. Right-click the VM and select 'Edit Settings'.
4. On the hardware tab, click 'Add'.
5. Select Hard Disk, then click Next
6. Select 'Create a new virtual disk'
7. Click 'Next'.
8. Choose SCSI then
9. Click 'Next'
10. Enter the size of the disk you want to create, making sure you have enough physical space for it.

You should ensure that the disk is split into 2GB files as this will aid backup and defrag operations on the host as well as possible future migrations to ESX server. Choosing to "Allocate all space now" is optional; however, performance on both the host and the VM will increase dramatically by selecting it.



**EMAIL SECURITY VIRTUAL APPLIANCE (ESVA)
INSTALL AND ADMINISTRATION GUIDE**

11. Click 'Next'.
12. Give the new disk a meaningful name – “quarantine.vmdk” is suggested – Click Finish when done. The new disk will now be created – This might take some time.



13. Start your ESVA up.
14. Login as root on the console
15. Enter the following commands:

```
cd /tmp
fdisk /dev/sdb
n
p
1
<enter>
<enter>
w
mkfs.ext3 /dev/sdb1
mkdir /tmp/quarantine
chown postfix:apache /tmp/quarantine
chmod 0770 -R /tmp/quarantine
service MailScanner stop
mount -t ext3 /dev/sdb1 /tmp/quarantine
mv /var/spool/MailScanner/quarantine/* /tmp/quarantine/
echo “/dev/sdb1 /var/spool/MailScanner/quarantine ext3 defaults 0 0”>>/etc/fstab
umount /dev/sdb1
rm -rf /tmp/quarantine
init 6
```

16. Your ESVA will now restart

**EMAIL SECURITY VIRTUAL APPLIANCE (ESVA)
INSTALL AND ADMINISTRATION GUIDE**

17. Confirm the success of the operation by typing `df -h` on the console as root. You should see all your mount points and sizes displayed e.g. below:

```
[root@mail-gw ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
                3.3G  1.3G  1.8G  42% /
/dev/sda1       99M   11M   84M  11% /boot
/dev/shm        252M   38M  214M  16% /dev/shm
/dev/shm        252M   8.0K  252M   1% /var/spool/MailScanner/incoming
/dev/sdb1       32G  177M   30G   1% /var/spool/MailScanner/quarantine
[root@mail-gw ~]#
```

Customizing your ESVA

While the ESVA is usable (and very effective) immediately after reboot from the initial configuration, there are some customizations, depending on your environment, that may need to be made.

What's to customize?

- Disabling “Report as SPAM”
- Making sure that the “Report as SPAM” link shows up on email for all of your domains, not just the first one you initially set up.
- Email Address verification (destination) on incoming email.

Disabling “Report as SPAM” footer

In some locations, it is not legal to store email on any system once it has been delivered (spam is not delivered, and can therefore be stored). Since the ability to report “clean” mail as SPAM requires that all email, both clean and SPAM, be kept on the server (so the filters can re-learn the “clean” mail as SPAM), local law may require you to remove this capability.

Since it is MailScanner that determines what will be bounced/deleted/stored/forwarded for delivery, you will need to modify this through the Webmin interface.

1. Log into Webmin with an administrative account.
2. Click on Servers
3. Click on MailScanner
4. Click on What to do with SPAM
5. Modify the “Non Spam Actions” (3rd option down) by removing “store” from the list:
Original: store deliver header “X-Spam-Status: No”
Modified: deliver header “X-Spam-Status: No”

The downside to this process is that you will not be able to train MailScanner with mail that was spam and got through as clean, as there is no reference for the email any longer. It is also suggested that you then modify the signature file(s) at /etc/MailScanner/reports/inline.sig.html and /etc/MailScanner/reports/inline.sig.txt to remove the link which will no longer work.

Report as SPAM footer for Multiple Domains

When configuring ESVA for a single domain, all scanned email that is delivered as clean has a link at the bottom of the email to report false negatives as SPAM. In an environment with multiple domains, however, a few additional steps are required to place the link on email for ALL domains.

1. Log into your ESVA using an SSH client (putty or similar) as the username created during the setup process, then switch to the root account (type su-l and enter the root password when prompted)
2. Edit the /etc/MailScanner/rules/sig.html.rules and/or sig.text.rules files:
[root@mail-gw ~]#nano -w /etc/MailScanner/rules/sig.html.rules
3. The file will only have 1 active line to begin with that we are concerned with here:
To: *@yourinitialdomain.com /etc/MailScanner/reports/en/inline.sig.in.html
4. Add a line for each domain you are accepting mail for:
#This rule will only come into force if the domain is specified in...
#From: *@domain1.com /etc/MailScanner/reports/domain1.sig.txt
To: *@yourdomain.com /etc/MailScanner/reports/en/inline.sig.in.html
To: *@yourotherdomain.com /etc/MailScanner/reports/en/inline.sig.in.html
To: *@yourthirddomain.com /etc/MailScanner/reports/en/inline.sig.in.html
To: default /etc/MailScanner/reports/en/inline.sig.out.html

Report as HAM footer

Inbound email already gets a footer attached that says it has been checked and a link to allow the user to report the message as SPAM in case it made it through the filters.

You can also add an additional link to let the user report the message as HAM (not SPAM) in order to help the system learn. In the existing system the user would have to navigate what may be a 'confusing to a non-techie' system of screens to classify their email.

Although the admin user has the Message Operations screen they would have to decide for the user which messages were which.

Follow the steps below to add a link to the sig.in files that allows the user to classify the current message as *either* spam or ham.

--

This message was scanned by ESVA and is believed to be clean.

[Click here to 'learn' this message as spam.](#)

[Click here to 'learn' this message as ham \(not spam\).](#)

1. Log into your ESVA using an SSH client (putty or similar) as the username created during the setup process, then switch to the root account (type su-l and enter the root password when prompted)
2. Copy learn-msg.cgi to learn.spam.cgi and learn.ham.cgi
cp learn-msg.cgi learn.spam.cgi
cp learn-msg.cgi learn.ham.cgi

3. Modify the following in learn-ham.cgi
Change the --spam flag to --ham.
Change the success redirect url to learned-ham.html.
4. Modify the following in learn-spam.cgi
Change the success redirect url to learned-spam.html.
5. Copy learned.html to learned-spam.html and learned-ham.html in /var/www/html:
cp learned.html learned-spam.html
cp learned.html learned-ham.html
6. In learned-ham.html, modify the text to reflect the fact that you are learning ham.
7. Modify learned-spam.html to correct the word 'acheive'.
8. Modify inline.sig.in.txt and .html to include the additional link in
/etc/Mailscanner/reports/en: (or your language(s))
Click here to report this message as spam.
[http://mail.mydomain.com/cgi-bin/learn-spam.cgi?id=\\$id](http://mail.mydomain.com/cgi-bin/learn-spam.cgi?id=$id)
Click here to report this message as ham (not spam).
[http://mail.mydomain.com/cgi-bin/learn-ham.cgi?id=\\$id](http://mail.mydomain.com/cgi-bin/learn-ham.cgi?id=$id)

Destination Address Verification on Incoming Mail

One additional step you can take to reduce the amount of SPAM you have to process is to enable address verification on inbound messages. By configuring ESVA to check the validity of an email address, and store the result in a database, you can cut the number of messages you have to process by a hundreds or even thousands of messages a day.

Postfix performs the address verification before it accepts the email in the first place. The verification transaction takes less than a second to verify good vs. bad addresses, and it stores them in a cache by doing the following:

```
helo mygateway.foo.bar
mail from: <postmaster>
rcpt to: <checkingrecipient>
-----??? RESPONSE ???----- (either 250 or 550)
rset
quit
```

250 = good, 550 = bad. These results are cached in the verify.db.

When initially configuring this feature, be sure to configure it in "warn" mode first to make sure your target server supports it properly. Instructions on how to configure warn are at the end of this section.

In order to configure address verification, modify your /etc/postfix/main.cf file (this example will use the command line).

```
[root@mail-gw ~]#nano -w /etc/postfix/main.cf
```

Navigate to the end of the file to a section that looks similar to the following. You will need to add the lines in **RED**:

```
# Note: avoid hash files here. Use btree instead.  
address_verify_map = btree:/var/postfix/verify
```

```
smtpd_recipient_restrictions = permit_mynetworks,  
reject_non_fqdn_recipient,  
reject_unknown_recipient_domain,  
reject_unauth_destination,  
check_recipient_access hash:/etc/postfix/recipient_access, check_policy_service inet:127.0.0.1:60000,  
reject_unverified_recipient
```

The first line you add (after the comment) is the database that caches good and bad emails as they are learned. The last line is where the invalid emails are rejected. This command tells postfix to use the verify command on all incoming messages and reject invalid recipients.

Once you have the above lines in main.cf, make sure you do the following:

```
mkdir /var/postfix.  
chown postfix:postfix /var/postfix  
service postfix reload
```

Enabling WARN on new settings

When you're testing any new settings in the main.cf file, you should enable warning for the new setting (especially if it would reject with no chance or recovery). To warn instead of outright rejecting an unverified recipient (in case your server isn't configured right, just in case), you would configure the last line from above as follows:

```
warn_if_reject reject_unverified_recipient
```

Instead of actually bouncing the message (or all messages if verify isn't working properly), you will get a warning in maillog (grep for reject_warning in maillog). Once you are satisfied that legitimate email would be getting through and only mail to invalid addresses are being stopped, remove the warn_if_reject from the main.cf file and restart postfix again.