



Verimation Mail Security Gateway Installation and Configuration Guide *Version 5*

Table of Contents

Overview	3
Installation	3
Supported Linux Distributions	3
Prerequisites for VMSG	3
Port Availability	4
Disabling Applications	4
Finding a process currently bound to a port	5
Installing VMSG	5
Download the distribution.....	5
Set permissions	5
Run the installation script	6
Quick Configuration	8
Minimum Required	8
Additional Steps	12
Testing the Configuration	12
Testing Inbound Mail	12
Testing Outbound Mail.....	12
Troubleshooting Inbound Mail Configuration.....	13
Troubleshooting Outbound Mail Configuration.....	14
Optional Configuration	14
Adding Users.....	14
External Directory.....	14
Batch Import from CSV	15
Manual Creation	16
Configuring VMail®	16
Configuring VMail® Policies	17
Configuring VMail® Send Policies	19
Configuring VMail® Send Policies	21
SMTP Rules Overview.....	22
Fine-tuning SMTP Rules	23
Setting the Product License	24



Overview

The Verimation Mail Security Gateway offers the best protection available today against mail-borne threats with the highest possible detection rates for spam, phishing and viruses and the lowest possible false positive rates. But that's not all. VMSG also supports VMail®. VMail is a new way to send and receive e-mail over the Internet that offers these benefits:

- Both sending and receiving servers can verify one another ensuring only legitimate servers send VMail
- Encrypted transport of all messages over the Internet ensuring the privacy of your mail conversations
- Automatic message status notification including that a message has been successfully delivered
- Visual indication that a message is VMail (Supported by most mail clients)
- Separate send and receive policies with per-user requirements/exceptions for fine-grained control
- Compatible with existing mail infrastructure

Installation

Before installing VMSG, please make sure that the minimum requirements for your Linux distribution are met.

Minimum System requirements for the Server:

- Minimum 2 GB of free hard drive space for neonInsight installation
- neonInsight installation directory is /opt/insight
- User Disk Space - To be determined by user activity
- Minimum of 512MB swap partition
- Pentium 4 class or higher i686 based processors
- 1 GB Ram (If SpamAssassin is to be used: Minimum of 2 GB Ram)
- Network Interface Card/Ethernet

Supported Linux Distributions

VMSG supports a variety of Linux operating systems and will run on most major distributions.

The following has been tested with neonInsight:

- SuSE Linux Enterprise Server 10 or higher
- Debian GNU/Linux 4.0 or higher
- Red Hat Enterprise Linux 5 or higher
- Fedora Core 5 or higher
- CentOS 4 or higher

Prerequisites for VMSG

The following section lists the prerequisites for installing VMSG. The installation will utilize these prerequisites when configuring the mail server. This information must be correct prior to installing the software. If this information is not correct, it will not be configured properly and could stop your mail server from functioning properly.



- TCP/IP address of mail server
- Hostname of mail server
- VMSG will automatically configure the initial (primary) domain with the hostname of the server. It is important that this information be correct prior to installation.
- Domain in which the server will reside
- VMSG license key or demo key

The following commands can be used on your Linux server to validate that the items above are properly configured:

COMMAND ACTION

hostname -a Hostname of the system

hostname -d Domain name of the system

hostname -f Fully Qualified Domain Name (FQDN)

netstat -tan Displays ports that are currently being used

Port Availability

The following ports will be used by VMSG:

Port Description of Port Use

25 SMTP

80 HTTP

389 LDAP

443 HTTP over SSL

2525 Outbound SMTP (may be changed as needed)

4369 Port Mapper Daemon

10024 Amavisd

10025 Amavisd

33333 VMSG Admin Interface

Disabling Applications

Most Linux distributions install certain applications by default. For example, sendmail is a standard MTA that is usually installed by default on most major Linux distributions. Since VMSG is its own mail server, sendmail can cause conflict and will need to be disabled. The same is true with Apache. The following shows how to disable sendmail and Apache:

sendmail:

Red Hat-type servers:

```
#chkconfig sendmail off
```

Debian-type servers:

```
#update-rc.d -f sendmail remove
```

This will permanently disable sendmail from starting up during the reboot process.

Apache:

Red Hat-type servers:

```
#chkconfig httpd off
```



Debian-type servers:

```
#update-rc.d -f apache2 remove
```

This will permanently disable the Apache process from starting up during the reboot process.

NOTE: For proper installation of VMSG, SELinux and AppArmor must be disabled.

Finding a process currently bound to a port

To locate which process is currently bound to a given port, use the netstat command. A portbound process can keep the server from installing properly. Use the port requirement chart above with the netstat command to determine what is stopping the software installation. For example, if you have a slapd process running on your server, port 389 will most likely be bound to it. To verify this, type:

```
#netstat -tanp|grep 389
(results)
tcp 0 0 0.0.0.0:389 0.0.0.0:* LISTEN 13097/slapd
```

These results show that the slapd process is bound to port 389. To continue with the installation, this process must be stopped.

Red Hat-type servers:

```
#chkconfig ldap off
```

Debian-type servers:

```
#update-rc.d -f ldap remove
```

This will permanently disable slapd from running on this server.

Installing VMSG

Overview:

- Download the distribution
- Set permission
- Run the installation script

Download the distribution

The latest release of the VMSG can be downloaded from:
<http://techserv.verimation.se/products/vmsg/latest/>

Set permissions

Once the package has been downloaded, the permissions must be set. The downloaded file needs to have the following permissions:

Owner – Read, Write, Execute

other users – Read, Execute



To change permissions on the downloaded file, type the following command at a command line prompt:

```
#chmod 755 <vmsg-filename> <enter>
```

Permissions can also be changed by typing the following at a command line prompt:

```
#chmod a+x <vmsg-filename> <enter>
```

Run the installation script

Installing VMSG is completed with a few simple steps:

1. As “root”, navigate to the directory where the install script is located.
NOTE: Installation must be performed as the “root” user. When using the “su” (substitute user) command, be sure to also add “-“. Executing “su -“ grants the full “root” shell and environment whereas simply executing “su” retains the original user’s shell and environment.
2. Add any special install flags (optional)
 - a. Flags include
 - i. ADMINPASSWORD=password
Replace “password” with the password you would like set for this account. If this flag is not used, a password will be assigned and displayed at the end of the installation process.
 - ii. LICENSE=your license number
Entering in a license number will automatically register the server during the installation process.
How the flags would look with the installation script:


```
# ADMINPASSWORD=admin LICENSE=key ./neonInsight-gateway-5.2-i386-123.sh
```
3. Or simply start the installer
 - a. ./neonInsight-gateway-5.2-i386-123.sh

```
test1:~# ADMINPASSWORD=qwerty ./neonInsight-gateway-trunk-i386-126.sh
```

NOTE: the file name above is for example purposes only. To install your version of the neonInsight Server, you must use the specific file name that you downloaded.

Once the Installation has started the license agreement will be displayed.

```
titled to subsequent support except at full fair market value. If Custod
6.MAINTENANCE:
--More--
```

One page at a time will be displayed. You move to the next page by pressing the spacebar.

On the last page you will be asked whether you accept the license agreement or not. Type “yes” to agree and continue with the installation or “no” to abort the installation.

```
Type 'yes' to agree to the license terms and continue, or 'no' to abort the installation.
```

If you typed “yes” the installation will start. You will get feedback that the installation is in progress by additional “dots” being added to the output line.

```
Installing to /opt/neonInsight.....
```



NOTE: You will be notified of the default administrator account name and password. If you did not specify the password on the command line you should make a note of the randomly generated password and change it as soon as possible.

Quick Configuration

The following configuration instructions assume the system will act as the outermost (Internet) mail server. It is divided into 2 parts: minimum required configuration and optional settings that you may or may not want or be able to use depending upon your internal infrastructure.

VMSG may be placed anywhere in an SMTP chain. However, some functionality may only be used when VMSG acts as the outermost SMTP server.

Minimum Required

The system is pre-configured to act as the outermost SMTP server. As such, it assumes it will receive mail on port 25 like any other SMTP server and send the mail via SMTP to the internal mail system. It also assumes that outgoing mail will be received from the internal mail system via SMTP on a different port (port 2525 by default).

The first thing to do is configure the proper routing.

1. Start your favorite web browser and type the URL of the VMSG server using either its name or IP address. For example:

http://mail.my.com

or

http://10.75.18.123

NOTE: You may also use *https* in the URL for an SSL connection.

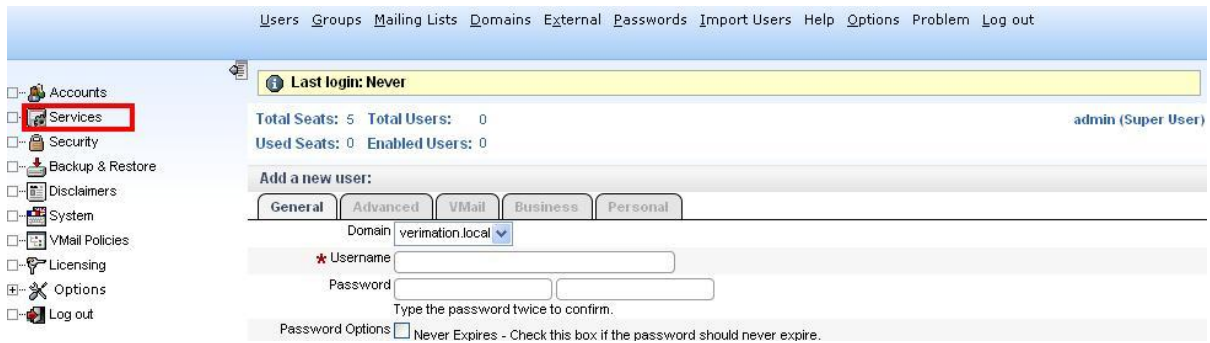


2. On the login page set the username to "admin" and the password to the password you set during installation or the automatically-generated password if you did not explicitly set one during installation.





3. Select the "Services" node in the left-hand tree.



4. Under "Delivery Services" click the "Configure" icon for the "SMTP (InboundDelivery)" service



5. On the "Advanced" tab under "Message Routing", set the Server Address and Port of the SMTP server that should receive inbound mail. For example:

Server Address: *internalmail.my.com*

Port: 25

OR

Server Address: *10.75.18.321*

Port: 12345

Configure SMTP (InboundDelivery)

Basic Settings | **Advanced Settings**

Session Limitations

Max. Sessions: ⓘ

Max Data Chunk: ⓘ

Retry Settings

Retry Interval: ⓘ

Warning Interval: ⓘ

Abandon Interval: ⓘ

Message Routing

Server Address: ⓘ

Port: ⓘ

Server DNS Lookup Type: ⓘ

6. Click the "Save" button

7. On the Services Summary page under "Client Services" click the "Configure" icon for the "SMTP (OutboundDelivery)" service

Client Services

Service	Address	Port	
SMTP (External-SMTP)	localhost	25	  
SMTP (From-Amavis)	127.0.0.1	10025	  
SMTP (OutboundDelivery)	localhost	2525	  

8. On the "Basic Settings" tab, set the "Port" the server should listen on for outbound mail coming from your internal mail system.

NOTE: Your internal mail system must be configured to send outbound mail to VMSG on this port. You MAY NOT specify port 25 for "OutboundDelivery" port as it is already in use for incoming mail from the Internet.

Configure SMTP (OutboundDelivery)

Basic Settings | **Advanced Settings** | SMTP Rules | VMail Settings | Extensions

Name: OutboundDelivery ⓘ

Port: ⓘ

Auto-start: ⓘ

SSL: ⓘ

Trace Level: ⓘ

9. Click the "SMTP Rules" tab, then the "Recipient Rules" tab

Configure SMTP (OutboundDelivery)

Basic Settings | Advanced Settings | **SMTP Rules** | VMail Settings | Extensions

Connect Rules | HELO Rules | Sender Rules | **Recipient Rules**

Available Rules

- * check-client-access
- * check-greylist
- * check-recipient-access
- permit-authenticated
- permit-config-local-recipient
- permit-local-recipient
- permit-local-recipient-only
- permit-local-sender
- * permit-recipient-from-network
- * permit-recipient-to-domains

Selected Rules

- reject-vmail-only
- enforce-local-mail-only
- reject-nonauthorized-mailinglist
- * permit-networks
- reject-nonauthenticated

SAVE | RESET

10. Double-click the "permit-networks" rule in the "Selected Rules" window

Configure SMTP (OutboundDelivery)

Basic Settings | Advanced Settings | **SMTP Rules** | VMail Settings | Extensions

Connect Rules | HELO Rules | Sender Rules | **Recipient Rules**

Configure permit-networks

Explicitly permits action when the client's IP address matches at least one of the IP-address-patterns. Set the 'networks' parameter as a comma-separated list of IP addresses, using the '*' wildcard as needed.

networks: 192.168.30.151

OK | Cancel

Available Rules

- * check-client-access
- * check-greylist
- * check-recipient-access
- permit-authenticated
- permit-config-local-recipient
- permit-local-recipient
- permit-local-recipient-only
- permit-local-sender
- * permit-recipient-from-network
- * permit-recipient-to-domains

SAVE | RESET

11. Enter the IP address of your internal mail server in the "networks" text field. For example

networks: 10.75.18.321

If multiple servers/machines will be sending outbound mail separate the addresses with a comma. For example:

networks: 10.75.18.321,10.75.18.322,10.75.18.323

You may also use "*" as a wildcard:

networks: 10.75.18.32*

or

networks: 10.75.18.*

NOTE: Use of wildcards can be a security risk since any address matching the wildcard pattern will be allowed to send outbound mail.

12. Click the "Save" button



13. Congratulations! VMSG is now configured and ready for use. Please see the "Testing the Configuration" section for tips on how to verify the routing.

Additional Steps

If you installed VMSG on the same machine as your existing gateway server there is little left to do except check out the "Optional Configuration" section to see if there are configuration options that meet your needs.

If you have installed VMSG on a different machine you will need to ensure that the new machine is added as an MX record in DNS. Your network administrator and/or Internet Service Provider can assist with this. Additionally, you should probably also add a "reverse lookup" record (a so-called PTR record) to DNS. It has become increasingly common that receiving servers will not accept mail from your server if there is no PTR record.

Testing the Configuration

Testing the configuration entails ensuring that mail coming from outside makes it to your internal mail system and mail going out to the Internet goes out.

Testing Inbound Mail

The easiest way to test inbound mail is to send a mail to yourself from some external mail system, for example your home mail account or one of the free public services like GMail, Hotmail or Yahoo. If VMSG is not yet "live", i.e. only accessible internally, or the MX record has not yet been updated it will take a little trickery to test inbound routing.

In this case, you will need an Internet mail client such as Windows Mail, Thunderbird or Outlook Express. How you configure them differs a bit but since we are only interested in the SMTP configuration those are the only parameters that need to be set correctly. The key parameters are:

1. Sender e-mail address for the account. You can pretty much use any real or imagined address you like. The best choice is probably a real address from an external account (your home mail address, GMail, etc.) as you will be able to check it for bounced mail.
2. SMTP Server Address. Set this to the IP address of the VMSG server, for example 10.75.18.123.
3. Make sure the client is not configured to authenticate. Remember, we're trying to simulate mail coming from the outside where authentication is not used.
4. Make sure that SSL/TLS is turned off entirely (Some clients have a "use if available" setting). VMSG supports SSL/TLS. By ensuring the client does not attempt to use it we eliminate any potential client configuration issues.

Once configured, try sending a mail to your internal address. If the mail ends up in your Inbox everything is configured correctly. If not, it may or may not indicate a configuration problem as the mail may have quarantined as potential spam. See the **Troubleshooting Inbound Mail Configuration** section for tracking down configuration issues.

Testing Outbound Mail

Testing the outbound mail configuration is similar to in the inbound tests but in reverse. That is, you send a mail from your internal mail system to an address outside the system to verify that the mail actually arrives at its destination.



See the **Troubleshooting Outbound Mail Configuration** section for tracking down configuration issues.

Troubleshooting Inbound Mail Configuration

The first thing to determine is whether VMSG accepted the mail for delivery. Normally, the client will indicate some kind of error occurred if the mail was rejected directly during its conversation with the server. In most cases, the client will display some kind of error message, and most will allow you to see more detailed information, for example what the server said was the reason.

In most cases, this will be caused by VMSG not recognizing the "To" address as an address it accepts mail for. It may be that the address is misspelled, or if you have created users in the system, that the address does not exist. If this is the case, the error message from the server will be something like "must be authenticated" or "relay not allowed".

Some clients do not follow the SMTP specification. The default configuration will reject mail from senders that do not present a so-called "fully-qualified EHLO hostname" and the error message will be something to that effect. You can temporarily work around that problem by easing the controls a little bit:

1. In the web admin, select Services and click the "Configure" icon for the "SMTP (External-SMTP)" client service.
2. Click the "SMTP Rules" tab and then the "Sender Rules" tab
3. Remove the "reject-non-fqdn-helo-hostname" rule from the "Selected Rules" window (Click it and then click the left arrow icon).
4. Click the "Save" button

If you have not received any error from the client you'll want to check the different mail queues to see if it is stuck in one of them for some reason. The first place to look is the queue intended to send the mail on to your internal mail system. You view that queue as follows:

1. In the web admin, select Services and click the "Queue" icon for the "SMTP (InboundDelivery)" delivery service (the magnifying glass icon to the far left).

If there is anything in the queue you'll see it there. Depending upon the cause, there may also be a message giving you a hint as to what the problem might be. In this case, the message is from the server you have configured VMSG to send inbound mail to.

Regardless of whether there is a "hint" or not you must make sure the server address and port you configured as the next hop is correct, and that that server is configured to accept mail from VMSG.

If the "InboundDelivery" queue is empty you'll next want to check the "SMTP (internet)" queue. A message in this queue is almost certainly a "bounce" mail (triggered by the test mail you sent) that could not be sent for some reason. If you simply made up an e-mail address for your sender address it will not be able to contact the server and will attempt to resend the mail (standard practice within SMTP when the server or DNS appears to be down). If it was a real mail address then the receiving server has probably temporarily rejected the mail for some reason.

If no mail is in the "internet" queue you'll next want to check the account from which you sent the test mail (assuming it was a real account). If you received a bounce mail in that account it should contain information as to why the mail was bounced. This mail may have been generated by VMSG or by your internal mail system. If it was generated by VMSG you should ensure the "InboundDelivery" server address and port settings are correct and that the server you have configured VMSG to send to is also properly configured to accept mail from VMSG.



If there is no mail in any of the queues and you did not receive a bounce mail then you'll want to check the spam quarantine:

1. Click the "Security" node in the left hand tree. This should open Maia Mailguard in a new window or possibly a new tab, depending upon your browser, and you should be automatically logged in as admin.
2. Click the "Admin" node in the Maia left hand tree
3. Click "Users"
4. Click the "Find Users" button
5. Click the e-mail address of the account you sent the test mail to.
6. On the page that displays, if the mail was quarantined you will see "You have 1 items in your spam cache." on the second line in the table (where the number of items may be different but will be non-zero).

If none of this helps, you can turn on the trace function for one or all of the "Client" and "Delivery" services. Trace may be turned on from the configuration page of each of the services where "Detailed Trace" should provide enough information. The trace files will be found on the VMSG machine under /opt/neonInsight/var/neon/trace where the "Client" service files will be named neon_smtpin_trace<port_number>.txt (for example neon_smtpin_trace25.txt) and the "Delivery" service files will be named neon_delivery_<queue_name>.txt (for example neon_delivery_InboundDelivery.txt).

The trace files will contain date/time information, the IP address of the the other application and the SMTP conversation. If the trace does not help track down configuration issues please contact your VMSG representative for assistance.

Troubleshooting Outbound Mail Configuration

Troubleshooting outbound mail is similar to inbound mail but in reverse. That is, first you must verify that the mail has left the internal mail system and where it has been sent. If it has been sent to VMSG, you should check the queues to determine if it has gotten stuck somewhere.

Optional Configuration

The following sections outline common additional configuration that you may want or need. For more complex scenarios please contact your VMSG representative for assistance.

Adding Users

In order for VMSG to know which mail addresses are valid or not it must have access to "user" information. There are several different ways to create user information. The following sections outline the different methods.

External Directory

VMSG is capable of directly importing user information from Microsoft Active Directory and Samba. To import user information from Active Directory or Samba do the following from the web administration:



1. Click on the “Account” node in the left-hand tree
2. Click the “External” icon in the toolbar at the top
3. Check the “Get users from an external directory” checkbox
4. Select the “Active Directory” or SAMBA radio button
5. Specify the server name or IP address and the port of the external directory to import from
6. Specify the LDAP Base DN from which to start finding users. If users are all grouped under a single node in the external directory you’ll want to set that node as the Base DN.
7. Specify the LDAP Distinguished Name and password of a user that has read access to the user information. This may be any existing user but it is probably best to create a new user in AD/SAMBA whose password will not expire.
8. Set the “Automatic refresh interval” to the number of seconds between automatic updates from the external directory. If you do not want automatic updates set this to “0” (zero).
9. Click the “Refresh Now” icon to populate VMSG’s directory with the user information.
10. Click the “Set” button to save your settings

Batch Import from CSV

VMSG is capable of importing user information from a specially formatted CSV file. It is possible to auto-generate the CSV file from information exportable from either directory server but requires some custom processing which lies outside the scope of this document. For Active Directory there is a Windows-based tool for generating the CSV file directly. Please contact your VMSG representative for details.

The CSV file may also be generated manually. You may download a template file from the web administration or create it entirely by hand. Please see the **Creating the CSV File by Hand** for more information.

NOTE: *While these instructions primarily explain how to perform the first import, the import functionality allows you to batch update user information as well.*

Importing the CSV File

The CSV file import is performed through the web administration. To import the file do the following:

1. Click the “Accounts” node in the left hand tree
2. Click the “Import Users” toolbar button at the top of the page
3. Click the “Browse” button and select the file to import

NOTE: *Clicking anywhere on the “Click here to download the Import User CSV template” will download the CSV template file which may be used to create a properly formatted CSV file.*

4. If you have configured more than one mail domain you will need to select the domain in which to import the users.
5. Click the “Next” button
6. The default settings on the next page should be OK so click the “Next” button
7. Verify that the information appears to be correct, i.e. the proper values appear in the proper columns. If so click the “Import” button.



When the import is finished you will come to the “Results” page telling you how things went. From there you can view more detailed information button, download your CSV with updated values (including any randomly-generated passwords), print the information or start a new import.

Creating the CSV File by Hand

The CSV format consists of a “header” line followed by one or more lines of user information with one line representing the information for one user. While the format is called CSV (Comma Separated Values” either a comma (“,”) or semicolon (“;”) may be used to separate the header line names and the user entry values.

Many spreadsheet applications, for example Excel and the Open Office Suite, are capable working with CSV files. But because it is a text-based format any text editor will do.

At a minimum, the “username” and “email” fields should be set for each user. If a user has more than one e-mail address, set the primary mail address as the “email” field value and the additional addresses as a quoted string with each separated by a comma in the “alias” field. For example:

```
username,email,alias
```

```
alice,alice.smith@my.com,"alice@my.com,asmith@my.com,sales@my.com"
```

```
bob,bob.jones@my.com,bob@my.com,bjones@my.com,marketing@my.com
```

If users should be able to access the mail quarantine then you should also add “newpassword” to the header and provide a value for each user. If no password value is found in the CSV file randomly generated password values will automatically be set.

NOTE: A random password is only generated if no value for the “newpassword” field is in the file AND the user does not already exist.

Manual Creation

Users may be created manually via the web administration. As a practical matter, there are two types of users that you may want to create this way. The first is System Administrators. System Administrators have essentially the same rights as the “admin” user, i.e. they are capable of accessing and configuring all parts of the system. The advantage of System Administrator accounts is that changes made to the system can be tracked to individuals rather than several people all using the admin account.

The second type is normal users. By creating users in the system, VMSG is able to determine whether incoming mail to a given address represents a valid mail address. Without access to this information, it will accept mail to any address as long as the domain part of the address is known to the system.

NOTE: Even if you have configured the system to automatically synchronize with an external directory you may still create other users in the system. This may be useful for users not listed in the external directory where adding, disabling or deleting them may be quicker and easier via VMSG to get mail working for them.

Configuring VMail®

VMail® is a new way to send and receive mail over the Internet. For the first time, it is now possible for users to send and receive mail over the Internet without having to have an Internet e-mail address. This removes spammers, whether bulk-mail server or bot-net based, entirely from the picture keeping your Inbox clear of dangerous content. VMail also enforces the security policies you set down to the user level allowing for fine-grained control over who can do what and with whom.



NOTE: In order to use VMail you must also create users in VMSG using one of the methods outlined in the Adding Users section.

The first step in configuring VMSG for VMail is obtaining a VMail certificate. To obtain a “production quality” certificate please contact your VMSG representative for assistance. If you would like to give VMail a try please do the following:

1. In the web administration click the “System” node in the left-hand tree
2. Click the “Try VMail” link on the bottom line, right-hand column
3. Fill in the form fields with the proper information and click the “Try Now” button

NOTE: The information you enter in the form is only used to populate the appropriate fields in the Certificate.

Upon successful completion the certificate(s) will have been generated and installed in VMSG. You must still specify the certificate to use for incoming VMail:

1. In the web administration click the “System” node in the left-hand tree
2. Click the “VMail” icon in the toolbar at the top of the page
3. Select the domain from the drop-down list to use as the default and make sure the “Enabled” button is checked.
4. Click the “Update” button
5. Click the “Services” icon in the web administration left-hand tree
6. Click the “Configure” icon for the “SMTP (External-SMTP)” Client Service
7. Click the “VMail” tab
8. Select the certificate to use (if more than one) from the drop-down list
9. Check the “Enabled” checkbox
10. Click the “Save” button

Inbound VMail is now configured. To configure VMail for outbound mail do the following:

1. Click the “Services” icon in the web administration left-hand tree
2. Click the “Configure” icon for the “SMTP (internet)” Delivery service
3. Check the “VMail” checkbox near the bottom of the form and then the “Save” button

NOTE: The proper VMail certificate for outbound mail is selected based on the domain part of the sender’s e-mail address. If there is no certificate for that domain then VMail will not be used.

Configuring VMail® Policies

VMail policies can provide fine-grained control over when or if VMail is used in different situations. There are two main types of VMail policies: Send Policies and Receive Policies. These govern when or if VMail should be applied when sending or receiving mail, respectively.

While the policies are defined at the system level, they are applied at the user level. This is accomplished by associating a policy with each user. In addition, some policy aspects may be customized for individual users where the users themselves, if allowed, may also customize that portion for themselves. If no policy is associated with a given user, the system-defined default will be used.



There are two pre-defined policies for each of the Send and Receive policy types, “VMail if Available” and “VMail Required”. As implied by their names, the “VMail if Available” policy will use VMail if the other side supports it, otherwise mail is sent/received as normal Internet mail. The “VMail Required” policy, on the other hand, will not send/receive the mail unless both servers are VMail-capable. The factory default Send and Receive policies are “VMail if Available”, i.e. VMail will always be used when supported by both sides, otherwise normal Internet mail if use. Keep in mind that the policy used is governed on a per-user basis depending upon the policy associated with the user.

Policies may be further refined through the use of the policy’s “Required” and “Exceptions” lists. These lists can consist of individual e-mail addresses or entire e-mail domains. As the name implies, the “Required” list means that VMail **MUST** be used when sending/receiving mail with the addresses or domains in the list. This is useful for the “VMail if Available” policy to ensure that VMail is always used when communicating with specific individuals or domains. The “Exceptions” list works in the reverse, i.e. mail from/to the given addresses and/or domains do not require VMail. This is useful for users with the “VMail Required” policy who sometimes need to communicate with non-VMail systems.

“Required” and “Exception” lists may be further tuned on a per-user basis by specifying the required or excepted addresses and/or domains on the user entry. This makes maintaining the system policies easier by not cluttering them with information that applies only to one or a few users. It is also possible to specify whether the users themselves are allowed to edit their own lists, either on a system policy basis or an individual user basis.


The pre-defined “VMail if Available” and “VMail Required” Send Policies are probably the only ones you’ll need. You may, however, create new policies if needed, and may set which policy is the default. Note that changing the default policy will not change the policy already associated with users.





The primary task of configuring and maintaining the VMail Policies is maintaining the “Required” and “Exceptions” lists. While there are no hard and fast rules, the rule of thumb is that only addresses and/or domains that apply to all users with the associated policy should be set on the policy. Addresses and/or domains that only apply to one or a few users should be set on the users themselves.


You can view and edit the policies by clicking the “VMail Policies” in the web admin left-hand tree.





VMail Policies

VMail policies offer a convenient way to manage your VMail Send and Receive settings. Each user is associated with a set of policies that govern when or if VMail will be used in different situations. When a Send or Receive Policy is changed, that change applies automatically to all associated users.

 **VMail Send Policies**

-   **VMail If Available (VMail not required, Have Required Addresses, No Exception Addresses)**
-   VMail Required (VMail Required, No Required Addresses, Have Exception Addresses)

 **VMail Receive Policies**

-   **VMail If Available (VMail not required, Have Required Addresses, No Exception Addresses)**
-   VMail Required (VMail Required, No Required Addresses, Have Exception Addresses)



The initial view provides an overview of your current policy settings. The page is divided into Send and Receive policies, with all policies of a given type listed under its corresponding heading. The default policy for each type is displayed in bold. Each policy also displays key information about the policy within parentheses.

You may access and edit the properties of the policy by clicking the “+” sign next to the policy name:

VMail Policies

VMail policies offer a convenient way to manage your VMail Send and Receive settings. Each user is associated with a set of policies that govern when or if VMail will be used in different situations. When a Send or Receive Policy is changed, that change applies automatically to all associated users.

VMail Send Policies

-  **VMail If Available (VMail not required, Have Required Addresses, No Exception Addresses)**
-  **VMail Required (VMail Required, No Required Addresses, Have Exception Addresses)**

VMail Receive Policies



-  **VMail If Available (VMail not required, Have Required Addresses, No Exception Addresses)**
-  **VMail Required (VMail Required, No Required Addresses, Have Exception Addresses)**

To delete a policy click the trash can icon next to the policy name.


VMail Policies

VMail policies offer a convenient way to manage your VMail Send and Receive settings. Each user is associated with a set of policies that govern when or if VMail will be used in different situations. When a Send or Receive Policy is changed, that change applies automatically to all associated users.

VMail Send Policies

-  **VMail If Available (VMail not required, Have Required Addresses, No Exception Addresses)**
-  **VMail Required (VMail Required, No Required Addresses, Have Exception Addresses)**

VMail Receive Policies



-  **VMail If Available (VMail not required, Have Required Addresses, No Exception Addresses)**
-  **VMail Required (VMail Required, No Required Addresses, Have Exception Addresses)**

To create a new policy, click the “Create” icon on the policy type heading line.


VMail Policies

VMail policies offer a convenient way to manage your VMail Send and Receive settings. Each user is associated with a set of policies that govern when or if VMail will be used in different situations. When a Send or Receive Policy is changed, that change applies automatically to all associated users.

VMail Send Policies

-  **VMail If Available (VMail not required, Have Required Addresses, No Exception Addresses)**
-  **VMail Required (VMail Required, No Required Addresses, Have Exception Addresses)**

VMail Receive Policies

-  **VMail If Available (VMail not required, Have Required Addresses, No Exception Addresses)**
-  **VMail Required (VMail Required, No Required Addresses, Have Exception Addresses)**

NOTE: Changes made to policies, including creating and deleting policies, do not take effect until after you click the “Update” button.

The following sections explain the Send and Receive policy settings in more detail.

Configuring VMail® Send Policies

By clicking on the “+” sign next to the policy name you gain access to the available settings for the policy:



VMail Send Policies

VMail If Available (VMail not required, Have Required Addresses, No Exception Addresses)

Name:

Description:

Check this box if VMail should be required when sending outside the system.

Success DSN Option:

VMail Required Addresses: +

VMail Exception Addresses: +

Check this box to allow users to edit their own Exception and Required addresses.

Use as the Default Send Policy

The available settings for Send Policies are:

Setting	Description
Name	A short unique name for the policy
Description	Text describing the policy and/or its intent
VMail Required checkbox	If this box is checked, the policy requires VMail on the receiving side in order to send mail. Only addresses and domains listed in the VMail Exception Addresses list can receive non-VMail from users associated with this policy. If the box is not checked, VMail will be used if available on the receiving side, otherwise mail will be sent as normal Internet mail unless it is addresses to addresses or domains in the VMail Required Addresses list, in which case it will only be sent if VMail is available on the receiving side.
Success Delivery Notification	This setting determines in which cases a “Success” Delivery Status Notification will be sent back to the sender of a mail. A Success DSN is returned when a mail has been successfully delivered to a recipient’s mailbox.
Required Addresses	A list of e-mail addresses or domains to which VMail is required in order to send the mail. If VMail is not available on the receiving side the mail will not be sent, and therefore returned to the sender. Note that Required addresses only have an effect on “If Available” policies.
Exception Addresses	A list of e-mail addresses or domains to which VMail is NOT required in order to send the mail. If VMail is not available on the receiving side of a “VMail Required” policy the mail will not be sent unless the address or domain is in the exception list. Note that Exception addresses only have an effect on “VMail Required” policies.
Allow User Edit checkbox	Checking this box means that users associated with this Policy may edit their own Exception and Required lists, i.e. the lists associated

	with their user entries. Otherwise, users cannot edit their per-user Required and Exception lists. <i>Note that this setting only governs the per-user lists. The policy lists may only be changed by an administrator.</i>
Default Policy checkbox	Check this box to make the policy the default send policy. <i>Note that users already associated with a policy will not be affected by the change.</i>

Configuring VMail® Send Policies

By clicking on the “+” sign next to the policy name you gain access to the available settings for the policy:

VMail Receive Policies

VMail If Available (VMail not required, Have Required Addresses, No Exception Addresses)

Name:

Description:

Check this box if VMail should be required when receiving from outside the system.

VMail Required Addresses: +

VMail Exception Addresses: +

Check this box to allow users to edit their own Exception and Required addresses.

Use as the Default Send Policy

The available settings for Receive Policies are:

Setting	Description
Name	A short unique name for the policy
Description	Text describing the policy and/or its intent
VMail Required checkbox	If this box is checked, the policy requires VMail on the sending side in order to receive mail. Only addresses and domains listed in the VMail Exception Addresses list can send non-VMail to users associated with this policy. If the box is not checked, VMail will be used if available on the sending side, otherwise mail will be received as normal Internet mail unless it is addressed to addresses or domains in the VMail Required Addresses list, in which case it will only be accepted if VMail is available on the sending side.
Required Addresses	A list of e-mail addresses or domains to which VMail is required in order to accept the mail. If VMail is not available on the sending side the mail will not be accepted. <i>Note that Required addresses only have an effect on “If Available” policies.</i>
Exception Addresses	A list of e-mail addresses or domains to which VMail is NOT



	<p>required in order to accept the mail. If VMail is not available on the sending side of a “VMail Required” policy the mail will not be accepted unless the sender address or domain is in the exception list.</p> <p><i>Note that Exception addresses only have an effect on “VMail Required” policies.</i></p>
Allow User Edit checkbox	<p>Checking this box means that users associated with this Policy may edit their own Exception and Required lists, i.e. the lists associated with their user entries. Otherwise, users cannot edit their per-user Required and Exception lists.</p> <p><i>Note that this setting only governs the per-user lists. The policy lists may only be changed by an administrator.</i></p>
Default Policy checkbox	<p>Check this box to make the policy the default send policy.</p> <p><i>Note that users already associated with a policy will not be affected by the change.</i></p>

SMTP Rules Overview

VMSG offers a large set of rules that may be applied during different parts of the inbound SMTP conversation. These rules are part of the layered anti-spam/anti-virus handling allowing SMTP conversations to be cut short when problems with the sending side are discovered.

Rules may be applied at different stages of an SMTP conversation starting with the initial connection. Rules for each stage are processed one at a time until a definitive “permit” or “reject” is returned by a rule. If no definitive result is returned and all rules have been processed, the stage is implicitly accepted and we move on to the next stage.

Most rule names begin with either “permit” or “reject”. As a general rule, “permit” rules will explicitly permit an action if the rule criteria are met but will not explicitly reject if the rule criteria is not met. By the same token most “reject” rules will explicitly reject but not explicitly accept.

This processing and rule logic is important to know not least for inbound SMTP from the Internet. Improper configuration, in particular of the “Recipient Rules” can lead to the server acting as an open relay. For this reason, you should pretty much always set the “reject-nonauthenticated” rule as the last Recipient rule.

SMTP Rules are configured by clicking the “Configure” button on the “Services” page for the instance you want to configure, and then the “SMTP Rules” tab. There are tabs for each configurable stage of an SMTP conversation where the left-hand window contains appropriate rules available for that stage and the right hand window contains the any select rules.

There are two ways to add an Available Rule as a Selected Rule. The first is to select the rule in the Available Rules window and then click the right arrow icon. The second is to double-click the rule in which case a dialog box opens displaying help text about the rule. Clicking the OK button in the dialog will add the rule to the Selected Rules window. Note that you may select multiple rules using the SHIFT and CTRL buttons when clicking on rules.

The order of the rules in the Available Rules window is important since rules are processed top to bottom and the order they appear can affect the overall logic for the stage. You can move rules up or down by selecting the rule(s) and clicking the up or down icons.

Some rules require information in order to work properly. These are denoted with an asterisk before the rule name. To provide the additional information you simply double-click the rule and fill in the information in the field(s) provided.



Some rules require the fully-qualified path and filename to a file residing on the server. You must, of course, create the file and its contents but important to note is that VMSG is installed under a so-called chroot. This means the file you create must be located somewhere under the chroot so that it is accessible to the server. It also means that the fully-qualified path and filename you specify in the rule dialog must be relative to the chroot and not the root of the file system.

The root location of the chroot is /opt/neonInsight. If you create the file under /opt/neonInsight/etc/neon/ (the preferred location for these types of files) then the path you specify in the rule dialog would be /etc/neon/.

One final note about external files: The files must be readable by the server. This means you either need to make it world-readable or change the file ownership to the user the server process runs as. To make it world-readable type the following command from a Linux shell (changing the path and filename to correspond to your file):

```
# chmod +r /opt/neonInsight/etc/neon/myfile
```

To change ownership of the file to the server process user type the following commands (again changing the path and filename to correspond to your file):

```
# neonInsight shell
# chown neon:neon /etc/neon/myfile
# exit
```

Fine-tuning SMTP Rules

While we will not go into all of the rules here, there are two rules worth special mention for inbound mail from the Internet. The factory default setting for deciding whether or not to accept mail for a given mail address is based solely on the domain part of the recipient e-mail address. If you have created users in the system AND want VMSG to verify the full e-mail address please do the following:

1. Click the “Services” icon in the web administration left-hand tree
2. Click the “Configure” icon for the “SMTP (External-SMTP)” Client service
3. Click the “SMTP Rules” tab
4. Click the “Recipient Rules” tab
5. In the left-hand “Available Rules” window select the “permit-local-recipient-only” rule and click the right arrow icon to move it to the “Selected Rules”.
6. Select the “permit-local-recipient-only” rule just added and click the up arrow icon to move the rule just below the “permit-local-recipient” rule.
7. Click the “permit-local-recipient” rule and then the left arrow icon to remove it from the “Selected Rules” window.
8. Click the “Save” button to save the changes

The difference between the “permit-local-recipient” and “permit-local-recipient-only” rules is that the former only verifies that the domain part of the recipient address is one handled by this server whereas the latter ensures that the recipient address is listed as the primary address or an alias of any of the users listed in the system.

The second rule worth special mention provides real-time blacklist lookup of the IP address of the entity trying to send mail and has proven very effective for minimizing the amount of mail accepted, and therefore AS/AV processed at a later stage.



By default this rule is not enabled as there are a large number of RBL (real-time blacklist) systems on the Internet, each with their own policies regarding how an address ends up on the list and any costs or limitations associated with using the service.

To configure RBL lookup do the following:

1. Click the “Services” icon in the web administration left-hand tree
2. Click the “Configure” icon for the “SMTP (External-SMTP)” Client service
3. Click the “SMTP Rules” tab
4. Click the “HELO Rules” tab
5. Double-click the “reject-rbl-client” rule
6. Fill in the name of the RBL authority in the space provided
7. Click the OK button
8. Click the “Save” button

NOTE: While the “reject-rbl-client” rule may be configured at any stage of the SMTP conversation, including directly after the sending entity has connected, the earliest point at which it should be set is in the HELO rules. If set in the Connect rules, the VMSG will not be able to give the sending side any indication as to why the connection is being dropped thus preventing possibly erroneously blacklisted sites from getting usable feedback as to why their mail is being rejected.

Setting the Product License

To set the product license key please do the following:

1. Click “Licensing” in the web administration left hand tree
2. Type or paste the license key into the field provided
3. Click the “Update” button

