Xeams User Guide

Table of Contents

Important: Please read the End User Software License Agreement before using the accompanying software program(s). Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Contact Information

Customer feedback is extremely valuable to us at Synametrics Technologies. We take all inputs and suggestions into consideration and incorporating them into our products. It is also our mission to help you quickly solve any technical issues or questions that might arise.

Sales

Should you have a questions regarding features, pricing or additional product information contact our sales team:
Phone: 609-705-0007 x 1
Email: Sales@synametrics.com

Support

Should you have any technical questions or concerns, contact our support team:
Phone: 609-705-0007 x 2
Email: Support@synametrics.com

Online Support

If you have any questions about Xeams, check out these additional resources:
https://xeams.com/forum
https://xeams.com/KnowledgeBase.htm
https://xeams.com/FAQ.htm
https://xeams.com/blog
https://xeams.com/troubleshoot.htm

Overview

Xeams is a secure and powerful mail server that is capable of running on multiple Operating Systems. Xeams supports SMTP, POP3 and IMAP, includes a strong junk mail filtering engine that eliminates up to 99% of junk mail upon installation and setup, and is extremely user friendly. *Xeams User Guide* is designed to provide detailed instructions for installing, configuring, and using the program. It also includes details about advanced features such as clustering, live monitoring, live logging and more.

Audience

Xeams User Guide is designed for use by home users, business professionals, corporate system administrators, and other technical staff.

Important Concepts

Introduction

This chapter provides information about the setting up Xeams.

In this chapter

This chapter contains the following topics:

Modes of Operation

After inputting the administrator username and password, you will be asked which mode you would like to run Xeams with. There are 3 different modes of operation. You can switch from one mode to the other at any time using the **Admin Console**.

Stand Alone Mode

In this mode, Xeams runs as a full email server. SMTP, IMAP and POP3 protocols are fully supported. All users have their own inbox. Spam filters check all incoming emails before they are forwarded to the appropriate inboxes.

Users can access their emails with any client, such as Xeams web client, MS Outlook, Thunderbird, or any other that support POP3 or IMAP protocols to fetch new emails.

Stand alone is the default mode of operation. No other email server is required if you use Xeams in this mode.

Spam Firewall

In this mode, Xeams acts as a firewall that sits in front of your corporate email server. Xeams checks each inbound email before being forwarded to the actual email server. Similarly, every outbound message is checked before being delivered to its final destination.

Xeams works with any email server that supports the SMTP protocol, including Microsoft Exchange, Sendmail, Novel Groupwise, Lotus Notes and others.

Xeams provides two types of SMTP servers while operating in this mode:

- Regular SMTP Server
- SMTP Proxy Server

Hybrid Mode

This mode is a combination of Stand Alone and Spam Firewall modes. User's inboxes are created in two locations: Xeams and your corporate email server. Users have a choice of using either one.
Although, every email gets copied at two locations, it provides redundancy for your corporate email infrastructure.

Deployment Scenarios

Xeams can be installed and configured in several different network environments, depending on your preference:

1. **Installing and Configuring Xeams when Xeams is the only email server on my network.**

   This scenario applies when you are using Xeams as standalone mode; you do not have any other email servers running in your network.

   Please see instructions on the installation section here.

2. **Installing and Configuring Xeams to filter for another server downstream.**

   A. Xeams running on a different machine as your primary server.

   - This scenario applies when you already have an email server on your network, and would like to use Xeams to filter messages for it. You would like to install Xeams on a different machine than the one that has your email server.
   - Please see instructions on the installation section here.

   B. Installing and Configuring Xeams on the same machine where my primary server is running.

   - This scenario applies when you already have an email server on your network, and would like to use Xeams to filter messages for it. You would like to install Xeams on the same machine where your primary server is running.
   - Please see instructions on the installation section here.

Inbound and Outbound Filtering

Inbound

Xeams can filter inbound messages for your SMTP server. This is done by having incoming emails go through Xeams first. Once filtered, those messages will go to your corporate email server. It is important to ensure that all emails go through Xeams first, otherwise filtering will only be 40% efficient.

Outbound

Xeams can also filter outbound messages for your primary email server. The emails that come from your primary email server will first go to Xeams for filtering then will be sent outside to the Internet. Outbound messages are already filtered when you use Xeams as your primary outbound SMTP server.

Note: You cannot use the proxy server to filter outbound messages. You must use the regular SMTP server for outbound message filtering.

Licensing and Editions

Xeams is Available in two editions:

1. Community
2. Enterprise

The Community Edition is geared for home users and is recommended not to be licensed in a commercial environment, therefore, there is no cost to use this edition. In addition, the spam filtering feature is enabled in the community edition for up to five home users.

The Enterprise Edition is based on a yearly subscription, priced by the number of users you have in your system. The most important feature in the Enterprise Edition, junk mail filtering, is based on the number of recipients for whom it will filter messages helps admin determine the number of users.

For more information about the differences between these two editions, please visit http://www.xeams.com/Cost.htm.

Defining a User

Two factors contribute to defining a user:

1. Individual users

   A. Individual users can have one or more email addresses associated with them. For example, johnny@xyz.com, john.smith@xyz.com. Both of these variations of addresses belong to the same person and are counted as one user. To ensure Xeams does not count them separately, ensure you properly associate johnny@xyz.com and john.smith@xyz.com with John's account in Xeams.
   Note: Associations MUST belong to the same user inbox. For example, jim@xyz.com and james@xyz.com is the same mailbox.

2. Business Rules

   B. Businesses can have one or more email addresses associated with them. For example, sales@xyz.com and support@xyz.com. Both of these variations of addresses belong to the same company and are counted as one user. Two features contribute towards this factor: Distribution List and Mail/Discussion List.
   Note: Distribution Lists will NOT count toward a license if all of the recipients are local.

Note: Click About under the Tools menu in the Admin Console to see how many active users you have. This is the number of licenses you should purchase.

For more information on how users are calculated, please visit http://xeams.com/user-license.htm.

Installation

Introduction

This chapter provides information about downloading, installing, and configuring Xeams.

In this chapter

This chapter contains the following topics:

System Requirements

Xeams is a 32-bit and 64-bit program that runs on Microsoft Windows 2000,2003,2008, XP Vista or a newer version, any distribution of Linux, UNIX solaris, HP-UX, AIX, Mac OSx and BSD. The following system requirements do not take into consideration machines running multiple programs simultaneously. If you plan on running several programs on the computer at the same time, that computer should exceed these recommendations.

Requirements	Description
Memory	Fewer than 1000 emails per day: 512 MB min (1 GB recommended) Fewer than 20000 emails per day: 1GB min (2 GB recommended) Over 20000 emails per day: 4GB min (8 GB recommended) It is recommended to assume around 5MB/per email for processing. If you assume 500 **simultaneous** emails getting processed, you should assign about 2.5GB of memory usage.
Disk Space	60 MB for installation. Additional space will be required to store messages, which could potentially be in gigabytes. For example, if you anticipate 10,000 emails per day and each email on average is about 50KB, you will need 500 MB per day. You can optionally configure Xeams to remove junk messages after a few days to conserve disk space.
Network Protocol	TCP/IP
Client Software	Internet Explorer, Mozilla Firefox, Google Chrome or Apple Safari
Other	Internet/Intranet communication capabilities

Windows

Follow the steps below to install Xeams on a Microsoft Windows machine.

1. Log in as Administrator.
2. Download the installer from the website. (Ensure you are using the correct version of architecture 32 or 64-bit according to your machine).
3. Extract the zipped file and run setup.exe.
4. Towards the end of the setup, a new service for Xeams will be installed and it will start in the back-ground. For future reference use Windows services applet in the Control Panel to start and stop the service.
5. Using your browser connect to http://localhost:5272 to access the administrator console.

Warning: Do not install Xeams in the **Program Files** folder. The server creates numerous files and folders in the installation directory once the program starts running.

If you try to install it in the **Program Files** folder, you will run into several permission problems.

Linux

Follow the steps below to install Xeams on a Linux machine.

1. Log in as root.
2. Download the installer**.**

   Note: For certain Linux distributions, you can also use **wget** command to download the link. For example, -wget http://xeams.com/files/XeamsLinux.tar.

3. Extract the tar file using the following command: tar -xf XeamsLinux.tar (XeamsLinux64.tar if you have downloaded the 64-bit version of Xeams).
5. Ensure the permissions for Install.sh is set as an executable. If not, use the chmod +x Install.sh command to change its permission.
6. Execute Install.sh script (./Install.sh).
7. By default, the installation script will install the server in /opt folder. You can change this location to any other value if desired. Additionally, it will create necessary scripts in /etc/init.d/ folder so that the server comes up when you restart the machine.
8. Using your browser connect to http://localhost:5272 to access the administrator console.

Other Operating Systems

Please Note: Installation file for these platforms does not come with a JRE (Java Runtime Environment). Therefore, you will need to install a JRE before installing Xeams. Additionally, Java must be in your machine path.

Follow the steps below to install Xeams on any other platform including UNIX (Solaris, HP-UX, AIX) Mac OSx and BSD.

1. Log in as root
2. Download the installer
3. Extract the tar file into any directory using the following command: **gunzip -c XeamsJava.tar.gz | tar -xvf -**
5. Change the permissions on run.sh so that it becomes an executable by using the following command: **chmod +x run.sh**
7. Execute run.sh to start the server
8. Optionally, write a script to start the server when the machine restarts. Refer to the documentation for your platform to see how to run scripts at startup.
9. Using your browser connect to **http://localhost:5272.**
10. If you are installing the server on Solaris, it is very likely that the JRE is already installed on the machine.

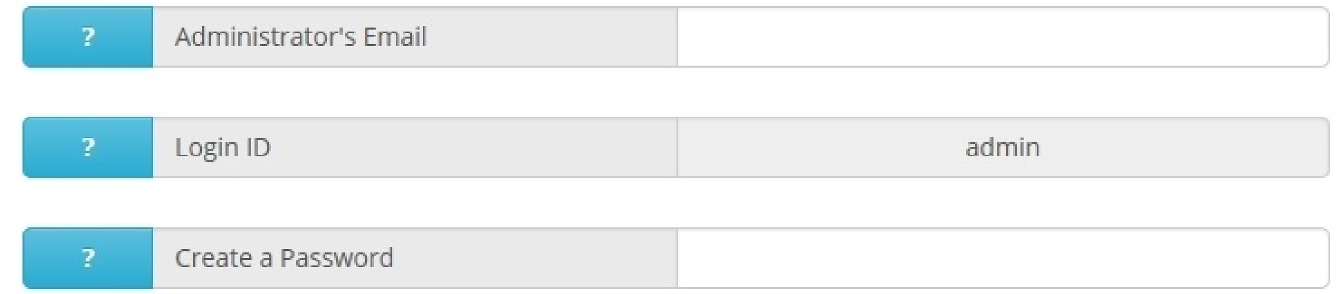
Firewall Configuration

You will need to forward all traffic for Port 25 to Xeams' IP address instead of the actual email server's IP address. If you want to use a different port number, please specify in the **Admin Console** as well as in your network firewall.

Note: Please refer to your network documentation for instructions on how to change this.

Post Installation Actions

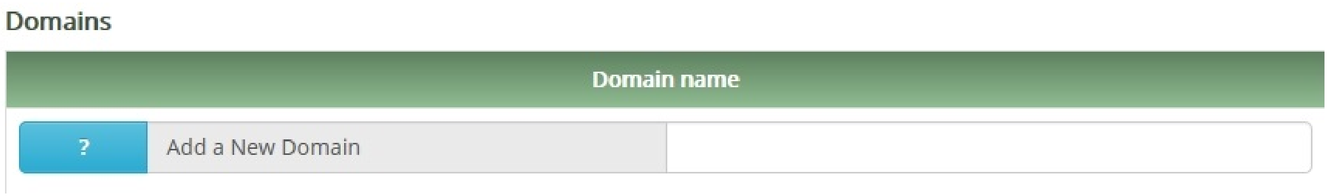
Once Xeams has finished installing, the **Admin Console** will open when you click finish.Once the **Admin Console** opens, it will prompt you to input the administrator’s email, username, and password:



?	Administrator's Email	
?	Login ID	admin
?	Create a Password	

You will need to choose the mode of Xeams you would like it to operate in. Please consult *Important Concepts* for more information about the different modes of operation for Xeams.

Finally, Xeams will ask you to input a local domain name:

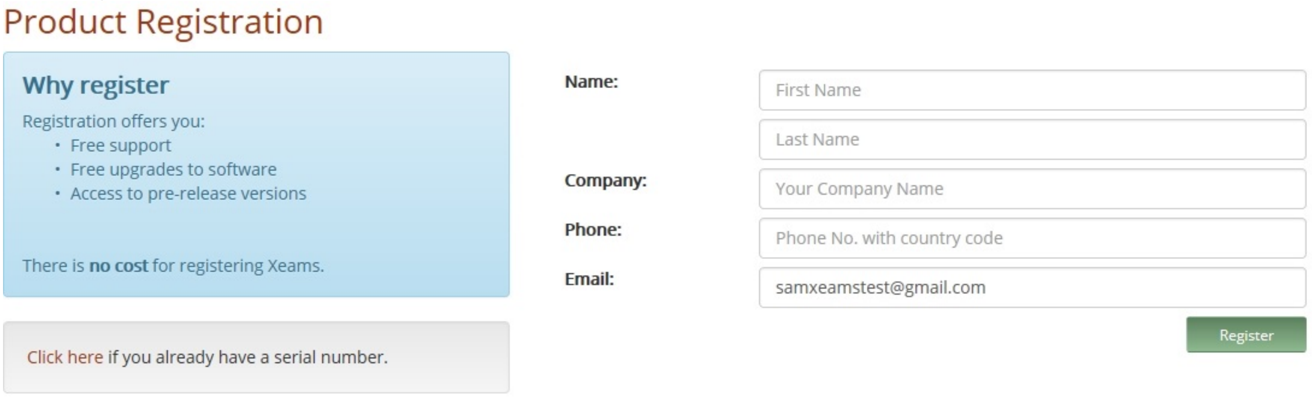


Domains

Domain name		
?	Add a New Domain	

After the setup, you will have to register in order to use the **Admin Console** for Xeams.

Note: You are required to register for Xeams, even if you intend to use the Community Edition. Please ensure values are filled in for all entries. If you are using Xeams for a home environment, you can put your name as the company name.



Product Registration

Why register

Registration offers you:

- Free support
- Free upgrades to software
- Access to pre-release versions

There is **no cost** for registering Xeams.

Click here if you already have a serial number.

Name:	First Name
	Last Name
Company:	Your Company Name
Phone:	Phone No. with country code
Email:	samxeamstest@gmail.com

Note: If you are not able to register Xeams, fill out the form in this page to obtain a serial number. Apply this serial number by clicking on the "click here" link beneath the **Why Register** box.

Admin Console

Introduction

This chapter provides information about configuring the web interface of Xeams.

In this chapter

This chapter contains the following topics:

Connecting as Admin Vs Non-Admin

The login page between users and the administrator have different functionalities.

The following options are available Administrators only:

- Clustering and multi-profile management.
- Message filtering management.
- View email reports and modify alerts.
- Search messages, modify action management, manage outbound queue.
- Configure server options, including administering users.
- View logs, live logs/emails and simulate spam and other troubleshooting utilities.

The following options are available to users when they log in:

- View and search own message repositories.
- Black and whitelist specific email addresses and/or domains (only applies to user).
- Manage out-of-office notifications.
- Manage temporary emails.

Creating Users

Creating users in Xeams is important, especially if you are using Xeams in Standalone mode. Additional users are also required if:

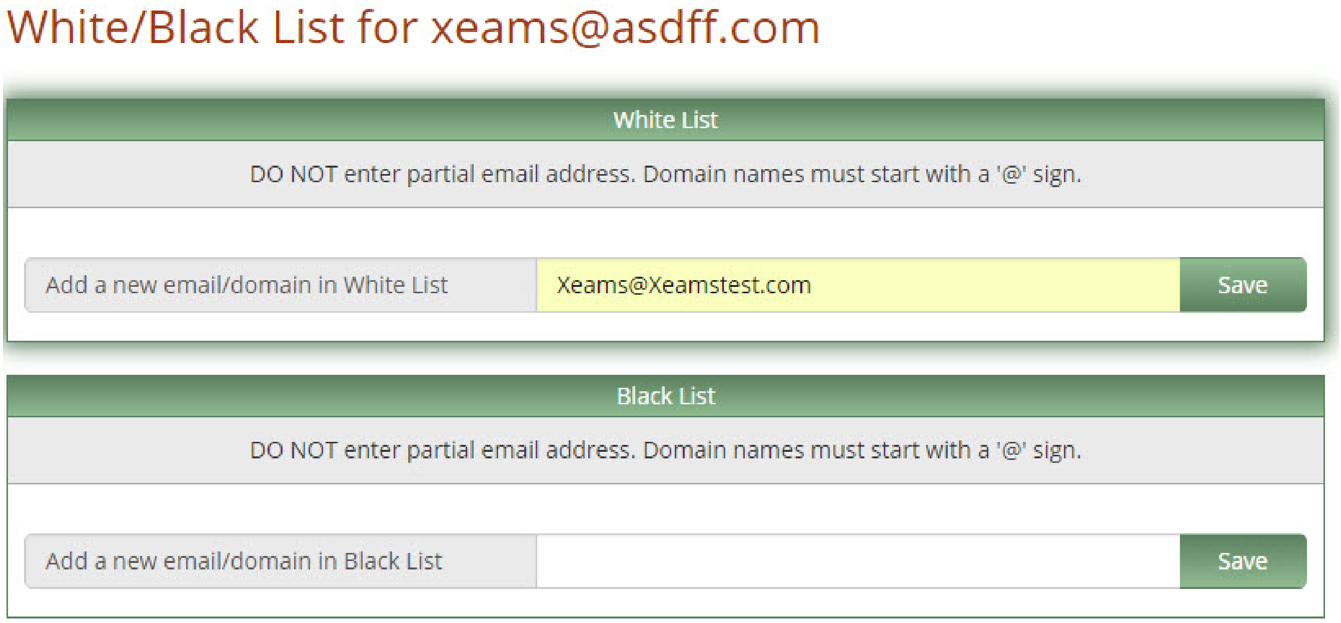
- You want use the POP3 or IMAP server.
- You want to use SMTP authentication for outbound emails.
- You want to generate a Notification Report for your employees containing a list of messages that are quarantined by the server.
- You want individual employees in your company to log in to the Admin Console and manage their own rules.

Benefits of Creating Users

Creating users in Xeams is very beneficial regardless of which mode you operate in. These benefits include:

- Users can receive summary reports. These reports contain emails that have been quarantined for a user. The user can restore any message that gets incorrectly quarantined by the system. Please see the *Daily Summary Report* section for more details.
- Users have the ability to manage their own rules. When the user logs into Xeams, they can search messages, view their repositories, or configure black and whitelists. To black or whitelist a domain or an email address, the user clicks on the **Manage White/Blacklist** button. Afterwards, they will add the email address or domain name and click save.

  See image below:



White/Black List for xeams@asdff.com

White List

DO NOT enter partial email address. Domain names must start with a '@' sign.

Add a new email/domain in White List: Xeams@Xeamstest.com

Black List

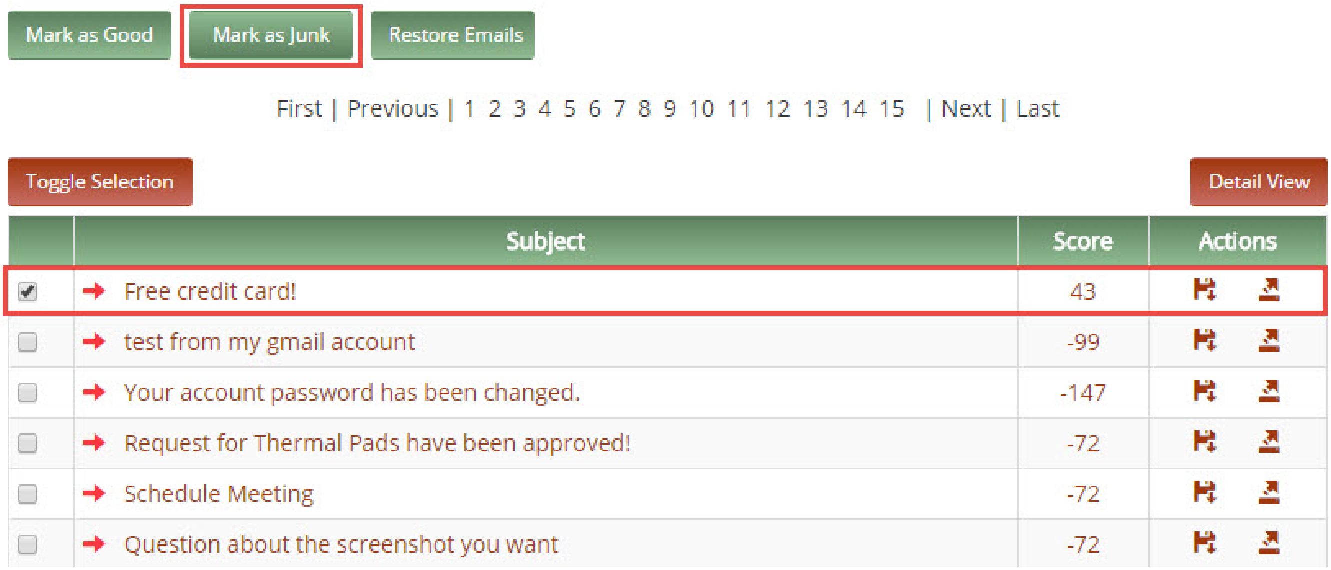
DO NOT enter partial email address. Domain names must start with a '@' sign.

Add a new email/domain in Black List:

User xeams@asdff.com is adding email address Xeams@Xeamstest.com to his whitelist. In this case, any message coming from Xeams@Xeamstest.com to the xeams@asdff.com will get a positive score.

The user can also move a message that is in the incorrect repository. For example, if a user received a spam email that was considered “good” by Xeams but is actually a junk message, the user can mark the message as “junk” and move it to the spam section.

See image below:


Mark as Good
Mark as Junk
Restore Emails
First | Previous | 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 | Next | Last
Toggle Selection
Detail View

	Subject	Score	Actions
☑	➜ Free credit card!	43	
□	➜ test from my gmail account	-99	
□	➜ Your account password has been changed.	-147	
□	➜ Request for Thermal Pads have been approved!	-72	
□	➜ Schedule Meeting	-72	
□	➜ Question about the screenshot you want	-72	

The user sees an email that marked incorrectly. To mark the email in the correct category, the user must check mark the email and click on the button **Mark as Junk** as shown above. After clicking on **Mark as Junk**, the user selects **Move Email** to move the message to the correct repository.

Types of Users

There are two types of non-admin users in Xeams: Local Users and AD Integrated Users.

The most important difference between these two types of users is where the password is stored. Local user passwords are stored in Xeams and has no association to their OS password. The user’s passwords that are integrated with Active Directory are never stored in Xeams. When a user logs in, Xeams will send the authentication parameters to AD which will confirm the password. If this user is trusted by AD they will also be trusted by Xeams.

Creating Integrated users with Active Directory

When Active Directory integration is enabled, a local user in Xeams is automatically created when that person tries connecting to the web interface of Xeams using their OS credentials.

Note: In this case the login ID must match you use on your OS, which is not your email address. For example: john.doe.

Creating Local Users

There are four ways to create accounts for an end-user:

1. **Creating Manually** - this must be done by an Administrator.
2. **Using a Wizard** - this must be done by an Administrator.
3. **By Users Themselves** - this can be done by the end user.
4. **Import Users from a Text File** - this must be done by an Administrator.

Creating users in Xeams manually:

1. Launch the **Admin Console** and log in.
2. Click **Manage Users** under the **Server Configuration** menu.
3. Click **Add New User** to add a new user.

There are several options in the **Create Users** page:

- **Email/Login ID**: Email addresses of the user. This is also the user login ID.
- **Password**: Password for the user. This password is used to connect to the **Admin Console**, as well as authenticating in IMAP, POP3, or SMTP authentication. It is recommended to give the users a generic password, and ask them to change their passwords at a later time.
- **Activate User**: If unchecked, the user is not able to log in to the **Admin Console**. They will still be able to connect using an POP3 or IMAP email client.
- **Restrict inbound emails to buddy list**: Every inbound email will automatically be marked as junk unless the sender's email address is in the whitelist.
- **Add outbound recipients to the whitelist**: When a user sends an outbound message, the system automatically adds the recipient's email address to the whitelist.
- **Allow user to associate other addresses**: Users will be able to associate other email accounts to their account. It is recommended to only enable this feature for trusted users.
- **Create associations**: The new user will automatically be associated with every domain name that is local to this server. Consider the following scenario:

Assume the 3 domains below are local to your server:

1. DomainUno.com
2. DomainDos.com
3. DomainTres.com

You add a new user using **John@DomainUno.com** as the email login ID. The server will automatically associate **John@DomainDos.com** and **John@DomainTres.com** to John's user account.

Server's hostname: Hostname of the server where Xeams is running with respect to the end user. Due to NAT, the IP address of the machine might be different than the actual address from the user's perspective.

Consider the following scenario:

Assume the machine's IP address where Xeams is running is 192.168.1.5, which is the address inside your network. If a user is connecting over the Internet, this address won't be valid anymore. You can specify the outside Internet IP address of your network so that users can access over the Internet.

Send notification messages: If checked, a summary of every email that was blocked by the server will be sent to the user around midnight every day. Please see the *Benefits of Creating Users* section for more information.
Notification Times: These values are the time of the day Summary Reports are sent. Reports that are generated at midnight will contain data for the previous day. Reports for any other time will contain data since midnight.

Creating users in Xeams with a Wizard

Xeams has an option that allows you to create users, using the wizard. This allows you to create multiple users at once. The wizard examines the email address of the users who have received emails in the past 24 hours. A list of these email address is displayed on the following screen allowing you to select the user you wish to create an account for.

Creating Users as a User

An end user can create an account by clicking the **Create Account** link on the login screen. Before the account is created, a verification email will be sent to the address the user provided. This email will contain additional instructions to the user on how to create the account.

Note: If the admin wishes to have this feature disabled, please do the following:

Locate the Xeams installation directory. By default, the locations are as follows:

1. Windows - C:\Xeams\.
2. Linux - /opt/Xeams/.
3. Open the config folder. You should see a file called **AppConfig.xml.** Open this file with a text editor.
4. Look for the line that has the following:

<loginCreationDisabled>false</loginCreationDisabled>.

5. Set the value **false** to **true**. Save the file afterwards.
6. Restart Xeams.

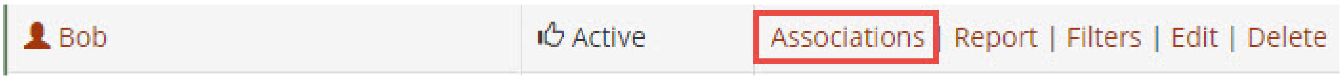
Importing Users from a Text File

Xeams also has an option to import the users from a text file. This allows you to create many users at once. To do this, login as the administrator in Xeams and go to Manage Users under Server Configuration. Next, click on the Import Users option to import the users.

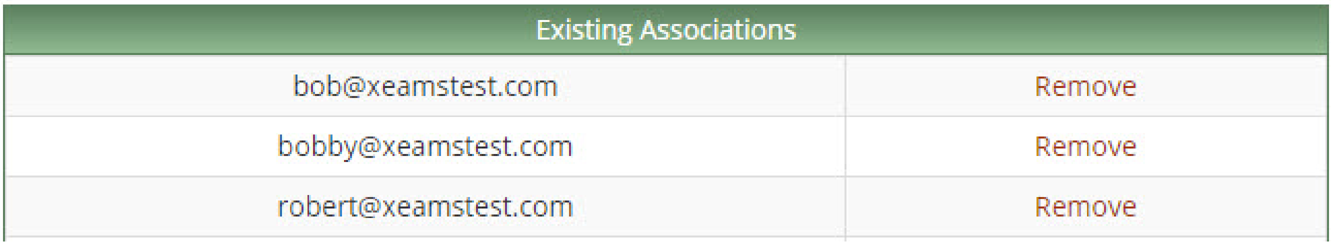
Associating Multiple Email Addresses of One User

If a user has multiple emails (For example, **bob@xeamstest.com**, and **bobby@xeamstest.com**), the admin can associate all emails to one account. This is beneficial because Xeams will count all these emails as one user.

To add the association, hover over **Server Configuration** and click on the **Manage Users** page. Click on the **Associations** button under the action tab:



In this page, the admin will see the option to add an associated email address, as well as the list of existing associations:



Existing Associations	
bob@xeamstest.com	Remove
bobby@xeamstest.com	Remove
robert@xeamstest.com	Remove

Calculating the number of users

Licensing in Xeams is based on the total number of users. A user is identified by either an individual or a business role that accepts email. For example:

- **john.doe@yourcompany.com**
- **sales@yourcompany.com**

Note: To see how many active users you have in Xeams, click **About** under the **Tools** section. A number of active users will appear in the upper left side of the screen. This is the number of licenses you should purchase. If you feel this value is incorrect, check to see if you have rejected invalid users in your email server.

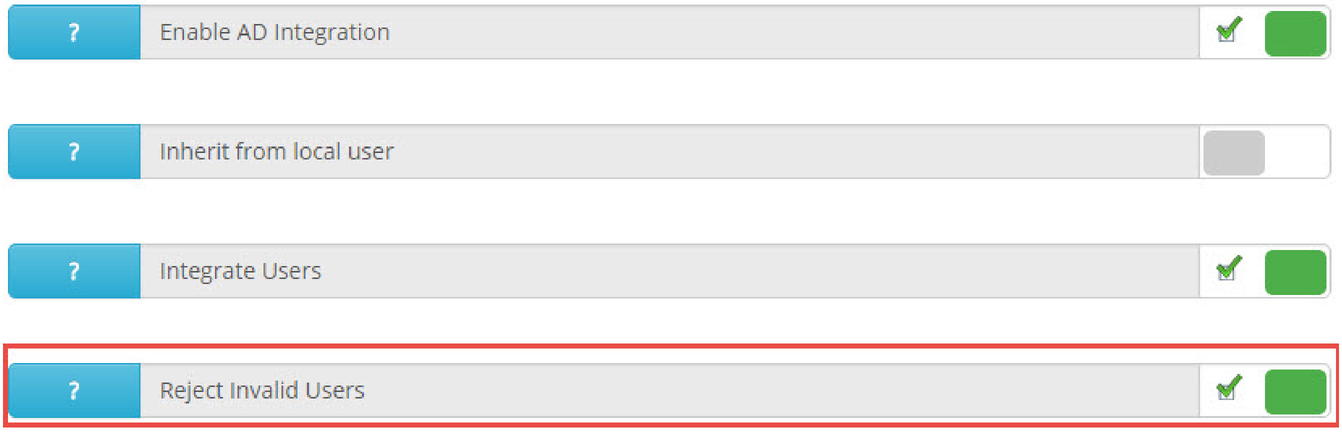
Rejecting invalid users when using SMTP Proxy server for inbound emails

When using the proxy server, it is important to reject emails for invalid users. Keep in mind the acceptance and rejection of emails is done by the actual email server (e.g. Exchange) when using the proxy server.

There are three ways to reject invalid users:

1. Configure your actual email server not to accept emails for invalid users. If you are using exchange 2013 and above, see this page on our website on *How to Reject Invalid Users for Exchange*. Once this is done, your Exchange server should reject invalid users.

2. Use Active Directory to reject invalid users. The following configuration must be set in order for this to work:
   Enable and configure integration with Active Directory (Server configuration > Active Directory Integration) and select **Reject invalid users**:



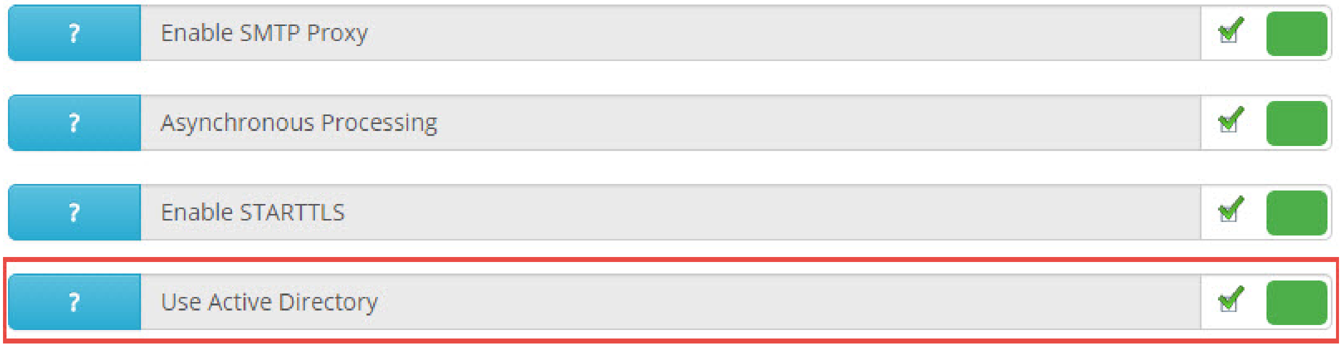
? Enable AD Integration ✓

? Inherit from local user

? Integrate Users ✓

? Reject Invalid Users ✓

Check the "**Use Active Directory**" option under **SMTP Proxy Configuration**:



? Enable SMTP Proxy ✓

? Asynchronous Processing ✓

? Enable STARTTLS ✓

? Use Active Directory ✓

For additional information with active directory integration, please refer to *Active Directory Integration*.

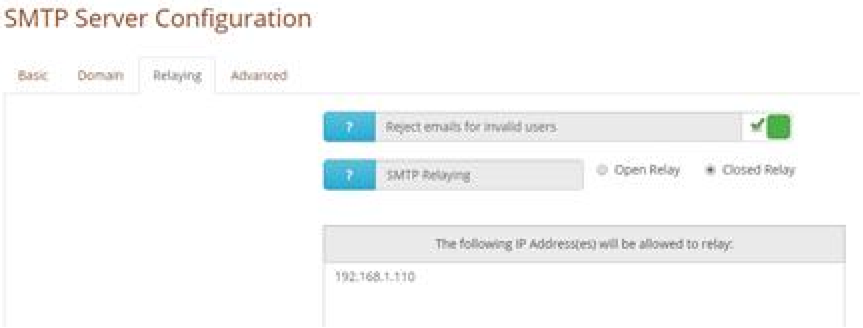
Use the Dynamic Recipient Verification. Please see *Dynamic Recipient Verification* for more details.

Rejecting invalid users when using the regular SMTP server for inbound emails

There are three ways to reject emails for invalid users.

Note: You must use step 1 for both of the options:

1. Check rejected emails for invalid users under the **Relaying** tab for **SMTP Server Configuration**:


SMTP Server Configuration

Basic | Domain | Relaying | Advanced

? Reject emails for invalid users ✓

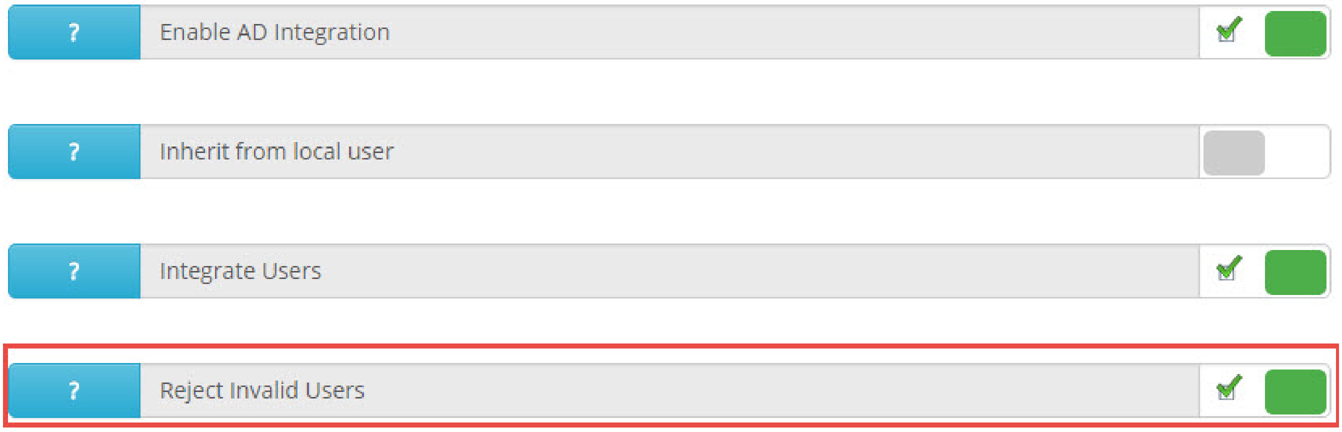
? SMTP Relaying ○ Open Relay ● Closed Relay

The following IP Address(es) will be allowed to relay:

192.168.1.110

AND either one of the following below:

A. Enable and configure integration with Active Directory (Server configuration ---> Active Directory Integration) and select **Reject invalid users**:


? Enable AD Integration ✓

? Inherit from local user

? Integrate Users ✓

? Reject Invalid Users ✓

B. Use the Dynamic Recipient Verification. Please see the *Dynamic Recipient Verification* section for more details.

C. Add the users locally under Server Configuration - Manage Users.

User Count Regarding Outbound Emails:

Outbound emails do not affect the user count. There are two ways for Xeams to determine if a message is being sent out:

1. It is originating from a server whose IP is allowed to relay
2. SMTP authentication is used to deliver the message

Frequently Asked Questions

Q: My company has 3 domains with 20 employees. How many user licenses should I buy?

A: Assuming every employee has 3 email addresses, such as user1@compA.com, user1@compB.com and user1@compC.com, you will only need 20 licenses.

Q: I use Xeams as a Spam Firewall without any local users. How many user licenses should I purchase?

A: Every inbound email that goes through Xeams will add to the user's count. Therefore, if you don't have local users in Xeams, check the number of user accounts in your actual email server to determine the amount of licenses you need.

Q: I only have 20 users but the active user count says 30, why?

> A: This happens when Xeams is configured to accept emails for invalid users. In this case, Xeams cannot distinguish between real and invalid users. If you are using the SMTP proxy server to accept in-bound emails in Firewall or Hybrid mode, you must configure your actual email server to reject invalid users.
>
> Please see the *How does Xeams Know How Many Users I Have* section for more details on how to reject invalid users.

Q: I have multiple variations/aliases of an email address, why?

> A: These variations are called "Associations" in Xeams. If you pull users from an AD, Xeams will automatically create these associations. You can also create them manually if needed.
>
> Associations are created under the **User Management** screen. Once they are created, the actual user count will go down.

Q: I already made necessary changes to reduce the actual user count but I don't see any change in Xeams?

> A: Xeams looks at five days of data to determine the user count. Therefore, if the changes are made today, the actual user count will go down after five days.

Q: How does Xeams know how many users I have?

> A: Xeams uses different methods to determine the actual number of users depending on the mode:
>
> > **Xeams in Standalone Mode:**
> >
> > Calculating users in Standalone mode is determined by the number of users in Xeams. Click **Manage Users** under **Server Configuration** to see the actual number.
> >
> > **Xeams in Spam-Firewall and Hybrid Mode:**
> >
> > Any incoming emails accepted by the system constitutes a user. One exception to this rule is when an incoming email belongs to associated emails in Xeams. Therefore, it very important not to accept messages for invalid users. There are several ways to reject emails for invalid users:

Dynamic Recipient Verification

DRV is a mechanism used to validate the recipient of an incoming email with another SMTP server. Consider a scenario where you filter emails for multiple domains that are then forwarded to more than one SMTP server. Using DRV, Xeams can check if the recipient of an incoming email is valid and will be accepted by the next SMTP that is supposed to receive the message after it has been filtered by Xeams.

Consider using DRV if you are using the regular SMTP server to process incoming emails and you do not want to create a local user in Xeams.

Steps to enable DRV:

1. Login to the web interface as an admin
2. Click on **SMTP Configuration** under the **Server Configuration** menu
3. Click on the DRV link on the left side.

4. Add the server(s) you want to validate incoming recipients. You will need to enter in the domain name, SMTP server, and TCP/IP port.

Distribution list

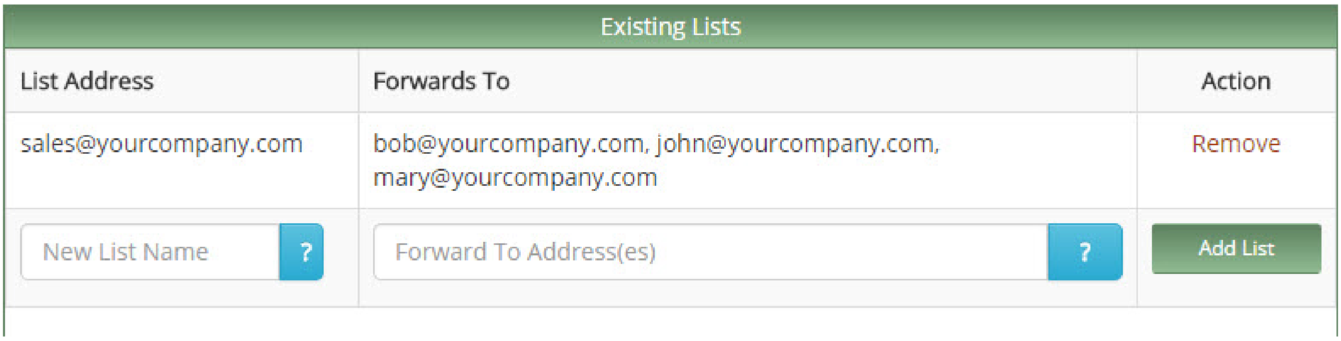
A distribution list (formerly called Aliases) allow you to receive emails to one address, which is then distributed among multiple recipients. For example, sales@yourcompany.com, support@yourcompany.com and marketing@yourcompany.com are all examples of a distribution list since emails received to these addresses are typically forwarded to multiple individuals in a company.

Creating a Distribution List

1. Log in to the **Admin Console** as administrator
2. Select **Manage Distribution List** under **Server Configuration**
3. Type sales@YourCompany.com for new list name
4. Type bob@YourCompany.com, John@YourCompany.com, Mary@YourCompany.com for the **Forward to Addresses** field.

Note: multiple addresses are separated by a comma.

5. Click the **Save** button. The end result should be the following:



Existing Lists

List Address	Forwards To	Action
sales@yourcompany.com	bob@yourcompany.com, john@yourcompany.com, mary@yourcompany.com	Remove
New List Name ?	Forward To Address(es) ?	Add List

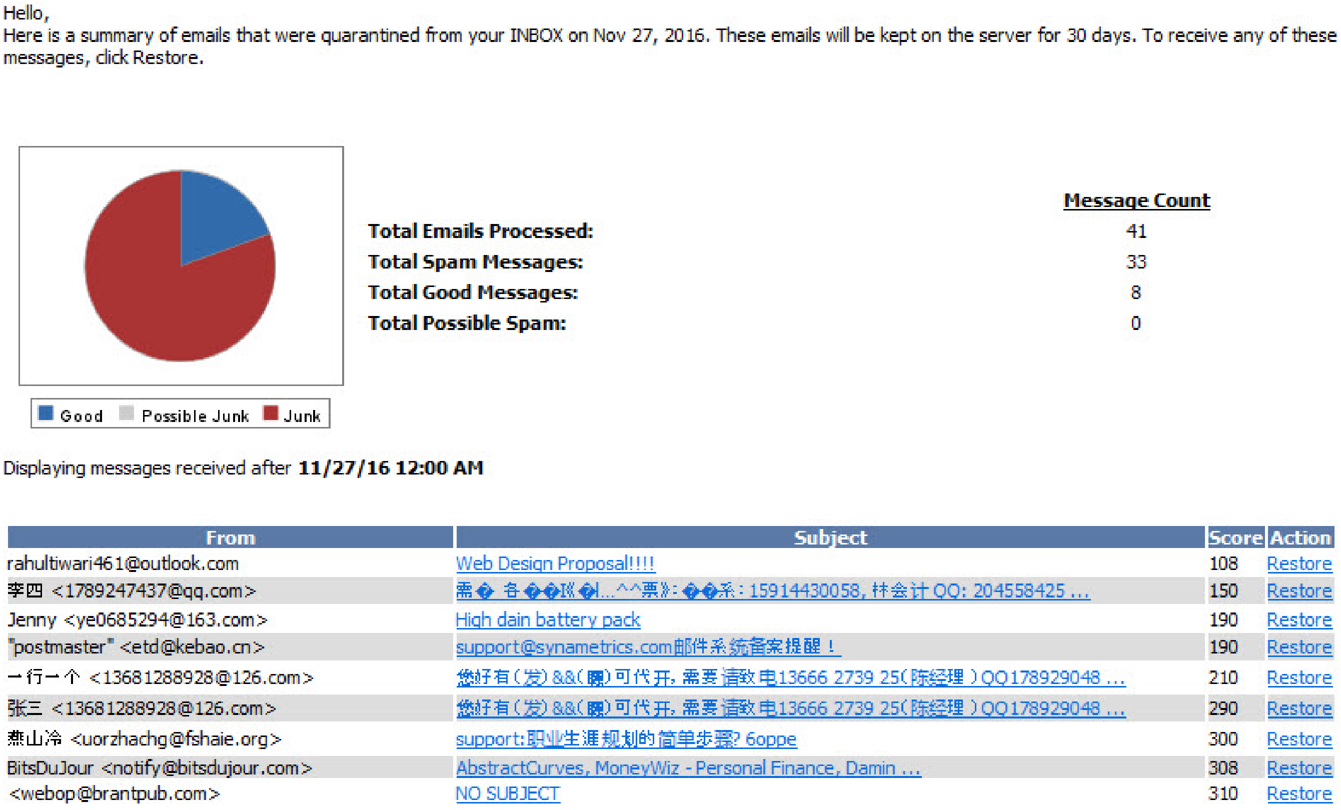
As shown in the image above, any email going to **sales@yourcompany.com** will be forwarded to three recipients; **bob@yourcompany.com**, **john@yourcompany.com** and **mary@yourcompany.com**

Daily Summary Reports

Xeams has the ability to automatically send notification reports containing a summary of emails that have been quarantined for a user. The report contains the subject, sender and score of the actual message. Using this report, an individual can restore any message that is incorrectly quarantined by the system. They can also mark a message as good to prevent it from getting blocked in the future.

The summary report is sorted by score. Users should look at the first few messages since messages with a lower score have a higher chance at being marked as junk incorrectly. Messages that have a lot higher of a score at the bottom are typically junk.

An example of a summary report is below:



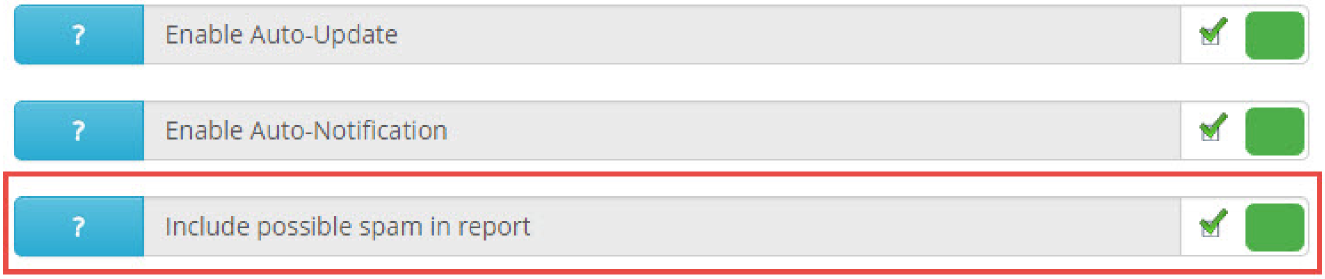
Hello,
Here is a summary of emails that were quarantined from your INBOX on Nov 27, 2016. These emails will be kept on the server for 30 days. To receive any of these messages, click Restore.

	Message Count
Total Emails Processed:	41
Total Spam Messages:	33
Total Good Messages:	8
Total Possible Spam:	0

Displaying messages received after **11/27/16 12:00 AM**

From	Subject	Score	Action
rahultiwari461@outlook.com	Web Design Proposal!!!!	108	Restore
李四 <1789247437@qq.com>	需� 各��I(�l...^^票》: ��系：15914430058, 林会计 QQ: 204558425 ...	150	Restore
Jenny <ye0685294@163.com>	High dain battery pack	190	Restore
"postmaster" <etd@kebao.cn>	support@synametrics.com邮件系统备案提醒！	190	Restore
一行一个 <13681288928@126.com>	您好有(发)&&(票)可代开, 需要请致电13666 2739 25(陈经理)QQ178929048 ...	210	Restore
张三 <13681288928@126.com>	您好有(发)&&(票)可代开, 需要请致电13666 2739 25(陈经理)QQ178929048 ...	290	Restore
燕山冷 <uorzhachg@fshaie.org>	support:职业生涯规划的简单步骤? 6oppe	300	Restore
BitsDuJour <notify@bitsdujour.com>	AbstractCurves, MoneyWiz - Personal Finance, Damin ...	308	Restore
<webop@brantpub.com>	NO SUBJECT	310	Restore

Good emails will never show up in the summary report. By default, possible spam messages will not show as well but can be configured to do so in the **Admin Console**. Once logged in to the **Admin Console**, click on **Server Configuration** the on the **Advanced** tab, and make sure the option **Include Possible Spam in Report** is checked:



Enable Auto-Update ✓

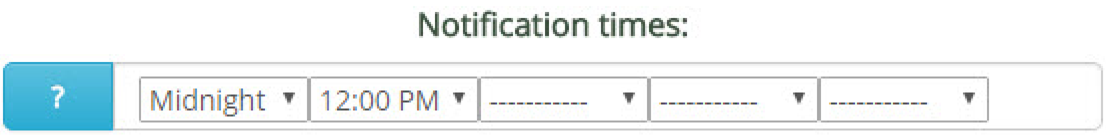
Enable Auto-Notification ✓

Include possible spam in report ✓

When are these reports sent?

By default, Xeams sends this report at midnight containing a list of emails that were quarantined in the previous day. Follow the steps below to change this default behavior:

1. Log in to Admin Console
2. Click **Manage Users** under **Server Configuration**
3. Click **Edit** next to the desired user
4. Specify the times you want Xeams to generate this report. You can specify up to 5 different times:



Notification times: Midnight, 12:00 PM, -----------, -----------, -----------

As directed in the image above Xeams will send a report at midnight, containing a list of emails that were quarantined in the previous 12 hours (12:00 P.M. to 12:00 A.M.). Afterwards, Xeams will send another report at noon containing emails that were quarantined between 12:00 A.M. and 12:00 P.M.

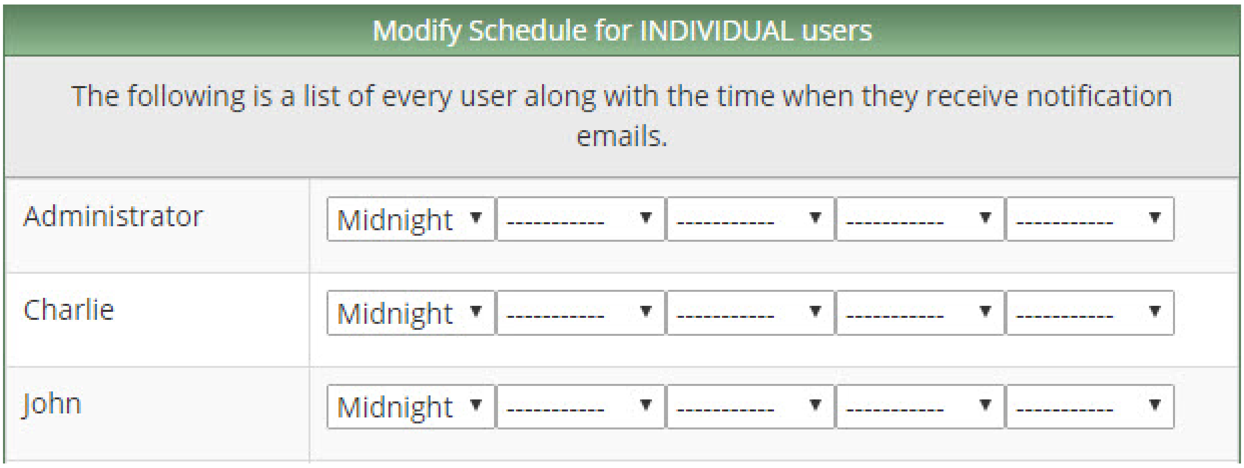
WARNING: It is very important that midnight is always the first scheduled notification time. Otherwise you will miss emails in the quarantine report. Please see here for more information.

Bulk modification

Follow the steps below to modify the report schedule for every user:

1. Log in to Admin Console
2. Select **Manage Users** under **Server Configuration**
3. Click **Modify report** schedule towards the top.

   In this page, you can either modify report times for all users:
   Or modify individuals on the same page:



Modify Schedule for INDIVIDUAL users

The following is a list of every user along with the time when they receive notification emails.

Administrator	Midnight ▼	----------- ▼	----------- ▼	----------- ▼	----------- ▼
Charlie	Midnight ▼	----------- ▼	----------- ▼	----------- ▼	----------- ▼
John	Midnight ▼	----------- ▼	----------- ▼	----------- ▼	----------- ▼

Live Logs

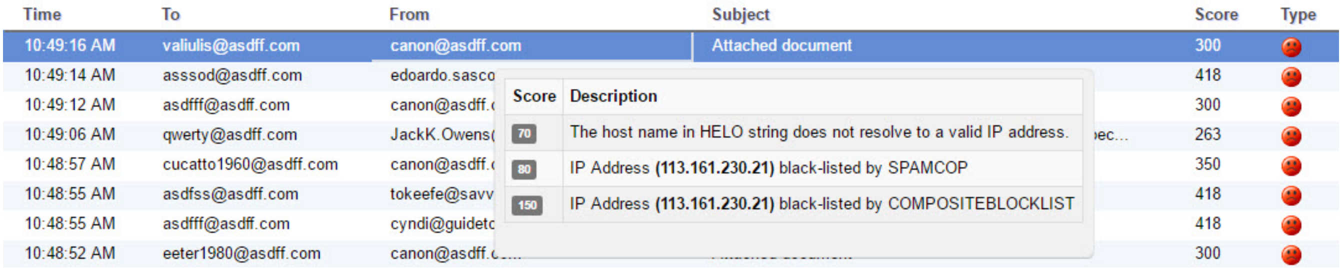
Xeams has a feature that allows administrators to view their logs file in real-time. One benefit of live logs is; you can check the SMTP communication between emails right away. To view this feature, click on the **Tools** tab and select **Live Logs**. Select which log file you wish to look at on the file name to view the specific log file.

Live Monitor

Live monitoring is a feature that allow administrators to watch emails as they arrive in the system. It provides a very efficient and easy method of troubleshooting incoming and outgoing messages in Xeams.

What you see in Live Monitor

When live monitoring is on, the Xeams server will send the subject, message type, and filtering reason to your client browser as messages come in. When a row is clicked the reason a message was labeled as junk will be displayed.



Time	To	From	Subject	Score	Type
10:49:16 AM	valiulis@asdff.com	canon@asdff.com	Attached document	300	☹
10:49:14 AM	asssod@asdff.com	edoardo.sasco		418	☹
10:49:12 AM	asdfff@asdff.com	canon@asdff.c		300	☹
10:49:06 AM	qwerty@asdff.com	JackK.Owens(	›ec...	263	☹
10:48:57 AM	cucatto1960@asdff.com	canon@asdff.c		350	☹
10:48:55 AM	asdfss@asdff.com	tokeefe@savv		418	☹
10:48:55 AM	asdfff@asdff.com	cyndi@guidetc		418	☹
10:48:52 AM	eeter1980@asdff.com	canon@asdff.c...		300	☹

Score	Description
70	The host name in HELO string does not resolve to a valid IP address.
80	IP Address **(113.161.230.21)** black-listed by SPAMCOP
150	IP Address **(113.161.230.21)** black-listed by COMPOSITEBLOCKLIST

The type of message is displayed by an emoticon with a specific color. Blue indicates the message is considered good, gray indicates the message is considered possible junk, and red indicates the message is considered spam.

Tools

Including live logs and monitoring, there are many troubleshooting utilities that Xeams provides for the administrator. The following options are available:

- **Spam simulator** - You can submit a message manually and check to see if your filters are working. Paste the contents of a specific email along with the header to the blank field. Please see *Simulating Spam* for more details.
- **Diagnostic Check** (Inbound and Outbound) - These checks ensure your Xeams will properly running in terms of inbound and outbound message flow.
- **View logs** - Displays different types of log files, such as SMTP communication, SMTP Queue, restorations. Click on **Modify Logging Configuration** in the View Logs page for more details on what each log file displays.
- **Reload message cache** - Refreshes the message caches. In message cache, Xeams caches the names of all files that are in the Spam, Possible Spam, and Good folder. Caching is used to prevent Xeams from reading the hard disk every time you go in to view messages.
- **Email validator** - Checks to see if the email address is valid or invalid.
- **DNS lookup** - Shows the DNS record for the domain specified in the field. **A** and **MX** record(s) are displayed here.
- **Reverse IP lookup** - Will try to get a DNS PTR record for the IP address specified in the field.
- **SPF Wizard** - Creates a SPF Record by providing arguments against each SPF mechanism. An SPF string is created as you apply different options. The new string must be added in your DNS server as a TXT record.
- **WHOIS lookup** - returns WHOIS results for a specified domain. You can see different information, such as who the domain name is registered to, when it was registered, and more.

Appearance

Appearance allows you to put your company name, tag line, and logo on the web interface. This feature is only available in the Enterprise Edition.

To access this option, log into the **Admin Console** as the administrator. Hover your mouse over **Home** and click on **Appearance**.

There are multiple options you can change the appearance of the web interface:

Top-Level Name - The value that is specified here will replace the word Xeams in the web interface.
Sub Heading - This value will replace the sub heading words that appear next to your product name.
Logo Image - Changes the image that is displayed in the upper left hand corner of Xeams' web interface. This value must be an absolute URL. For example, http://somecompany.com/images/somelogo.jpg.
Report Image - Changes the image specified in the daily quarantine reports. Recommended size is 750x100. This value must be an absolute URL. For example, http://somecompany.com/images/somelogo.jpg.
Hide Support Link – If enabled, this option hides the support link at the bottom for non-administrative users.
Hide Footer - If enabled, this option hides the footer at the bottom to remove links about Xeams and Synametrics Technologies, Inc. for non-administrative users.
Color Theme - Modifies the color theme of the web interface. Select the Custom theme to create a new custom color.

Sending and Receiving Emails

Introduction

This chapter provides information about sending and receiving emails.

In this chapter

This chapter contains the following topics:

SMTP Server vs. SMTP Proxy Server

Xeams has two types of SMTP servers; the regular SMTP server and the SMTP proxy server.

SMTP Server (Recommended)

This is a typical SMTP server that accepts emails and queues them for delivery. It requires that you specify a set of local domains handled by the server. If any email comes in from a different domain and relaying is allowed, the message will be delivered to the final destination server.

Note: The regular SMTP server can be used for both inbound and outbound mail delivery.

SMTP Proxy Server

This is not a full SMTP server. It is a proxy server, meaning it requires another SMTP server to connect to. Clients always connect to the actual server through the proxy server, which has the capability of monitoring emails, changing its contents, and blocking them if necessary. The proxy server can only be used for inbound emails.

WARNING: The proxy server is deprecated and thus not recommended to use. Please see here for more details

Async Vs Synchronous SMTP

It is strongly recommended to use Asynchronous processing in Xeams. If you use Synchronous processing, then the sender’s SMTP has to wait for the receiving SMTP’s response. This can cause delays and other issue regarding emails.

Receiving Emails over the Internet

There are 2 methods of filter inbound messages:

1. Use the regular SMTP server in Xeams to forward inbound emails (**Recommended**). The regular SMTP server is the default mechanism in Xeams to accept new messages from a client. This SMTP server accepts incoming emails and stores the message in a local repository. If the message is bound for another SMTP server, the message gets queued and is finally delivered to the destination. You can use the regular SMTP server in all 3 modes.

> **Advantage:** In the regular SMTP server, messages will get stored in a local repository. Xeams will still accept the messages when the primary SMTP goes down.
>
> In the regular SMTP server, you can also distribute emails to more than a single SMTP server. For example, you can set messages for domainone.com to go to one email server, while messages for domaintwo.com goes to a different email server.
>
> **Disadvantage:** The regular SMTP server has more configuration that the SMTP proxy server. You will need to add in the local domains for Xeams to know which SMTP server to send the emails to. In addition, if you want summary reports and the ability for users to manage their own black and whitelists, then you will need to create the users in Xeams.

To configure the regular SMTP server, go to the **SMTP Configuration** page that is under the **Server Configuration** in the **Admin Console**. If you are using it to filter messages for another SMTP server, you will need to add the domain name as well as the IP address of the email server in the domains tab. If you are using this in Standalone mode, you do not have to add in the IP address.

Consider using the regular SMTP server if the following matches your scenario(s):

You are using Xeams in Standalone mode. In this mode Xeams does not require any other email server and therefore, you cannot use the SMTP proxy server.

When you want Xeams to distribute incoming emails to more than one server. For example, domainone.com goes to MS Exchange and domaintwo.com goes to a QMail Server. You want to provide redundancy for your primary email server.

Note: The Proxy Server option below has been deprecated. Please use the regular SMTP server only.

2. Use the SMTP proxy server in Xeams to forward inbound emails to your actual email server. This can only be used if you have another server in your network that accepts emails. You cannot use the proxy server in standalone mode, it must be in either Spam Firewall or Hybrid Mode.

> **Advantage:** SMTP proxy server requires very little configuration. Domain name and users are not needed for configuration. The primary server decides which emails to accept.
>
> **Disadvantage:** The proxy server does not have a local queue. If the primary SMTP server is down, Xeams will go down as well.

To configure the proxy server, go to the **SMTP Proxy Configuration** page under **Server Configuration** in the **Admin Console**. Here you will input the IP address of your actual email server, as well as the port number. An example is below:

Consider using the proxy server if the following matches your scenario(s):

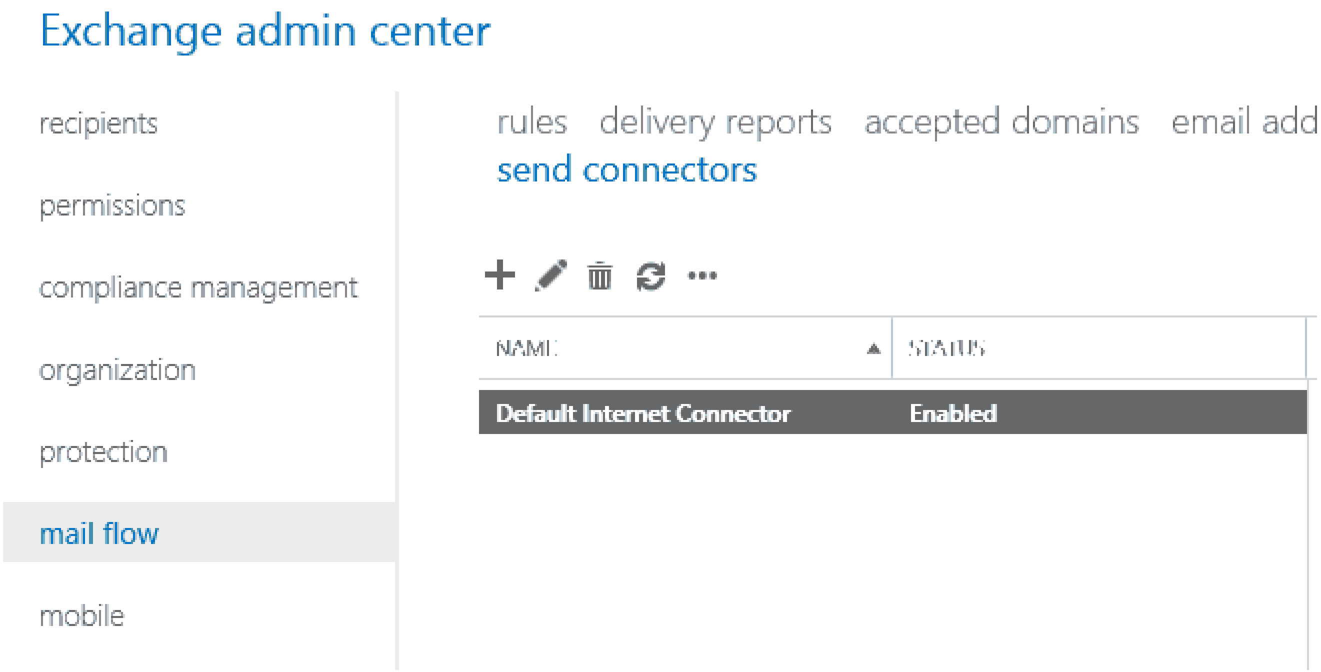
- Xeams is not the final destination for inbound emails.
- Xeams is configured in Spam Firewall or Standalone mode.
- You have users on the Internet not in your company's network who want to use your email server to send their outbound messages and you want to them to authenticate before accepting their message.

Integration with Microsoft Exchange

Configuring Outbound Filtering with Xeams

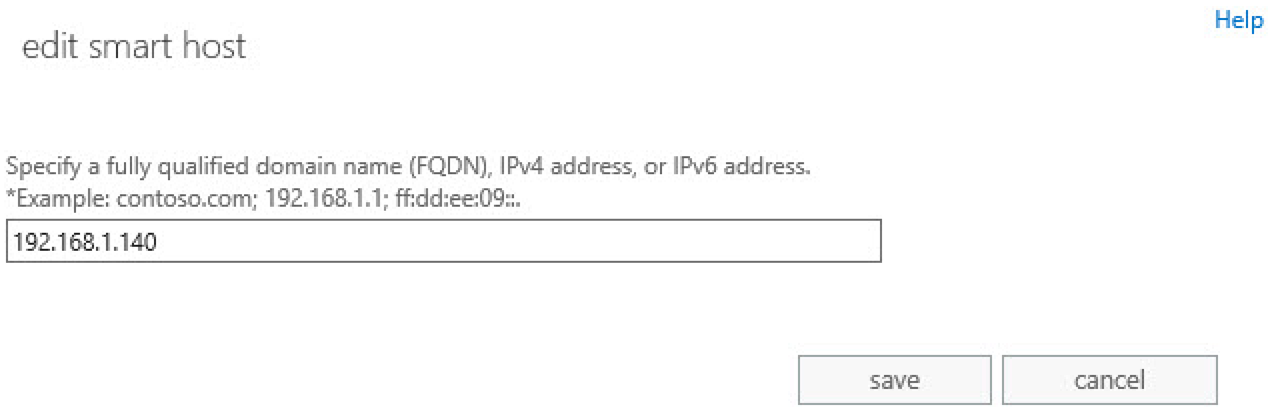
The following is an example to configure outbound filtering for an Exchange Server:

1. The first step in Exchange is to add/modify the send connector so outbound emails will go through Exchange:



NAME	STATUS
Default Internet Connector	Enabled

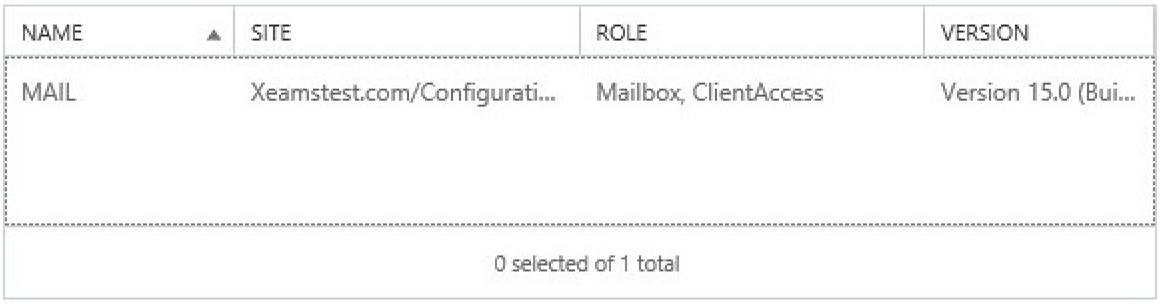
2. Next, in the send connector configuration, you will need to select route mail through smart hosts and add in the IP address of Xeams's regular SMTP server (In this case, 192.168.1.140):



Specify a fully qualified domain name (FQDN), IPv4 address, or IPv6 address.
*Example: contoso.com; 192.168.1.1; ff:dd:ee:09::.

192.168.1.140

You will then need to add the source server. Add in your exchange server here:

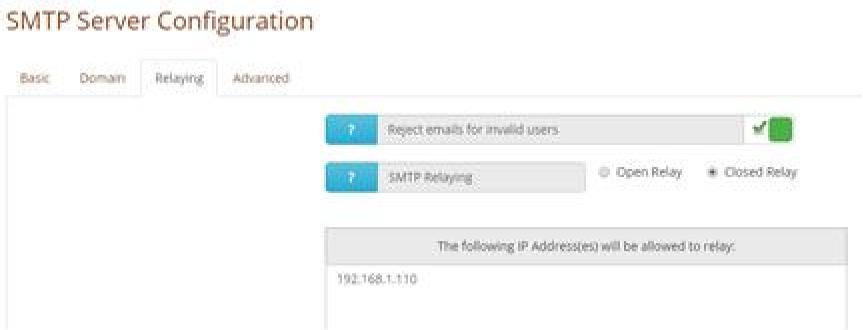


NAME	SITE	ROLE	VERSION
MAIL	Xeamstest.com/Configurati...	Mailbox, ClientAccess	Version 15.0 (Bui...

0 selected of 1 total

3. The final step is to add Exchange’s IP address (In this case, 192.168.1.110) in two locations in Xeams:

   A. Server Settings > SMTP Server Configuration > Relaying:



SMTP Server Configuration

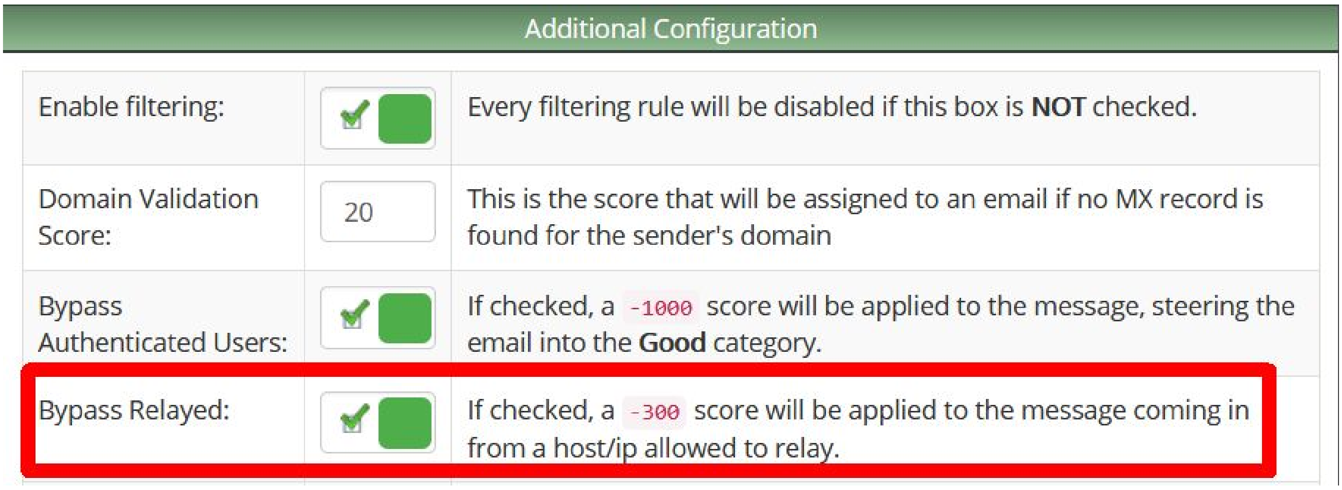
Reject emails for invalid users ☑

SMTP Relaying ○ Open Relay ● Closed Relay

The following IP Address(es) will be allowed to relay:

192.168.1.110

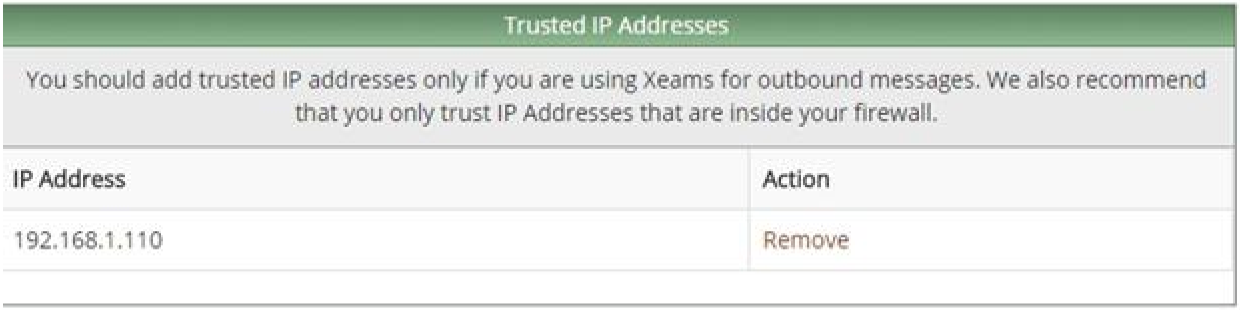
Note: Once you add the ip address to the relay list, make sure Bypass Relay is checked under Filter Management --> Score Configuration:



Additional Configuration

Enable filtering:	☑	Every filtering rule will be disabled if this box is **NOT** checked.
Domain Validation Score:	20	This is the score that will be assigned to an email if no MX record is found for the sender's domain
Bypass Authenticated Users:	☑	If checked, a `-1000` score will be applied to the message, steering the email into the **Good** category.
Bypass Relayed:	☑	If checked, a `-300` score will be applied to the message coming in from a host/ip allowed to relay.

B. Filter Management > Adaptive Filters > Auto Learn Sender Filter. Click Manage Trusted IP Addresses:



Trusted IP Addresses

You should add trusted IP addresses only if you are using Xeams for outbound messages. We also recommend that you only trust IP Addresses that are inside your firewall.

IP Address	Action
192.168.1.110	Remove

Active Directory Integration

Administrators can integrate Xeams with an existing Active Directory. If integrated, Xeams will use the AD for the following:

- When a new user needs to be created.
- To authenticate existing users.
- Reject invalid users when accepting inbound emails.

To enable **Active Directory**, go to **Server Configuration** and select **Active Directory Integration**. You will need to enter some AD information. The fields are the following:

Enable AD Integration: Enable or Disable the Active Directory Integration.
Integrate Users: Check if you want Xeams to create users based on the Active Directory. See Creating and Authenticating Users for more details.
Reject Invalid Users: If checked, the recipients email is validated with AD before accepting an incoming email.
Host Name/IP: Host name or the IP address of your domain controller.
AD Domain Name: This is the local domain name. For example: yourcompany.local.
Base DN: Leave this blank initially. Xeams will attempt to fetch this value from the server. You may see more than one value for this field, in that case you will have to pick the appropriate value.
Administrator's User ID: User ID that has enough privilege to perform an AD lookup. This is typically set to Administrator.
Password: Password for the User ID.

Creating and Authenticating Users

Xeams will create new user accounts automatically when Active Directory integration is enabled and the check box for Integrate Users is checked refer.

Consider the following scenario as an example:

> You have recently installed Xeams and have no users. John Doe, a user who has a valid account in your Active Directory, tries to connect to the **Admin Console**. John's User ID is john.doe. He inputs his ID for the login name and his password to connect to Xeams. Upon a successful authentication through Active Directory, Xeams will automatically create an account for John in Xeams.

Note: Ensure a valid email address is associated with John's account in your AD. Xeams will pull his email and automatically create an association with this new account. Xeams will not store John's password. Whenever a password is needed, Xeams will query the AD. From now on, John can use his AD credentials to login to the **Admin Console**.

Distribution List vs. Associated Emails

Many administrators confuse Distribution Lists with Associate Emails.

Distribution List

Distribution List can be accessed by clicking **Manage Distribution List** under the **Server Configuration** in the **Admin Console**. Prior to build 5852, the same menu item was called Manage Aliases. Distribution List is a convenient way of expanding emails sent to a single address to multiple recipients.

For example: you can create a Distribution List for hockey.practice@yourdomain.com and distribute emails sent to this address to:

- mike@yourdomain.com
- bob@gmail.com
- peter@hotmail.com

Note: Distribution List will NOT contribute to a user license if the all the recipients are local when using the Enterprise Edition of Xeams

Associated Emails

Associations are accessed through the **User Management** screen under the **Server Configuration** menu in the **Admin Console**. Administrators can associate one or more email addresses to a single user.

For example:

- mike.smith@yourdomain.com
- msmith@yourdomain.com
- michael.s@yourdomain.com

These addresses can be associated with a user named Michael Smith.

Note: Xeams will count all of the associated addresses as one user when counting total users towards a license.

Junk Filtering

Introduction

This chapter provides information about how filtering works and how to configure specific types of filters.

In this chapter

This chapter contains the following topics:

Score Configuration and Concepts

Every email in Xeams passes through several filters. Each of these filters assigns a specific score to each message. The higher the score, the higher the chance for the message being junk. The scoring is as follows:

- An email with a score higher than 100 is considered junk.
- An email with a score less than 60 is considered good.
- An email with a score between 60 and 100 falls in a gray area called possible junk.

By default, all quarantined emails are saved on the server for 15 days. All quarantined messages get stored in a different folder, which are easily accessible by either the web interface or any IMAP client such as MS Outlook and Mozilla Thunderbird.

Scoring Criteria

Scoring is done based on several built-in rules. Every rule in the system can take the score either in the positive or negative direction. The final score decides the category of the email. Rules in Xeams can be further divided into two categories:

1. User defined rules.
2. Adaptive Filters or self-learning rules.

Several user-defined rules are bundled with Xeams at the time of installation. All of the rules have a default score and are fully user configurable.

Adaptive filters adjust to the environment of your users. For example, it learns from the past history of emails to assign a score to future emails. One such rule is called Bayesian Analysis. Another example of a self-learning rule is when a local user sends a message to someone outside the network. Xeams remembers who the recipient is and gives credit to that user if they send a reply back.

Score Reasoning

Many spam filtering solutions block messages without giving an adequate reason of why it was selected as junk. Xeams on the other hand gives a detailed description of why a particular email is considered junk. This description is very useful for administrators who want to fine tune the filtering rules.

External Tags

Administrators can add external tags to let users know the emails came from outside. External tags are configurable for the subject and the body of the message.

Subject Tags

You can add a custom tag when a message is received from the Internet. Consider the following scenario when having such a tag is a good idea:

- A spammer goes to your public website and gathers the names of your employees. Many companies put the names of their senior management on their website.
- Once the perpetrator knows a relationship between two employees, they forge the sender's name hoping the recipient will open that message since he/she know the sender.
- Notice that they only forge the name, not the email address. Many email clients prefer displaying the name over email address when both values are available, giving the reader a false impression.

Xeams can be configured to add a tag to the subject line letting the recipient know this message came in from the Internet, allowing them to make better decision before open the message.

Consider the following example:

Original Subject

Subject: Attaching the updated invoice

Modified Subject

Subject: [EXTERNAL] Attaching the updated invoice

The added tag to the subject line gives some extra information to the reader so he/she is more careful before opening the message even through the sender name appears to be friendly.

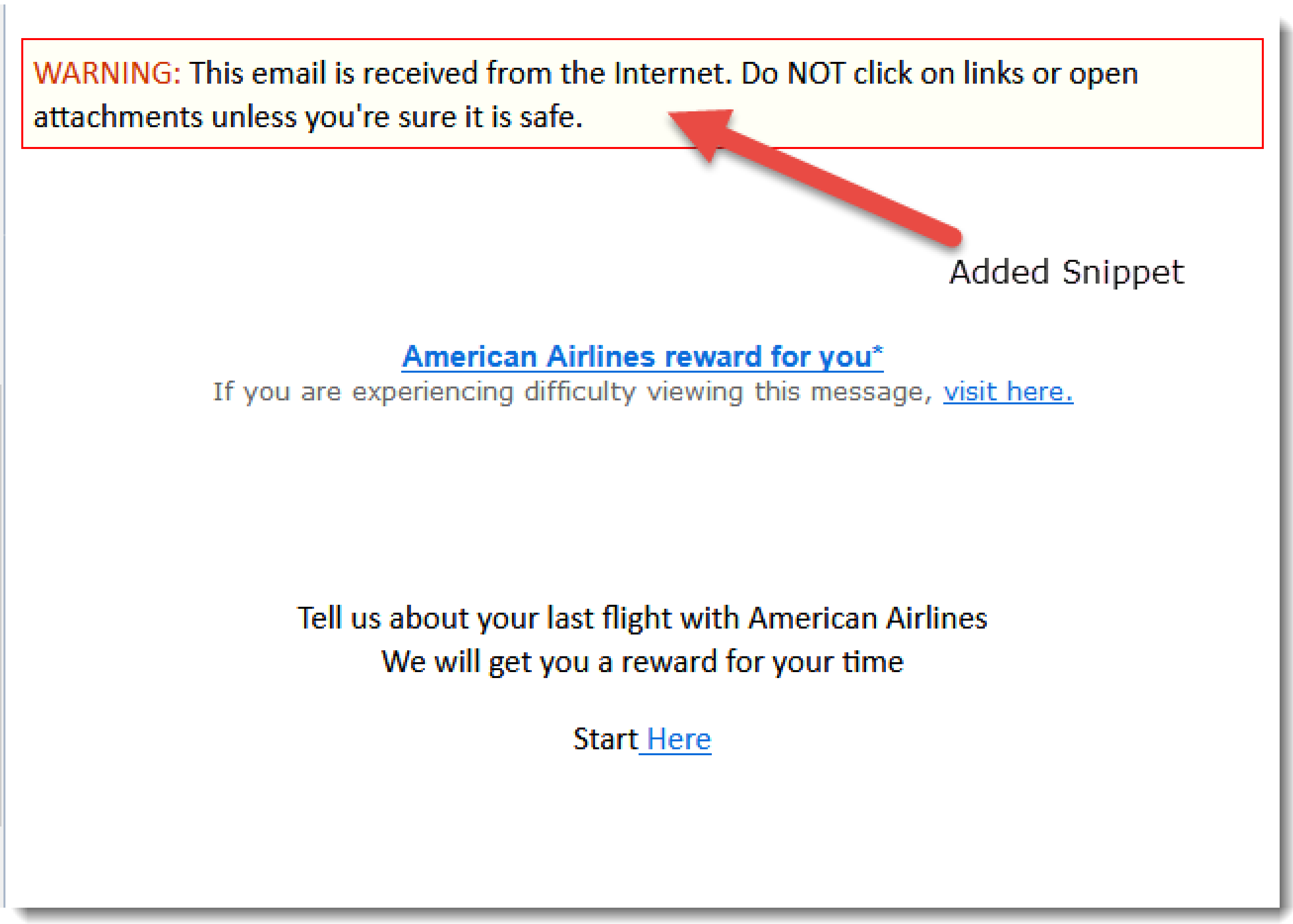
Note: The External subject tag only applies to inbound emails

To configure the external tag, go to Filter Management ---> Score Configuration.

Body Tags

Besides subject tags, administrators can also implement a body tag for emails. This message help novice users to think twice before clicking links or opening file attachments.

Here's an example of an custom body tag:



WARNING: This email is received from the Internet. Do NOT click on links or open attachments unless you're sure it is safe.

Added Snippet

American Airlines reward for you*

If you are experiencing difficulty viewing this message, visit here.

Tell us about your last flight with American Airlines

We will get you a reward for your time

Start Here

Note: Body tag is read from a file. You must create this file on the machine where Xeams is running.

Sample File

Copy the following contents and save it to a file.

```
<p style="border:1px solid red; background-color:#ffff6;padding:5px;">
<span style="color:#cc3300">WARNING:</span> This email is received from
the Internet. Do NOT click on links or open attachments unless you're
sure it is safe.</p>
```

Although you can save this file in any folder, we recommend saving it in **$INSTALL_DIR\config** where Xeams put every other configuration file. For example: **C:\Xeams\config\externalBodyTag.htm**

Steps to Configure

- Login as admin to the web interface
- Go to Filter Management → Score Configuration
- Specify the file name External Body File. This can be a relative path with respect to the **$INSTALL_DIR**. For example, **config/externalBodyTag.htm**. It can also be an absolute path.

Profiles

The multi-profile feature in Xeams allows you to do the following:

1. Specify separate spam filtering rules for a set of domains. In other words, you create a new profile.
2. Delegate administrative tasks for a certain domain(s) to someone else.

Consider the following scenario:

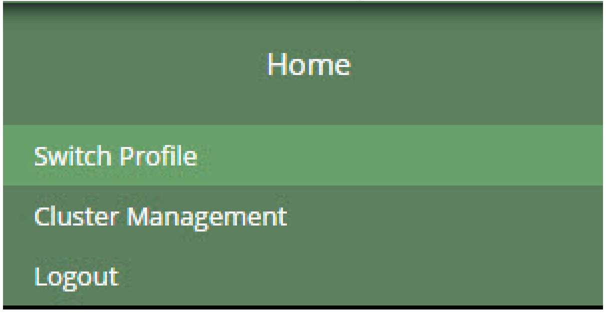
You handle emails for two or more companies. The domain name for these companies are: **CompanyA.com** and **CompanyB.com**. Using the multi-profile option, you can specify different rules for both of these companies and assign a person in these companies who will manage their rules.

Important: You must be using build number 5628 or higher in Xeams to use this feature.

Steps to enable this feature:

1. Log in to Admin Console.
2. Click **Server Configuration** on the main menu.
3. Click the **Advanced Configuration** tab.
4. Check the **Multi-Profile** option.

When this feature is enabled, you will see a new menu item under the **Home** link. Refer to the image below:



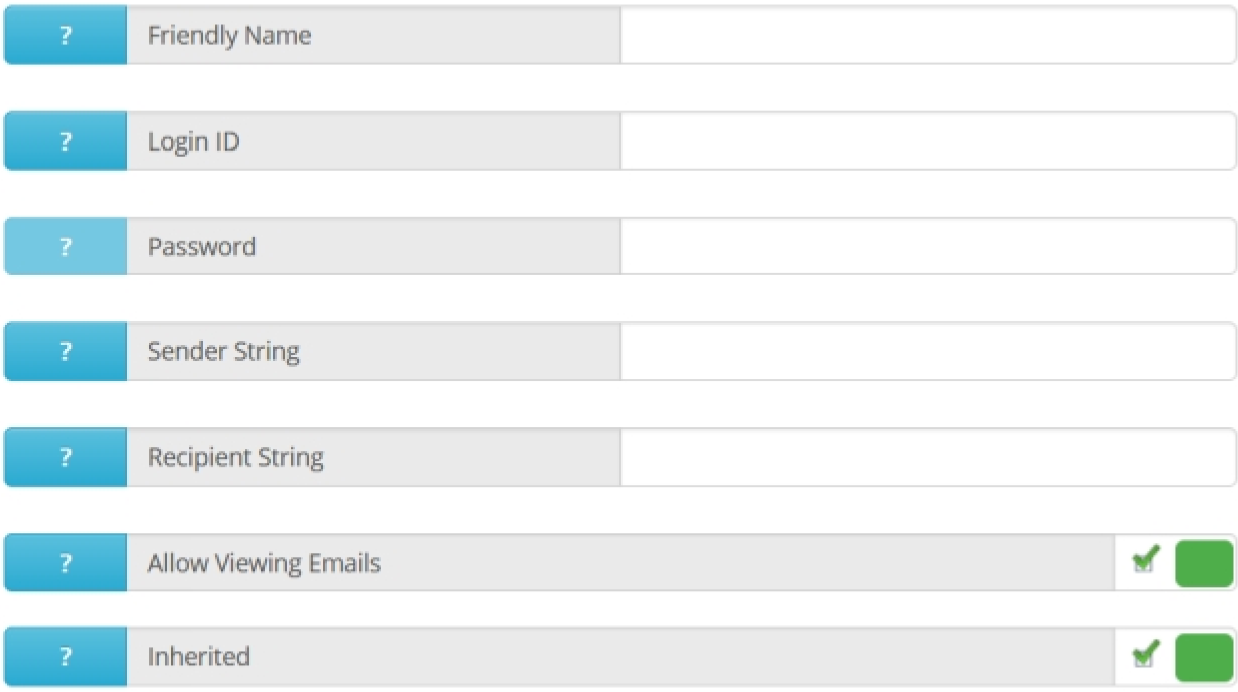
This option allows the administrator to view rules for other profiles. This page will automatically be displayed when an administrator logs into Xeams.

Creating New Profiles

Follow the steps below to create a new profile:

1. Click **Switch Profile** item under the **Home** link on the **Main Menu**.
1. Click **Add New Profile** link.

Once you click on the **New Profile** link, you will see the following fields below:



?	Friendly Name	
?	Login ID	
?	Password	
?	Sender String	
?	Recipient String	
?	Allow Viewing Emails	✓
?	Inherited	✓

Friendly Name - Name for the new profile
Login ID & Password - Username and password for the new profile. This is the login credentials for the profile in the Xeams **Admin Console**. When someone logs into this profile, they can only modify rules for the specified domain. This user is unable to change global settings.
Sender and Recipient String: Rules for this profile will apply if a matching string is found. For the sender, Xeams will try to match the FROM address, while it will try to match the TO/CC/BCC address in the recipient field.

For example, if the recipient field is set to @domainone.com, any emails that go to this domain will follow the profile's rules and filters. If you wish to have multiple domains, you can use a regular expression.

Note: If you want the profile to handle multiple domains and addresses, you can use regular expressions. For example:

@domainone.com, @domaintwo.com, and @domainThree.com will match for 3 domains.

Scalability Issues

It is highly recommended not to have more than 5 profiles per Xeams server. Every profile in Xeams will increase the memory usage by about 100MB.Creating too many profiles will cause your Xeams to run out of memory, particularly on a 32bit system.

If you decide to have more than 5 profiles per server, keep an eye on memory usage and increase the upper limit if the allocated memory hovers continuously near maximum memory.

Adaptive filters

Adaptive filters learn from the environment as time passes by. This learning ability improves the junk mail filtering functionality in Xeams.

There are two types of adaptive filters in Xeams; Bayesian Analysis and Auto-Learn Sender.

Bayesian Analysis

Bayesian spam filters calculate the probability of a message being spam based on its contents. Unlike simple content based filters, Bayesian spam filtering learns from spam and from good mail, resulting in a very robust, adapting and efficient anti-spam approach that returns hardly any false positives.

The Bayesian filter manages two databases; history of good word count, and history of bad word count. The database is stored in plaintext in the **Config Folder** in Xeams. These files are named SpamWords_001.dat for bad words and HamWords_001.dat for good words.

The Bayesian filter first starts in learning mode, it observes the contents of the messages coming in and learns which are considered spam or junk. After a certain amount of word count the Bayesian graduates. After it graduates, the filter only learns when a user specifically marks a message as good or spam. Graduation mode is there to avoid extensive memory usage.

The Bayesian score works in both directions. If it thinks the message is junk, a positive score is assigned. If the filter thinks the message is good, a negative score is assigned.

Auto-learn Sender

This filter is used when you use Xeams to handle outbound emails. Xeams learns and remembers email addresses on the Internet that receive emails from your local users. To understand this filter, consider the following scenario:

1. Bob **bob@yourcompany.com**, who is a user in your company, sends an email to Mary **Mary@outsideinternet.com** who is a user on the Internet.
2. You have configured Xeams to accept outbound messages.
3. Since Bob is a local user, Xeams will allow his message to go through and will also remember that Bob has sent an email to Mary.
4. When Mary replies back to Bob, the system gives credit to Mary's message hence avoiding a false-positive.
5. Each time Mary replies back to Bob, the auto-learn sender filter score will increase.

IP Filters

Blacklists and Whitelists

Although Xeams allows black and whitelisting, users, domains, and IP addresses, we strongly recommend you read the following section before making any changes to the rules.

- Whitelisting a single user is safe - Use the sender's entire email address when specifying the rule
- Whitelisting a domain name is generally safe - As long as the domain names do not belong to well-known companies, such as Hotmail.com, Gmail.com, BankOfAmerica.com, CitiBank.com, AOL.com, etc. However, is okay to whitelist a domain.
- Whitelisting an IP address is also safe - specify the IP address in the whitelist section.
- Blacklisting a user, IP address, or a domain is not recommended - This is because email addresses, IP addresses, and domain names can be easily forged. The only reason to blacklist a user is when you are 100% confident the sender is not forged.

Instead of white listing a domain, it is highly recommended to consider adding them as trusted domain.

How to black and whitelist a user or a domain

1. Click **Content Filters** under **Filter Management.**
2. Click **Sender Filters.**
3. Add a new sender filter.
4. Enter an email or domain name in the search string. For example: user@somecompany.com or @somecompany.com.
5. Enter a negative value to whitelist and a positive value to blacklist. Do not enter a very high number. A score around (+/-) 100 should be sufficient to drag an email in either direction.
6. Leave other values as-is.
7. Save the rule.

Steps to black or whitelist an IP address.

1. Click I**P Filters** under **Filter Management.**
2. Click either **Blacklisted IP** address or **Whitelisted IP** addresses depending on which one you want to add.
3. Enter the IP address you want to black or whitelist. You can also use an asterisk to block out a subnet. For example: 192.168.1. * .
4. The default 200 score should be enough. Click on save.

SPF

Sender Policy Framework or SPF is an extension to the SMTP standard. SPF makes it easy to counter most forged "From" addresses in email, and thus helps to counter email spam. The combination is also called SMTP+SPF.

How does SPF work?

SPF is a mechanism where domain owners announce where the email can come from for their domain. This announcement is done through a DNS server. For example, Microsoft exposes their SPF record in their DNS, which lists a set of IP addresses where an email can originate if the domain name is microsoft.com. If a message comes from any other IP address it should be considered as a forgery.

How can I create an SPF record for my domain?

Xeams comes with a SPF wizard that allows you to create a SPF string. Once the string is created, you need to create a TXT record in your DSN with this string.

To access the wizard, follow these steps:

1. Click **Tools** on **Admin Console**.
2. Scroll down and type your domain name for **SPF Wizard** and click **Proceed**
3. The generated string must be added in your DNS server as a TXT record

If you want to see the list of trusted domains you have in Xeams, hover your mouse over **Filter Management**, and click on **Sender Policy Framework**. This page allows you to configure SPF such as enabling or disabling it or modifying the scores. There is a button labeled **Manage Trusted Domains** on the right side. Clicking this opens a page where you can modify the existing list of trusted domains.

Country Filters

Note: Country filter is not recommended to use. Instead use the language filter in the Content Filter section. Please see here for more details.

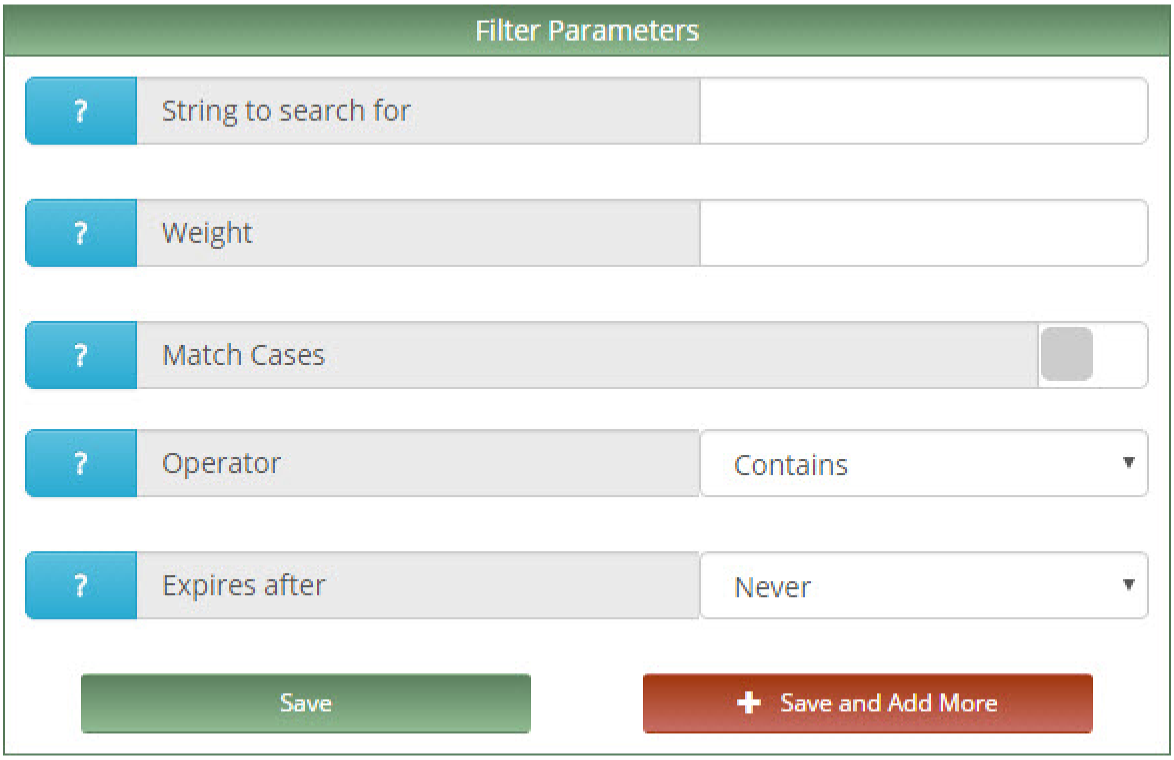
Xeams has an option to filter messages based on its country of origin. In every email the message contains a series of IP addresses that belong to the intermediate server that were involved in delivering the message. Xeams analyzes the IP addresses to find out the country of origin and assigns a score.

To create a new filter, hover the mouse over **Filter Management** and click **IP Filters**. Select the **Country Filtering** option to open up the menu. Select the country you wish to filter and set the score.

Content Filters

This section contains filters that inspect the contents of an email message. Each section looks at different parts of the email address to see if a message is considered spam.

Note: The template for creating a specific type of content filter has the same format as (excluding the body and header filter) the other content filters:



Filter Parameters

String to search for

Weight

Match Cases

Operator: Contains

Expires after: Never

String to search for - This field contains the text that be will be searched in the email. For example, if the string “credit” was here, then the filter applies a score in the message if the string credit was found in its contents.
Weight - This is the amount of score the filter will apply to the message. This value can be in either positive or negative.
Match Cases - Check this option if you want the search to be case sensitive.
Operator - This option informs Xeams how the search should be performed:

- Contains - the string can be searched anywhere. You can use the AND operator if you want to search for multiple strings.
  Contains word - The string being searched must be a word.
- Equals - The string being searched must exactly the same value.
- Starts with - The string being searched appears in the beginning.
- Ends with - The string being searched appears at the end.
- Does not contain - The string cannot contain this value.
- Is blank - This is useful if you are searching for blank strings.
- Regular Expression - This should only be used for advanced users.
- Expires after - This option allows the administrator to set an expiration date for the filter. This is useful if you want to add a temporary rule.

Attachment Filters

In this section of the filter, the administrator can modify the score Xeams gives to a message that contain attachments. They can associate score with a different type of file extensions. For example, if an administrator wants to block all .rar extensions, they can add a new attachment filter that ends with the string .rar and assign a score to it. Any email message containing a .rar attachment will get scored.

Sender Filters

This section of the filter inspects the sender’s email address. The administrator can specify an email address or other characters to filter the sender’s address. For example, if an administrator wants to block all email addresses coming from @freecreditcard.com, they can add a new sender filter where the sender’s address ends with @freecreditcard.com.

Body Filters

The body filter inspects the body content of the email for filtering. If an administrator wants to mark certain words as spam in an email, they can add a new body filter. There is also an option in the new filter labeled preprocessor.

An email body consists of 2 phases; Pre-processed phase, and post-processed phase. In pre-processed phase, the words are searched in the original email message as-is. In the post-processed phase, the server formats the message by removing any noise words such as HMTL tags, comments, and other character encoding. This option should be enabled if you are planning to search for HTML tags or any word that you want to phrase as-is.

Header Filters

This part of the content filter inspects the header of the email message. One difference in this filter is that there is a field called field name. In this option, the administrator can choose the field name to search the string for. For example, the field name TO searches for anything in the TO header. If you want the filter apply for other recipients, you can change the field name to CC or BCC. Additionally, you can input a custom header in the field name. The format must be the following:

Header Name: value

Custom Filters

Often, spammers use several tricks to avoid being filtered. In custom filters, Xeams looks for these tricks and assigns a score to the email message. An example of this is the **Macro Detector**. This custom filter looks for any macros inside a Microsoft word and excel document. Often, these documents contain macros that download viruses from malicious websites.

Language Filters

Often companies, particularly smaller organizations, seldom get emails in foreign languages. Xeams allow assigning scores if foreign characters are found. For example, there is a very good chance that an accounting firm in New York will never receive any good emails in Chinese.Xeams can detect foreign languages inside an email message.

DKIM

Domain Keys Identified Mail or DKIM is a mechanism to check if an incoming email's FROM address is valid or not.

DKIM adds a header to every outbound email. This header can be used to confirm the message authenticity. Xeams can also sign an outbound message with a private key that can be verified by a receiving server.

How to Enable DKIM in Xeams

In the **Admin Console**, hover your mouse over **Filter Management** and click on **DKIM**.

There are 2 sections in this page:

1. Left side: You can modify the spam score for incoming emails. If the DKIM authentication fails for a message, Xeams assigns this score to the email.
2. Right side: Specify domains that you would like to sign when sending outbound emails on the right hand side.

To prepare your domain for outbound messages, specify your domain name with a selector value. The selector can be any arbitrary value. Its purpose is to differentiate multiple SMTP servers in your company.

Consider the following scenario: You have two SMTP servers; Xeams and Exchange. Outbound emails are sent from both of them. In this case, the selector can be the word **Xeams** and **Exchange** for the other SMTP server.

In the background, Xeams automatically creates a pair of private and public keys. These keys are saved in the **$Install_Dir\config\dkimKeys** folder. It is strongly recommended to backup this folder. If you want to view the public key value for your domain, click on **View Details** for the desired domain name.

When a domain is added in Xeams, it will remain inactive until the public key is entered in your DNS server. This is done by design to avoid signing an outbound email without a DNS entry.

To add your public key in a DNS server, you will need to add a TXT record in your DNS server. The host name for this TXT record must be: **YourSelector._domainKey.YourDomain.com**

Copy and paste the value of your public key from the **View Details** screen for your domain.

DMARC

DMARC builds on top of SPF and DKIM. This not only helps prevent forgery but also provides a sophisticated reporting mechanism allowing the senders to fine tune their SPF and DKIM rules.

....

Xeams adds a score if DMARC alignment fails. Additionally, it can also process incoming reports and send outbound reports to other email servers on the Internet.

How to enable DMARC in Xeams

There are three aspects of DMARC in Xeams:

1. Assigning a score to an incoming email from the Internet if DMARC alignment fails.
2. Process incoming reports from other email servers.
3. Sending reports to other email servers.

Assigning Scores

Xeams will check DMARC alignment for every incoming email if DMARC is enabled on your Xeams. This happens even if you do not use DMARC for you own domain. A score is assigned if this alignment fails.

Every domain that publishes a DMARC record in their DNS also configures how a receiving server handle messages if alignment fails. This allows a gradual roll-out of DMARC for a company. When you first decide to use DMARC for your domain, you will not be sure how other email servers will treat your emails if DMARC alignment fails. Therefore, you may want to tell them not to reject any messages if messages from your domain are not aligned. Instead, send you a report letting you know why was DMARC failed, which helps you fine tune your DMARC record in the DNS server. There are three levels of actions when DMARC fails:

- None - This tells the receiving server to simply ignore DMARC but generate a report letting the sender know about the results.
- Quarantine - This tells the receiving server to do further filtering before considering the message junk
- Reject - The receiving server should consider the message junk

Displaying incoming reports

Xeams will automatically handle incoming reports for DMARC and create a summarized view for the administrator. Note that DMARC reports will only be available if you publish a DMARC record for your domain. The report provides the following information:

- Compliant Message Count - Number of emails that were compliant - meaning DMARC was fully aligned. Besides the count, you can also see the IP addresses where email generated from.
- Quarantined Message Count - Number of emails that were quarantined by the receiving servers. You will only see a number higher than 0 if your DMARC record policy is set to quarantine.
- Rejected Message Count - Number of emails that were rejected by the receiving servers. You will only see a number higher than 0 if your DMARC record policy is set to reject.
- SPF Passed - Contains the number of messages where SPF check passed.
- SPF Failed - Contains the number of messages where SPF check failed.
- DKIM Passed - Contains the number of messages where DKIM check passed.
- DKIM Failed - Contains the number of messages where DKIM check failed or a signature was missing.
- Total Reporters - Lists the domain names of servers on the Internet that sent a report.
- Total Reports - Holds a list of reports sent to your server in the last 15 days.

Note: Inbound reports are automatically processed and displayed when you click DMARC under Filter Management. Most servers send their reports once a day. Therefore, it could take up to 24 hours to see reports after you create a DNS entry for DMARC.

Xeams will display reports for multiple domains if your server handles more than one domain.

Sending outbound reports

In order for Xeams to send out-bound reports, you must check the Reporting Enabled checkbox in DMARC configuration. This option will generate an aggregate report for DMARC that will be sent to other servers on the Internet letting them know how their messages were treated by Xeams.

Using DMARC for your domain

In order to enable DMARC for your domain, you must create a TXT record in your DNS server. Although many tools are available on the Internet that can help you generate a DMARC record, in order to get you going without getting into too many details, we recommend the following value for your DMARC record.

When creating a DNS entry, use _dmarc.yourdomain.com for host name.

Use the following value for the first 90 days:

v=DMARC1; p=none; rua=mailto:dmarc.rua@yourdomain.com

Change the value for yourdomain.com with the appropriate name. This value tells other servers on the Internet to simply monitor DMARC alignment and report them to your Xeams, allowing you to fix problems with your SPF and/or DKIM signatures. Frequently check the report generated by Xeams for your domain to confirm SPF and DKIM are not failing for IP addresses belonging to you.

Other servers on the Internet will send their reports to dmarc.rua@yourdomain.com, which will automatically be handled by Xeams.

Once you are confident SPF and DKIM are not failing for your IP addresses, change the policy to quarantine by modifying your DNS record to:

v=DMARC1; p=quarantine; rua=mailto:dmarc.rua@yourdomain.com

Note: Notice the username part (value before the '@' sign) in the email address, which is set to dmarc.rua. This is the default username for emails in Xeams. If you decide to use a different value, ensure you specify that for the User for Aggregate Feedback field in DMARC configuration.

Every domain handled by your Xeams must have identical value for the User for Aggregate Feedback field.

ClamAV Integration

Xeams can be configured to work with ClamAV, an open source anti-virus software. You will need to run ClamAV in daemon mode. After this, Xeams will consult with ClamAV in determining if an email contains a virus.

It is recommend to run ClamAV on a dedicated Linux machine rather than Windows, because it uses less resources that can be trimmed down to exactly what you need. Alternatively, you can run Linux as a virtual machine using VMWare or VirtualBox on any host. If you prefer, you can install ClamAV on the same machine where Xeams is running.

Steps to configure ClamAV integration

1. Download ClamAV from www.clamav.net for your appropriate platform.
2. Run ClamAV in daemon mode. Click here for details. Additionally, please see here on how to fully install and configure it on Linux.
3. Login to the **Admin Console** as the administrator.
4. Specify the IP address or the host name of the machine where ClamAV is running and click save.
5. Once the values are saved, Xeams will send a test virus to ClamAV which should be detected if ClamAV is working properly.

If the IP address value cannot be saved, try the following:

1. Ensure ClamAV is running in daemon mode.
2. If Xeams is able to connect but a test virus is not detected, update the virus signatures in ClamAV.
3. Make sure a firewall is not blocking communication between Xeams and ClamAV daemon.

Company Policy Violations

Xeams can optionally trigger notification emails when an inbound or outbound message arrives that violates your company policies. Using these alerts management can ensure their employees are adhering to their company policies. Besides generating notification emails, Xeams can also block the message by assigning a score.

How to Create a New Policy Violation

To add a new policy, click on the **Add a New Alert** button.There will be 2 sections you will have to fill in to create the new policy violation alert; **Alert Options** and **Trigger Criteria**.

The Alert Options contains the following field:

Friendly Name - The name for this policy .
Alert Recipients - Email address(es) of the user(s) to whom this alert will be sent. To specify multiple addresses, use a comma.
Message Score - You can optionally set a score for the original email message, which allows you to block any email you deem necessary.
Attach Original - The original email will be attached to the notification message if this option is enabled.
Subject - Subject of the alert.
Sender -The email address you would like alerts to be sent to. For example, alerts@yourcompany.com.
Text - This is the actual message the user will receive in the alert.

The **Trigger Criteria** contains the following fields:

Sender Email - An alert is triggered when an inbound or outbound message contains this value.
Recipient Email - Similar to the sender email, but applies to the To, CC, and BCC fields.
Sender IP - An alert is triggered if a message comes from this IP address. You can use a * character as a wild card. For example, 192.168.1. *
Attachment - An alert is triggered if an email contains the specified attachment(s).
Subject - An alert is triggered if the subject of the email matches this value.
Body -An alert is triggered if the body of the email matches this value.

You do not have to fill every single trigger criteria field, only the ones you want. All the values can be specified as regular expressions.

Manage Disclaimers

When enabled Xeams will append text messages towards the bottom of emails. The message can be written in HTML. The following options are below:

- **Do not append disclaimers for local recipients** - If the recipients are local, don't apply the disclaimers.
- **Enable Disclaimers in Proxy Server** - Enable disclaimers when using the proxy server.
- **Apply disclaimer only if sender is authenticated** - If the sender is authenticated in Xeams, only then apply the disclaimer.

Action Management

This section allows administrators to configure how emails are handled once Xeams assigns a category to an email message. Action management is accessible in the **Admin Console** under **Message Repository**.

By default, good messages have no specific action, the email gets sent to the destination address after being filtered, possible spam messages have their subject changed, and spam messages are quarantined. If you want to modify any of these settings, you can change the action tab on each message category.

For example, if you also wish to quarantine possible spam messages, you can click on the action for possible spam and change the field from “Change Subject” to “Quarantine”.

Another option to modify the action is to forward the emails to a specific email address. For example, you can forward all your spam email addresses to one recipient (example, spamcollect@yourcompany.com) by entering in the email address in the **Forward To** column.

Simulating Spam

Spam simulator is a built-in utility that is used to fine-tune the filtering rules. After adding or modifying rules in Xeams you can paste the contents of any email message that was previously tagged incorrectly to confirm it is now being tagged correctly.

Follow the steps below to run the spam simulator:

1. Log in to the **Admin Console.**
2. Search for the desired message in **Message Repository.**
3. Click the subject to view the message and select the **Simulate** button.
4. Xeams will display the result determined by every rule that was applied to come up with a final score.

Alternatively, you can click on **View Code**, copy the contents, and hover your mouse to **Tools** and click on **Spam Simulator**. Afterwards you can paste the email contents and click proceed.

Message Repository

Introduction

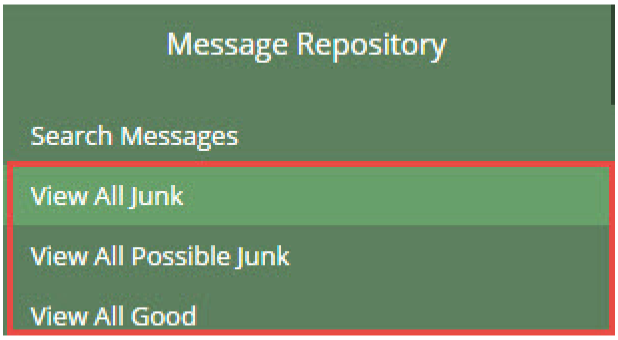
This chapter provides information about how to search for emails, as well as configuring message retention.

In this chapter

This chapter contains the following topics:

Viewing all messages

The administrator is able to view messages that came into Xeams by each category. This option is accessible in the **Admin Console** by clicking on **Message Repository**, or hovering your mouse on **Message Repository** and clicking on one of the view all category messages:



Once you click on the view all messages, the web interface will list all of the messages that came to Xeams. Here, you have the following options:

Mark a message as good or spam - If you see a message that was marked incorrectly, you can select the email and click on **Mark as Good** or **Mark as Junk** on the upper right side.
See the reason for the score of a message - Each email in this page will have the assigned score on the right column. Hovering your mouse over the score will list the reasons.
Restore an email - If an email was incorrectly marked as spam, you can restore the email. Xeams will attempt to deliver the email to the destination server.
Click to see the contents of a message. - You can click on an email to view the body contents of the message. Additionally, you can inspect attached files, view the raw code of the message, or run the email through the spam simulator.

Searching all Messages

Users and administrators can login to the web console to search individual emails. To do this, log into the web console of Xeams and hover you mouse over **Message Repository** and select **Search Messages**.

Note: non-administrative users automatically have a search message option as soon as they log in.

By default, message repository displays the most recent messages. Therefore, the searching feature comes in handy when a user needs to search a message received in the past. Additionally, Xeams creates an index for every message that makes the searching extremely fast.

Searching Tips

The following examples show some useful searching tips:

1. **Logging in as a user and searching for messages received in last 10 days**

    - When logged in as a user, Xeams displays messages the user has received since midnight. However, a user can search for older messages by doing the following:
        - Select the appropriate message type.
        - Select a date that is 10 days from current date.
        - Enter **10** for **Number of days to search for** field.
        - Select **Sender or Recipient's Email** in **Search Field**.
        - Enter your own email address in the **Search For** field.

2. **Searching for a particular user**

    Assume you want to search for an email you received from: **Bob Builder Bob@thebuilder.com** Use the following values:

    - Select the appropriate message type .
    - Select **Sender or Recipient's Email** in Search Field .
    - Enter any of the following values (that are in bold):

Builder	(Partial name)
Bob	(Partial name)
bbuilder	(Single word within email address)
bbuilder@thebuilder.com	(Entire email address)
thebuilder	(Single word within email address)

3. **Searching for words within an emails body**

    - Assume you want to search for multiple words in a message: **Medical Bills & Electric Bills**
    - Enter the following values:
        - Select the appropriate message type.
        - Select **Subject** or **Body** in Search Field .
        - Enter any of the following values in the Search For field:
            - **Medical AND Electric AND Bills.**

    Notice the use of uppercase **AND**. This predicate will make Xeams look for every word and will only return messages that contain all 3 words.

    Omitting this **AND** will implicitly change the predicate to an **OR** and Xeams will return messages containing any of the 3 words.

Message retention

Messages in Xeams are retained until they are deleted. By default, good messages are never deleted and messages tagged as Junk or Possible Junk are deleted after 30 days.

Click **Message Retention** under **Server Configuration** in the Admin Console to change this configuration.

Advanced Configuration

Introduction

This chapter provides information about additional configurations in Xeams.

In this chapter

This chapter contains the following topics:

Backing Up a Xeams Installation

Every file in Xeams gets installed in the installation folder. The installation folder on Windows is usually set to **C:\Xeams** and **/opt/Xeams** on Linux. Therefore, if you backup this entire folder, you can restore it if disaster strikes. However, backing up the entire installation folder is more than what you need. There are some folders that should be backed up, while other folders do not need to be backed up.

The following information describes the purpose of each folder and leaves the decision up to the administrator if they wants to back it up:

Config - This is the most important folder; it holds every configuration parameter. In fact, it has another sub-folder called archives, which holds a backup of every configuration file. You should see seven files in this folder containing a backup for every weekday.

Note: It is recommended you back up the entire config folder.

DB - This folder holds data that is used for reporting purposes. If this folder is missing, it will be recreated automatically provided the Reports folder is present. If both DB and Reports folders are missing, reports in Xeams won't display any data.
Good Emails - This folder holds every good email. You should backup this folder if you are using Xeams as the primary server. If you are using Xeams as a firewall, a copy of every good message already exist on your primary server. In that case, retaining these emails is optional.
Logs - This folder holds logs created by Xeams. Backing up this folder is optional.
MailingListSubs - You only have this folder if you are using the mailing list feature in Xeams. You don't have to backup this folder.
OutboundMailQueue - This folder holds messages that are waiting to be delivered.
Possible Spam - This folder holds message that fall into the possible junk category. If this folder is missing you won't see any email in the **Message Repository** for possible junk.
Reports - This folder, along with the DB folder is responsible for generating reports.
SearchIndexes - This folder holds search indexes that are used by the **Admin Console** to search messages in **Message Repository**. If this folder is missing you won't be able to find older email messages in the Admin Console. This folder should be backed up.
SpamEmails - This folder holds junk messages. If this is missing, you won't see any junk email in Message Repository.
UserRepository - This folder hosts email repository for POP3 and IMAP servers. This folder should be backed up.

The following folders **do not** need to be backed up, Xeams installer will create it at the time of installation:

- **Jre**
- **Lib**
- **Patches**
- **ProcessingMessages**
- **Uninstall_Xeams**
- **Webfront**

Moving Xeams to Another Machine

Follow these steps to move your Xeams server to another machine:

1. Use the installer to install Xeams on the new machine.
2. Stop Xeams server if it is running on the new machine.
3. Copy the contents of the following folders from old server to the new one. These folders are located off of the installation folder:

   - DB
   - GoodEmails
   - logs
   - OutboundMailQueue
   - PossibleSpam
   - ProcessingMessage
   - Reports
   - SearchIndexes
   - SpamEmails
   - UserRepostory
   -
4. Copy the contents of the config folder with the exception to two files:

   wrapper.conf - This file is specific to operating systems therefore, do not replace it on the newer machine.
   AppConfig.xml - This file contains IP addresses and other configuration parameters that may be different on the newer machine. There are two ways to merge this file from an older to newer installation:
   - Manually - by using a text editor. Open both old and new files in a text editor and selectively copy values. Although this method will save you some time, we do not recommend using it if you are not familiar with XML. Internet Explorer is a very good parser for XML. After changing this file, try opening it in IE. A notification will be given if the file contains syntax errors.
   - Using the **Admin Console** - Open the **Admin Console** on both machines and synchronize the settings. After saving values you can compare the two XML files to see what is left.
   -

   Note: If you are moving Xeams to a different Operating System, do not copy AppConfig.xml. This configuration file contains OS specific entries and will not work if you simply copy the file. A better approach is to set the parameters from the web interface.

5. Start the server on the new machine.

   Regardless of the edition of Xeams you are using, you are required to register Xeams again. If you have purchased the Enterprise edition you will need to enter the serial number again through the **About Screen**.

Configuring Maximum Log File Size

By default, every log file can grow up to 5 MB. Once a file size reaches 5MB, the file gets renamed to fileName.log.1 and a new file is created with the original name. This way you can have up to 10MB of logs.10MB of data is typically more than enough. However, if 10MB of data is not sufficient, use the following instructions to increase this value:

1. Locate **server.properties** file in $INSTALL_DIR\config folder. If the file is missing create a new text file with this name.
2. **Note:** Make sure the file name is called **server.properties**, NOT service.properties!
3. Copy the following text in a line by itself: **xeams.max.log.size=25MB** .
4. The above statement will modify the size of one file to be 25MB, which means you will have up to 50 MB of every log. You can change the value (25) to a number you want.
5. Save the file Restart Xeams.

Sending and Receiving Large Attachments

Configuring Maximum Email Size

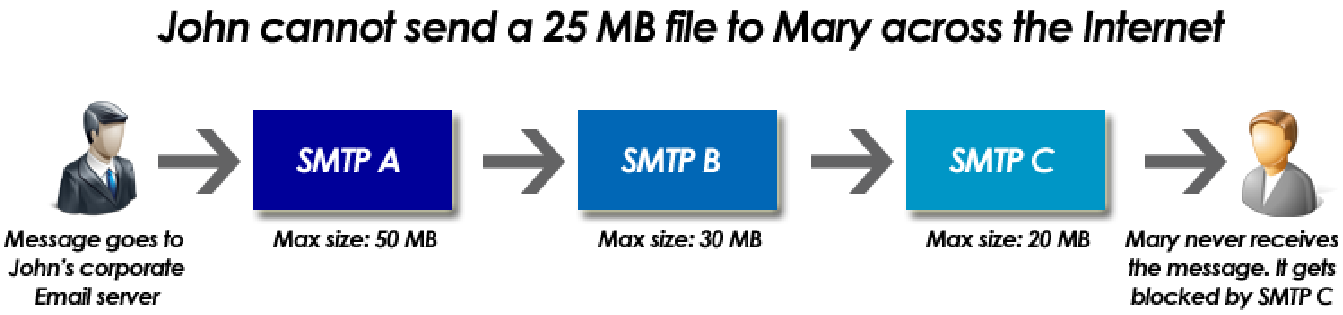
By default, Xeams rejects messages larger than 20MB but is configurable. However, please note that email servers are not designed to handle large attachments and neither is Xeams.This is because large messages require more memory for processing. This memory requirement affects Xeams more than other email servers that do not analyze incoming messages. Additionally, Xeams uses a multi-threaded architecture to process incoming messages. This mean messages containing large attachments can come in from different sources simultaneously adding up to a large memory usage.

Use the following steps to modify the maximum email size in Xeams. We strongly recommend not using a number higher than 30 MB, as that can potentially bring down the entire server:

1. Log into the **Admin Console** as the administrator.
2. Hover your mouse over **Filter Management**, and click on **Message Size**.
3. Modify the **Maximum Global Size** (NOT Maximum Actionable Size). This value is in bytes.
4. Click Submit to apply the change.

Receiving Large Attachments in an Email

A typical email server cannot accept emails larger than a few megabytes. Although some servers allow administrators to change this value to as high as 40 MB, sending large attachments in an email consumes a lot of system resources. Emails, by design, hop from one SMTP server to another before reaching the intended user's mailbox. Therefore, the server supporting the smallest email size dictates the maximum size of an email. Consider the image below:


John cannot send a 25 MB file to Mary across the Internet
SMTP A
SMTP B
SMTP C
Message goes to John's corporate Email server
Max size: 50 MB
Max size: 30 MB
Max size: 20 MB
Mary never receives the message. It gets blocked by SMTP C

Since SMTP C cannot accept emails larger than 20 MB, John's email never gets to Mary even if his server (SMTP A) supports attachments up to 50 MB.

SynaMan on the other hand, includes an embedded SMTP server that is especially designed to handle large emails. In fact, there is no upper limit on email size when it is sent through SynaMan's embedded SMTP server.

The following demonstrates how to integrate SynaMan with Xeams, allowing companies to put Xeams on the edge of their network and yet send and receive large attachments.

Configuration

1. The Enterprise Edition of SynaMan (purchased separately) must be installed on either the same machine or a separate machine. Typically, companies put Xeams on their DMZ and SynaMan on a machine inside their LAN.
2. Connect to Xeams **Admin Console** as admin and click **Send/Receive Large File**s under **Server Configuration**.
3. Specify the URL for SynaMan is running. For example: http://192.168.1.14:6060 or

https://files.yourcompany.com. This must be the same URL that you normally use to connect to SynaMan with your web browser.

4. Specify the IP address of Xeams in SynaMan's Embedded SMTP Server configuration. This step is not required if Xeams and SynaMan are running on the same machine. For example: 192.168.1.50.

How it Works

- Upon receiving a new email (inbound or outbound), Xeams inspects its message size. This message is forwarded to SynaMan if the message size is large. The actual size of the message is determined by what you have configured in SynaMan.
- SynaMan detaches the attached files and returns the message body back to Xeams. The returned body will contain a hyperlink allowing the recipient to download the originally attached files using their web browser.
- Once Xeams receives the message body back from SynaMan, it proceeds with its normal filtering process.
- Upon receiving the message, the end-user can download the attached files from SynaMan's web interface. The image below demonstrates the actual traffic flow.

Managing Security Alerts

Alerts are sent to administrators if someone has incorrectly entered their password multiple times in a span of 10 minutes. By default, the number of incorrect password attempts before an alert is sent out is 5.

To modify the alert threshold or unblock the IP addresses, do the following:

1. Log in to the **Admin Console** as the administrator.
2. Hover your mouse over **Server Configuration** and click on **Manage Alerts**.
3. Modify the value for the Alert Threshold.
4. If there are currently any IP addresses blocked Xeams will inform you that there are x amount of IP addresses block. If you want to unblock the address(es), click on the hyperlink to remove the blocked addresses.

In addition to the password alert, Xeams provides an alert if your Xeams folder is running out of disk space. These folders are the installation folder, message repository folder, and the temporary folder. You can modify the alert threshold in the disk space alerts section.

Extended Configuration

To avoid cluttering the web interface, some configurable parameters cannot be modified through the web interface of Xeams. These additional parameters are stored in a file called **server.properties** and is stored in **$INSTALL_DIR\config** folder.

This file is not present when you first install Xeams. Therefore, you may have to create a new file if you're asked by our support department to enter a parameter in this file. The contents of this file are in plain text.

Ensure the name of the file is **server.properties** and NOT service.properties or server.properties.txt

Values are entered in the following format:

```
# Lines starting with a # sign are ignored and can be used for user comments
# Parameter name appears on the LHS of equal sign, whereas the value appears on the RHS.
# For example:
parameter.one=50
parameter.two=Another Value
```

A Partial List of Parameters

Please see the server.properties KB article for a list of parameters.

Clustering

Introduction

This chapter provides information about the concept of clustering and how to configure it.

In this chapter

This chapter contains the following topics:

Concepts

Consider a scenario where you have more than one Xeams server for spam filtering:

- You have 3 MX records to process incoming emails.
- You are running Xeams on all 3 servers that filter junk messages.
- Eventually, good messages are sent to MS Exchange.
- The highest priority MX refers to a Xeams instance that is on the same network as your Exchange.
- Xeams is running on secondary and the MX is running somewhere on the Internet.

Since there are three instances of Xeams, it becomes easier from an administrative perspective to change a rule on the MASTER server and let it automatically propagate to the SLAVES.

Requirements:

- You must be using Xeams version 5.3 or greater.
- The build number between master and slave machines must match.

How to Enable Clustering

Enabling clustering is a two-step process:

1. Designate the highest priority Xeams as MASTER:

   - Login as admin to the web interface of the Xeams you wish to make the MASTER server.
   - Click on **Cluster Management** under the **Home** menu.
   - Select **Master** for **Role.**
   - Add one or more slaves.
   - Master and slave will communicate with each other over HTTP(S) using the same channel administrators used to connect to the web interface. Therefore, use the URL you normally use in your browser and ensure necessary TCP/IP port (5272 by default) is open between the two machines.
   - You can add as many SLAVES as you like.

Note: You will see **Not Authorized** for the status when a slave is first added. This is normal.

2. Authorizing a MASTER:

   - Login as admin to the web interface of the Xeams you wish to designate as the SLAVE server.
   - Click **Cluster Management** under the **Home** menu
   - Select **Slave** for **Role**
   - Add the IP address of the machine where the MASTER is running. If that machine has multiple IP addresses, you can separate them by a comma.
   - **Note:** that there can only be one MASTER. Do not put IP addresses for more than one machine in this field.
   - Once a MASTER is authorized, refresh the browser that is connected to the MASTER and ensure both machines can talk to each other by looking at the status.

Synchronization Between Master and Slave

The following configurations are synchronized:

- Modifications to filtering rules, such as Score Configuration, Content Filters, RBL Filters, and black and whitelisted IP address.
- Associations.
- Distribution List .
- User Configuration along with passwords .
- Trusted Domains.
- Profiles

The following are not synchronized:

- Server Configuration, such as TCP/IP ports, SSL certificates, server mode.
- Configuration for SMTP server or SMTP proxy server.
- Administrator's email and password.
- Active Directory, Message Retention, Alerts, Local Host File, ClamAV.
- Live Monitor.
- Log files.
- Global reports - daily, monthly, and yearly.
- Maximum global email size

Message Repository

Message repository is automatically synchronized between MASTER and SLAVES. Therefore, when you search messages or display a list of all messages, the MASTER will pull necessary information from the SLAVES and display one consolidated result. Additionally, different colors are used in the message repository when a message is pulled from a SLAVE.

The same applies for user reports that are sent on daily basis. Reports will only be sent out from MASTER and will contain records from the SLAVES. Users will only get one report that will pull data from every instance of Xeams.

What to Avoid When Clustering is Enabled

Do not change any configurations that are in the SLAVE machine(s). This includes filtering rules, AD Lists, User Configurations, and Trusted Domains. Any configuration from the MASTER will automatically apply to the SLAVE.

Trouble Shooting

Introduction

This chapter provides information about

In this chapter

This chapter contains the following topics:

Installation Problems

Scenario 1: You are unable to connect to the Admin Console

1. If you are running Xeams on Windows, ensure Xeams service is running. By default, the **Admin Console** listens for client connections on TCP/IP port 5272.
2. Confirm you have this port number specified in the URL. For example: http://localhost:5272.

Scenario 2: Xeams service will not start

1. First, ensure no other TCP/IP servers are listening on the ports that are used by Xeams. These ports are:
   - 5272 - web server for Administration console
   - 25 -SMTP server
   - 143 -IMAP server
   - 110 - POP3 server
   - 4949 - Connection server. This is used internally by Xeams.

2. Next, check the logs files for errors. The default location for the log files is %INSTALLATION_DIR%/logs. These logs files, particularly xeams.log, may contain some important information pertaining to the reason of why it is failing. Another log file to refer to is wrapper.log .
3. Lastly, try running Xeams server in debug mode. Follow the steps below to run in debug mode:

   A. Start a console window or a terminal window if you're on a Linux/UNIX machine. Change the current directory to the installation folder of Xeams.
   B. On Windows, type: run.bat debug. On Linux/UNIX type: ./run.sh debug.

   This will start Xeams manually, by-passing the Windows Service or Linux/UNIX cron job. Watch the console window closely for any errors.

Inbound Emails

Consider the Following Scenario:

- A user John, john@BusinessPartner.com, wants to send an email to Mary, mary@YourCompany.com.
- John is a user on the Internet who may or may not use Xeams.
- Mary is a user on your network and her emails go through Xeams.
- John wants to send an email to Mary.

In regard to this scenario, there may be times where something could go wrong in the process of receiving inbound emails.
Please see this article on the list of steps where it can go wrong and how to troubleshoot them

In addition to above, here are related scenarios regarding to inbound email issues:

- I'm not receiving the daily summary/quarantine report for my users.
- Confirm the email is not being blocked by a Front Door Rejector.
- Confirm the email does not exceed the Deletion Threshold.
- Confirm the email does not exceed the maximum global size.
- Confirm you are not receiving a error code 420.

Troubleshooting Outbound Emails

Consider the following scenario:

- A user, Mary, mary@YourCompany.com, wants to send an email to John, John@BusinessPartner.com.
- John is a user on the Internet who may or may not use Xeams.
- Mary is a user on your network and has specified the hostname or IP address of Xeams' machine in her MS Outlook or Thunderbird client
- Mary wants to connect to her email client and send an email to John.

In this scenario, there may be issues occurring during the process of sending out outbound emails.

Please see this article on the list of steps where it can go wrong and how to troubleshoot them.

Improving Junk Filtering

When an email comes into Xeams, there are numerous filters that apply a score to the message. Once the filters are applied, Xeams will determine if an email is junk, possible spam, or a good message based on the final score. Administrators can modify these filters to improve and fine tune the scores. In addition to modifying the filters, they can use certain tools and configure their server to enhance their junk filtering.

Please see this article for a list of ways to improve junk filtering.

Xeams is Not Starting After an Update

During an update, Xeams pulls files from our main website. Use the following steps to restore if you find Xeams is not starting after an auto update:

1. You must have access to the machine where Xeams is running.
2. Stop Xeams if it is running.
3. Open File Manager on Windows or Terminal on Linux and go the $INSTALL_DIR\lib folder. This path on Windows is typically set to C:\Xeams\lib and on Linux it is /opt/Xeams/lib.
4. Try starting Xeams service.
5. Once the service is up, download two files: Xeams.jar and webfront.zip and put them in $INSTALL_DIR\patches folder.
6. Do not extract the contents of webfront.zip. You should only have 3 files in the patches folder:

    - Patcher.jar
    - Xeams.jar
    - webfront.zip

7. Login to the web interface as admin.
8. Click Restart on the right hand side.

Xeams is running very slow/unresponsive

Certain configurations can slow down Xeams, making it unresponsive. Please take a look here to help you troubleshoot the root of the cause.

Additionally, please see the below scenarios:

- If clustering is enabled, confirm master and slave machines are able to ping to eachother.
- If multiple-profile is enabled in Xeams, confirm you do not have too many profiles.

Emails are not filtering

If your emails are not getting filtered, confirm the license has not expired. To check this, hover your mouse over Tools and click on About Xeams.

Additional articles/notes:

- Confirm the active user count does not exceed your license. If so, please see the troubleshooting incorrect user count page for more details.
- If the license is not expired and active user count is correct, confirm "enable filtering" is enabled. To check this, hover your mouse over Filter Management and click on Score Configuration. In this page, make sure enable filtering is checked.
- Sometime before the license expires, Xeams will send an email to the administrator letting them know the license will expire soon.

Emails show up in the wrong category

Every email coming into Xeams will be assigned a score. This score determines if the message is good or junk. Please take a look at our incorrect classification KB article on finding out why the emails are scored incorrectly.