JEP(S)

V2.4

Administrator manual

Spam filter for Exchange 2000-2010 and IIS SMTP

Document control	
Document name:	JEP(S) Administrator manual
Author:	Proxmea BV, Christoffer Järnåker
Last update:	december 3, 2009

Index

Overview

JEP(S) is a spam filter which intercepts mail sessions before the mail is received. This is done by using several technologies like greylisting, dynamic and static black- and white-lists and pattern analysis. By doing this it drastically reduces the load on the mail server as the spam mail is never received.

When JEP(S) suspects that a mail session is spam related it will send back a response to the sending mail server which indicates that the session has failed and that the mail has to be resent. The sending mail server will then queue the mail to be resent and retry at a later time. JEP(S) keeps track of this and when the mail is resent after a configured delay (normally 2-10 minutes) it will be allowed to be pass through to the mail system.

The benefit of refusing the mail before it's delivered is that you have never received the email that you're refusing. By doing this the sending mail system is informed while the session is still open that you're refusing the mail. If, for whatever reason, something goes wrong with the re-transmittal of the email then the sending user will be informed in clear text about what action was taken on the mail.

One of the key advantages of JEP(S) is to no expose the mail server with unnecessary sessions and it therefore makes your mail server run smoother as it uses fewer resources handling all spam sessions.

No more 'lost' email due to spam filters that believe that a mail is a spam and that doesn't inform the sender about this.

Who should read this document

This document is intended for systems administrators which are operating SMTP mail systems based on Exchange and SMTP services.

Requirements

- A server / workstation running either Exchange 2000/2003 with SMTP installed –or- Exchange 2007/2010 server with the edge role –or- IIS SMTP service installed and configured.
- The server needs to be internet facing and accept SMTP (mail) traffic directly from sending mail servers.
- .NET 2.0, 3.0 or 3.5 framework. Can be downloaded for free from Microsoft at http://www.microsoft.com/downloads/details.aspx?FamilyID=0C1B0A88-59E2-4EBA-A70E-4CD851C5FCC4&displaylang=en.
- (optional but recommended) SQL server 2005 or SQL server express.
  SQL server express can be downloaded for free from Microsoft at http://www.microsoft.com/sql/editions/express/default.mspx.
- (optional) Domain controller that answers LDAP queries for building email addresses.

Component overview

- **JEP(S) Sink** – Handles the mail connection on the SMTP service for mail on IIS and Exchange 2000-2003. Sends intercepted session information to the JEP(S) server for analysis.

- **JEP(S) Agent** – Handles the mail connection on the transport service for mail on Exchange 2007/2010. Sends intercepted session information to the JEP(S) server for analysis.
- **JEP(S) Server** – Receives queries from the JEP(S) sink and responds with Pass or Block depending on the outcome of the analysis. Logs events to the systems application event log.
- **JEP(S) Admin** – Administrates all settings and installs/uninstalls both the sink and the server.
- **JEP(S) Listener** – Listens to the outcome of the JEP(S) server result and displays this in real time.

Features of JEP(S)

JEP(S) combines four technologies to filter spam; greylisting, RBL's (Real time Blacklists), RWL's (Real time Whitelists) and email address lists. These four in combination gives you good spam protection with an extremely low rate of false positives in comparison with other spam filters. A low rate of false positives means that it's unlikely that legitimate email will be treated as spam and blocked. And the block rate of your JEP(S) installation will of course vary depending on the volume and the type of email you're receiving, but most of our implementations show an effective block rate of 94-98% on the greylist filter itself without taking into account the effect of the RBL feature.

JEP(S) analyses incoming data (IP, sender and recipient and result) to build a list of suspected spammers. This list, which doesn't contain any information about you or your server, is then sent off to a central server which compares all received lists against each other. When a certain percentage of submitted lists are reporting the same suspected spammer then this IP (the sender servers IP) is black listed.
JEP(S) can then query the same RBL and utilize these collective results for blocking spammers. This feature can be disabled in the licensed version of JEP(S).

There is also a graphing component of JEP(S) which plots real time and historical graphs which are saved as images. These images can then be included in reports and real-time monitoring systems.

The features of JEP(S) are:

- Greylist filtering.
- RBL or Real-time Black Lists.
- RWL or Real-time White Lists.
- Automatic white listing of outbound mail.
  This feature means that if you send Bob and email then his email address will be added to the whitelist for a limited period of time. If he responds within this timeframe, typically three days, then his email will be exempt from the filter and pass through instantly as well as be added to the JEP(S) database.
- Blocking of invalid mail addresses before they hit your mail server.
- Automatic Real time BlackList Submission (ARBLS).
- Support for standalone database as well as for Microsoft SQL server 2005.
  Stand-alone database types are MDB (Access) databases for 32-bit systems and SQL

Compact edition 32 and 64-bit systems.
JEP(S) works with SQL 2000 but there is limited support for it due to the old age of SQL 2000.

- Wizard setup for databases.
- Static whitelists for IP addresses, IP ranges, sender and recipient email addresses.
- Static blacklist for IP addresses, IP ranges, sender and recipient email addresses.
- Graphs. A standard set is included and you can write unlimited custom graph definitions to fit your needs.
- Tar pitting.
  To tarpit a mail session means that if a session is blocked that you will wait a certain amount of time before sending the reply to the sending mail server. This delays spammers in their work.
- Pass through for authenticated sessions.
- Logging to local log file.
  The logs are saved in a format compatible with several different statistical engines.
- Reply messages for greylist and RBL block are customizable.
- Optional encryption between all components.
- User interface available in English, German, French, Italian, Spanish, Portuguese, Russian, Swedish and Chinese.

In addition to these functions you have the possibility to install JEP(S)'s different main components on different servers. For example you can have two or more mail gateways running the JEP(S) Sink and let them work together against a central JEP(S) Server. This configuration even allows for installations over different time zones as all data saved by JEP(S) is in UTC time format.

JEP(S) can be installed and operate on a Microsoft Clusters to provide high availability.

The JEP(S) Listener utility allows you to see the live actions taken by the JEP(S) Server. This utility can be run locally on the JEP(S) Server or on a remote workstation. In addition to this you can add and remove white and blacklist entries based on the live traffic visible in JEP(S) Listener.

The theory of Greylisting

The basics of greylisting works by collecting what is called a triplet made out of the sending mail servers IP address, the senders email address and the recipient email address. An example triplet could look like this:

62.122.56.27,alice@companyxyz.com,bob@yourdomain.com
This information is saved in a database together with a time stamp of when this combination was first and last seen.

Before an email session is accepted the triplet is compared to what is saved in the database and depending on if it's a new entry or if this triplet has been seen before, it will be blocked or passed.

For example; the first time the above triplet is seen the session will be blocked as it has not been seen before.
If the mail is resent immediately (seconds after the first one), the triplet will be compared to what is in the database and then the server will see that it's only seconds old. This session will then also be blocked.
When the mail is transmitted next time (let's say 10 minutes after the initial session) then it will once more be compared to the database and now it will be passed.

A more in-depth article of how greylisting works in detail by Evan Harris can be found at www.greylisting.org/articles/whitepaper.shtml

Installation

JEP(S) installation takes place in two parts; first the executables are installed on the mail system and then JEP(S) is activated.

The installation of JEP(S)'s executables doesn't affect the mail system as such as it only requires the files to be extracted to a folder on the server. When JEP(S) admin is opened the necessary registry keys are created and set with their default values. This too doesn't affect the system.

Using JEP(S) Admin you can install the required service and enable the SMTP sink (IIS/Exchange 2000/2003) or agent (Exchange 2007/2010) – JEP(S) is now integrated with your email server, but is in a learning mode. In learning mode JEP(S) will intercept and process all mail sessions but will not block any messages.

This means that JEP(S) can in most cases be installed on production systems while still in use. After all settings has been configured and you're satisfied with its operations the JEP(S) can be enabled and it will then apply it's algorithms to block or pass mail sessions.

Downloading JEP(S)

Download the latest distribution from http://www.proxmea.com/download.

Selecting the distribution to download

JEP(S) Setup.exe	Contains both the 32-bit and the 64-bit installers and it will launch the appropriate once started. This is a setup guided installation.
JEP(S).zip	Contains both the 32-bit and the 64-bit executables for a manual

	install.
JEP(S) Setupx86.msi	The installer for 32-bit systems. This is a setup guided installation.
JEP(S) Setupx64.msi	The installer for 32-bit systems. This is a setup guided installation.

Setup guided installation procedure

Launch the setup program.

By selecting the top feature, JEP(S), you can change the installation directory by the browse button.

The different components available are:

JEP(S) Admin	Over all administration program for JEP(S) sinks and agents as well as for the JEP(S) Server. This should in most cases always be installed.
JEP(S) Server	The core of JEP(S) which does the analysis of mail sessions. This should be always be installed on single server setups.
JEP(S) Listener	The real-time monitoring utility which displays the actual mail flow on your system and the actions taken on each session.
JEP(S) Mail server components	This contains the necessary .dll's to integrate with your mail server. It should be installed on the server handling the incoming and outgoing traffic.
JEP(S) Documentation	Contains this administration manual and other JEP(S) documents.
SQL Server compact edition	The stand-alone version of Microsoft SQL Server compact edition v3.5. It installs into the same directory as JEP(S) to provide support for JEP(S) Admin and server. If you already have SQL Compact 3.5 installed on your system then you do not need to install it for the support to be provided. Note for 64 bit systems: If SQL Compact 32-bit has been installed but not the 64-bit package, then this needs to be installed together with JEP(S) even if not used as the SQL Compact is regarded as an incomplete installation.

When these components are installed the necessary start menu and desktop shortcuts will be provided if for the components that are user executable.

After this the installation is complete and you can go to the quick configuration or the main chapter Configuring JEP(S) to get started.

Manual installation procedure

Create a directory called JEP(S) in the location where you would like to install the software; for example c:\program files\JEP(S). Extract the downloaded files into this directory.

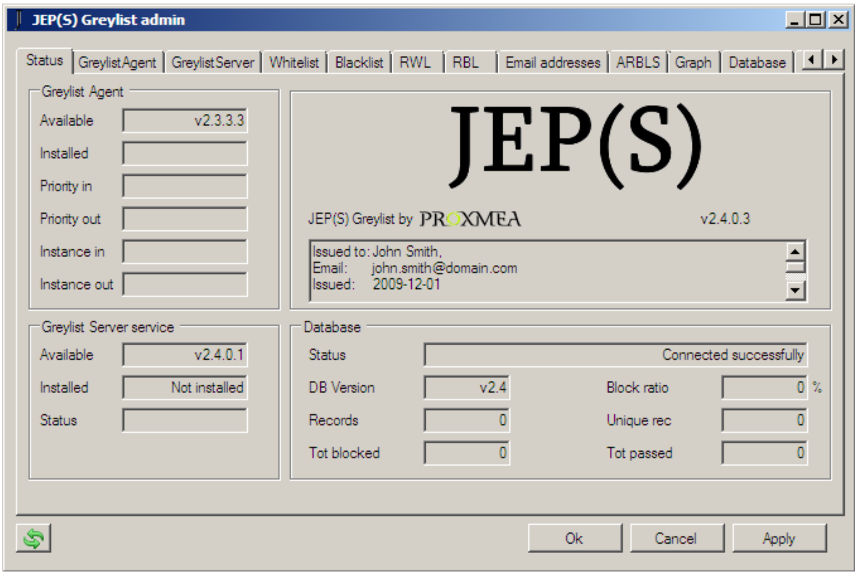
There will be no shortcuts created when installing JEP(S) manually and we recommend you to create shortcuts to the All users start menu for JEP(S) Admin and JEP(S) Listener. These shortcuts are not needed for normal operation but will help other administrators logging on to the server.

After this the installation is complete and you can go to the quick configuration or the main chapter Configuring JEP(S) to get started.

Quick configuration

Note: Depending on your mail server you will either see Greylist sink or Greylist agent in the administration program. These two are interchangeable but reflects the mail server type. IIS and Exchange 2000-2003 use sinks, while Exchange 2007-2010 use agents.

- If you have a trial or permanent license file for JEP(S) then extract this from the .zip archive and copy this to the JEP(S) install directory.
- Open JEP(S) Admin.
  If this is the first time JEP(S) is being launched on the system, then JEP(S) will attempt to create a local database. This can be confirmed by the Database status displaying 'Connected successfully'. This database can be changed if needed on the database tab or by the below procedure.



Greylist Agent
Available: v2.3.3.3
Installed:
Priority in:
Priority out:
Instance in:
Instance out:

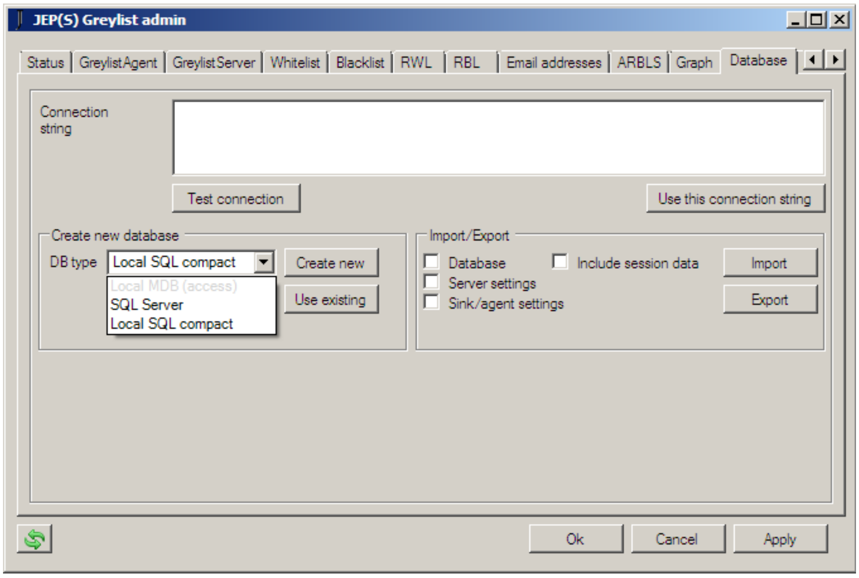
JEP(S) Greylist by PROXMEA v2.4.0.3
Issued to: John Smith,
Email: john.smith@domain.com
Issued: 2009-12-01

Greylist Server service
Available: v2.4.0.1
Installed: Not installed
Status:

Database
Status: Connected successfully
DB Version: v2.4
Block ratio: 0 %
Records: 0
Unique rec: 0
Tot blocked: 0
Tot passed: 0

Database setup

- ➢ If the database field displays 'Database connection not configured' then follow below database setup procedure.
- ➢ If the database field displays 'Connected successfully' then please jump ahead to Sink/Agent setup.
- Open the Database tab.
  To select the type of database click on the 'DB Type' dropdown box in the 'Create new database' field. It will display the unavailable choices in light grey as they're disabled.



Connection string:

Create new database

DB type: Local SQL compact

Local MDB (access)
SQL Server
Local SQL compact

Import/Export

☐ Database ☐ Include session data
☐ Server settings
☐ Sink/agent settings

Note that Local MDB (access) is not available on 64-bit systems.

Note that Local SQL compact is only available if this option has been installed.

Database recommendations

Local MDB	Suitable for single server installations with a low volume of mail sessions, typically less than 1000 per day.
SQL Server	Suitable for all installations. Always the preferred choice.
SQL Server compact	Suitable for medium size installations, typically up to 3-5000 mail sessions per day.

The above recommendations are guidelines only. They can vary depending on factors as mail sessions per day and how long data is kept.

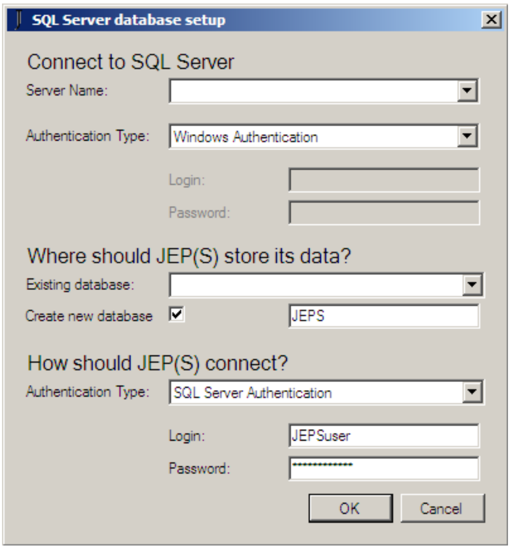
- Click ‘Create new’.

For local MDB and SQL compact the database is created automatically and you get the question if you’d like to use this database. Answer yes on this.

➢ After JEP(S) Admin is restarted please go to the Sink/Agent setup section if you’re using local MDB and SQL compact.

For SQL Server databases you will get a dialog to create the new database as below.

- SQL Server database setup dialog



Connect to SQL Server

Server Name:

Authentication Type: Windows Authentication

Login:

Password:

Where should JEP(S) store its data?

Existing database:

Create new database ☑ JEPS

How should JEP(S) connect?

Authentication Type: SQL Server Authentication

Login: JEPSuser

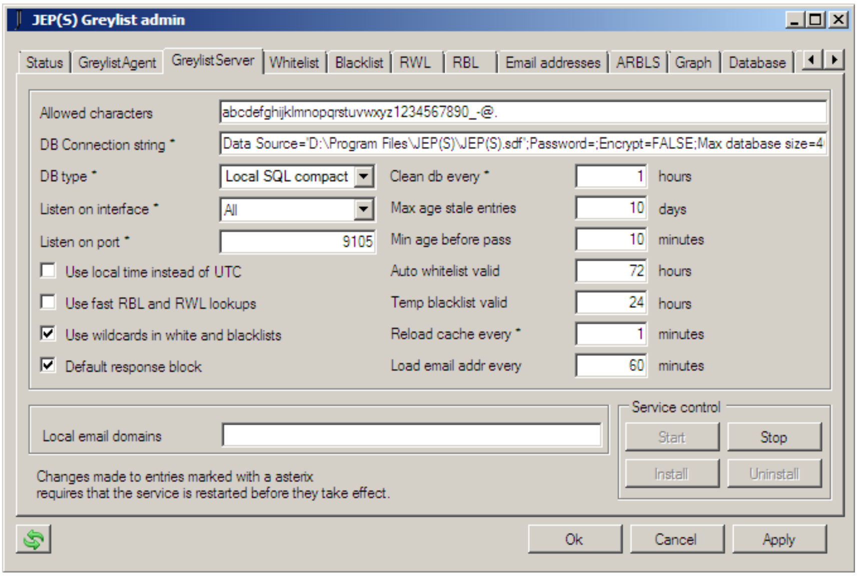
Password: ************

The top four fields are to provide the name and credentials to connect to the SQL server to create the database. The rest of the fields are what JEP(S) will create and later use when connecting to the SQL database.
The default login and password can be changed.
The auto generated password will be visible after creation in the connect string.

- Fill in the dialog appropriately and press OK. The database and user will now be created. If the user already exists then you will be asked if you want to reuse this username or not.

JEP(S) server setup

- Go to Greylist server and select Install and then start.
The JEP(S) server is now accepting traffic from the JEP(S) Sink / Agent.

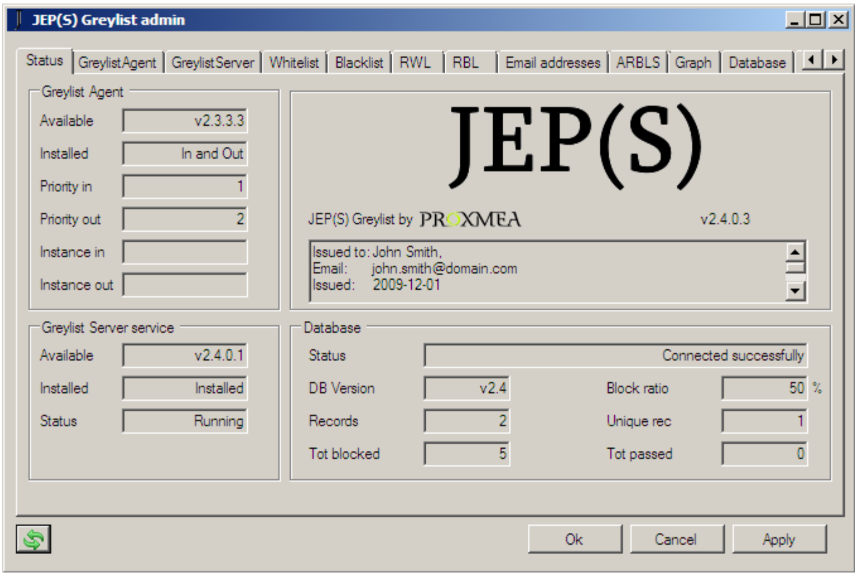


Allowed characters: abcdefghijklmnopqrstuvwxyz1234567890_-@.
DB Connection string *: Data Source='D:\Program Files\JEP(S)\JEP(S).sdf';Password=;Encrypt=FALSE;Max database size=4
DB type *: Local SQL compact
Listen on interface *: All
Listen on port *: 9105
□ Use local time instead of UTC
□ Use fast RBL and RWL lookups
☑ Use wildcards in white and blacklists
☑ Default response block
Clean db every *: 1 hours
Max age stale entries: 10 days
Min age before pass: 10 minutes
Auto whitelist valid: 72 hours
Temp blacklist valid: 24 hours
Reload cache every *: 1 minutes
Load email addr every: 60 minutes
Local email domains:

Changes made to entries marked with a asterix
requires that the service is restarted before they take effect.

Sink/Agent setup

- Go to the Greylist sink/Greylist Agent tab and select Enable in and Enable out.
The JEP(S) sink/agent is now active and will intercept incoming and outgoing SMTP sessions.
- Click Apply to save your settings.
- Send a test message from a known good mail server (external to yours) to test successful reception of the message.
- Go back to the Status page and confirm that you have at least 1 record according this screen.



Greylist Agent
Available: v2.3.3.3
Installed: In and Out
Priority in: 1
Priority out: 2
Instance in:
Instance out:

JEP(S) Greylist by PROXMEA v2.4.0.3

Issued to: John Smith,
Email: john.smith@domain.com
Issued: 2009-12-01

Greylist Server service
Available: v2.4.0.1
Installed: Installed
Status: Running

Database
Status: Connected successfully
DB Version: v2.4
Block ratio: 50 %
Records: 2
Unique rec: 1
Tot blocked: 5
Tot passed: 0

JEP(S) is now running in learning mode and won't actually block any traffic. To enable blocking go to Greylist sink/agent and select Mode – Enabled and press Apply.

Using the local database

The local databases are perfect for smaller installations and for evaluation purposes. This type of database is opened and managed directly by JEP(S) and this means that when using this on high load systems that it can affect the server's performance. For high load mail systems we recommend to use either a local SQL database or if possible an SQL server hosted on another server then the JEP(S) Server.

Note: If JEP(S) Server service is running and you then change database then you will need to restart this for the change to take effect.

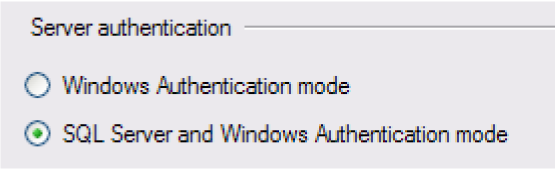
Automatic configuration of a SQL server database

By using a SQL server database you improve the speed of the transactions in two ways; the speed that a SQL server processes transactions is in itself a lot faster and you have the option to use a different server all together for the database and this offloads the server where JEP(S) is running.

We recommend the use of Microsoft SQL server 2005/2008 for JEP(S) which is available in several different versions, including SQL server express which can be downloaded for free from Microsoft.

The default way of configuring JEP(S) for SQL access is through SQL authentication. For this to be possible your SQL server needs to run in mixed mode configuration. You will need to check the windows authentication option if you are running your SQL server in windows authentication mode and then the JEP(S) server service under a manually created windows domain account.

If you have access to the SQL Management Studio you can confirm mixed mode authentication by accessing the properties of the server and checking the Security page.

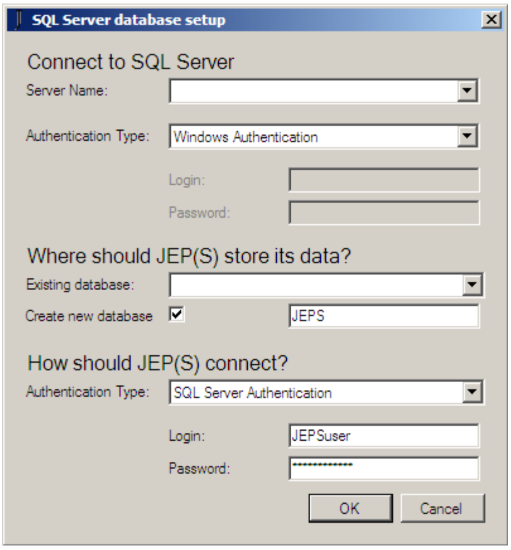


Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

You can read more about SQL authentication in the appendix.



SQL Server database setup

Connect to SQL Server

Server Name:

Authentication Type: Windows Authentication

Login:

Password:

Where should JEP(S) store its data?

Existing database:

Create new database ☑ JEPS

How should JEP(S) connect?

Authentication Type: SQL Server Authentication

Login: JEPSuser

Password: ************

To configure the JEP(S) database in this way requires that the logged on user has administrator privileges on the SQL server. If the logged on user doesn't have administrative privileges on the SQL server then you have three choices: (1)install the database manually as described below, (2) copy JEP(S) Admin to the SQL server, log on as a local administrator and then execute the Create database function from JEP(S), or (3) use SQL authentication for the creation of the database.
If you run JEP(S) Admin on the SQL server then you will need to copy the produced connection string from the SQL server to the server where JEP(S) Server is installed.

To configure the JEP(S) SQL database automatically follow these steps:

1. Tell JEP(S) Admin what SQL server to use and how to connect.
   This is done in the 'Connect to SQL Server' part of the wizard.
2. Define what database JEP(S) should store its data.
   This is defined in the 'Where should JEP(S) store its data' section.
3. Define how JEP(S) should connect to the database.
   This is done in the 'How should JEP(S) connect' section.

1. You can either type in the SQL Server name manually or use the browse functionality available in the dropdown box of server name. Please note that if your installation uses static ports then you will still need to specify the port number as below.

   To fill in the SQL server name. If you're running SQL as an instance then append \Instancename after the server name.

Ex: 10.31.0.123	Connect to SQL by IP
Ex: 10.31.0.123\MyInstance	Connect to SQL by IP and instance name

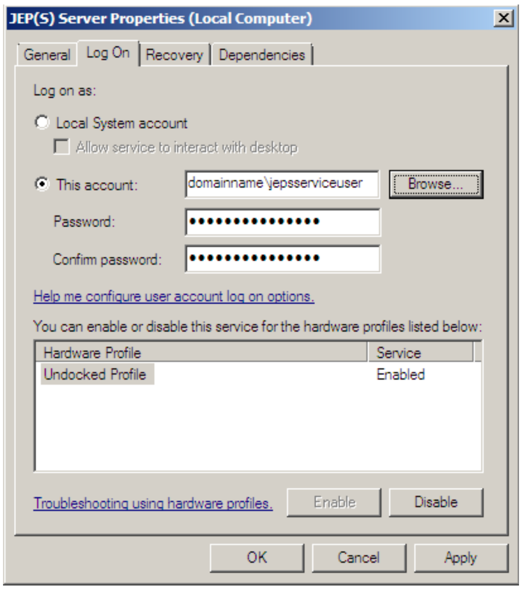
Ex: 10.31.0.123\MyInstance,1433	Connect to SQL by IP, instance name on specific port
Ex: servername.domain.com	Connect to SQL by the fully qualified name

If the user you are currently logged on as doesn't have SQL administrative privileges then you can specify to connect to the SQL server by SQL authentication instead. These credentials are only used for the duration of the wizard and are not later used by JEP(S).

2. By clicking on the 'Existing database' dropdown box JEP(S) will attempt to connect to the database server specified in the above section with the specified credentials.
   If successful then it will display a list of existing databases. If there's an issue with the connection, e.g. wrong server name or wrong instance name, then it can take some time before you get a blank result.
   A blank result means that the connection wasn't successful and that no databases were found.
   By selecting a database from this list you will use this for JEP(S).

   If you want to create a new database then check the checkbox 'Create new database' and fill in the desired name. This is by default JEPS and can be changed.
3. By default JEP(S) will connect to the SQL server with SQL authentication. The default username and password can be changed if desired. The auto generated password is 12 characters long and is based on random upper and lower case together with numbers.

   If you specify 'Windows authentication' then JEP(S) will connect in the context of the user. This means that JEP(S) Admin will connect as the currently logged on user, while JEP(S) Server by default will connect as 'Local system'. This means that you need to use the windows services mmc to open the properties for the JEP(S) Server service and specify a user which holds the necessary login rights on the local server as well as on the SQL Server. More about this is discussed in the appendix 'Running the JEP(S) Server service under AD user account'.



JEP(S) Server Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: domainname\jepsserviceuser

Password: •••••••••••••••

Confirm password: •••••••••••••••

Help me configure user account log on options.

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Undocked Profile	Enabled

Troubleshooting using hardware profiles.

By pressing OK the database will be created (if needed), the user created (if not already exists) and the database will be populated with the default tables.

After this JEP(S) will attempt to connect to the database and if successful you'll get a question if you want to use the newly created database. If you select yes then the settings will be saved and the application is restarted. If you select no, then you're returned to JEP(S) Admin together with the connection string for the newly created database.

Note: If you have already started the JEP(S) Server service then you will need to restart this for the change to take effect.

Manual configuration of a SQL server database

If you're comfortable with SQL databases then you can setup a database manually and give either a local SQL user or windows account permissions to it.

A sample SQL script to create the database is available for download at www.Proxmea.com/Download.

When the database is created you will need to manually fill in the connection string to fit to your SQL server.

For SQL user authentication use the following format:
PROVIDER=SQLOLEDB;DATA SOURCE=sqlservername;Initial Catalog=jepsdatabasename;User ID=myusername;Password=mypassword

For windows authentication use the following format:
PROVIDER=SQLOLEDB;DATA SOURCE=sqlservername;Initial Catalog=jepsdatabasename;Integrated Security=SSPI

When the connection string is filled in you can test the connection and the select Use this connection string.

Configuring JEP(S)

JEP(S) is designed to give the mail administrators full control over all parameters that JEP(S) is using. This means that there are many parameters that can be changed but it should be noted that the default parameters are in most cases the best choice, so only change these if you know the effect they will have on the operation.

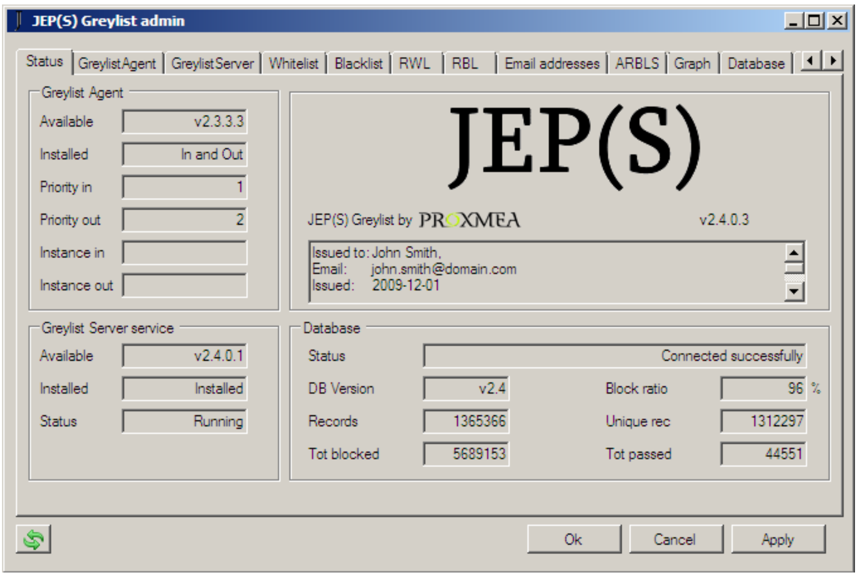
The user interface of JEP(S) Admin

The interface is divided into several tabs grouped into the function they control.

Changing most options have an immediate effect after pressing Apply, but some options need the JEP(S) Server service to be restarted. These options are marked with an asterisk (*).

OK By pressing OK you will save any changes and exit JEP(S) Admin.
Cancel By pressing Cancel you will not save any changes and exit JEP(S) Admin.
Apply By pressing Apply you will save any changes and stay in JEP(S) Admin.
Refresh By pressing refresh you will reload statistics and all lists.
(two green arrows)

Status



Greylist Agent
Available v2.3.3.3
Installed In and Out
Priority in 1
Priority out 2
Instance in
Instance out

JEP(S) Greylist by PROXMEA v2.4.0.3

Issued to: John Smith,
Email: john.smith@domain.com
Issued: 2009-12-01

Greylist Server service
Available v2.4.0.1
Installed Installed
Status Running

Database
Status Connected successfully
DB Version v2.4 Block ratio 96 %
Records 1365366 Unique rec 1312297
Tot blocked 5689153 Tot passed 44551

Main window

The main window describes what version of JEP(S) admin you are currently running. The above screenshot shows version 2.4.0.3.
It also shows the license information (if available) and to who the license is registered. This information is only for informational purposes and is not communicated anywhere at any time.

Greylist Sink / Greylist Agent

Available	Describes if the JEP(S) sink.dll is present and what version it is.
Installed	What sinks are installed.
Priority in	What priority the inbound sink has.
Priority out	What priority the outbound sink has.
Instance in	Describes on which instance the inbound sink is running on.

Instance out	Describes on which instance the outbound sink is running on.

Greylist Server service

Available	Describes if the JEP(S) server service.exe is present and what version it is.
Installed	Describes if the service is installed or not.
Status	The current status of the service.

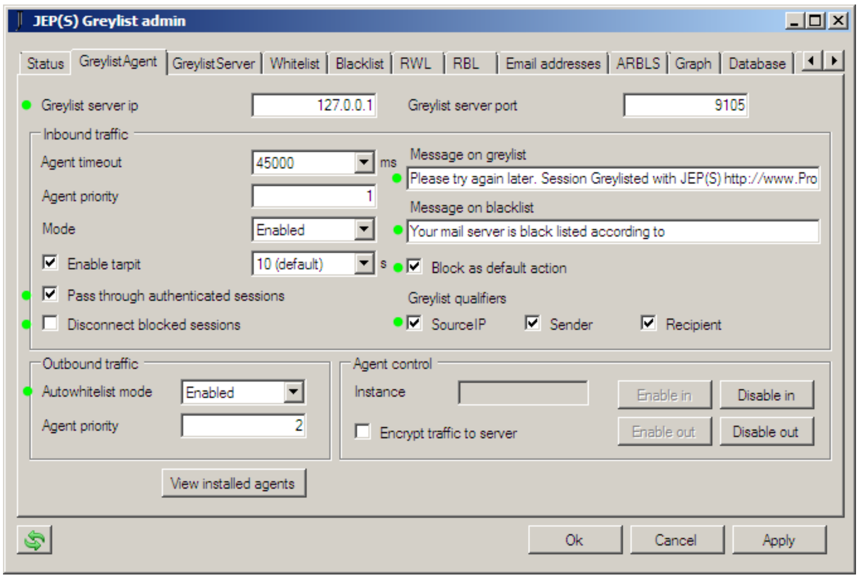
Database

Status	Describes if JEP(S) could connect to the database successfully.
DB Version	The version of the JEP(S) database.
Records	The total amount of triplet records in the database.
Tot blocked	The total amount of blocked items since the database was installed.
Block ration	The ratio between blocked and passed items in the database. This gives a good indication of the efficiency of JEP(S).
Unique rec	Total amount of unique records in the database. These are the triplets combinations that have only been seen once.
Tot passed	The total amount of items that has been allowed to pass through since the database was installed.

Greylist Sink / Greylist Agent

Items marked with a green dot are not available or can't be changed in the free version.

Depending on what mail system you're running on you will be presented with the term 'Sink' for IIS and Exchange 2000/2003 or 'Agent' for Exchange 2007. The functionality of the sink and agent are very similar and therefore when its discussed about the sink this also applies to the agent.



● Greylist server ip: 127.0.0.1
Greylist server port: 9105
Agent timeout: 45000 ms
Agent priority: 1
Mode: Enabled
☑ Enable tarpit: 10 (default) s
● ☑ Pass through authenticated sessions
● □ Disconnect blocked sessions
Message on greylist: ● Please try again later. Session Greylisted with JEP(S) http://www.Pro
Message on blacklist: ● Your mail server is black listed according to
● ☑ Block as default action
Greylist qualifiers: ● ☑ SourceIP ☑ Sender ☑ Recipient
● Autowhitelist mode: Enabled
Agent priority: 2
Instance:
□ Encrypt traffic to server

The View installed sinks button will produce a report of all SMTP event sinks or transport agents currently installed to this server. This information can be invaluable when troubleshooting SMTP server operation.

Inbound traffic

Greylist server ip	This value can only be changed in the licensed version. This value instructs the sink where the JEP(S) Server is available. In a normal installation this should be 127.0.0.1 as the service is installed on the same machine. If the service is installed on a separate server then fill in that server IP number here.
Greylist server port	The default port for communication between the sink and the service is 9105, but this can be changed here. If you change it here then don't forget to also change it on the GreylistServer tab. Communication is taking place over TCP towards the server service and UDP towards the JEP(S) Listener.
Sink timeout	This value instructs the sink how long time it will wait for a response from the JEP(S) Server service. If the timeout value is hit then the current session will not be blocked but automatically passed. The reason for this is to ensure continued operation of the SMTP service in the case of interruption between the sink and server. The default value 5000ms.
Sink priority	This is the priority that this sink has and describes when in the receiving process that the inbound sink will be invoked. A lower value

	means earlier in the process, which is recommended. This value can be changed to ensure interoperability with other mail software or other products like antivirus scanners. Default value is 100.
Mode	Disabled means that the sink is active but no processing will be made and all sessions will be left untouched. Enabled means that all sessions will pass through the JEP(S) server algorithms to qualify for a pass or block. This is the normal operational mode of JEP(S). Learning means that all sessions will be passed but the data will be passed on to the JEP(S) server and all algorithms will be executed for the session. This is the default install mode.
Enable tarpit	Enabling the tarpit means that if a session is blocked then it will wait for the specified number of seconds before returning the message to the sending mail server. Even though this has little impact on normal mail traffic it is very interrupting for spammers. Default is unchecked.
Pass through authenticated sessions	This function is only available in the licensed version. If enabled then the sink with check if the mail session is authenticated and if this is the case then it will pass through without passing through the filter. This is useful if you use SMTP for sending email from external IP's and external workstations. Default is unchecked.
Disconnect blocked sessions	If enabled then the session will be dropped instantly if blocked. This works very well on high volume mail systems, but doesn't work together with receiving larger mailing lists. Use with caution. Default is unchecked.
Message on greylist	This value can only be changed in the licensed version. This is the message that will be sent back to the sending mail server on a block. The message is prefixed with '4.5.1' which means temporary error. If the sending mail system doesn't resend the mail then this message will be returned to the sender.
Message on blacklist	This value can only be changed in the licensed version. This is the message that will be sent back to the sending mail server if the sending mail server was found on a black list. The message is prefixed with '5.5.0'
Block as default action	When enabled then JEP(S) will always default to sending a block action if the JEP(S) Server is unavailable. This is useful to ensure that no spam gets through while the JEP(S) Server is being rebooted.
Greylist qualifiers	These values can only be changed in the licensed version. The three checkboxes describes what qualifiers should be considered when a session is passing through the greylist filter. In normal operation all check boxes should be checked, but you have the option to 'loosen' the filter by for example un-checking recipient. If this is done then only source IP and sender email address will be used for greylisting.

Outbound traffic

Autowhitelist mode	This function is only available in the licensed version.

	If this is enabled then emails that are outbound (sent) will be saved in the whitelist database as a whitelisted sender for a number of hours. The amount of hours can be adjusted on the GreylistServer tab under Auto whitelist valid. If it is disabled then no automatic whitelisting will be done.
Sink priority	This is the priority that this sink has and describes when in the sending process that the outbound sink will be invoked. A higher value means later in the process, which is recommended. Default value is 24575.

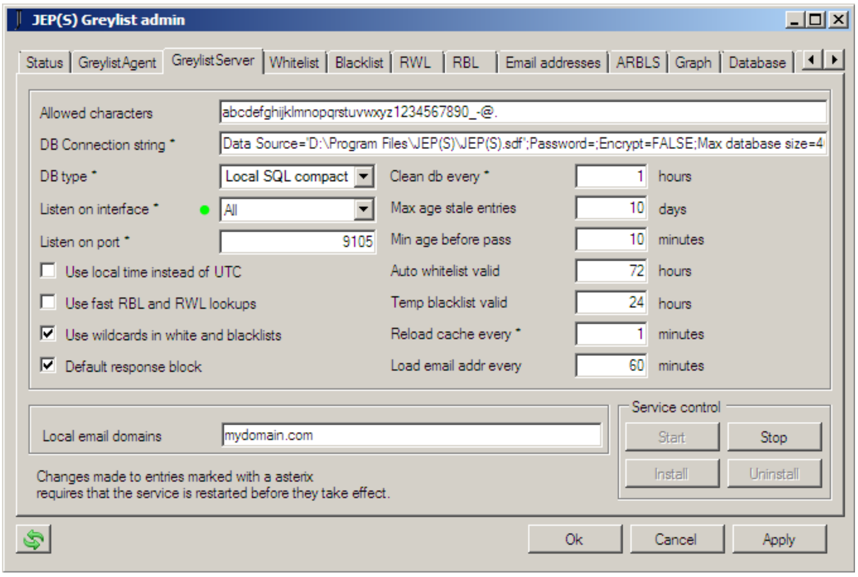
Sink / Agent control

Instance	This is the instance affected by the enable and disable commands. Not enabled when using together with Exchange 2007/2010.
Encrypt traffic to server	Causes the sink to encrypt all communication with the JEP(S) Service.
Enable in	Installs the inbound sink (receiving email). This change is instant.
Enable out	Installs the outbound sink (sending email). This change is instant.
Disable in	Will uninstall the inbound sink. Even though the sink is instantly deactivated, the dll will only be unloaded after an restart of the IIS service.
Disable out	Will uninstall the outbound sink. Even though the sink is instantly deactivated, the dll will only be unloaded after an restart of the IIS service.

Greylist Server

Items marked with a green dot are not available or can’t be changed in the free version.

Items marked with an asterisk (*) requires the JEP(S) Server service to be restarted for the changes to take effect.



Allowed characters: abcdefghijklmnopqrstuvwxyz1234567890_-@.

DB Connection string *: Data Source='D:\Program Files\JEP(S)\JEP(S).sdf';Password=;Encrypt=FALSE;Max database size=4

DB type *: Local SQL compact

Listen on interface * ●: All

Listen on port *: 9105

☐ Use local time instead of UTC

☐ Use fast RBL and RWL lookups

☑ Use wildcards in white and blacklists

☑ Default response block

Clean db every *: 1 hours

Max age stale entries: 10 days

Min age before pass: 10 minutes

Auto whitelist valid: 72 hours

Temp blacklist valid: 24 hours

Reload cache every *: 1 minutes

Load email addr every: 60 minutes

Local email domains: mydomain.com

Changes made to entries marked with a asterix
requires that the service is restarted before they take effect.

Allowed characters	This field contains all characters that are allowed in JEP(S). If an email address for example contains the character ! then it will be removed before being saved in the JEP(S) database. This is to protect JEP(S) against injection attacks. This does not affect the rest of the mail system, but is only used within JEP(S). You can add or remove characters here, even though the default set is sufficient for all languages.
DB Connection string	This is the connection string that is used for the server to connect to the database. It can be edited here, but it’s better to do this on the database tab where you can also test the connection before applying it.
DB type	This tells the server what kind of database type to expect. It’s set automatically when setting the database on the database tab.
Listen on interface	This value can only be changed in the licensed version. In an installation where all JEP(S) components are installed on the same server this should be set to Localhost. By changing this to All you will allow the server to communicate with any other IP. Note that if you do this then you should protect communications to and from the JEP(S) Server with an appropriate firewall.
Listen on port	This value sets the port that the JEP(S) server listens for incoming connections. This value should be the same as on the GreylistSink tab.
Use local time instead of UTC	Instructs JEP(S) to use the local timestamps for the database.
Use fast RBL and RWL lookups	When selected then JEP(S) will use the windows DNS function for lookups. It is faster than JEP(S) internal lookup routine, but much less

	accurate. Should only be used on systems with more then 2-3 sessions per second.
Use wildcards in white and blacklists	When selected this allows you to specify wildcards as * (asterisk) before mail addresses and mail domains. By unchecking this it will use addresses with the 'like' method where mail@domain.com matches someemail@domain.com. Default is checked.
Default response block	When enabled then JEP(S) will always default to sending a block action if the database is unavailable. This is useful to ensure that no spam gets through while certain servers are being rebooted.
Clean db every	This defines how often database maintenance should be performed. This value should be set relatively low and never more than 24 hours. Default value is 1 hour.
Max age stale entries	When an entry, or rather triplet, hasn't been updated for x days then it will be removed. Setting this value to low (<7 days) will cause normal email to have to be resent more often than necessary. Setting this value to high (>90) can cause the database to be unnecessary big, but doesn't have a negative impact on the algorithms.
Min age before pass	This defines how old an entry must be before it is accepted. Setting this value to 0 will cause email to only have to be resent only once. Setting this value to anything higher than 0 will enable the time limit. Setting this value to high (>60 min) can cause emails not to be received, depending on the sending mail servers settings. The default value is 2 minutes.
Reload cache every	This defines how often the whitelist, RBL and RWL should be checked for updates. Setting this to high (>5) can cause whitelist entries to come in effect to late. Default value is 1 minute.
Auto whitelist valid	When the Autowhitelist is enabled, then this entry specifies how long it should stay in the whitelist. After this time the entry will be removed from the whitelist automatically during the database maintenance.
Temp blacklist valid	This specifies how long entries added with the JEP(S) Listeners 'Add server to temp blacklist' will be valid. After this time the entry will be removed from the blacklist automatically during the database maintenance.
Load email addr	If internal email address sources are specified on the email address tab, then this value defines how often the email address lists will be loaded into memory. Default value is 60 minutes.

Local email domains

	Local email domains is a comma separated list of domain names, like domain.com,otherdomain.com, which lets JEP(S) know what email addresses to treat as internal. Internal email domains will always be excluded from auto whitelisting.

Service control

Start	Starts the server service.
Stop	Stops the server service. It’s preferred to use this instead of the Windows services control, as it checks for a proper shutdown.
Install	Installs the server service.
Uninstall	Removes the server service.

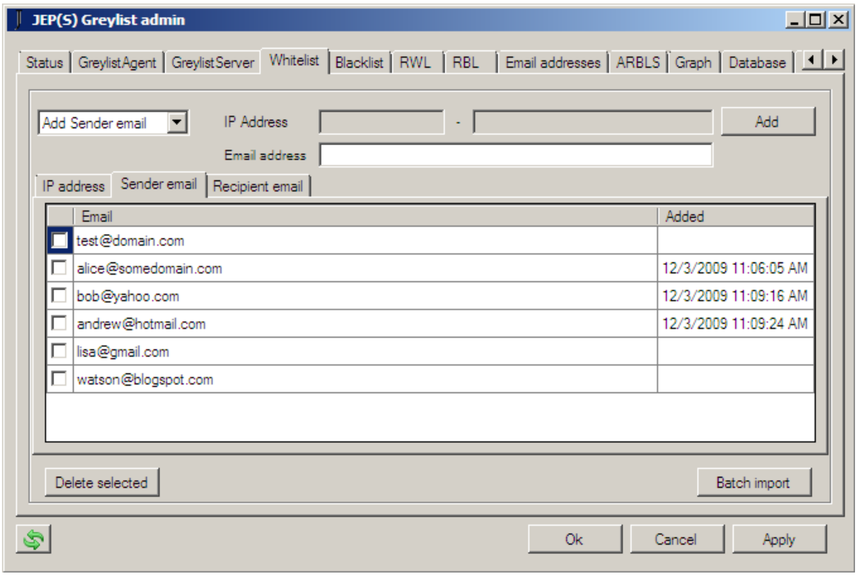
Whitelist

The Whitelist tab allows you add and remove the following types of entries:

- IP Addresses and IP ranges.
- Sender email addresses.
- Recipient email addresses.

On the sender tab you can see dates next to certain entries and these what have been added by the auto whitelist. The date and time stamp is in UTC time and states when the entry was added or last updated. The other tabs do not contain this column.

The reason for UTC time stamps to be used is to enable JEP(S) to work in large organizations where several installations are working over different time zones.



Add Sender email

	Email	Added
☐	test@domain.com	
☐	alice@somedomain.com	12/3/2009 11:06:05 AM
☐	bob@yahoo.com	12/3/2009 11:09:16 AM
☐	andrew@hotmail.com	12/3/2009 11:09:24 AM
☐	lisa@gmail.com	
☐	watson@blogspot.com	

Changes to the whitelist are instantly added or removed from the database but only loaded into the server on the next cache reload.

To add whitelist entries follow these steps:

- IP addresses.
  Select Add IP address from the drop down list, fill in the IP and press Add.
- IP Ranges.
  Select Add IP range from the drop down list, fill in the two IP numbers and press Add.
  You can add IP ranges that are across subnets, e.g. 192.168.0.250 – 192.168.22.100, as long as the latter IP address is greater than the first one.
- Sender email address.
  Select Add Sender email from the drop down list, fill in the email address and press Add.
  This causes all email from this email address to be whitelisted and hence pass through the filter.
- Recipient email address.
  Select Add Recipient email from the drop down list, fill in the email address and press Add.
  This causes all email to this email address to be whitelisted and hence pass though the filter.

When an entry is added it is passed through the allowed characters filter to match how JEP(S) looks at the entries. If you add an email address with a character that doesn't exist in this character filter then it will appear without those characters. This is normal and can be ignored.

To delete a whitelist entry simply check the checkbox next to the entry and press Delete selected.

Note: When adding JEP(S) to a network that has network scanners or other devices that use SMTP on the server to send email, it is best to immediately add the local subnet to the whitelist. This prevents those devices from failing to send.

Commonly devices that have a "Scan to email" feature will not retry and must therefore be whitelisted for correct operation.

Blacklist

The Blacklist tab allows you add and remove the following types of entries:

- IP Addresses and IP ranges.
- Sender email addresses.
- Recipient email addresses.

The blacklist functions in JEP(S) Admin works the same way as the whitelist. Once difference is the added field which is not available under the sender section but under the IP address section. The functional difference on the blacklist IP address is that an entry can be added temporary with the JEP(S) listener and this entry will later be removed once the entry is older than the value defined on the Greylist server tab.

Wildcards

JEP(S) does by default support wildcards by the * asterisk character. To ensure correct operation the 'Use wildcards in white and blacklists' on the server tab should be checked.

Simply enter an asterisk plus for example the domain name, for example *@domain.com or *support@domain.com.

Legacy support

Version prior to 2.3 did not support wildcards as described below. By unchecking 'Use wildcards in white and blacklists' on the server you enable the previous behavior.

The following behavior is here for legacy reference.

To make use of wildcards in email addresses that are in the whitelist you need to enter the partial rightmost part of the email address instead of the full one.

For example if you would like to whitelist a sender domain then you enter the at sign plus the domain name like *@domain.com* and add this to the sender whitelist. Now all mail from domain.com will be whitelisted.
If you would like to whitelist a partial recipient email address for like sales.info@domain.com or promotion.info@domain.com then you enter *info@domain.com* and add this to the recipient whitelist.

Do not use asterisk * as wildcard.

Batch import

The batch import function allows you to import CSV separated or line separated text files into the three different whitelists.

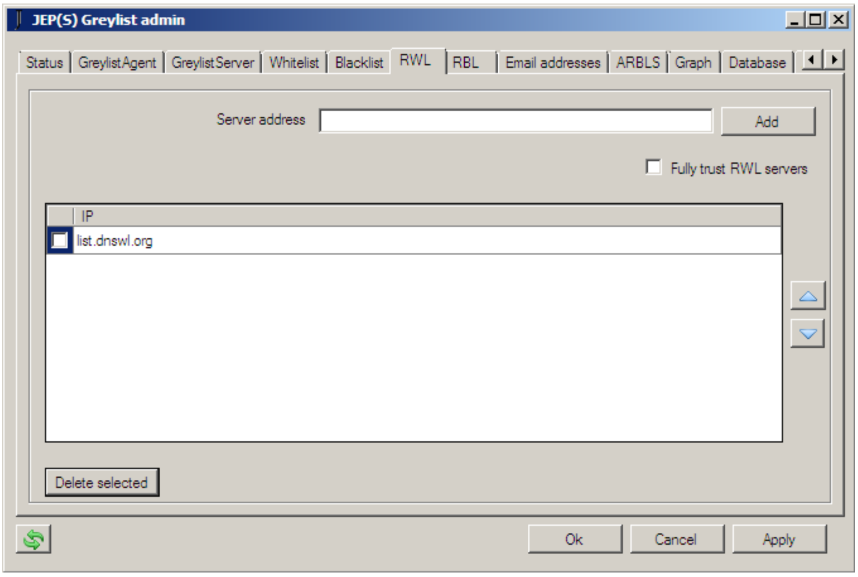
RWL – Real time Whitelist

The RWL is only available in the licensed version of JEP(S).

A RWL is an external (or internal) server which keeps track of known good servers. These lists contains references to servers of the like of hotmail.com, google.com, gmail.com, ibm.com and other major companies which have proven to not send spam.

JEP(S) utilizes RWL's in a mean of deciding if the source IP address should be considered or not. It's common that if a company like hotmail.com sends an email and on the first try it it's blocked, that it then will try to resend from another mail gateway. This causes a new triplet to be generated and JEP(S) sees this as a completely new session.

By excluding the source IP from these servers the triplet becomes a duplet only containing sender and recipient email addresses. When this is done then the email can be resent from a new mail gateway without any problems.



Server address

□ Fully trust RWL servers

	IP
□	list.dnswl.org

To add a new RWL simply enter the name of the RWL into the server address field and press Add.

We have tested the RWL list.dnswl.org extensively and recommend this one. It should be noted that it's completely outside our control and that we can't guarantee the results coming from this RWL, even though we're satisfied with its results. More information can be retrieved from http://www.dnswl.org/
This RWL is provided free of charge by the provider.
Please note that they do only allow 100.000 RWL queries per day and IP. If you require more queries per day then you can find instructions on their website on how to resolve this.

The option of Fully trust RWL server causes any session that has a sending mail server that is on a RWL to be passed as whitelisted.

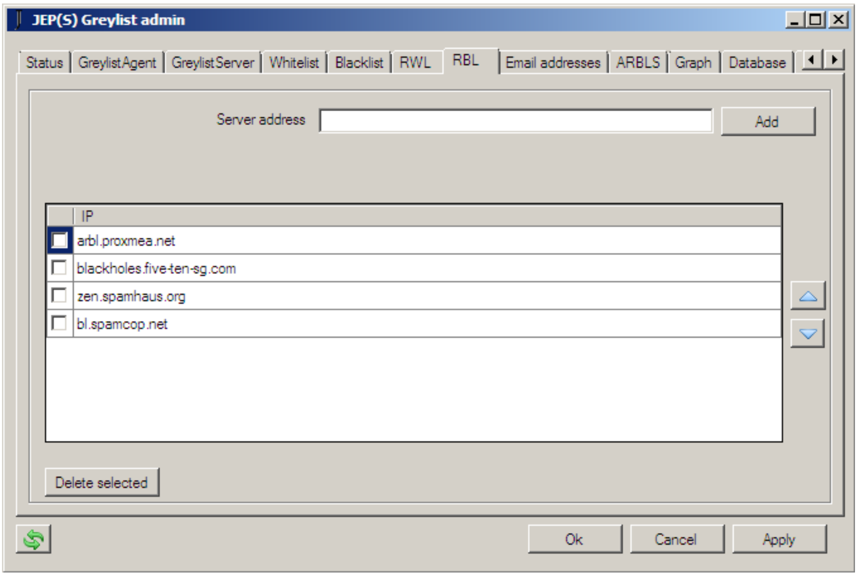
To delete a RWL entry mark the checkbox and press Delete selected.

RBL – Real time Blacklist

The RBL is only available in the licensed version of JEP(S).

A RBL is an external (or internal) server which keeps track of known bad servers. These lists contain references to servers which are known to send spam or other uncontrolled content.

JEP(S) utilizes RBL's as implicit sources. If a sending mail servers IP address is found on a RBL it will be blocked until the entry is removed from the list.



	IP
□	arbl.proxmea.net
□	blackholes.five-ten-sg.com
□	zen.spamhaus.org
□	bl.spamcop.net

To add an RBL simply enter the name of the RBL into server address and press Add.

We have tested the RBL's from Spamcop and Spamhaus extensively and recommend these. It should be noted that these are completely outside our control and that we can't guarantee the results coming from these RBL's, even though we're satisfied with its results. More information can be retrieved from http://www.spamcop.net/ and http://www.spamhaus.org/.

Blackholes.five-ten-sg.com is a more aggressive blacklist which has also been successfully tested. Please monitor the performance of this blacklist when you initially start using it as it's more aggressive in its classification of spammers.

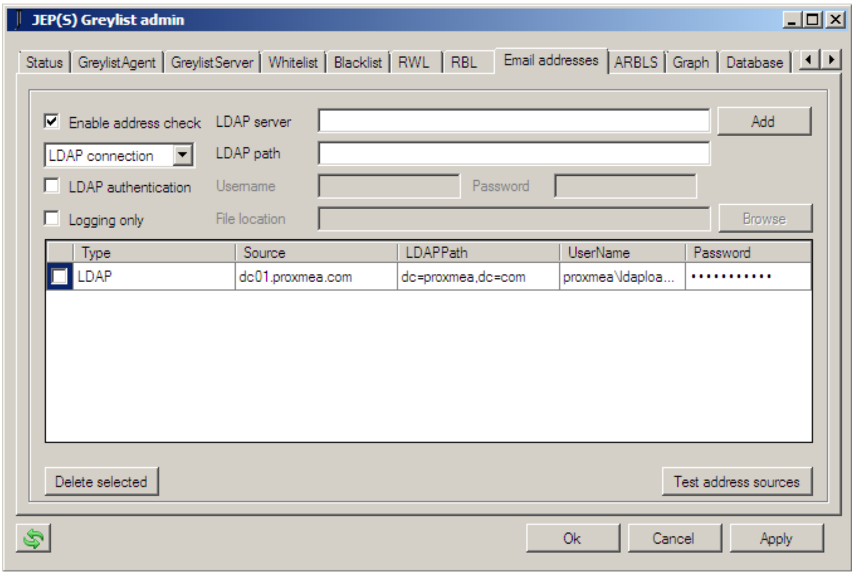
Arbl.proxmea.net is the blacklist constructed from ARBLS (page 29) data submitted from JEP(S). This blacklist identifies spammers in the early stages of spamming, typically between 15 minutes and 24 hours of the start of spamming from one IP.

These RBL's are provided free of charge by the provider.

To delete a RBL entry mark the checkbox and press Delete selected.

Email addresses

The email addresses feature is only available in the licensed version of JEP(S).



☑ Enable address check

LDAP connection

☐ LDAP authentication

☐ Logging only

	Type	Source	LDAPPath	UserName	Password
☐	LDAP	dc01.proxmea.com	dc=proxmea,dc=com	proxmea\ldaploa...	•••••••••••

Enable address check	Enables the filter.
LDAP connection	Selects what type of source to add, LDAP or file.
LDAP authentication	If your LDAP server requires authentication for the query to succeed then check this box. This will enable the username and password fields.
Logging only	Enables the filter to be active but not executed against mail sessions.
LDAP server	Describes the IP, NetBIOS name or FQN / DNS name of the LDAP server.
LDAP path	The search root where the query will start searching for email addresses in the LDAP directory.
Username	The username which will be used for authentication against the LDAP directory.
Password	The password which will be used for authentication against the LDAP directory.
File location	The full path to the file containing the email address list. This can be typed or selected with the Browse button (recommended).
Add	Will add the current configured entry to the database for loading.
Delete selected	Will delete any entries marked with the checkbox.
Test address sources	By selecting this a connection will be made with the JEP(S) server service and a query will be sent for it to load the addresses from the sources. It will then respond with the number of email addresses found or a failure.

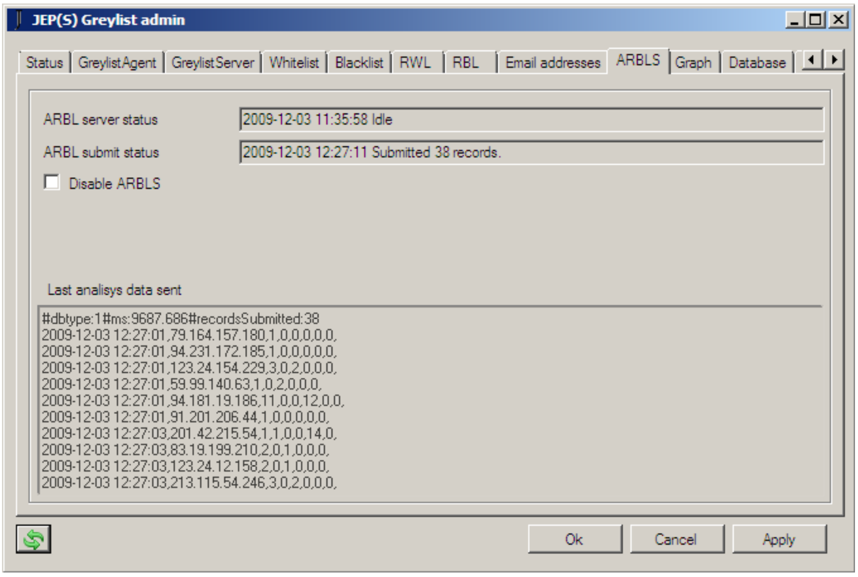
By enabling the address check you move the perimeter one level closer to the session. Without this a session with an invalid recipient will be able to reach your mail server where it would be denied. Two other benefits with letting JEP(S) controlling valid and invalid recipient are that this information will be included in the ARBLS analytical engine and also be used to build graphs that reflect this.

There are two ways to add lists of email addresses. You can do it by an LDAP connection, usually against one or more Windows domain controllers, or by loading the addresses from a CSV file or a line separated file.

If the filter is enabled but one or more sources fail to load then an event log message will be logged and the filter will not be used until it has successfully loaded again. This is to prevent that JEP(S) will block valid recipients which have email addresses which have not been loaded.

It's recommended that while you set this feature up that you check the box 'Logging only'. This will allow for the filter to be enabled but not executed. Once you're happy with the configuration just uncheck the box and select Apply.

ARBLS



ARBL server status: 2009-12-03 11:35:58 Idle

ARBL submit status: 2009-12-03 12:27:11 Submitted 38 records.

□ Disable ARBLS

Last analisys data sent

```
#dbtype:1#ms:9687.686#recordsSubmitted:38
2009-12-03 12:27:01,79.164.157.180,1,0,0,0,0,0,
2009-12-03 12:27:01,94.231.172.185,1,0,0,0,0,0,
2009-12-03 12:27:01,123.24.154.229,3,0,2,0,0,0,
2009-12-03 12:27:01,59.99.140.63,1,0,2,0,0,0,
2009-12-03 12:27:01,94.181.19.186,11,0,0,12,0,0,
2009-12-03 12:27:01,91.201.206.44,1,0,0,0,0,0,
2009-12-03 12:27:03,201.42.215.54,1,1,0,0,14,0,
2009-12-03 12:27:03,83.19.199.210,2,0,1,0,0,0,
2009-12-03 12:27:03,123.24.12.158,2,0,1,0,0,0,
2009-12-03 12:27:03,213.115.54.246,3,0,2,0,0,0,
```

Automatic Real time Black List Submission is a new technique which builds on multiple JEP(S) servers observations of sender mail server's behavior patterns.

ARBL server status	Displays the current status of the internal ARBLS server.
ARBL submit status	Displays information about the last submit.
Disable ARBLS	When checked the ARBLS server will be deactivated. Before disabling it please remember that this will have a negative impact on the efficiency of the RBL made out of these submits. You can only disable it in the licensed version.
Last analysis data	Displays the first 10 lines of the last submit in the format: Date Time, Reported IP, Count of rule1, Count of rule2, etc.

When JEP(S) observes a suspicious behavior it will count how often a particular sending mail server has done this and adds this to an internal list. This list is sent to a central server by a regular HTTP post request every 10 minutes.
These lists from different installations are then compiled and when a certain percentile of reporting servers have been reported the same sending server to behave according to the same patterns then this source IP will be considered for black listing.

This blacklist can then be queried by JEP(S) to identify spammers in the early stage of their spamming attempt.

With this technique we can identify spammers within 15 minutes of their start of activity. It's simply put a joint effort between all JEP(S) servers to identify the spammers and then use this information against them.

For example if 20% of the reporting servers in USA reports 193.13.13.222 to attempt to send email to non-existent email addresses then no action will be taken.
But when an additional 10% of reporting servers in Europe joins up reporting the same suspicious activity then the cumulative effort will black list 193.13.13.222 for a shorter period of time depending on the severity.
When more static blacklists like bl.spamcop.net have caught up with this server then this entry will be removed from the ARBL blacklist.

Usage of the resulting BL

To make use of the ARBL consolidated data add an entry to your RBL for *arbl.proxmea.net.*

Privacy

From the privacy perspective there's been great efforts in protecting your privacy and private internal information. The data submitted will never contain your internal IP's or information about your system or environment.
There is one small exception to this rule and that is that the type of database your using is inside the request to inform the central server of what intelligence to expect in the report. This is only reported as a 0 (for local database) or as a 1 (for SQL database) or as a 2 (for SQL Compact).

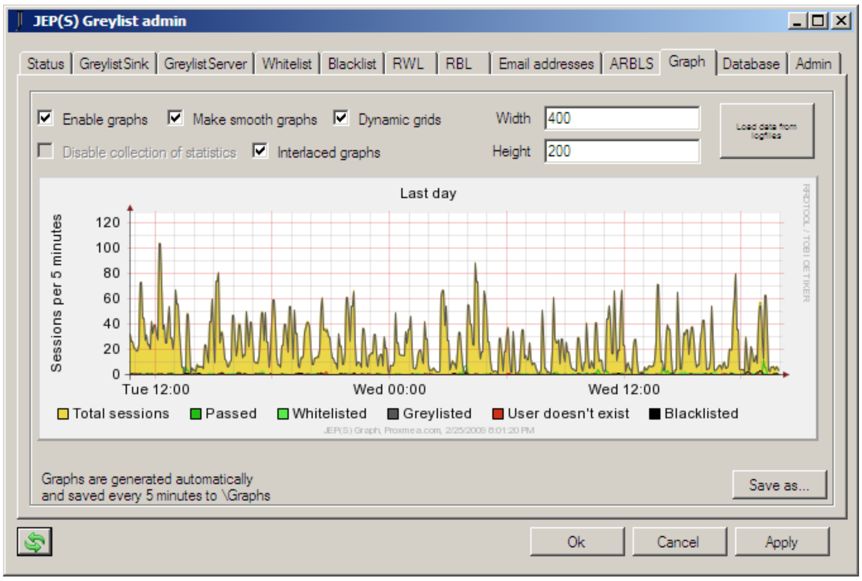
The information in the submission looks like this:

```
#dbtype:1#ms:374.9976#recordsSubmitted:25
2007-12-11 20:37:08,66.90.82.44,0,0,52,0,
2007-12-11 20:37:08,201.92.200.2,3,0,2,0,
2007-12-11 20:37:08,83.132.195.58,1,0,1,0,
2007-12-11 20:37:08,84.189.42.166,1,0,0,0,
2007-12-11 20:37:08,151.48.187.196,1,0,0,0,
2007-12-11 20:37:08,201.86.39.222,1,0,0,0,
2007-12-11 20:37:08,66.90.82.47,0,0,74,0,
2007-12-11 20:37:08,66.90.82.48,0,0,140,0,
2007-12-11 20:37:08,83.98.177.240,0,0,6,0,
2007-12-11 20:37:08,83.98.177.43,0,0,2,0,
more entries….
```

The first line contains information about the database type, time it took to analyze the last 10 minutes records in milliseconds, and the total amount of records submitted.
The consequent lines contains observation time in UTC, suspected spammer IP, count of rule 1, count of rule 2, count of rule 3, etc…
Rule 1 = Check if sending to an non-existing email address (if email address sources are configured in enabled or logging mode)
Rule 2 = Check if sender and recipient are the same
Rule 3 = Check for same ip, different sender, same recipient
Rule 4 = Check for same ip, same sender, different recipient

Graph

JEP(S) Graph is only available in the licensed version.



☑ Enable graphs ☑ Make smooth graphs ☑ Dynamic grids

□ Disable collection of statistics ☑ Interlaced graphs

Width 400

Height 200

Graphs are generated automatically
and saved every 5 minutes to \Graphs

Enable graphs	Will enable the collecting of statistical graph data.
Disable collection	Will disable the whole internal statistical engine used by graphs and ARBLS. This option is only available if graphs and ARBLS are disabled.
Make smooth graphs	Removes the edge of the displayed default graphs.
Dynamic grids	Displays grids only where necessary for default graphs. For example if this is disabled then the above graph would show 10, 20, 30, etc. With it enabled it will only show 0, 20, 40, etc.
Interlaced graph	Saves the produced images as interlaced for default graphs.
Width	The X size of default graphs.
Height	The Y size of default graphs.
Load data from log files	Opens the import window. This gives you the ability to rebuild the whole graph database in the case of a corrupt database or if you have had graphs disabled previously. An import is a onetime operation.
Image	By clicking on the image you it will be updated.
Save as…	Saves the displayed image to disk.

JEP(S) can save statistics to a separate round robin database which can contain up to one year of data. This database is kept as a local file and is only a couple of hundred of kB. It does this once every 5 minutes and saves the last 5 minutes data of number of passed, whitelisted, greylisted, blacklisted sessions as well as number of sessions to unknown email addresses (if email address sources are configured in enabled or logging mode).

Default operation

When enabled the JEP(S) server service will collect statistical data and produce graphs every 5 minutes. The 6 default graphs will be saved to a subdirectory to the JEP(S) installation called Graphs. As these images are rebuilt every five minutes it’s easy to have a scheduled task copying these to an internal web server or to share the directory.

Graph types

There are two different sets of graphs. JEP(S) will always produce 6 default graphs which have a static time period and layout.

In addition to this you can write your own graph definitions which will also be built every 5 minutes.

Custom graphs

JEP(S) is using RRDTool for generating the graphs. This is a free tool and an open format, so if you're comfortable in undertaking the configuration of this kind of files then you can write your completely own definitions and completely control what is included in the graphs, where they're saved and how they look.

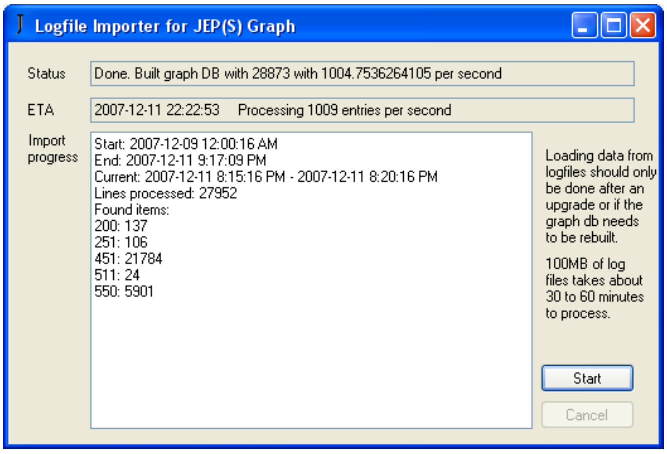
There are two sample custom graphs included with JEP(S) which can be used as a start point. It is safe to delete these two files if you don't want these graphs to be generated.

When you write your own definitions you need to save them as *JEP(S)_XXXX.def* or the server will not automatically generate them for you.

More information of RRDTool is available at http://oss.oetiker.ch/rrdtool/

Neither RRDTool or custom graphs are supported by Proxmea.

Load data from log files



Logfile Importer for JEP(S) Graph

Status: Done. Built graph DB with 28873 with 1004.7536264105 per second

ETA: 2007-12-11 22:22:53 Processing 1009 entries per second

Import progress:

```
Start: 2007-12-09 12:00:16 AM
End: 2007-12-11 9:17:09 PM
Current: 2007-12-11 8:15:16 PM - 2007-12-11 8:20:16 PM
Lines processed: 27952
Found items:
200: 137
251: 106
451: 21784
511: 24
550: 5901
```

Loading data from logfiles should only be done after an upgrade or if the graph db needs to be rebuilt.

100MB of log files takes about 30 to 60 minutes to process.

If you need to rebuild the graph database then this can be done with the Load data from log files button. This will invoke a importer which will load all log files into memory and analyze them from there.

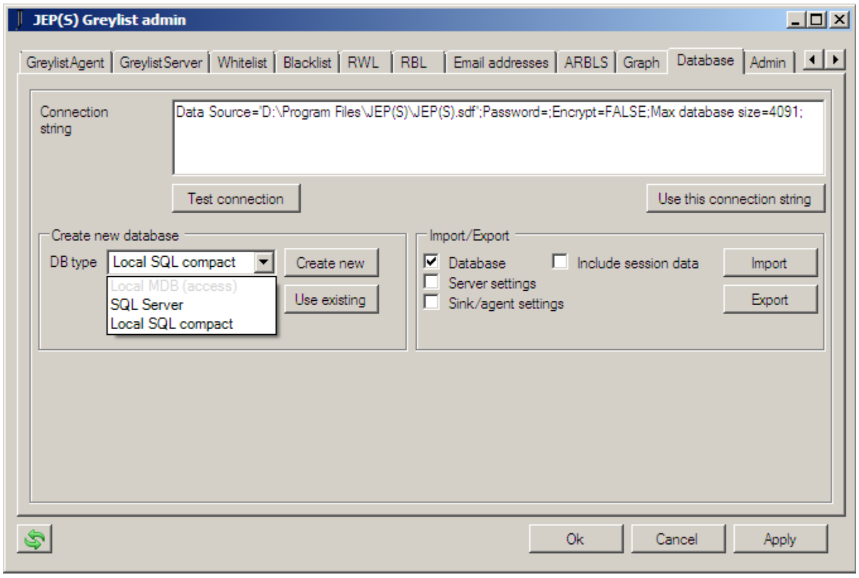
The importer thread itself is running with the lowest possible priority as such an import can take quite some time depending on the amount of data that needs to be imported and how fast your server is.

A rule of thumb is that a 100MB of log files takes 30 minutes on a Xeon 3040 @ 1.86 Ghz.

You can run this on a live system in production and it shouldn't influence the performance of the JEP(S) server even though this can easily use 80-90% of available CPU capacity.

This said – it's always preferred to do this off hours.

Database



Connection string: Data Source='D:\Program Files\JEP(S)\JEP(S).sdf';Password=;Encrypt=FALSE;Max database size=4091;

DB type: Local SQL compact
Local MDB (access)
SQL Server
Local SQL compact

☑ Database
☐ Include session data
☐ Server settings
☐ Sink/agent settings

Connection string	This defines how JEP(S) will connect to the database together with the setting db type. You can edit this or insert a custom connection string here and after selecting db type on the Greylist server tab you can test the connection string and the select ‘Use this connection string’.
Test connection	Uses the dbtype specified on the Greylist server tab together with the specified connection string to test the connection.
Use this connection string	Writes the selected connection string to the settings and restarts the application.

Create new database

The database setup is described under the installation procedure on page 9.

DB type	Selects the database type to do an action on. Types not available are greyed out and are not selectable.
Create new	Creates a new database. For Local MDB and Local SQL the database is created in the local JEP(S) installation directory. For SQL server a new dialog window is opened which is described on page 9. If the setup is successful then the connection string will be shown in the connection string box and you will get the question if you’d like to use this database. If you select yes then the string is committed to the settings and the application is restarted. If you select now then the string is left in the window and you can continue.
Use existing	Similar to the create new function with the exception that it will ask you to locate the existing database in place of creating it.

Import / Export

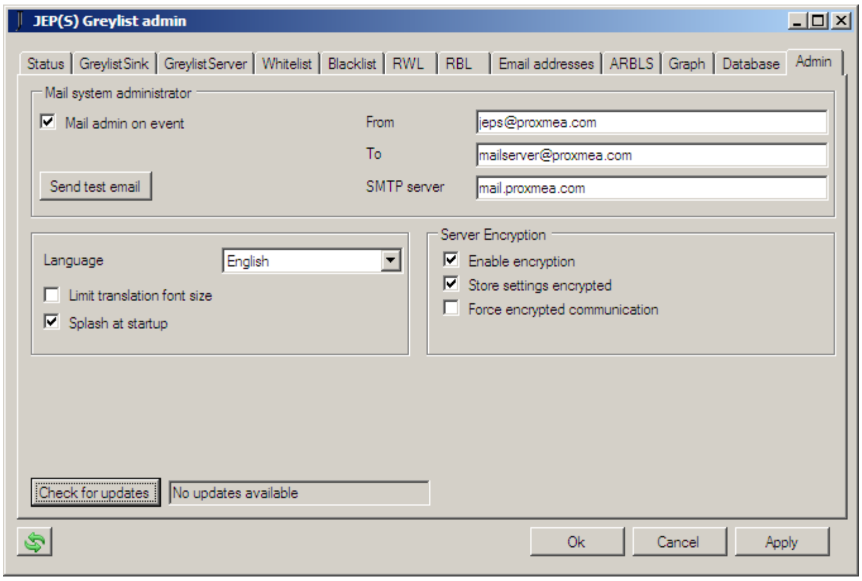
The export functions produces and XML file which contain the database tables and settings that JEP(S) uses. This XML can be edited after export to exclude existing entries or include new entries. The export is done on the checked options as described below.

The import function uses the exported XML file to import database tables and settings defined in the export file. It will only import entries matching the checked options if they exist in the export file.

An export can be done for all options and later an import can be done on only the options desired.

Database	All settings and lists in the database. This includes whitelists, blacklists, RWL, RBL, email address sources and blocked/passed count.
Include session data	On export this defines all sessions which are not unique, e.g. sessions that have been seen more the one time. On import this includes all defined entries in the export file.
Server settings	All registry stored settings for the JEP(S) Server. If the export file contains database settings then you will get a question on import if you would like to import these settings. By selecting no the database settings will be left as they are already defined.
Sink/agent settings	All registry stored settings for the JEP(S) Sink and Agent.
Import	Performs the import action.
Export	Performs the export action.

Admin



Mail system administrator

☑ Mail admin on event

From: jeps@proxmea.com

To: mailserver@proxmea.com

SMTP server: mail.proxmea.com

Language: English

☐ Limit translation font size

☑ Splash at startup

Server Encryption

☑ Enable encryption

☑ Store settings encrypted

☐ Force encrypted communication

No updates available

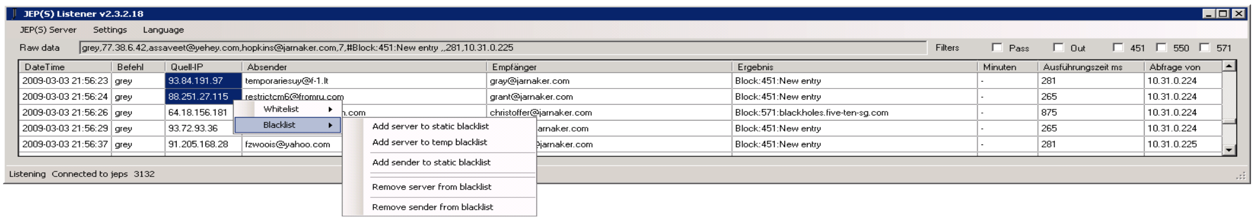
These functions are only available in the licensed version.

Mail admin on event	Enables JEP(S) to send email as well as writing events to the event log.
Send test email	Will notify the JEP(S) Service to send a test email.
From	This email address will be used as the sender of the email
To	This is the address where the email notification will be sent
SMTP Server	IP address or FQDN of a mail server to relay the mail to the address in

	the to field.
Language	Selects the language for the JEP(S) Admin user interface. Available language at the time of writing this manual are: English, German, French, Spanish, Italian, Brazilian Portuguese, Swedish and traditional Chinese. If the system is missing fonts for a language then this language will not be selectable.
Limit translation font size	When translations are active some labels will switch to a small font to fit the translation. This option prevents the font to be to small.
Splash on startup	Enables or disables the JEP(S) Admin splash screen
Enable encryption	Enables the encryption options
Store settings encrypted	Will encrypt the settings and strings stored in the registry
Force encrypted communication	When unchecked then encrypted traffic from JEP(S) Agent, Sink and Listener is accepted but optional. When checked then unencrypted traffic will be denied.
Check for updates	Contacts Proxmea.com to see if there are any recommended updates available.

JEP(S) Listener

The JEP(S) Listener utility allows you to view the real-time traffic passing though JEP(S) and the resulting actions. You can also interact with the white and blacklists by selecting one or more items and then selecting the action from the menu by right clicking in the grid.


JEP(S) Listener v2.3.2.18
JEP(S) Server
Settings
Language
Whitelist
Blacklist
Add server to static blacklist
Add server to temp blacklist
Add sender to static blacklist
Remove server from blacklist
Remove sender from blacklist

Raw data: grey,77.38.6.42,assaveet@yehey.com,hopkins@jarnaker.com,7,#Block:451:New entry ,,281,10.31.0.225

Filters □ Pass □ Out □ 451 □ 550 □ 571

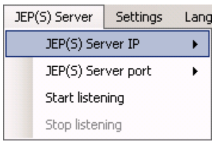
DateTime	Befehl	Quell-IP	Absender	Empfänger	Ergebnis	Minuten	Ausführungszeit ms	Abfrage von
2009-03-03 21:56:23	grey	93.84.191.97	temporariesuy@f-1.lt	gray@jarnaker.com	Block:451:New entry	-	281	10.31.0.224
2009-03-03 21:56:24	grey	88.251.27.115	restrictcm6@fromru.com	grant@jarnaker.com	Block:451:New entry	-	265	10.31.0.224
2009-03-03 21:56:26	grey	64.18.156.181	n.com	christoffer@jarnaker.com	Block:571:blackholes.five-ten-sg.com	-	875	10.31.0.224
2009-03-03 21:56:29	grey	93.72.93.36		arnaker.com	Block:451:New entry	-	265	10.31.0.224
2009-03-03 21:56:37	grey	91.205.168.28	fzwoois@yahoo.com	@jarnaker.com	Block:451:New entry	-	281	10.31.0.225

Listening Connected to jeps 3132

Connecting to the JEP(S) Server

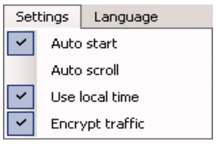
By default JEP(S) Listener is set to connect to 127.0.0.1 or port 9105. This can be changed on the JEP(S) Server menu under respective menu item.

Please note that if you want to connect to a JEP(S) Server other then on the local machine that you will (1) need a license on the JEP(S) Server installation and the JEP(S) Server needs to be set to (2) be set to listen on all interfaces.

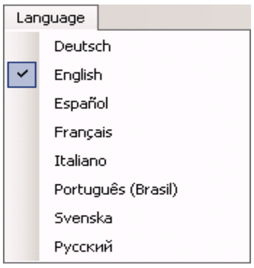


After confirming these settings select ‘Start listening’ to instruct the JEP(S) Server to start sending data to the listener.

Settings



☑ Auto start
Auto scroll
☑ Use local time
☑ Encrypt traffic



☑ English

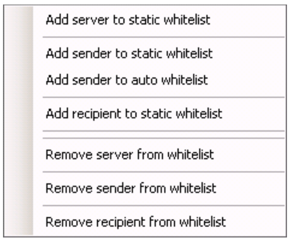
Auto start	When selected the listener will attempt to connect immediately after the program has started.
Auto scroll	When selected the focus in the grid will change to the last incoming entry. This is overridden by manual selections.
Use local time	Displays the incoming traffic in local time instead of UTC
Encrypt traffic	Communicates with the JEP(S) Server with encryption and requests the real-time data to be sent with encryption.
Language	Selects the language for the JEP(S) Listener user interface.

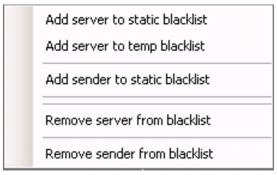
	Available language at the time of writing this manual are: English, German, French, Spanish, Italian, Brazilian Portuguese, Swedish and traditional Chinese. If the system is missing fonts for a language then this language will not be selectable. The language selection will only be reflected on the grid columns after a restart of JEP(S) Listener. This is a licensed feature.

Live management of white and black lists

This is a licensed feature.

You can add or remove entries from the white and blacklists by selecting an item or more in the JEP(S) Listener and then right clicking on the grid. You can then select one of the options from the menu and the result is displayed in the status field in the bottom left corner of the window.


Add server to static whitelist
Add sender to static whitelist
Add sender to auto whitelist
Add recipient to static whitelist
Remove server from whitelist
Remove sender from whitelist
Remove recipient from whitelist


Add server to static blacklist
Add server to temp blacklist
Add sender to static blacklist
Remove server from blacklist
Remove sender from blacklist

When selecting an entry the row the item is selected on is what determines what server, sender or recipient will be added or removed. It is thus only important that ‘a’ item on the right row has been selected, not what item.

You can add an entry multiple times without it actually being added more than once.

Add server to static whitelist	Add the server IP to the static whitelist.
Add sender to static whitelist	Add the sender email address to the static whitelist.
Add sender to auto whitelist	Add the sender email address to the auto whitelist. An entry added to this list will be removed once the it expires, normally 72 hours.
Add recipient to static whitelist	Add the recipient email address to the static whitelist.
Remove server from whitelist	Remove server IP from the whitelist.
Remove sender from whitelist	Remove sender email from whitelist.
Remove recipient from whitelist	Remove recipient email from whitelist.

Add server to static blacklist	Add the server IP to the static blacklist.

Add server to temp blacklist	Add the server IP to the temp blacklist. An entry added to this list will be removed once it expires, normally 24 hours.
Add sender to static blacklist	Add the sender email address to the static blacklist.
Remove server from blacklist	Removes the server IP from the blacklist.
Remove sender from blacklist	Removes the sender email address from the blacklist.

Filters

In the rightmost region of the listener there are five checkboxes for filtering what is displayed in the grid. The filters can be combined.

None checked	All traffic is displayed.
Pass	Display traffic that has passed successfully
Out	Display traffic that has passed though the autowhitelist
451	Display traffic that was blocked by the greylist filter. Aka 4.7.1
550	Display traffic that was blocked by the recipient not existing. Aka 5.1.1
571	Display traffic that was blocked by a realtime blacklist. Aka RBL.

About the communication

The JEP(S) Server is capable to send real-time information to a maximum of 10 JEP(S) Listeners.

To initiate the listening process the JEP(S) Listener is contacting the JEP(S) Server over TCP. The JEP(S) Server responds after the handshake to send real-time information back to the listener on the same port as the traffic was initiated on, but on UDP.

Appendix

Logfile format

All sessions that are filtered by JEP(S) are saved to a log file in the subdirectory \Log and are saved per day (according to UTC times).

The format of the log file is:
Date Time Sender Recipient – SourceIP Type - Result 0

Date	Date of session. In UTC.
Time	24 hour format of session. In UTC
Sender	The sending email address
Recipient	The recipients email address
-	Not used
SourceIP	The IP number of the sending mail server.
SMTP	Describes that this is a log entry for SMTP
-	Not used
Result	200 – Something in the session was found on a whitelist 250 – Session passed after previously being blocked 451 – Session blocked 511 – Email address doesn’t exist (if address checking is enabled) 550 – Source IP found on RBL
0	Not used

Extract from log file

```
2007-08-19 17:46:15 cxtdyr@boscaini.com.au francis@domain.com - 190.13.8.227 SMTP - 451 0
2007-08-19 17:46:22 ycgdi@blckdiamond.com freeman@ domain.com - 76.185.81.23 SMTP - 451 0
2007-08-19 17:46:51 prosperity.com@worldwide.com 1@ domain.com - 65.191.29.208 SMTP - 451 0
2007-08-19 17:47:18 pqh0slob@ups-scs.com higgins@ domain.com - 80.90.116.8 SMTP - 451 0
2007-08-19 17:47:46 akstctwmgmnsdgs@twmg.net higgins@ domain.com - 77.100.66.65 SMTP - 550 0
2007-08-19 17:47:55 vnyap89iemsp@toto.net fleming@ domain.com - 83.208.130.134 SMTP - 550 0
2007-08-19 17:48:26 wmi@juanita chris@ domain.com - 10.31.0.205 SMTP - 200 0
2007-08-19 17:49:33 johnp@hotmail.com gardner@ domain.com - 89.43.29.14 SMTP - 250 0
```

CLI

The communication between the sink, the listener and the JEP(S) service is all done over TCP. You can connect to the JEP(S) server through the listening port and instruct it to do certain tasks, or use this to integrate other software components with JEP(S).

Available commands for the JEP(S) server are:
helo   Returns Hello and your connection as IP:Port
qry sourceip,senderemail,recipientemail[,qualifiers]

Queries if a combination exists in the database

Returns False if the combination doesn't exist

Returns True and age if the combination exists

grey sourceip,senderemail,recipientemail[,qualifiers]

Runs a complete greylist query against the database

If the entry doesn't exist then it's created

Returns Block and age if the combination doesn't exist

Returns Block and age if the combination exists but isn't old enough

Returns Pass and age if the combination exists and is old enough

cleandb [date before all should be deleted]

Purge all data before the date.

If no date is supplied then a regular cleanup will be run

adddynwhite emailaddress

Adds a dynamic whitelist entry for the specified email address

This entry will be removed when it's older then max age for dynamic entries

showlists

Displays all whitelist entries currently in the cache

qrylis

Displays connection information for the JEP(S) listener, if available

testemail

Logs an informational event which will be sent to admin if available

loademail

Instructs the server to load all email addresses from the email sources

showemail

Displays all email addresses known to JEP(S)

arblstatus

Displays arbl server and submit status

analyzearbl

Instructs the server start analyzing ARBL data

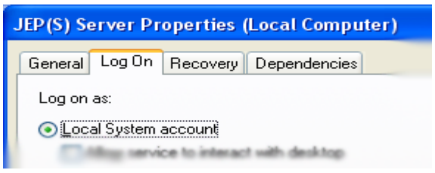
updategraph

Instructs the server to update graph data at the datetime entered

If no datetime is entered then now is assumed

Running the JEP(S) Server service under AD user account

When installing the JEP(S) service from JEP(S) Admin you install it as local system. While this is fully correct there are scenarios where it’s beneficial to run the service under another user account, like if you would like to use windows authentication against your SQL server.

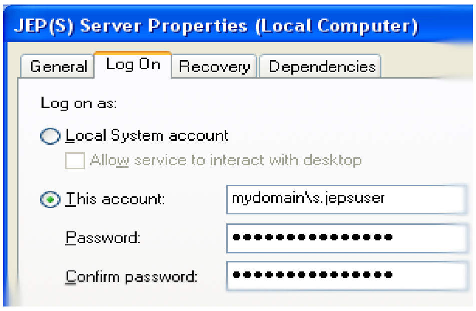


Log on as:

● Local System account

□ Allow service to interact with desktop

To edit the service startup account open services.msc and open the JEP(S) Server service and go to the log on tab.


JEP(S) Server Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: mydomain\s.jepsuser

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

The select this account and fill in your domain\username and the password twice. Then press apply or OK and you will be displayed with a informational dialog informing you that the account now has rights to log on as a service.

Do not restart the service yet.

After this go right click on the JEP(S) installation directory and confirm that the service account has explicit modify rights on this directory and all sub directories.

Go back to the service console and restart the JEP(S) service.

General Best Practice for installing the .NET Framework 2.0

Prior to installing the .NET Framework 2.0 it is advised to perform a full restart of the server and check for any Event Logs which indicate problems during startup.

These should be researched prior to installing the .NET Framework 2.0.

Following installation of the .NET Framework 2.0, all security updates should be applied to the server that relate to the .NET Framework 2.0.

A further reboot should occur after the installation and event logs should be reviewed to ensure no problems have been created by the installation of the .NET Framework 2.0.

It is best to review these logs prior to commencing the installation of JEP(S).

Installing the .NET Framework Version 2.0 on Windows Server 2000

Add the following registry entries after installing the .NET Framework 2.0. This primarily prevents hundreds of errors being logged in the Application Event Log relating to performance counters.

This has been known to fill the Application Event Log and cause the server to shutdown/fail unexpectedly.

This shutdown is not caused by JEP(S), but as a result of the .NET Framework 2.0 being installed to a Windows 2000 or Small Business Server 2000. This problem is documented in Microsoft Knowledgebase Article MSKB267831.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ASP.NET\Performance]
"Disable Performance Counters"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ASP.NET_2.0.50727\Performance]
"Disable Performance Counters"=dword:00000001
```

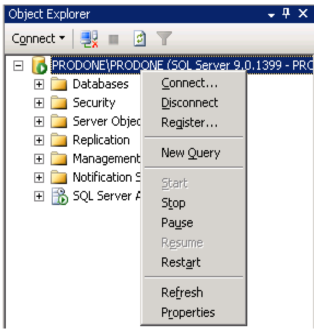
SQL Server configuration

Determine authentication mode.

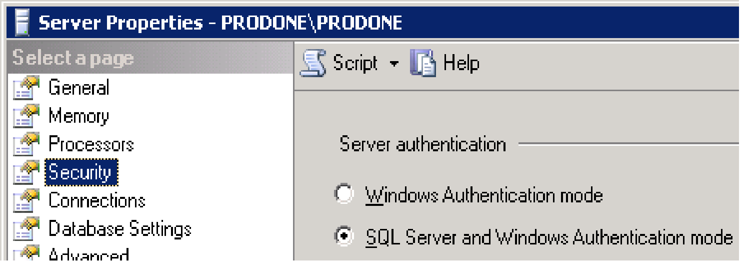
There are three ways to determine if you're running your SQL server in mixed or windows authentication mode.

A. Through the SQL Server Management Studio

1. Open SQL Server Management Studio and connect to the server
2. In the object explorer right click on your server and select Properties



3. You can find the current setting under the security tab


Server Properties - PRODONE\PRODONE

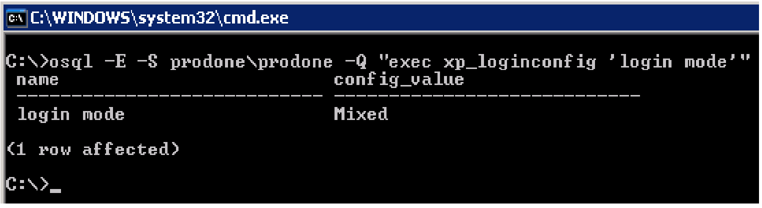
Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

B. Through a command prompt on the SQL server

1. Execute the SQL command line tool with the following command:
`osql -E [-S <servname\instance>] -Q "exec xp_loginconfig 'login mode'"`


C:\WINDOWS\system32\cmd.exe

```
C:\>osql -E -S prodone\prodone -Q "exec xp_loginconfig 'login mode'"
 name                             config_value
 -------------------------------- ----------------------------------
 login mode                       Mixed

(1 row affected)

C:\>_
```

Note, if you are executing this on the server and you are using the default instance or full SQL Server 2005 product the command can be abbreviated to:
`osql -E -Q "exec xp_loginconfig 'login mode'"`

C. Through a SQL server query window

1. Execute the following string in the query window:
   `exec xp_loginconfig 'login mode'`

JEP(S) database permissions

The default permissions of the user which is created on the JEP(S) database is db owner. While this is not fully necessary it is the only supported permissions setup when upgrading JEP(S). Under normal circumstances you can remove this privilege and replace this with datareader and datawriter.