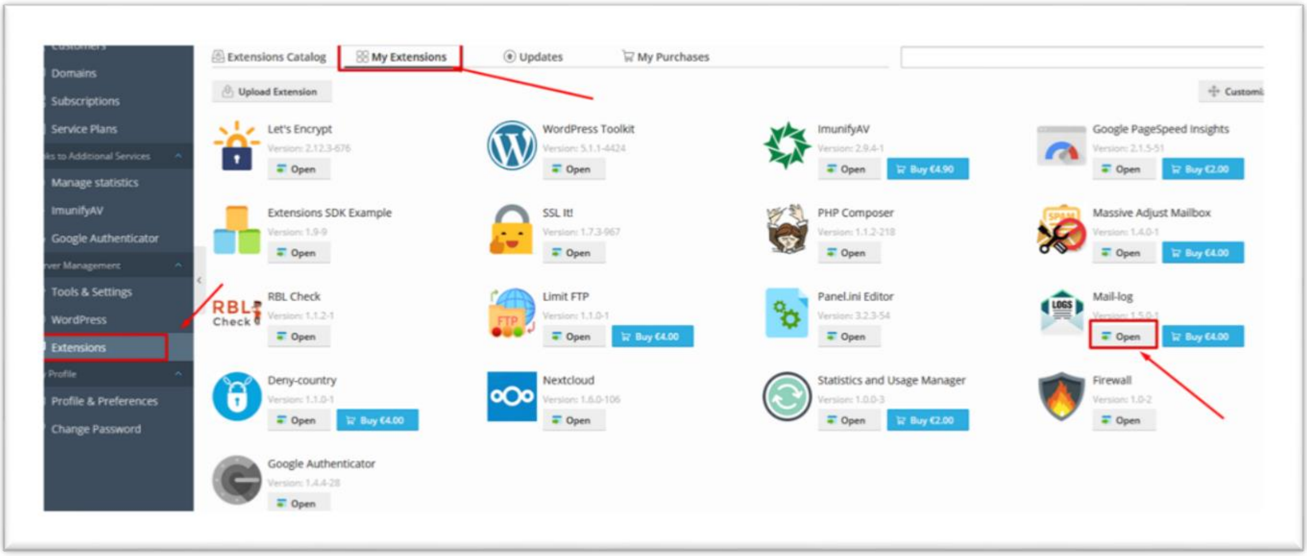
Mail Log (Plesk Extension) **user manual**

By

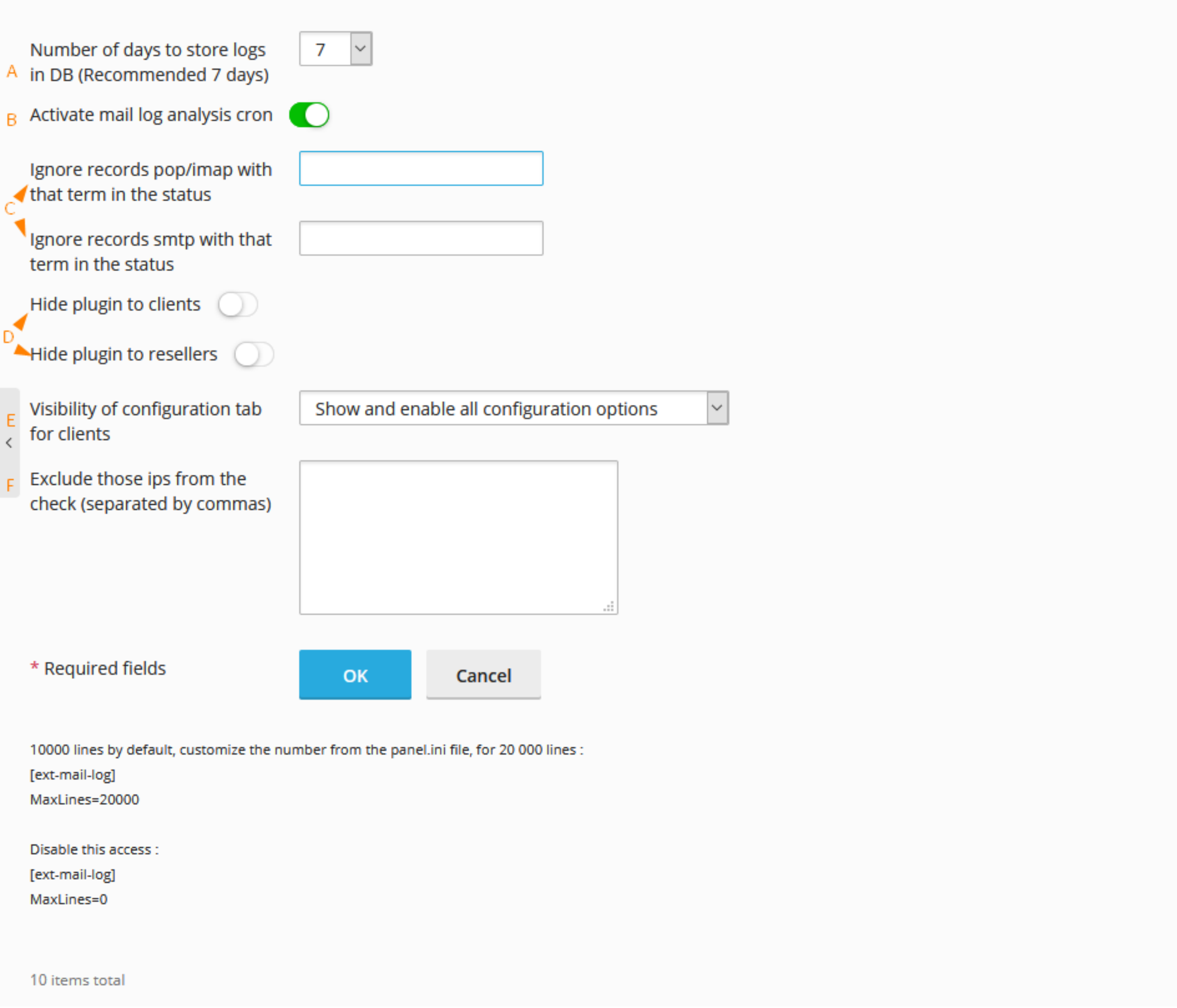
ConfigBOX

01 – Admin options

First of all we are going to review the **administration options** of the Mail Log extension.
To do this, we will go to the Extensions section of Plesk> My extensions> Mail-log> Open



Once we click on "Open" of Mail log we will find several options:



A Number of days to store logs in DB (Recommended 7 days) 7

B Activate mail log analysis cron ●

C Ignore records pop/imap with that term in the status

Ignore records smtp with that term in the status

D Hide plugin to clients ○

Hide plugin to resellers ○

E Visibility of configuration tab for clients Show and enable all configuration options

F Exclude those ips from the check (separated by commas)

* Required fields OK Cancel

10000 lines by default, customize the number from the panel.ini file, for 20 000 lines :
[ext-mail-log]
MaxLines=20000

Disable this access :
[ext-mail-log]
MaxLines=0

10 items total

A. The first field "**Number of days to store logs in DB (Recommended 7 days)**" defines the number of days that logs remain in the database, we recommend not extending this time too much since the database can grow significantly and make response times longer when listing the records (note that the number of records per days, depending on the server, can be very high).

B. The second option "**Activate mail log analysis cron**", allows enable or disable the analysis of logs. It is not recommended to deactivate it since it would leave the plugin without results but it may be necessary at some point if you have to do any maintenance on the server.

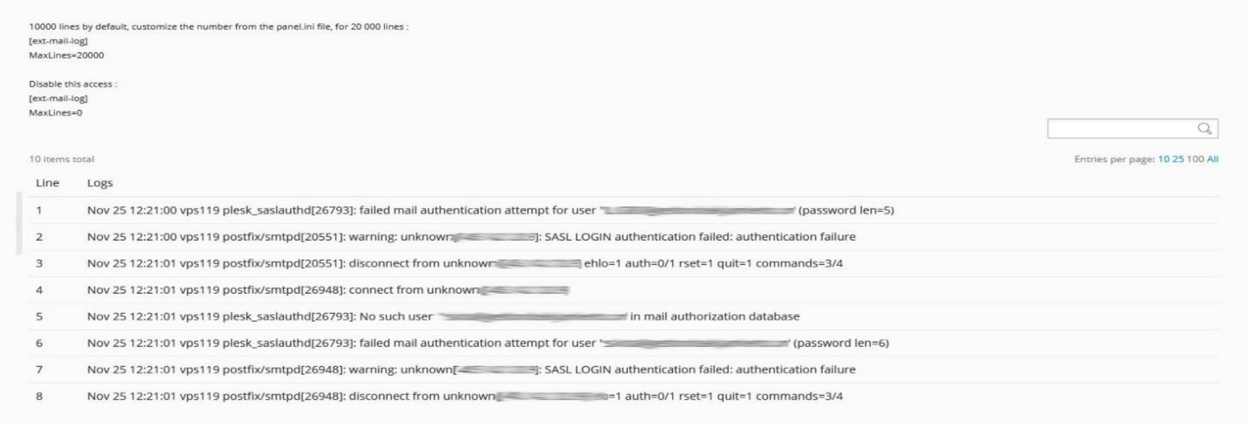
C. The **"Ignore records pop/imap with that term in the status"** **"Ignore records smtp with that term in the status"** allows you to hidden line of mail-out/mail-in that have the specific tem in status line. It can be useful if you use postfix filter (in this case, some line can be duplicate in logs)

D. The "**Hide plugin to clients" "Hide plugin to resellers"** options allows the administrator to define if the plugin should be visible or not for them.

E. The select field "**Visibility of configuration tab for clients**" defines if the client will see the notifications section, and if so, they will only see that section or will have the possibility to configure it.

F. The last option "**Exclude those ips from the check (separated by commas)**" allows to exclude at the server level (that is, any domain will be affected), the checks on the defined ips, whether they are from a country selected as "valid / usual "or not one.

At the bottom, we will see the **last lines of logs**:



10000 lines by default, customize the number from the panel.ini file, for 20 000 lines :
[ext-mail-log]
MaxLines=20000

Disable this access :
[ext-mail-log]
MaxLines=0

10 items total

Entries per page: 10 25 100 All

```
Line  Logs
1     Nov 25 12:21:00 vps119 plesk_saslauthd[26793]: failed mail authentication attempt for user '[redacted]' (password len=5)
2     Nov 25 12:21:00 vps119 postfix/smtpd[20551]: warning: unknown[redacted]]: SASL LOGIN authentication failed: authentication failure
3     Nov 25 12:21:01 vps119 postfix/smtpd[20551]: disconnect from unknown[redacted] ehlo=1 auth=0/1 rset=1 quit=1 commands=3/4
4     Nov 25 12:21:01 vps119 postfix/smtpd[26948]: connect from unknown[redacted]
5     Nov 25 12:21:01 vps119 plesk_saslauthd[26793]: No such user '[redacted]' in mail authorization database
6     Nov 25 12:21:01 vps119 plesk_saslauthd[26793]: failed mail authentication attempt for user '[redacted]' (password len=6)
7     Nov 25 12:21:01 vps119 postfix/smtpd[26948]: warning: unknown[[redacted]]: SASL LOGIN authentication failed: authentication failure
8     Nov 25 12:21:01 vps119 postfix/smtpd[26948]: disconnect from unknown[redacted]=1 auth=0/1 rset=1 quit=1 commands=3/4
```

By default, they are limited to 10,000 lines, but it is something that can be increased or even disabled from the panel.ini file (usually in /usr/local/psa/admin/conf/panel.ini):

```
[ext-mail-log]
MaxLines=20000
```

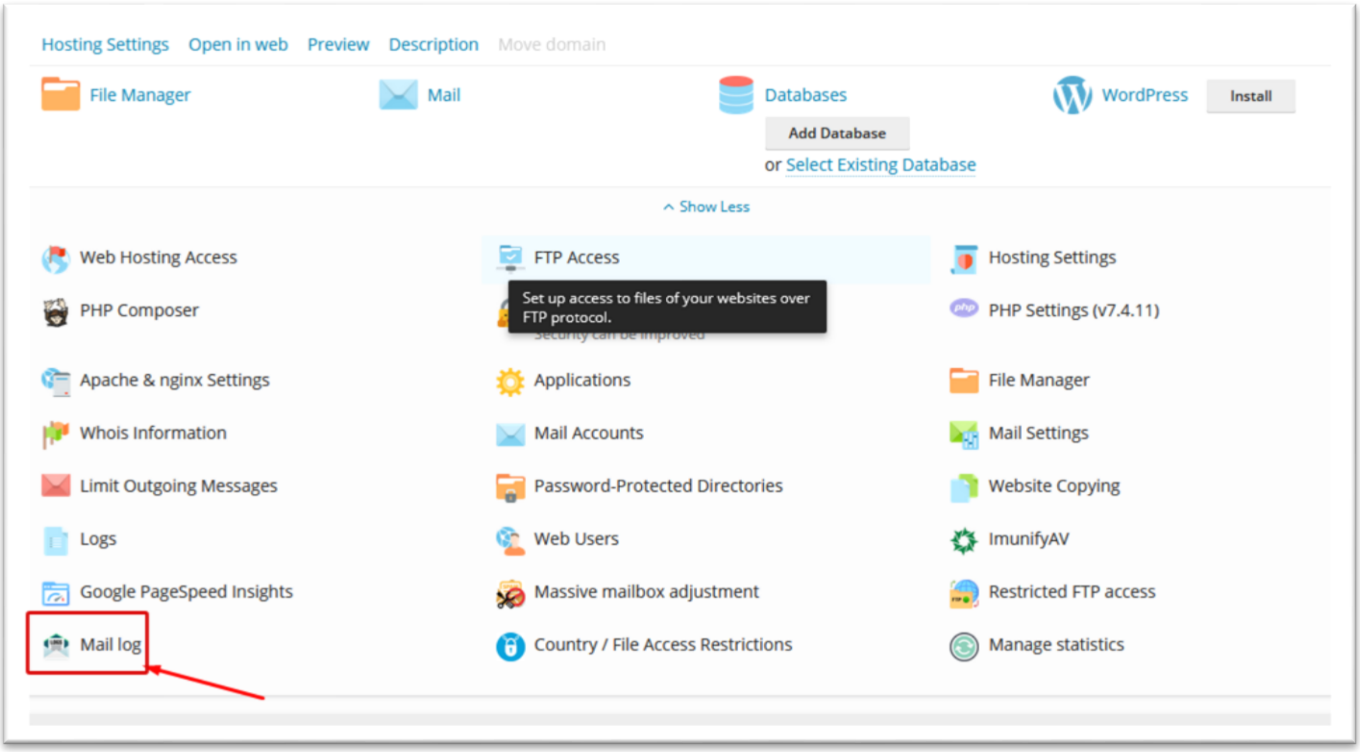
In this example, we expand from the default 10,000 lines to 20000

```
[ext-mail-log]
MaxLines=0
```

In this example, we set up that we don’t want any log lines to be seen in that section.

02 USER/SUBSCRIPTIONS OPTIONS

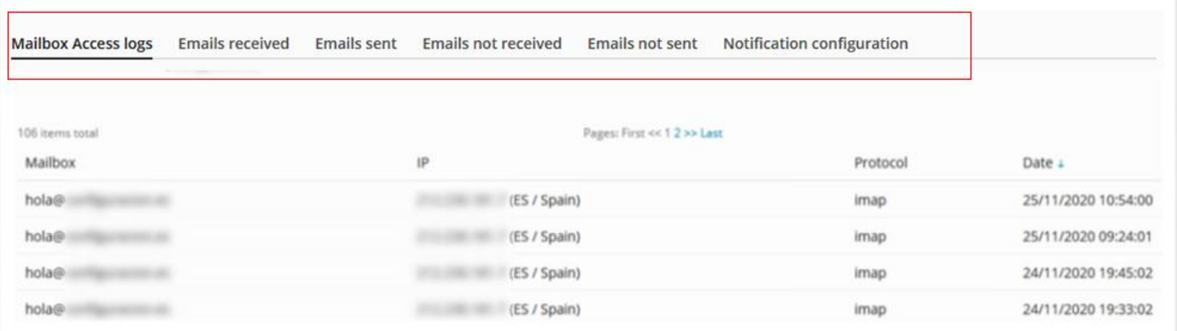
If the administrator has allowed it (**Hide plugin to clients (only show for Admin): deactivated)**, the client will see the plugin in their subscription:



Set up access to files of your websites over FTP protocol.

Security can be improved

By clicking on the "**Mail log**" icon, the user will access a screen with 6 tabs (if the option "Visibility of configuration tab for clients" is not defined with "Hide config tab for client, show only for admin"):

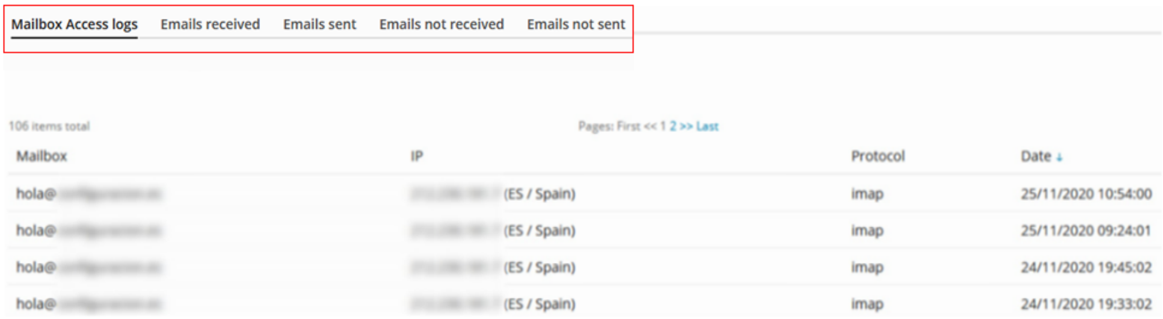


106 items total

Pages: First << 1 2 >> Last

Mailbox	IP	Protocol	Date ↓
hola@[redacted]	[redacted] (ES / Spain)	imap	25/11/2020 10:54:00
hola@[redacted]	[redacted] (ES / Spain)	imap	25/11/2020 09:24:01
hola@[redacted]	[redacted] (ES / Spain)	imap	24/11/2020 19:45:02
hola@[redacted]	[redacted] (ES / Spain)	imap	24/11/2020 19:33:02

If we have applied the option "Hide config tab for client, (show only for admin" activated) only 5 tabs will be shown:



106 items total

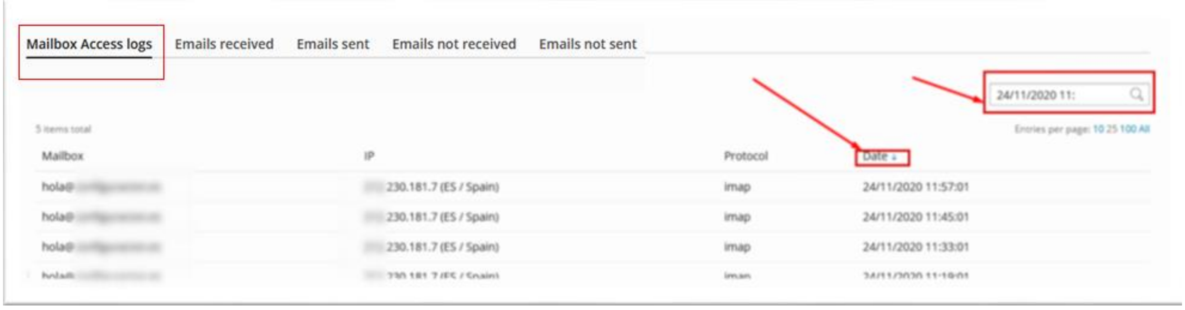
Pages: First << 1 2 >> Last

Mailbox	IP	Protocol	Date ↓
hola@[redacted]	[redacted] (ES / Spain)	imap	25/11/2020 10:54:00
hola@[redacted]	[redacted] (ES / Spain)	imap	25/11/2020 09:24:01
hola@[redacted]	[redacted] (ES / Spain)	imap	24/11/2020 19:45:02
hola@[redacted]	[redacted] (ES / Spain)	imap	24/11/2020 19:33:02

"Mailbox Access logs" Tab

By clicking on this tab we see the accesses to the different mailboxes of the client. There are several columns: "**Mailbox**", from which " **IP / Country**" of has accessed the mailbox, through which "**Protocol**", and on what "**date**".

You can search for any information with the search engine or order the fields you want:



24/11/2020 11:

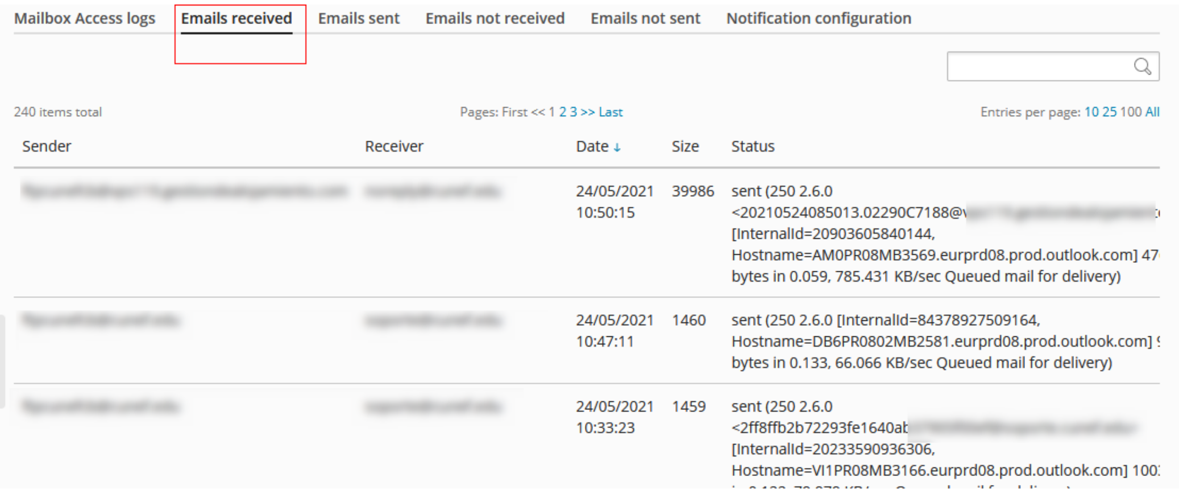
5 items total

Entries per page: 10 25 100 All

Mailbox	IP	Protocol	Date ↓
hola@[redacted]	[redacted] 230.181.7 (ES / Spain)	imap	24/11/2020 11:57:01
hola@[redacted]	[redacted] 230.181.7 (ES / Spain)	imap	24/11/2020 11:45:01
hola@[redacted]	[redacted] 230.181.7 (ES / Spain)	imap	24/11/2020 11:33:01
hola@[redacted]	[redacted] 230.181.7 (ES / Spain)	imap	24/11/2020 11:19:01

"Emails received" Tab

By clicking on this option you will access information about **emails received**, **from which sender** and **to which mailbox of your domain**, at what **date** / time, **weight, status** and the email **identifier**:



240 items total

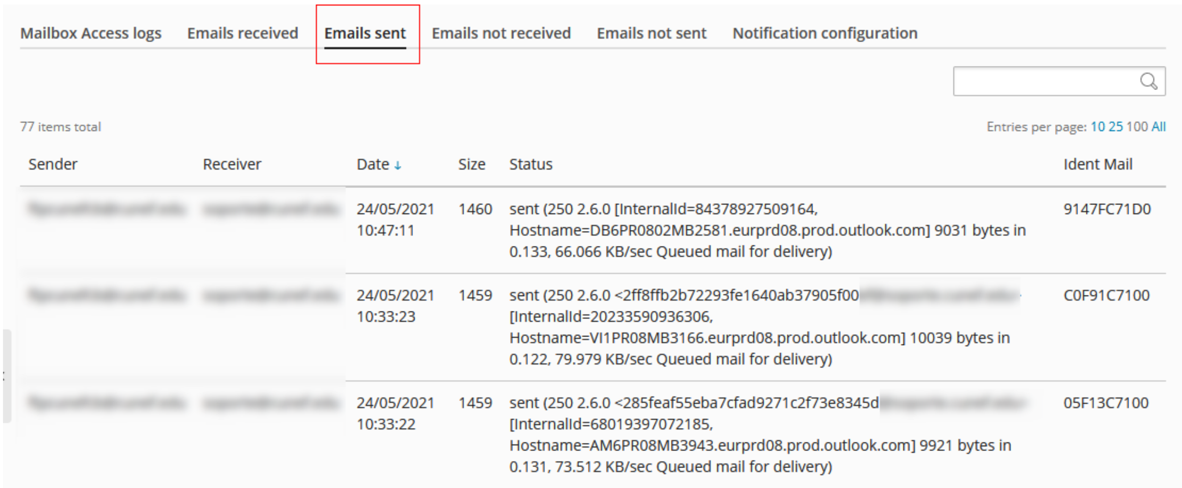
Pages: First << 1 2 3 >> Last

Entries per page: 10 25 100 All

Sender	Receiver	Date ↓	Size	Status
[redacted]	[redacted]	24/05/2021 10:50:15	39986	sent (250 2.6.0 <20210524085013.02290C7188@[redacted] [InternalId=20903605840144, Hostname=AM0PR08MB3569.eurprd08.prod.outlook.com] 47 bytes in 0.059, 785.431 KB/sec Queued mail for delivery)
[redacted]	[redacted]	24/05/2021 10:47:11	1460	sent (250 2.6.0 [InternalId=84378927509164, Hostname=DB6PR0802MB2581.eurprd08.prod.outlook.com] bytes in 0.133, 66.066 KB/sec Queued mail for delivery)
[redacted]	[redacted]	24/05/2021 10:33:23	1459	sent (250 2.6.0 <2ff8ffb2b72293fe1640ab[redacted] [InternalId=20233590936306, Hostname=VI1PR08MB3166.eurprd08.prod.outlook.com] 100

"Emails sent" Tab

Here you can Access information about the **emails sent** and **from which mailbox**, **to which recipient**, at what **date** / time, email **weight**, **status** and the email **identifier**:



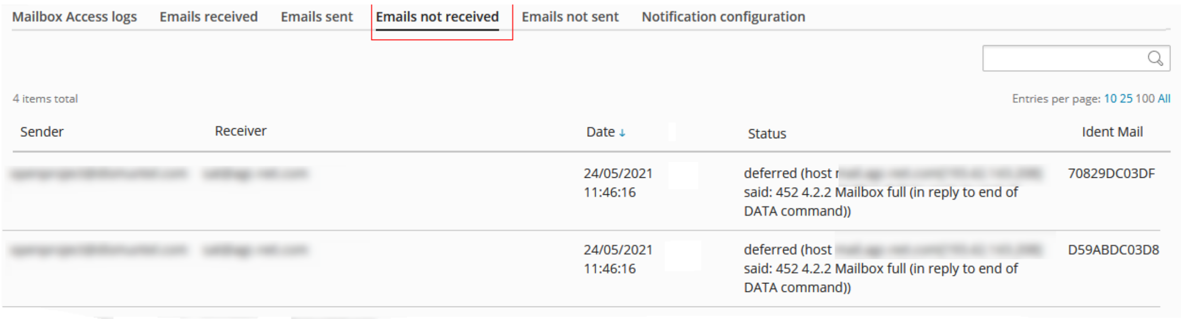
77 items total

Entries per page: 10 25 100 All

Sender	Receiver	Date ↓	Size	Status	Ident Mail
[redacted]	[redacted]	24/05/2021 10:47:11	1460	sent (250 2.6.0 [InternalId=84378927509164, Hostname=DB6PR0802MB2581.eurprd08.prod.outlook.com] 9031 bytes in 0.133, 66.066 KB/sec Queued mail for delivery)	9147FC71D0
[redacted]	[redacted]	24/05/2021 10:33:23	1459	sent (250 2.6.0 <2ff8ffb2b72293fe1640ab37905f00[redacted] [InternalId=20233590936306, Hostname=VI1PR08MB3166.eurprd08.prod.outlook.com] 10039 bytes in 0.122, 79.979 KB/sec Queued mail for delivery)	C0F91C7100
[redacted]	[redacted]	24/05/2021 10:33:22	1459	sent (250 2.6.0 <285feaf55eba7cfad9271c2f73e8345d[redacted] [InternalId=68019397072185, Hostname=AM6PR08MB3943.eurprd08.prod.outlook.com] 9921 bytes in 0.131, 73.512 KB/sec Queued mail for delivery)	05F13C7100

"Emails not received" Tab

By clicking on this option you will access information about **emails not received**, **from which sender** and **to which mailbox of your domain**, at what **date** / time, **status error** and the email **identifier**:



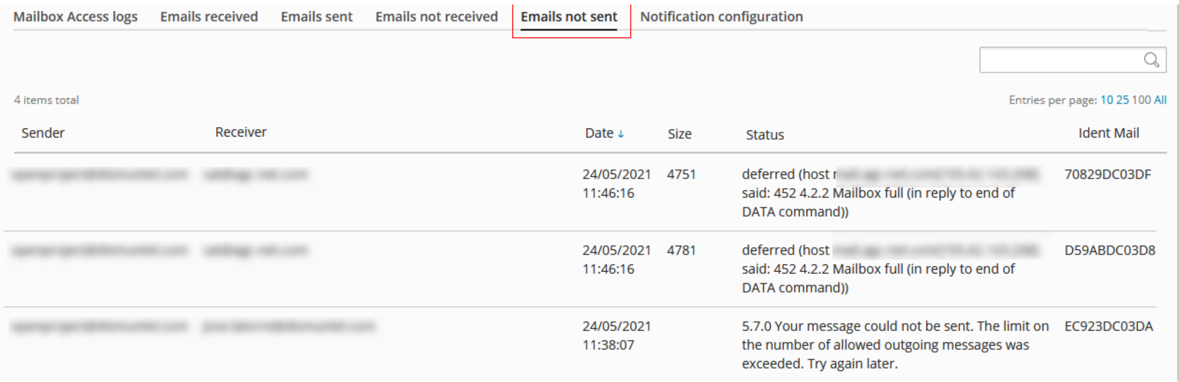
4 items total

Entries per page: 10 25 100 All

Sender	Receiver	Date ↓	Status	Ident Mail
[redacted]	[redacted]	24/05/2021 11:46:16	deferred (host r[redacted] said: 452 4.2.2 Mailbox full (in reply to end of DATA command))	70829DC03DF
[redacted]	[redacted]	24/05/2021 11:46:16	deferred (host [redacted] said: 452 4.2.2 Mailbox full (in reply to end of DATA command))	D59ABDC03D8

"Emails not sent" Tab

Here you can Access information about the **emails not sent** and **from which mailbox**, **to which recipient**, at what **date** / time, email **weight**, **status error** and the email **identifier**:



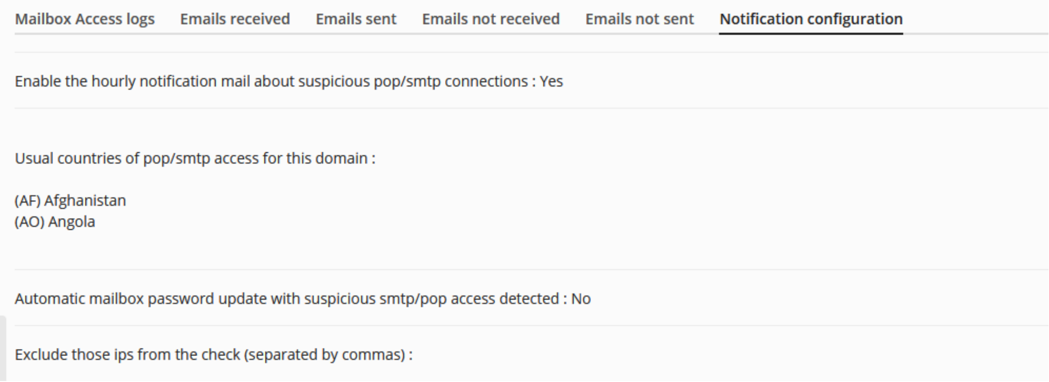
4 items total

Entries per page: 10 25 100 All

Sender	Receiver	Date ↓	Size	Status	Ident Mail
[redacted]	[redacted]	24/05/2021 11:46:16	4751	deferred (host [redacted] said: 452 4.2.2 Mailbox full (in reply to end of DATA command))	70829DC03DF
[redacted]	[redacted]	24/05/2021 11:46:16	4781	deferred (host [redacted] said: 452 4.2.2 Mailbox full (in reply to end of DATA command))	D59ABDC03D8
[redacted]	[redacted]	24/05/2021 11:38:07		5.7.0 Your message could not be sent. The limit on the number of allowed outgoing messages was exceeded. Try again later.	EC923DC03DA

"Configuration" Tab

If it is in read-only mode, the subscription user will see the settings assigned by the administrator:



Enable the hourly notification mail about suspicious pop/smtp connections : Yes

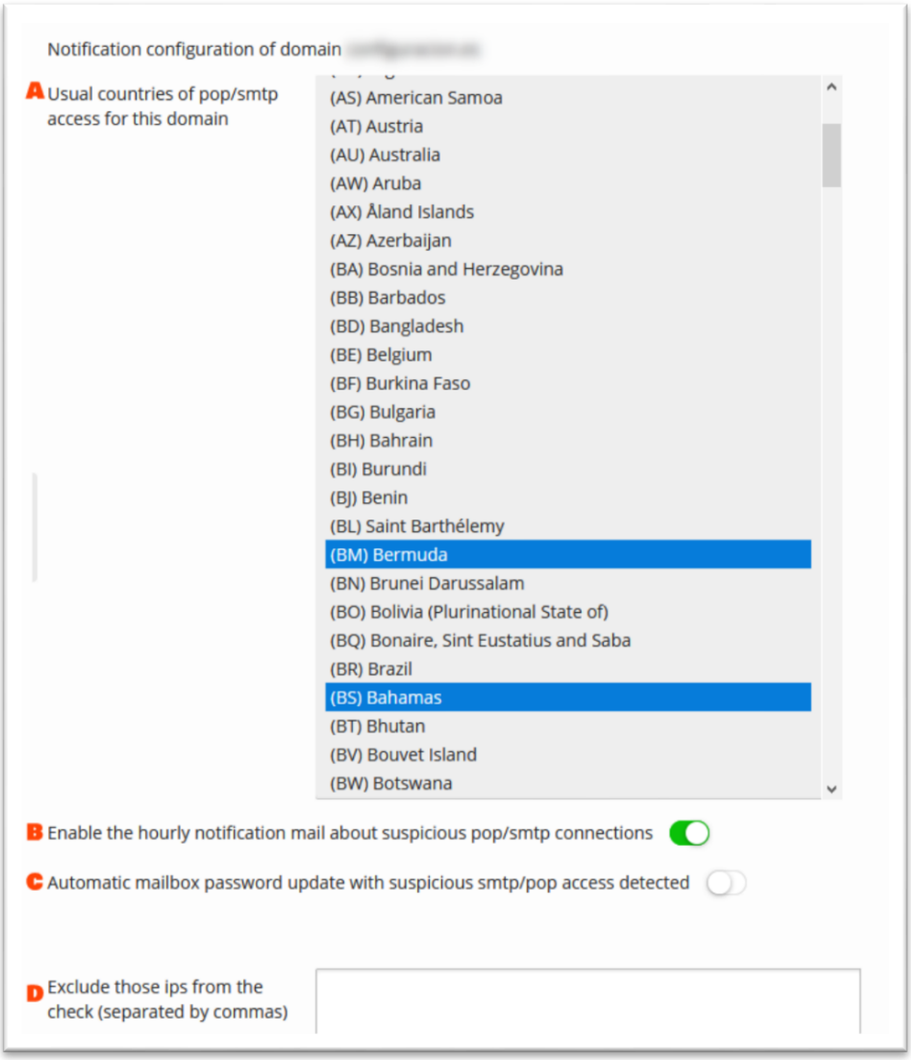
Usual countries of pop/smtp access for this domain :

(AF) Afghanistan
(AO) Angola

Automatic mailbox password update with suspicious smtp/pop access detected : No

Exclude those ips from the check (separated by commas) :

Otherwise, the user can configure the notifications:



Notification configuration of domain [redacted]

A Usual countries of pop/smtp access for this domain

(AS) American Samoa
(AT) Austria
(AU) Australia
(AW) Aruba
(AX) Åland Islands
(AZ) Azerbaijan
(BA) Bosnia and Herzegovina
(BB) Barbados
(BD) Bangladesh
(BE) Belgium
(BF) Burkina Faso
(BG) Bulgaria
(BH) Bahrain
(BI) Burundi
(BJ) Benin
(BL) Saint Barthélemy
(BM) Bermuda
(BN) Brunei Darussalam
(BO) Bolivia (Plurinational State of)
(BQ) Bonaire, Sint Eustatius and Saba
(BR) Brazil
(BS) Bahamas
(BT) Bhutan
(BV) Bouvet Island
(BW) Botswana

B Enable the hourly notification mail about suspicious pop/smtp connections ●

C Automatic mailbox password update with suspicious smtp/pop access detected ○

D Exclude those ips from the check (separated by commas)

A. From "**Usual countries of pop / smtp access for this domain**", you can select the "regular / usual" countries from which users connect to their mailboxes. If the ips that connect to your mailboxes by pop / imap or smtp do not match those countries, they will be detected by the notification system.

B. The second option allows you to **activate / deactivate email notification**. When it is activated, suspicious accesses are notified the next hour (for example, warnings at 10:09 that have occurred between 9 and 10 o'clock are notified).

C. The third option, forces a password change in case of a suspicious access, also occurs at the same time as the notification and the new password that is sent already defined in that notification email. This option CANNOT be activated if the notification system is not activated (second option).

D. Here you can allow ip exceptions on a specific domain in addition to those defined at the server level. For those ips, the connection country will not be checked and they will not be considered suspicious.