B.L.S. Consulting s.r.l.

Janusmail

Manuale utente

Revisionato il 30/12/2019

Versione 2.4.0

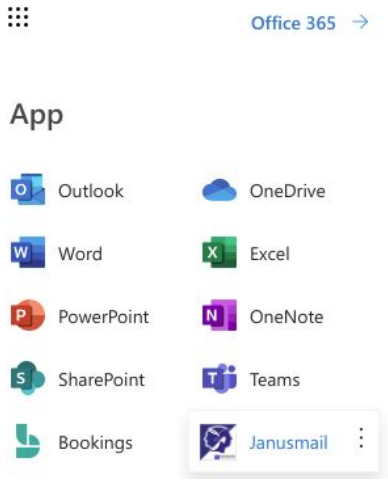
DASHBOARD

La Dashboard di Janusmail permette agli utenti di accedere all'elenco delle email spedite e ricevute, visualizzare lo stato di consegna, rilasciarle se sono state bloccate per spam e richiedere agli amministratori il rilascio di email erroneamente bloccate in quanto reputate pericolose.

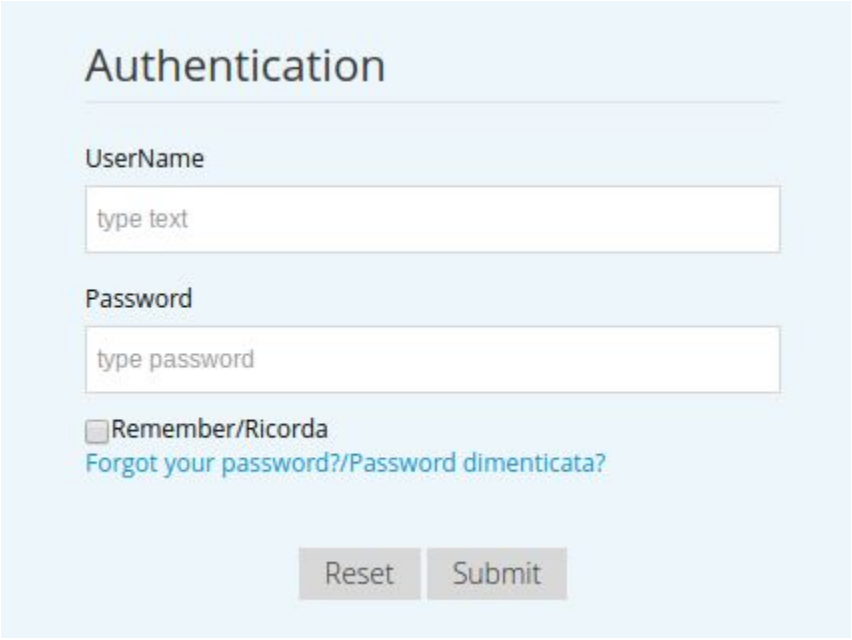
Gli amministratori possono visualizzare alcune funzioni aggiuntive che verranno descritte in seguito.

Si può accedere alla dashboard direttamente all'indirizzo inviato nella email di benvenuto, dall'opzione **Antispam dell**a barra di Zimbra**:**

o da menu di Microsoft Office 365/Exchange on-line, selezionando l'opzione Janusmail:

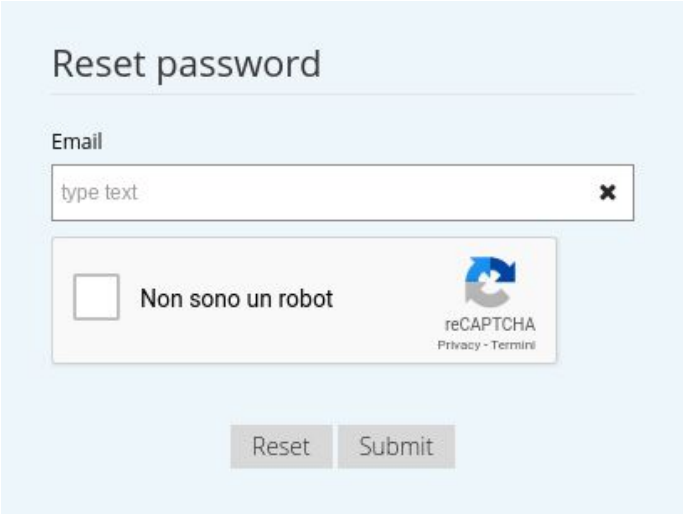


Al primo accesso è necessario autenticarsi utilizzando l'account usato per accedere alla propria casella di posta:

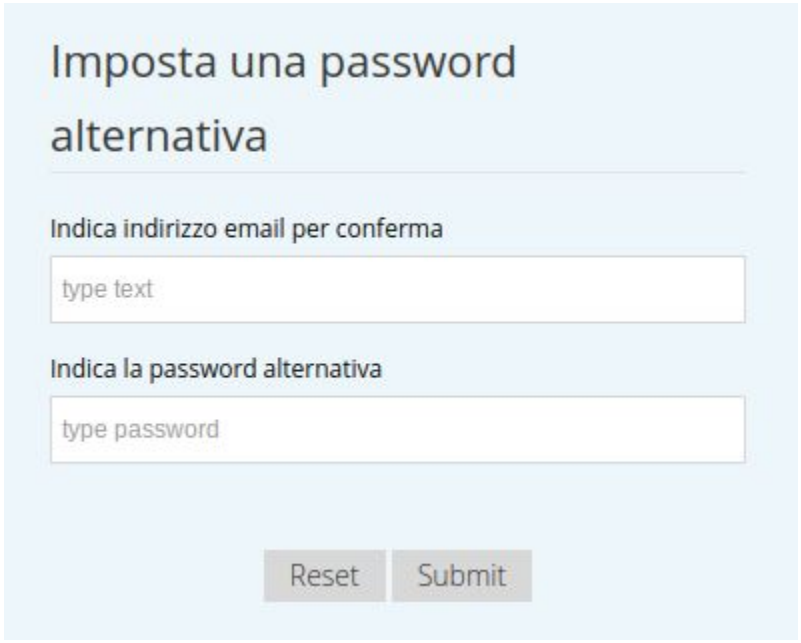


Spuntando la casella "Remember/Ricorda", al prossimo accesso da rete sicura, si accede direttamente alla dashboard senza che venga richiesta l'autenticazione.

Se non ricordate/conoscete la password di accesso potete cliccare su “Forgot your password/Password dimenticata?”, vi verrà richiesta la vostra email e dopo aver spuntato la casella “Non sono un robot”



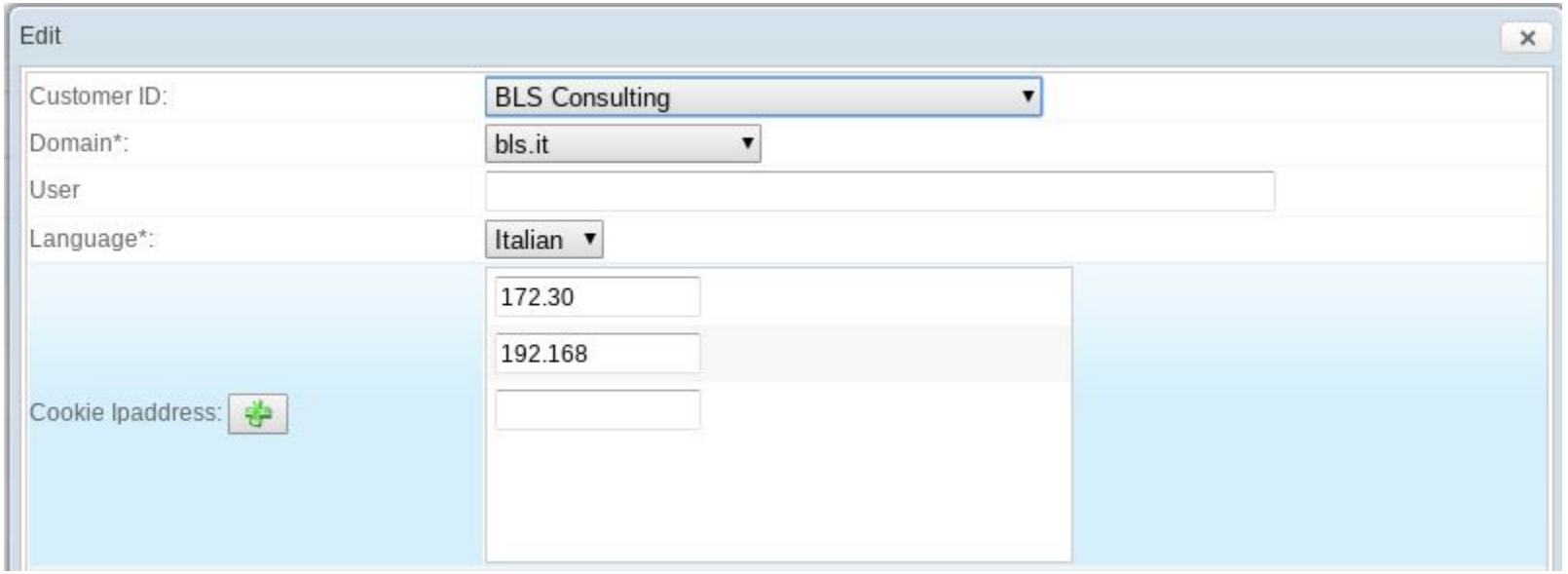
vi verrà inviata una email per impostare una nuova password:



Inserite l’indirizzo email per conferma e una password alternativa.

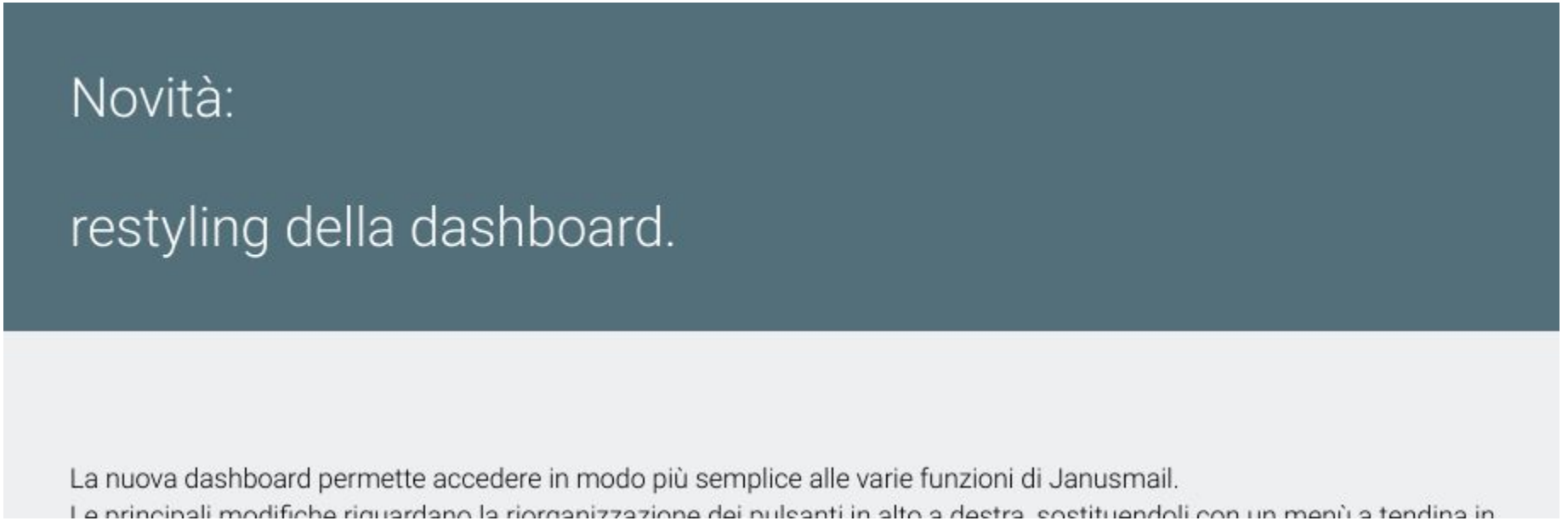
Successivamente potete accedere alla dashboard con questa password alternativa.

Le reti sicure si configurano nelle preferenze dei domini/Cookie IP address:

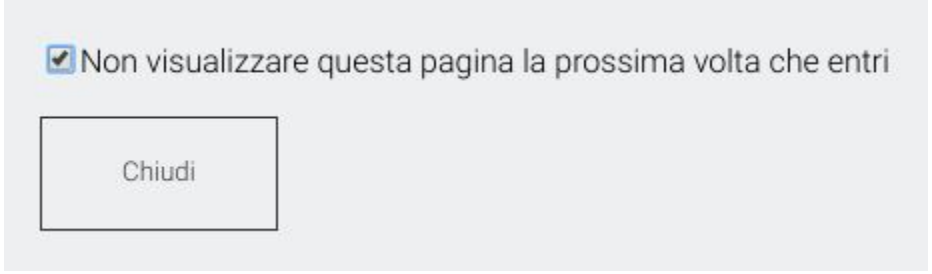


In questo esempio saranno considerati reti sicure quelle che hanno indirizzi che iniziano per 172.30 e 192.168

Prima di entrare nella dashboard verranno visualizzate eventuali novità.



Spuntando l’apposita casella a fine pagina è possibile evitare che vengano visualizzate:



Nella parte alta della dashboard sono visualizzati il menù funzioni, i campi di ricerca e le icone per accedere alle varie funzioni descritte in seguito.

I Campi per Ricerca permettono di eseguire la ricerca da data a data e corrispondenza perfetta di termini in destinatario, mittente ed oggetto.
Per corrispondenza perfetta di termini si intende che se il mittente è mrossi@dominio.com e si cerca rossi non verrà trovato, mentre se si cerca **mrossi**, oppure **dominio** oppure **com** verrà trovato.
Quindi, inserendo un termine completo esatto, verranno visualizzate tutte le email che contengono tale termine nel destinatario/i, nel mittente o nell'oggetto.

Una volta impostati i parametri di ricerca, premere l'icona per avviare la ricerca, cliccando invece sull'icona verranno visualizzati i parametri avanzati di ricerca (funzione descritta in seguito)

Due ulteriori opzioni permettono di velocizzare le ricerche:

Solo email personali: presente solo per gli amministratori, permette di visualizzare solo le email dell'amministratore stesso

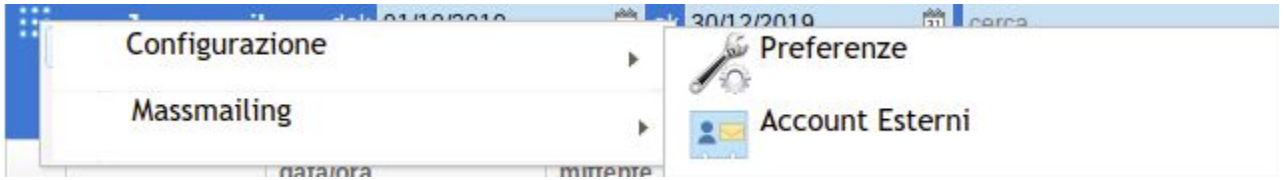
Solo da rilasciare: se spuntata visualizza solo le email che possono essere rilasciate

Le icone  permettono accedere nell’ordine alle seguenti funzioni:

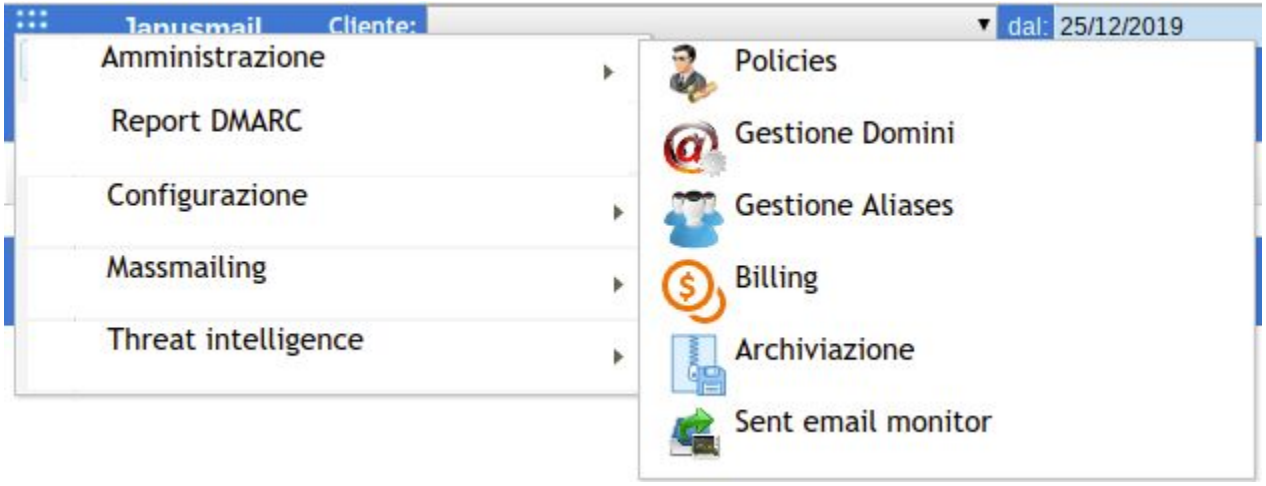
- report antispam: verrà visualizzato il report delle email bloccate da Janusmail
- guida utente: guida rapida alle principali funzioni della dashboard
- manuale: manuale completo di Janusmail
- news: ultime novità di Janusmail
- preferenze: permette all’utente impostare alcuni parametri di configurazione
- notifiche: visualizzazione delle notifiche di eventuali email infette o di phishing che per errore sono state consegnate
- logout: permette uscire dalla dashboard

L'icona in alto a sinistra permette accedere al menù delle funzioni, le funzioni visualizzate dipendono dal tipo di utente che accede alla dashboard.

Esempio di menù per utente base con opzione di massmailing:



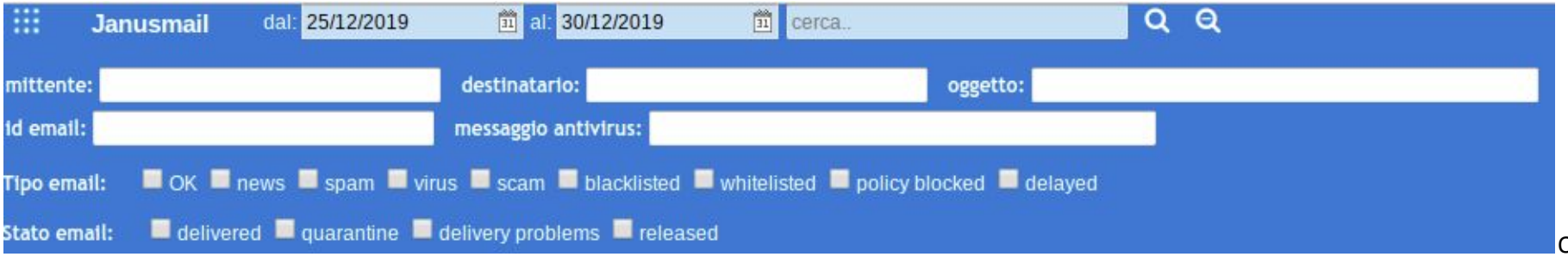
Esempio di menù per amministratore:



Le singole funzioni verranno descritte in seguito in questo manuale.

RICERCA AVANZATA

Per attivarla, cliccare sull'icona a forma di lente di ingrandimento con un "+".
Cliccando l'icona, compariranno i campi aggiuntivi di ricerca, una volta inseriti i parametri cliccare sulla lente di ingrandimento per effettuare la ricerca.



Questa modalità di ricerca non lavora per termini esatti, bensì per parole o porzioni di esse contenute nei campi di ricerca.
Riprendendo l'esempio di prima, se il mittente della email è mrossi@dominio.it e si inserisce ad es. nel campo di ricerca mittente la parola "mrossi", "rossi", "mross", "mrossi" o "ssi@dom", l'email verrà trovata. Nell'esempio seguente si può vedere come, impostando "Bounc" come termine di ricerca nel campo oggetto, compaiano tutti i risultati includenti quella serie di caratteri senza per forza combaciare precisamente, nell'esempio "Bounce".

Spuntando una o più caselle “Tipo email” verranno visualizzate le email di tale tipo, Spuntando una o più caselle “Stato email” verranno visualizzate le email filtrate per stato di consegna.

Inserendo l’ID esatto della email nel campo omonimo si potrà cercare una specifica email. Tale valore è recuperabile dal header della email:

X-Mrelayin-QIDOUT: x26C1GFU030514 (email ricevuta)

X-Mrelayout-INQID: x25GpZ90065114 (email spedita)

Gli header delle email sono visualizzabili con la funzione “Mostra originale” o similare del proprio client di posta.

ELENCO EMAIL RICEVUTE/INVIATE

Nella zona centrale della dashboard vengono visualizzate le email spedite e ricevute e che soddisfano gli eventuali parametri di ricerca impostati.

		data/ora	mittente	destinatari	oggetto	stato	opzioni
☐	SPAM	06/03/2019 13:47:36	return-3-console_hercu_e1826-3833234-02d6fb=2@bounce3.ilconsumo.com	info@bls.it	Sino a 700â¬ di sconto per festeggiare il 25mo compleanno di Materassi Fabricatore	quarantine	
☐	SPAM	06/03/2019 13:47:36	jeffreyharris@webiar.net.br	info@bls.it	What are your plans for tomorrow?	quarantine	
☐	SCAM	06/03/2019 13:41:27	markwright@neweramsr.com.au	mbruse@bls.it	Ho davvero bisogno di aiuto	quarantine	
	OK	06/03/2019 13:40:59	newsletter@mailant.it	info@bls.it	Fino al 10 marzo -52% sul listino	delivered	
☐	NEWS	06/03/2019 13:36:15	bounce-back.mnid2m.3577.34573818.4249.0.399455	mbruse@bls.it	Manovra 2019: novitÃ per le imprese. Scopri lâAgenda della conferenza	quarantine	

A inizio riga è presente una casella per selezionare l’email, dopo averle selezionate sarà possibile rilasciarle tutte insieme cliccando sul pulsante “Rilascia” a fine pagina o segnalarle come spam cliccando sul pulsante “Segnala spam” a fine pagina.

Si possono evidenziare email classificate come spam, news, scam, virus, delayed e rilasciarle o email ok o delayed e segnalarle come spam, il numero tra parentesi indica quante email verranno rilasciate o segnalqte come spam.

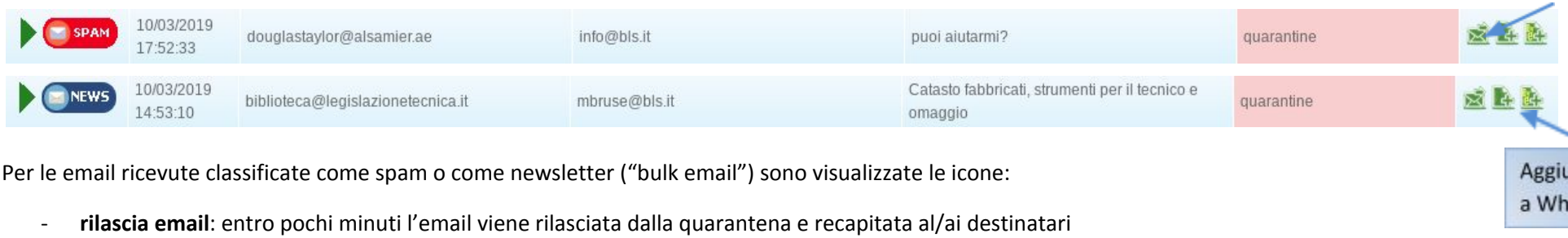
L'ultima riga permette rilasciare o segnalare come spam le emai spuntate (casella a sinistra di ogni email). Sono anche presenti le icone per muoversi tra le pagine.

Nella dashboard vengono visualizzate solo le ultime 2000 email che rispettano i parametri di ricerca, un apposito messaggio avvisa se ci sono più di 2000 email.

Se le email ricercate non vengono visualizzate perchè oltre le 2000 email affinare i parametri di ricerca.

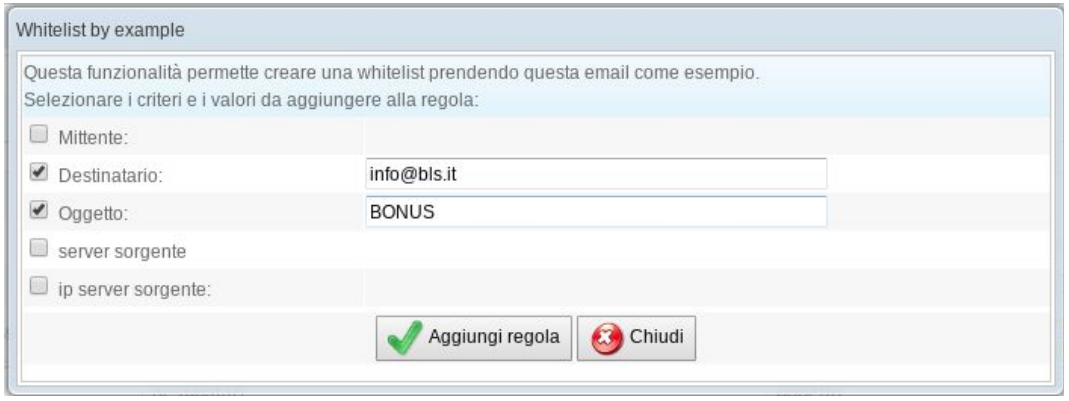
In base alla classificazione delle email (spam, virus, policy blocked, ecc.) verranno visualizzate delle opzioni specifiche in fondo alla riga dell'email.

Spam e newsletter



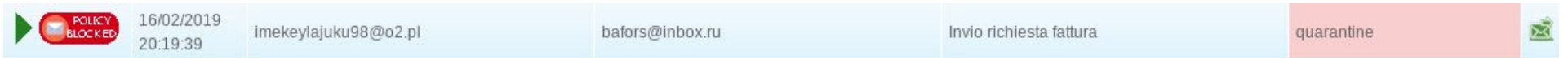
Per le email ricevute classificate come spam o come newsletter ("bulk email") sono visualizzate le icone:

- **rilascia email**: entro pochi minuti l'email viene rilasciata dalla quarantena e recapitata al/ai destinatari
- **aggiunta in whitelist**: l'aggiunta in whitelist comporta che una successiva email proveniente dallo stesso mittente e destinata allo stesso destinatario verrà consegnata e non più bloccata, inoltre anche le email provenienti dal dominio del mittente verranno recapitate
- **whitelist by example**: gli amministratori possono impostare delle whitelist con più flessibilità prendendo ad esempio una email bloccata e definendo i parametri che permettono di identificare le email da non bloccare:



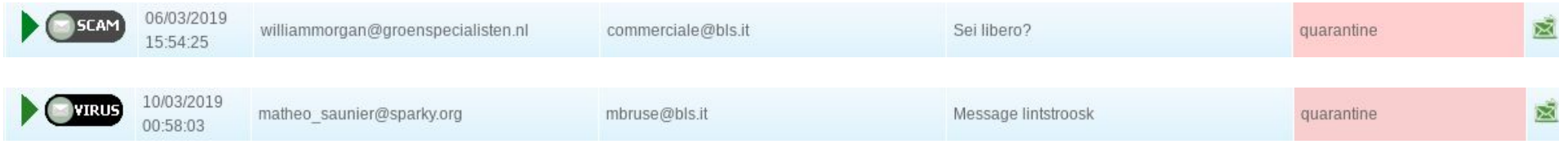
Questa regola varrà se il destinatario è info@bls.it e contemporaneamente l'oggetto contiene la parola BONUS.

Policy blocked



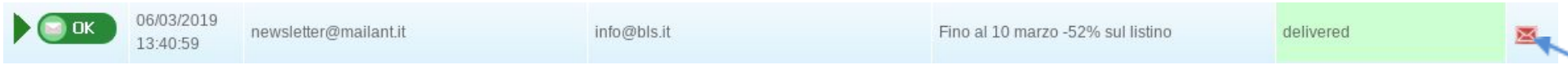
Per le email ricevute classificate come policy blocked (ad es. allegati pericolosi) è visualizzata l'icona richiedi rilascio: l'utente non ha diritto di rilasciare in autonomia l'email, ma può richiedere agli amministratori (del cliente, di dominio o del cluster) di analizzare l'email, verificare che non costituisce pericolo e quindi rilasciarla. Viene richiesto all'utente se conosce il mittente e sta aspettando l'email, queste informazioni vengono passate all'amministratore per aiutarlo a prendere una decisione.

Scam o virus



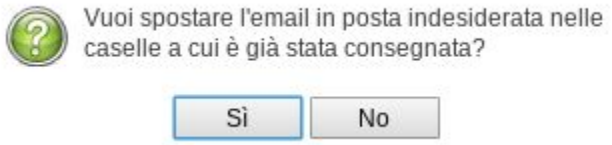
Per le email ricevute classificate come scam (ad es. email di phishing, truffa o in generale pericolose ma senza virus) o virus (contenenti allegati pericolosi con virus, ransomware, trojan o in generale segnalati pericolosi) è visualizzata l'icona richiedi rilascio: l'utente non ha diritto di rilasciare in autonomia l'email, ma può richiedere agli amministratori del cluster di analizzare l'email, verificare che non costituisce pericolo e quindi rilasciarla. Viene richiesto all'utente se conosce il mittente e sta aspettando l'email, queste informazioni vengono passate all'amministratore per aiutarlo a prendere una decisione.

OK



Per le email ricevute classificate come OK (quindi non bloccate) è visualizzata l'icona segnala come spam: in questo caso il sistema analizzerà l'email e utilizzerà le informazioni per contribuire a bloccare in futuro eventuali email simili.

Se è attivo il modulo Zimbra Advanced verrà richiesto:



Premendo su Si l'email già consegnata verrà spostata nella cartella posta insesiderata.

Whitelisted

Per le email ricevute e su cui ha agito una whitelist sarà possibile rimuovere dalla whitelist cliccando sull'icona corrispondente.

BARRA CONTEGGIO EMAIL

La barra conteggio email è presente nella parte alta della schermata principale, le email sono raggruppate a seconda della tipologia.

A sinistra, ci sono le EMAIL INVIATE, raggruppate in:

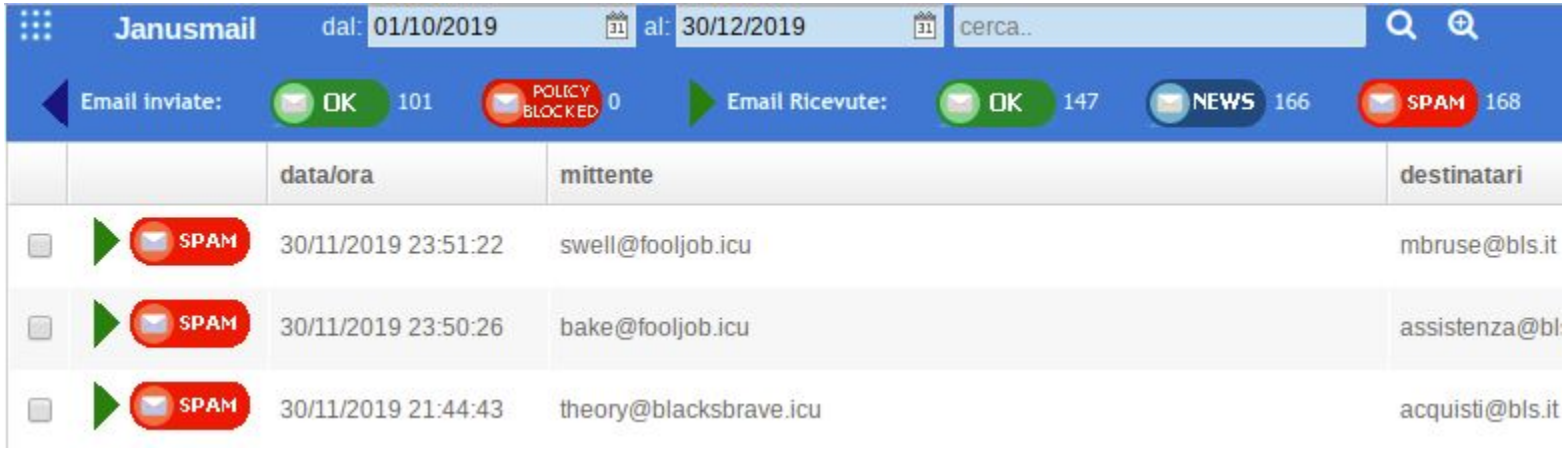
- “OK”: le email correttamente spedite
- “Policy Blocked”: email bloccate per policy

A destra, le EMAIL RICEVUTE sono raggruppate in:

- “OK”: email ricevute e che hanno passato tutti i controlli
- “News”: le newsletter
- “SPAM”: email bloccate in quanto ritenute Spam
- “Virus”: email bloccate perché risultate positive ai controlli Antivirus e Anti-malware
- “Scam”: email bloccate in quanto considerate tentativi di truffa o phishing
- “Whitelisted”: le email lasciate passare perché incluse in una Whitelist
- “Blacklisted”: email bloccate perché presenti nelle Blacklist
- “Policy Blocked”: email bloccate perché risultate positive ai filtri di Policy

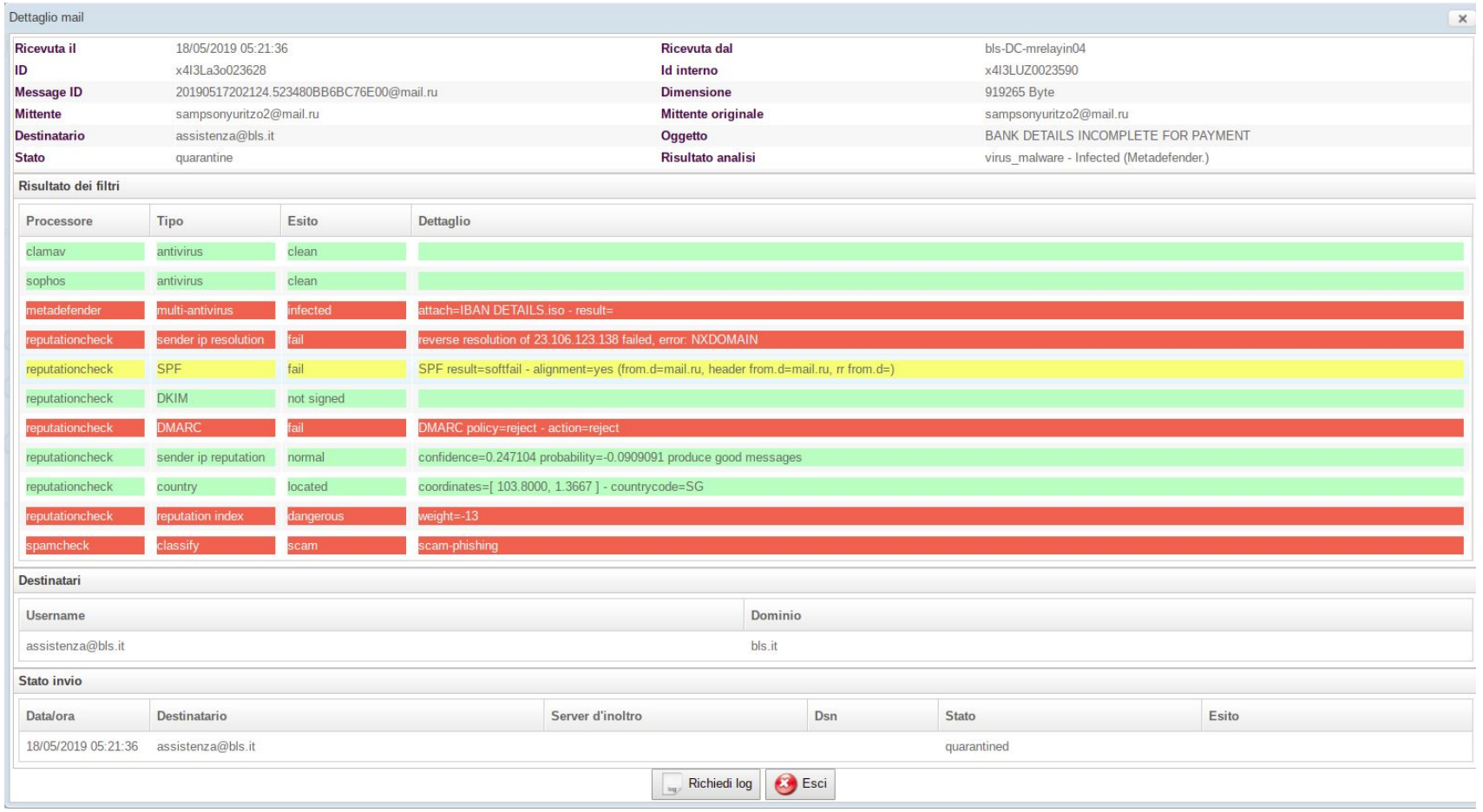
Cliccando su una tipologia di email, nell'elenco compariranno le email presenti in quel gruppo.

Nell'esempio seguente è stato cliccato il pulsante SPAM:



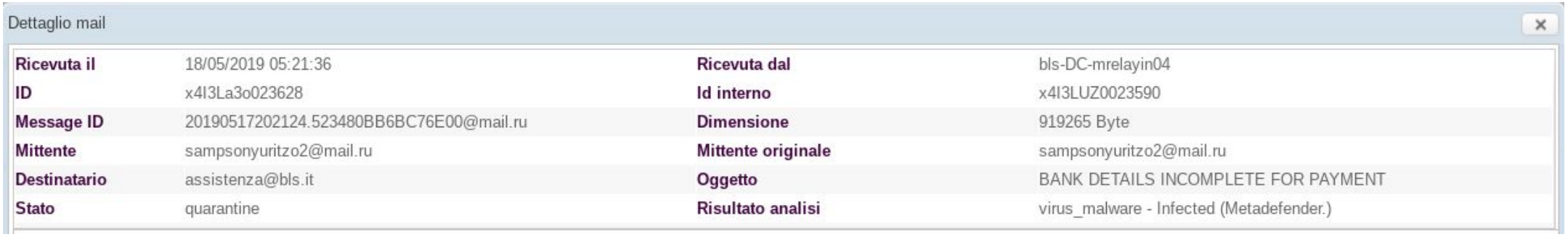
DETTAGLI EMAIL

Dall'elenco di email presente nella DASHBOARD si possono selezionare le singole email inviate o ricevute, ottenendo una schermata che fornisce dettagli sull'invio/ricezione, sul percorso, sul mittente e destinatario e sui test effettuati dal sistema.



La sezione DETTAGLIO MAIL si trova nella parte alta della schermata, visualizza un riepilogo delle informazioni riguardanti l'email:

- Ora, server che ha ricevuto l'email (mailrelay) e indirizzo IP/server da cui è stata ricevuta
- ID dell'email
- Mittente, ovvero il campo "From" dell'email
- Mittente Originale, ovvero chi è effettivamente il mittente della email, che per una email inoltrata indica il reale mittente.
- Destinatario o destinatari delle email
- Oggetto
- Stato di consegna
- Risultato analisi



Successivamente viene visualizzata la sezione **risultato dei filtri**:

Risultato dei filtri

Processore	Tipo	Esito	Dettaglio
clamav	antivirus	clean	
sophos	antivirus	clean	
metadefender	multi-antivirus	infected	attach=IBAN DETAILS.iso - result=
reputationcheck	sender ip resolution	fail	reverse resolution of 23.106.123.138 failed, error: NXDOMAIN
reputationcheck	SPF	fail	SPF result=softfail - alignment=yes (from.d=mail.ru, header from.d=mail.ru, rr from.d=)
reputationcheck	DKIM	not signed	
reputationcheck	DMARC	fail	DMARC policy=reject - action=reject
reputationcheck	sender ip reputation	normal	confidence=0.247104 probability=-0.0909091 produce good messages
reputationcheck	country	located	coordinates=[103.8000, 1.3667] - countrycode=SG
reputationcheck	reputation index	dangerous	weight=-13
spamcheck	classify	scam	scam-phishing

Questa sezione dettaglia le analisi effettuate sull'email e il relativo esito, Janusmail applica numerose ottimizzazioni, quindi non tutte le analisi vengono fatte su tutte le email, ma solo quelle necessarie. Ad es. se una email è già stata classificata come infetta non verranno effettuati tutti i controlli antispam.

La prima colonna indica quale **processore** (o sottosistema) ha eseguito l'analisi, sono implementati i seguenti processori:

- clamav: antivirus in grado di identificare email contenenti malware, email di spam o di scam
- sophos: antivirus secondario utilizzato se si dispone della relativa licenza e se clamav non ha identificato come infetta l'email
- metadefender: multi-antivirus che analizza i singoli allegati utilizzando gli antivirus **ESET, Total Defense, Bitdefender** e **K7**, utilizzato se attivata la funzionalità Advanced security, se presenti allegati e se clamav e sophos non hanno identificato come infetta l'email

- attach check: sistemi di analisi degli allegati, in particolare sono implementati i seguenti controlli:
    - identificazione degli allegati pericolosi (eseguibili o ad alto rischio) mediante estensione del file o tipologia di file (mime-type) in base a quanto definito nella policy allegati pericolosi (vedere per i dettagli il prossimo capitolo)
    - identificazione degli allegati pericolosi mediante un database degli hash come illustrato in seguito in questo stesso capitolo, utilizzato se attivata la funzionalità Advanced security,
    - identificazione dei pdf pericolosi, utilizzato se attivata la funzionalità Advanced security,
    - identificazione dei documenti office pericolosi, utilizzato se attivata la funzionalità Advanced security,
    - identificazione dei documenti pdf o office criptati
- url check: sistemi di analisi del rischio degli URL presenti nella email come illustrato di seguito in questo capitolo, utilizzato se attivata la funzionalità Advanced security,
- reputation check: sistemi di analisi della reputazione del server mittente mediante i seguenti controlli:
    - analisi della risoluzione dell'indirizzo ip del server mittente
    - SPF
    - DKIM
    - DMARC
    - analisi della reputazione del server mittente mediante una valutazione statistica che determina la probabilità (valori da -1 email buone a +1 email cattive) che il server invii email pericolose o spam e la confidenzialità della valutazione (valori da 0 poco affidabile a 1 certo)
    - la nazione da cui origina l'email
    - indice di reputazione complessiva valutato utilizzando i risultati dei test precedenti (valore zero neutra, valori positivi buona reputazione, valori negativi fino a -5 reputazione sospetta, valori negativi inferiori a -5 reputazione scarsa)
- spam check: sistemi di identificazione delle email di spam, sono implementati due sistemi:
    - sistema di classificazione delle email, in grado di identificare il tipo di email di spam, scam o in alcuni casi malware mediante un database di caratteristiche aggiornato costantemente e contenente oltre 200mila entry
    - sistema di identificazione delle email di spam mediante caratteristiche delle stesse, filtro baiesano, blacklist/whitelist e sistemi collaborativi; questo sistema seppur affidabile è dispendioso in termini di risorse di elaborazione e quindi viene eseguito solo se i sistemi precedenti non sono stati in grado di classificare l'email i modo affidabile

La seconda colonna identifica il **tipo** di analisi effettuata, mentre la terza l'**esito** dell'analisi, in base all'esito la riga viene evidenziata con un colore diverso:

verde: esito positivo o nessun esito

giallo: esito sospetto, ma non sufficiente per prendere una decisione

rosso: esito negativo

L'ultima colonna riporta alcune informazioni di **dettaglio** sulla singola analisi, come illustrato di seguito:

Per Clamav, Sophos e Metadefender è indicato **"clean"** se non sono state identificate minacce, oppure è indicato l'identificativo del malware, della firma di phishing o di spam se sono state identificate minacce.

Janusmail utilizza diversi database di firme per Clamav indicate nel dettaglio, in particolare **SecuriteInfo, Sanesecurity, Porcupine o firme ufficiali di Clamav**. Ad es. **Sanesecurity.Phishing.Fake.Coin.27677.UNOFFICIAL** sta ad indicare che la firma è del database Sanesecurity, non è ufficiale di Clamav, bensì un database aggiuntivo, si tratta di un Phishing (e quindi l'email verrà classificata come Scam) e in particolare la firma è denominata Fake.Coin.27677.

Se la minaccia è stata identificata da Sophos, verrà indicato mediante la parola Sophos. che precede il nome della firma, ad es.: **Sophos.Exp/20180802-B**

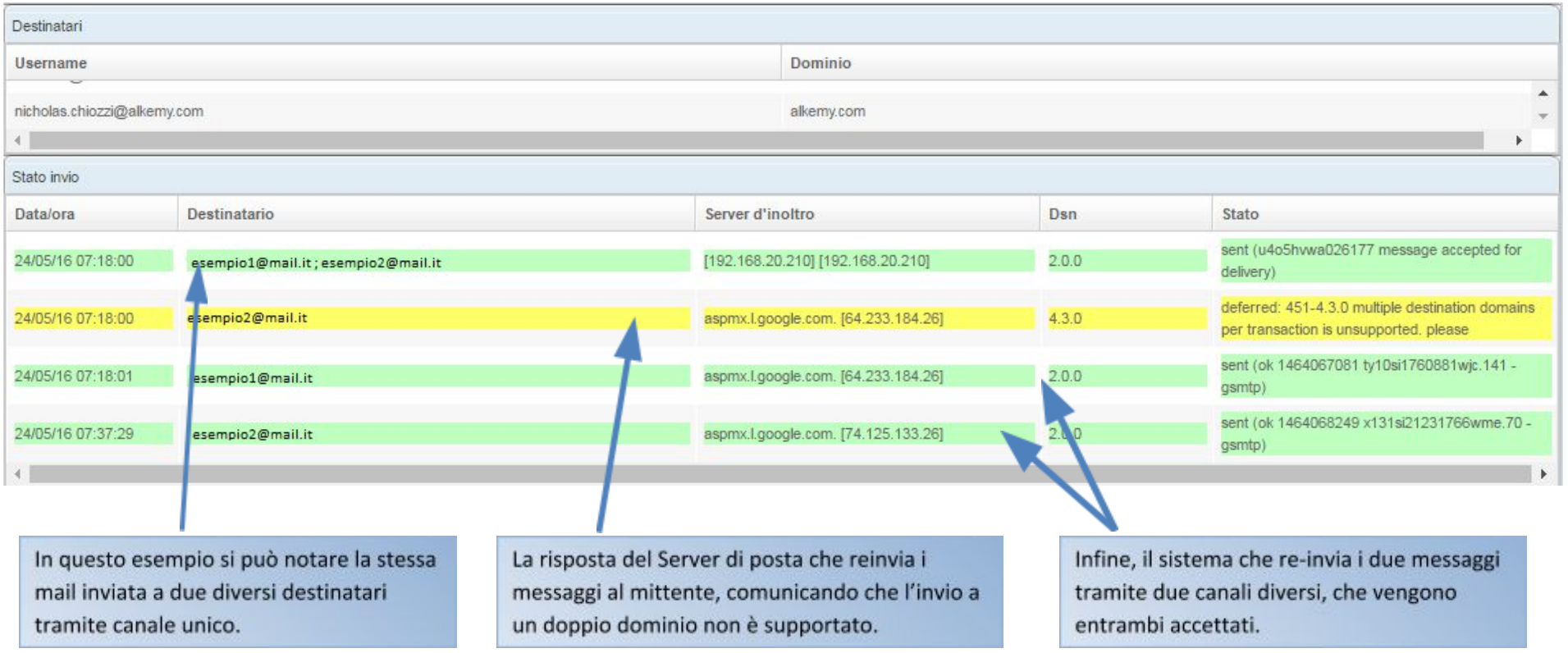
Metadefender è in grado di identificare la minaccia mediante quattro antivirus e di conseguenza viene indicato l'antivirus o gli antivirus che hanno dato esito positivo, ad es. **ESET,a variant of Win32/GenKryptik.DILP trojan;**, in questo caso l'antivirus che ha dato esito positivo è **ESET** e il nome della minaccia è "**a variant of Win32/GenKryptik.DILP"** e si tratta di una minaccia di tipo "**trojan**"

Metadefender è in grado di identificare i file non controllabili o pericolosi è lo indica come segue: **Password Protected Document**

Nel dettaglio delle analisi di metadefender è anche indicato il nome dell'allegato analizzato e l'ID dell'analisi (richiamabile per successive analisi dall'appliance di Metadefender), ad es.: "**attach=Purchase Order.rar - id=f5ea86962c9942de934eeb84915a31fd - result=ESET, a variant of Win32/GenKryptik.DILP trojan;**"

Sotto **risultato dei filtri** vengono visualizzate altre due sezioni:

- **Destinatari**: elenco dei destinatari dell'email
- **Stato invio**: in cui viene riassunto il percorso effettuato dall'email.
  Viene indicata l'ora di Invio, il destinatario, il server di inoltro e lo stato dell'invio (il quale influenza anche il colore della riga, che sarà verde per le email correttamente consegnate, gialle per le email sospese e rosso per quelle rifiutate).



Le righe evidenziate in giallo indicano problemi temporanei che potrebbero risolversi, quindi il sistema ritenterà l'invio dopo un tempo che dipende da diversi fattori, mentre una riga evidenziata in rosso indica un errore definitivo, quindi non risolvibile (ad es. destinatario inesistente), in questo caso il sistema non tenterà nuovamente di consegnare l'email ed invierà una comunicazione al mittente indicandogli la tipologia del problema.

La tipologia dell'errore non è sempre chiara, viene generata dal server destinatario dell'email, un esempio molto frequente è "Service unavailable", potrebbe indicare un problema di funzionamento del server destinatario o più tipicamente una dimensione eccessiva dell'email.

Le sezioni seguenti non sempre sono visualizzate, e sono:

- Operazioni richieste
- URL
- Allegati
- Zimbra Log
- Mailbox Log

Nella sezione denominata "Operazioni richieste" sono elencate le operazioni effettuate sull'email.

Stato invio

Data/ora	Destinatario	Server d'inoltro	Dsn	Stato
22/05/16 23:31:42	mbruse@zimbra-solutions.com			quarantined
22/05/16 23:37:31	mbruse@zimbra-solutions.com	[192.168.20.66] [192.168.20.66]	2.0.0	sent (ok: queued as 7060d185aa8)

Operazioni richieste

Data richiesta	Richiedente	Operazione
22/05/16 23:33:22	mbruse@bls.it	rilascia

Nell'esempio, si può vedere come per l'email, messa in Quarantena dal sistema, sia stata poi richiesto il rilascio dall'utente.

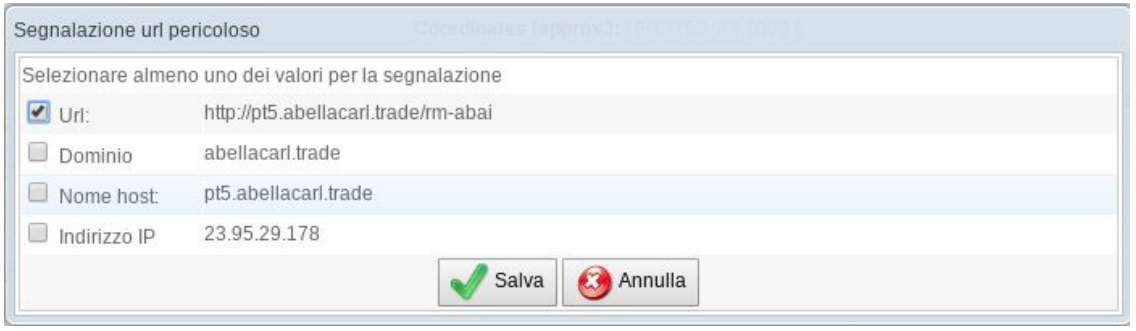
Alcune di queste operazioni sono automatiche, in questo caso nella colonna richiedente viene visualizzato "automatic", ad es. il rilascio di delle email delayed o la rimozione delle email già consegnate e successivamente identificate come pericolose (post delivery threat remove.)

Nella sezione denominata “URL” sono elencate le eventuali URL (indirizzi web) presenti nell’email.
Questa sezione viene visualizzata solo se è attiva la licenza “Advanced security”.

Se l’URL è ritenuta pericolosa, o lo sono il nome host (nell’esempio pt5.abellacarl.trade) o il dominio (nell’esempio abellacarl.trade) o l’indirizzo IP corrispondente all’hostname, allora l’URL viene evidenziata in rosso.

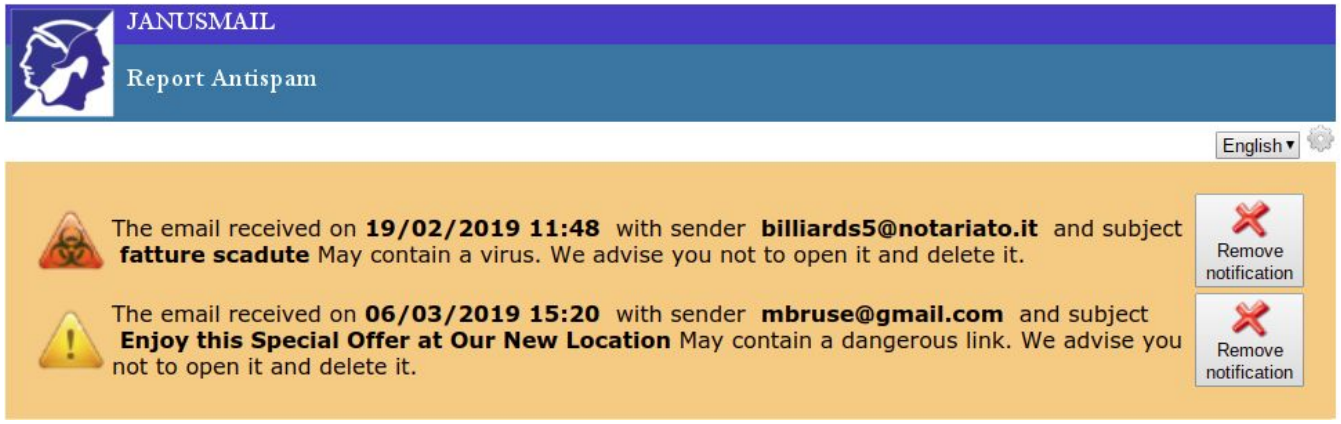
Nella colonna stato è indicato quale sezione dell’URL è ritenuta pericolosa (URL, Nome Host, Dominio, Indirizzo IP) ed eventualmente il motivo (ad es. phishing, fraud, involved in spam, malware, ecc.). Se non è indicato il motivo (viene visualizzato un trattino “-”) è perché è stato segnalato pericoloso da un amministratore e per garantire la privacy non viene visualizzato il nome.

Se l’utente è un amministratore e vuole segnalare un URL come pericoloso può cliccare sul triangolo giallo di pericolo.
Sarà possibile segnalare quali sezioni del URL vanno considerate pericolose spuntandole nel riquadro che apparirà:

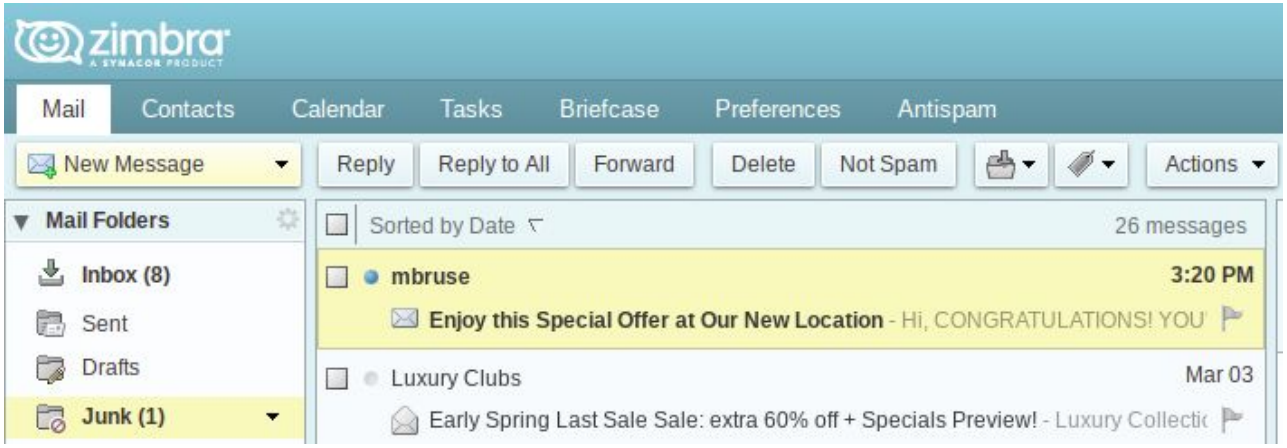


Successivamente viene visualizzato l’elenco delle email già ricevute che contengono lo stesso URL per permettere eventualmente di avvisare gli utenti.

Le eventuali email consegnate con lo stesso URL verranno anche segnalate all'utente nella testata del report antispam (descritto in seguito):



Inoltre se è attiva la licenza "Zimbra advanced" l'email verrà spostata dopo pochi secondi nella cartella "Posta indesiderata" (funzione post-delivery threat remove):



L’operazione di spostamento della email viene chiaramente registrata nelle operazioni e nel log della mailbox:

Mailbox LOG

Server	Data/ora	Casella	id	operazione	descrizione
bls-zimbrastore02	2019-03-06 15:20:40.0	mbruse@bls.it	904369	Adding Message	Adding message to Inbox folder
bls-zimbrastore02	2019-03-06 17:11:24.0	mbruse@bls.it	904369	moving Message	webmail moving Message to Folder Junk (id=4)

Operazioni richieste

Data richiesta	Richiedente	Operazione
06/03/2019 17:10:20	automatic	post-delivery threat remove

Nella sezione denominata “Allegati” sono elencati eventuali allegati presenti nella email. Questa sezione viene visualizzata solo se è attiva la licenza “Advanced security”.

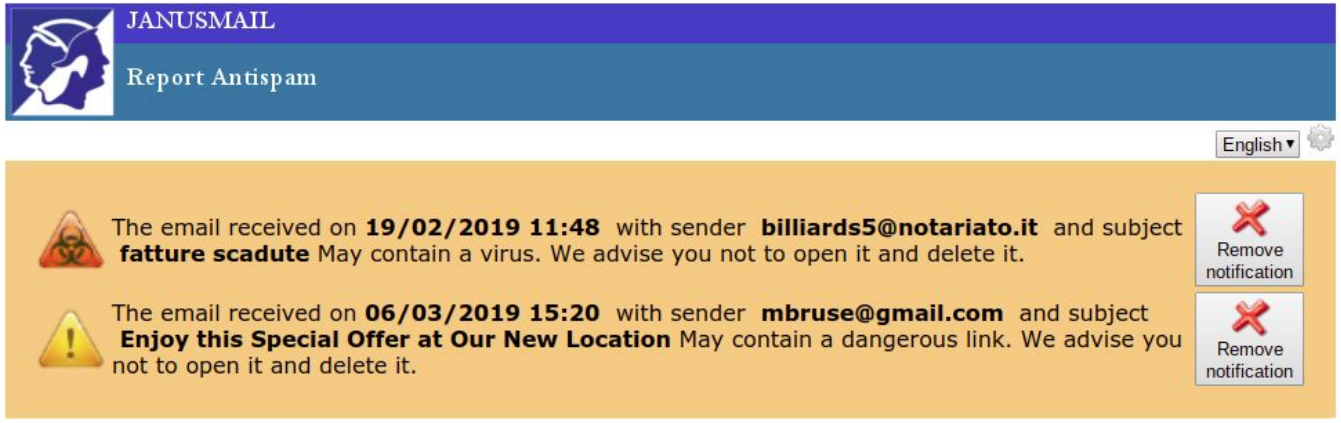
Se l’allegato è ritenuto pericoloso allora viene evidenziato in rosso.

Nella colonna stato viene indicata la fonte dell’informazione (ad es. Metadefender, Alienvault, Yara, ecc.) tranne se l’allegato è stato segnalato pericoloso da un amministratore e per garantire la privacy non viene visualizzato il nome (viene visualizzato un trattino “-”).

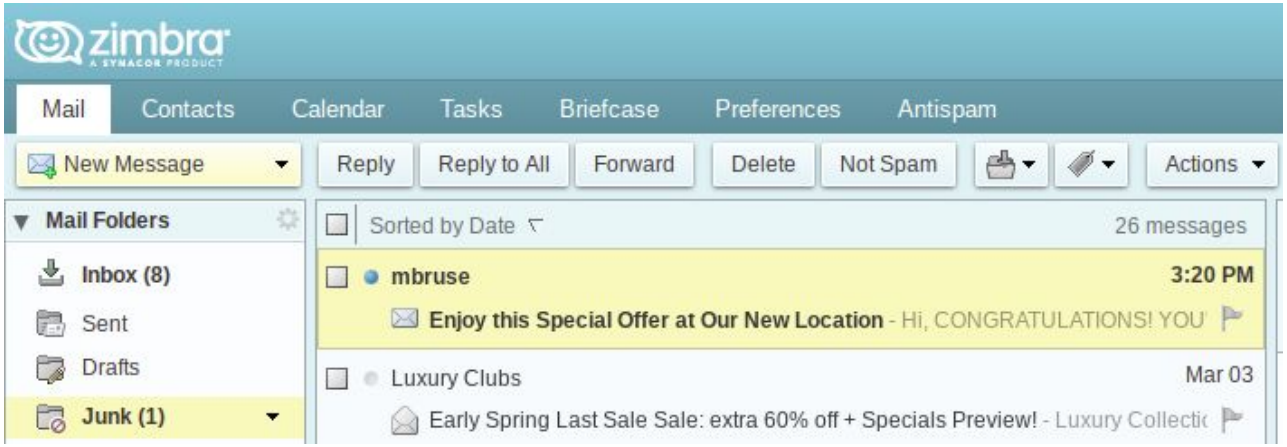
Se l’utente è un amministratore e vuole segnalare un allegato come pericoloso può cliccare sul triangolo giallo di pericolo.

Successivamente viene visualizzato l’elenco delle email già ricevute che contengono lo stesso allegato per permettere eventualmente di avvisare gli utenti.

Le eventuali email consegnate con lo stesso allegato verranno segnalate anche all’utente nella testata del report antispam (descritto in seguito):



Inoltre, se è attiva la licenza “Zimbra advanced”, l’email verrà dopo pochi secondi spostata nella cartella “Posta indesiderata” (funzione **post-delivery threat remove**):



L’operazione di spostamento della email è chiaramente registrata nelle operazioni e nel log della mailbox:

Mailbox LOG

Server	Data/ora	Casella	id	operazione	descrizione
bls-zimbrastore02	2019-03-06 15:20:40.0	mbruse@bls.it	904369	Adding Message	Adding message to Inbox folder
bls-zimbrastore02	2019-03-06 17:11:24.0	mbruse@bls.it	904369	moving Message	webmail moving Message to Folder Junk (id=4)

Operazioni richieste

Data richiesta	Richiedente	Operazione
06/03/2019 17:10:20	automatic	post-delivery threat remove

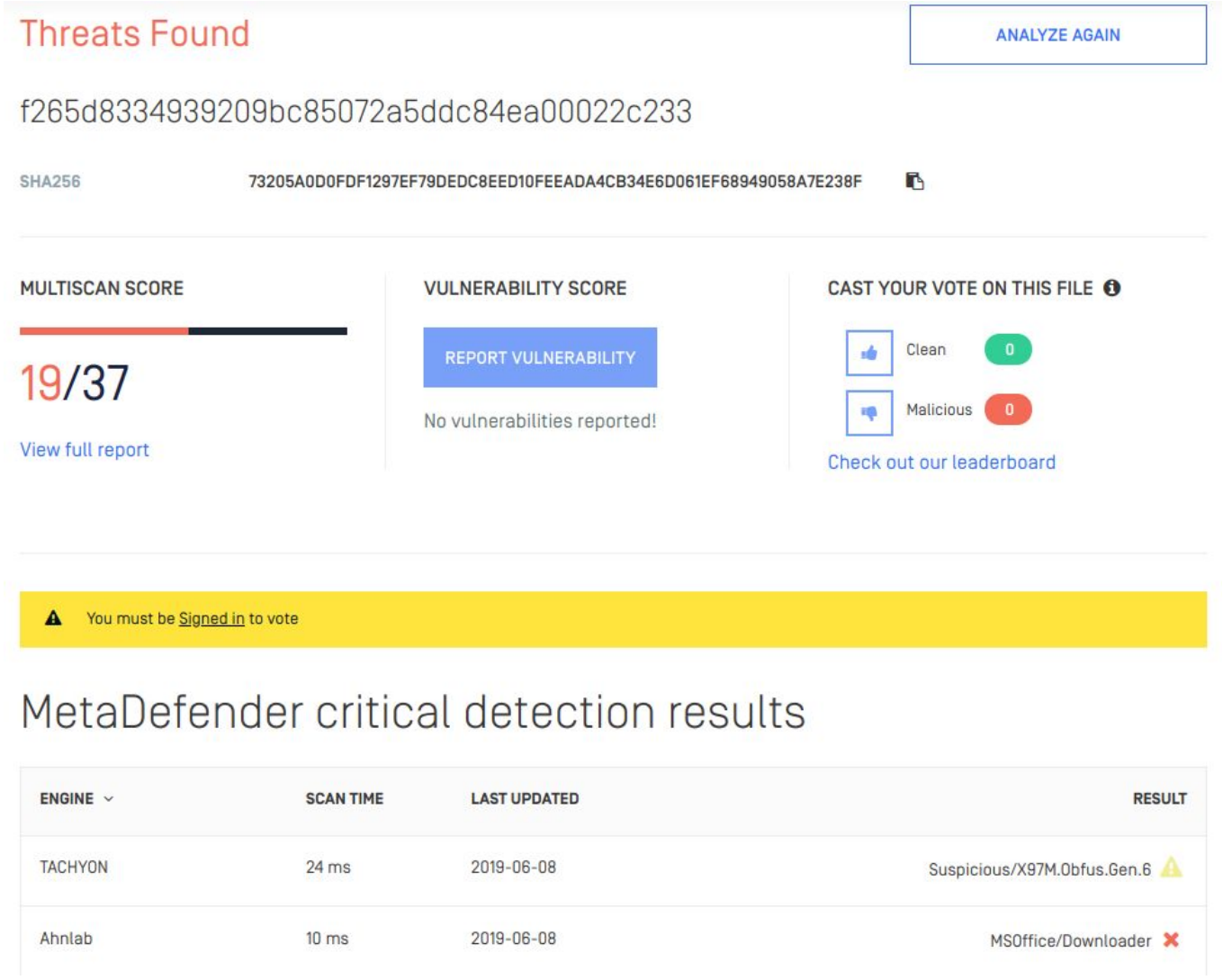
Cliccando invece su una delle prime quattro icone seguenti:

vengono visualizzate rispettivamente le pagine di:

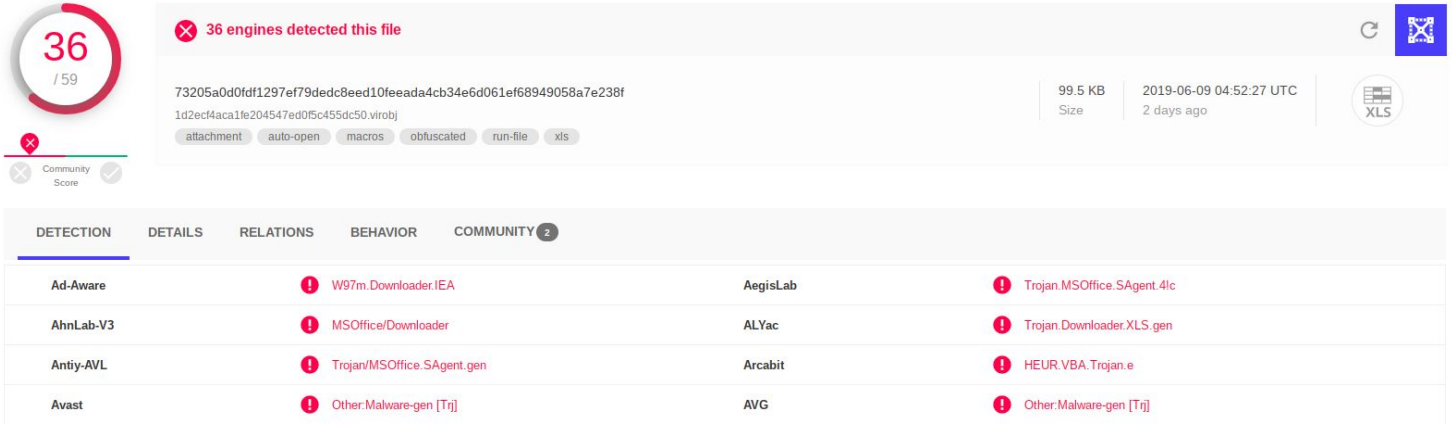
- Metadefender
- Virustotal
- Joe Sandbox
- Falcon Sandbox

Se l'hash corrisponde a quello di un file già controllato verranno visualizzati i risultati delle analisi, ciò vi permetterà di analizzare un allegato sospetto e capire se è già stato classificato come malware.

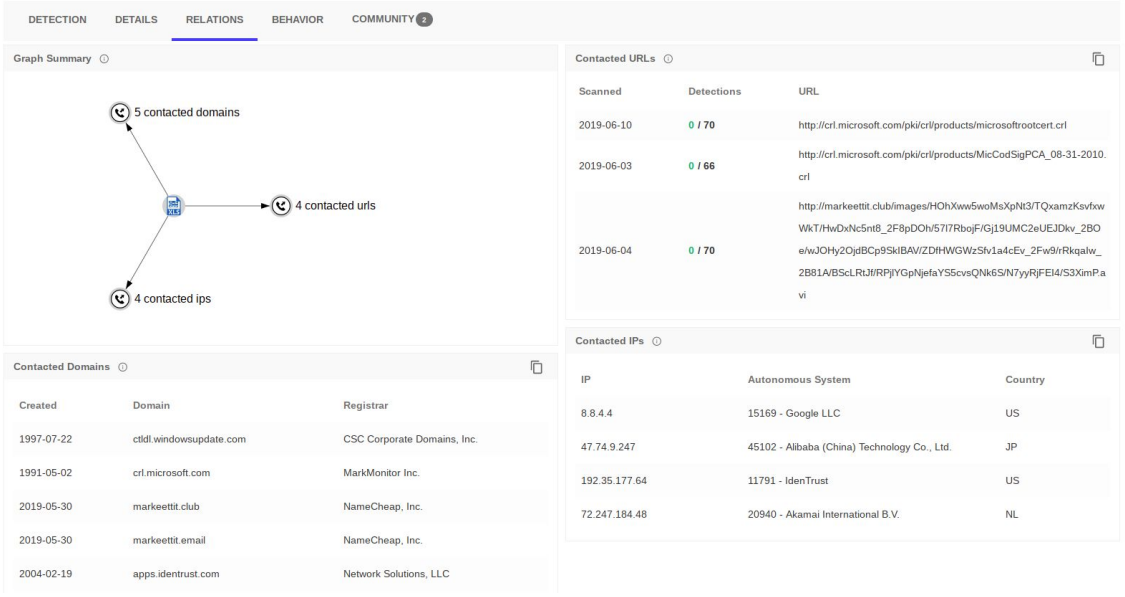
Nella pagina di Metadefender vengono visualizzati quanti antivirus hanno identificato un malware, se il file è vulnerabile e se la comunità ha dato dei punteggi positivi o negativi sul file:



Virustotal da delle informazioni simili:

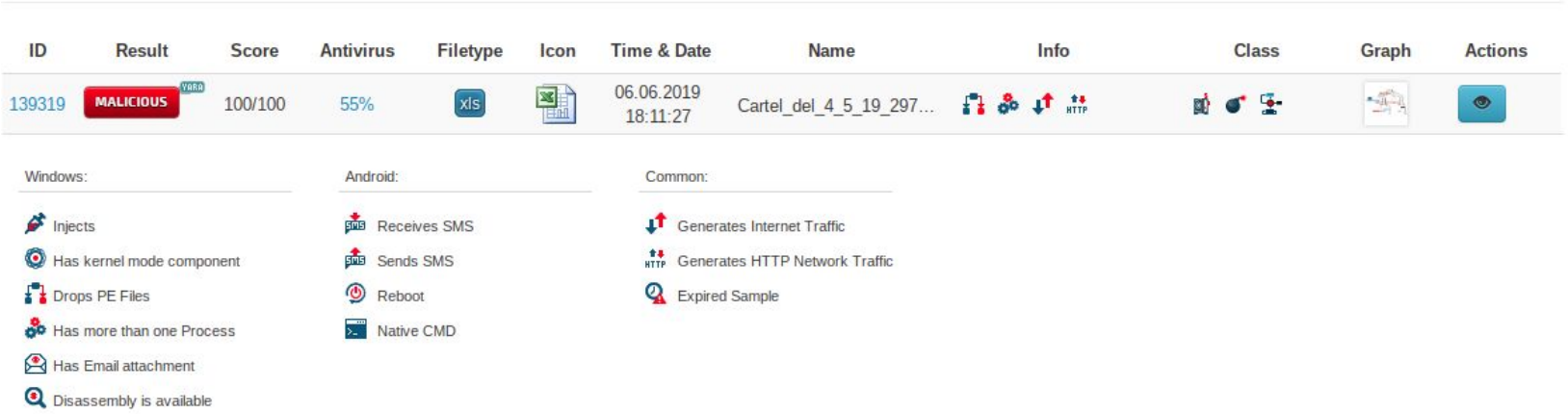


Inoltre in relations si possono vedere siti, domini e indirizzi ip acceduti dal malware:

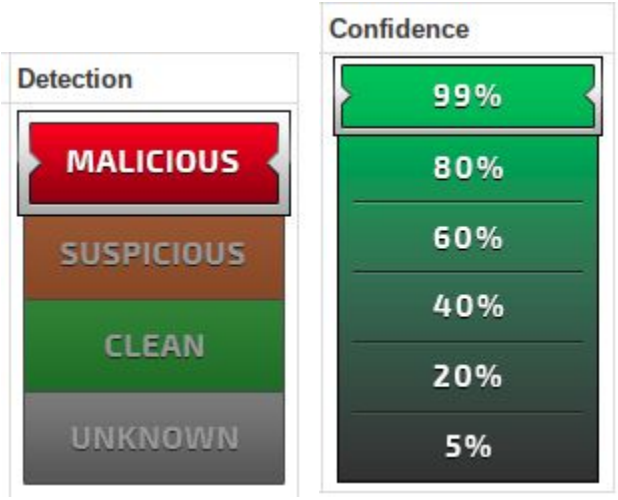


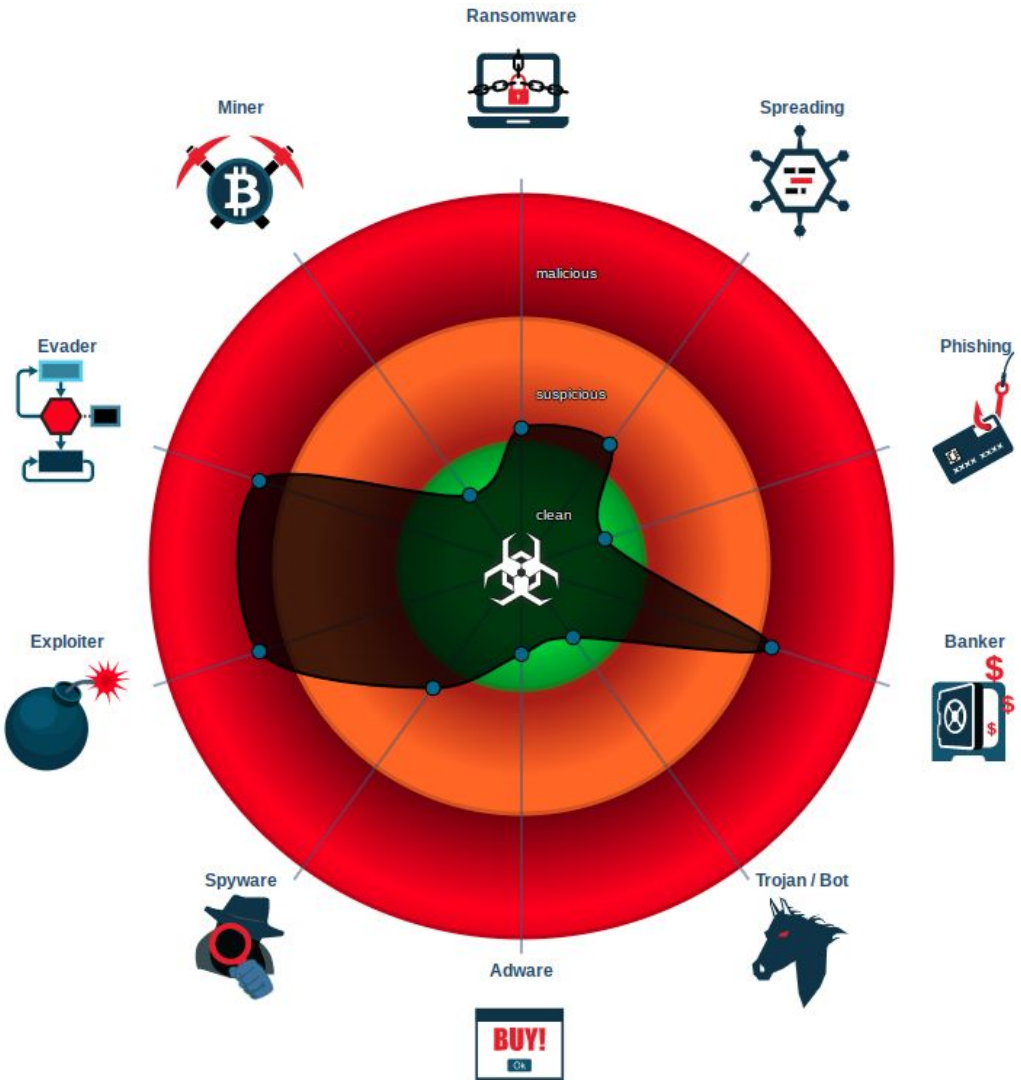
Le sandbox sono dei sistemi che simulano l'apertura del malware su un computer e verificano se hanno dei comportamenti sospetti, quindi anche se non è ancora riconosciuto dagli antivirus può essere riconosciuto come malware.

Joe Sandbox visualizza le analisi fatte ed il risultato:

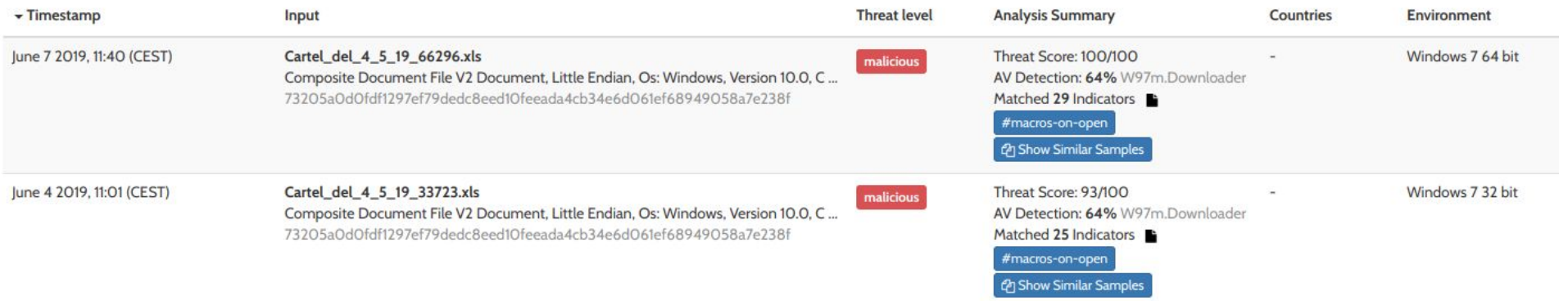


Cliccando sull'ID si accede all'analisi dettagliata dove tra l'altro viene visualizzato il risultato dell'analisi, il livello di confidenza e la classificazione:




Ransomware
Miner
Spreading
malicious
Evader
Phishing
suspicious
clean
Exploiter
Banker
Spyware
Trojan / Bot
Adware
BUY!

Falcon Sandbox è molto simile:

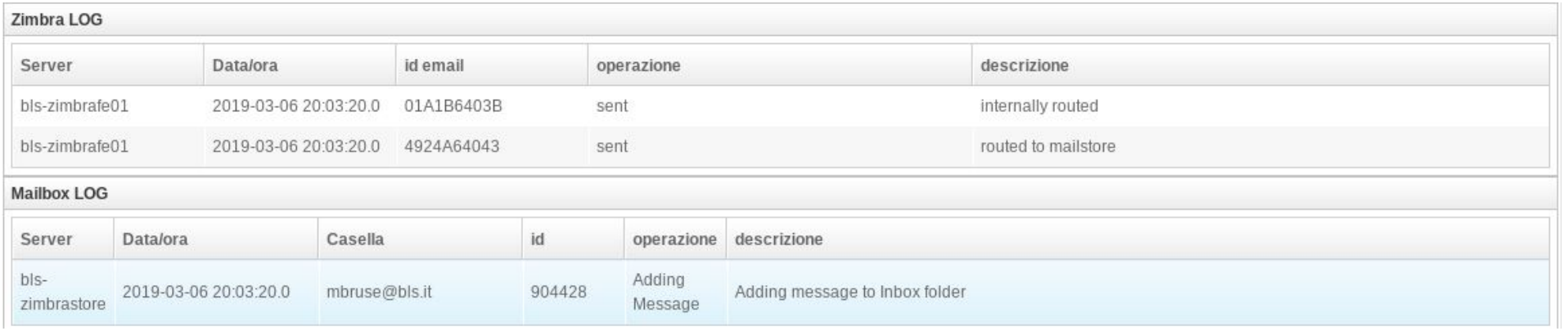


Riassumendo le prime due icone visualizzano il risultato fornito da decine di antivirus, mentre la terza e la quarta delle simulazioni di apertura dell'allegato.

Notare che la privacy è garantita in quanto l'unica informazione passata a questi siti è l'hash indicato nella stessa riga e che identifica univocamente il malware.

Se è attiva la licenza "**Zimbra advanced**" nel dettaglio email vengono visualizzate le sezioni:

- **Zimbra LOG**: riporta i log di ricezione e smistamento della email sul/sui server Zimbra
- **Mailbox LOG**: riporta le operazioni effettuate sull'email sul server Zimbra



Zimbra LOG

Server	Data/ora	id email	operazione	descrizione
bls-zimbrafe01	2019-03-06 20:03:20.0	01A1B6403B	sent	internally routed
bls-zimbrafe01	2019-03-06 20:03:20.0	4924A64043	sent	routed to mailstore

Mailbox LOG

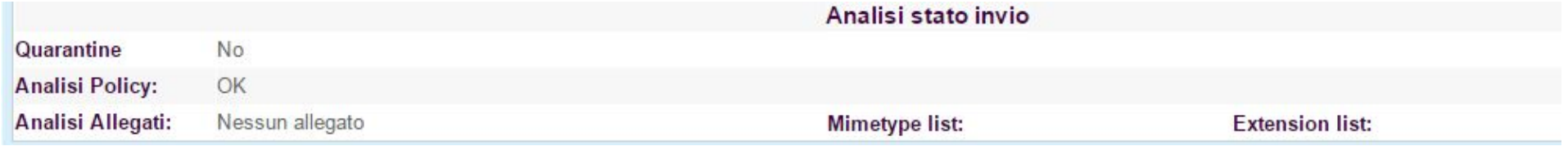
Server	Data/ora	Casella	id	operazione	descrizione
bls-zimbrastore	2019-03-06 20:03:20.0	mbruse@bls.it	904428	Adding Message	Adding message to Inbox folder

Ciò permette di tracciare l'email fino alla casella dell'utente, visualizzando inoltre le eventuali operazioni effettuate (cancellazione email, spostamento nella cartella posta indesiderata o in altre cartelle, lettura/cancellazione email con protocollo POP3 o IMAP, ecc.) o eventuali errori di consegna (ad es. Message-ID duplicato).

Per privacy ogni utente può controllare solo le proprie email/operazioni effettuate.

DETTAGLIO EMAIL STORICHE

Il dettaglio email per le email precedenti a Maggio/Giugno 2019 aveva un formato diverso da quello descritto, dopo i dati dell' email viene visualizzato l'analisi dello **stato di invi**o, per le email spedite, o dello **stato di ricezione**, per le email ricevute, come illustrato di seguito:



Analisi stato invio			
Quarantine	No		
Analisi Policy:	OK		
Analisi Allegati:	Nessun allegato	**Mimetype list:**	**Extension list:**

Nello stato di invio i dati visualizzati sono:

- quarantena (se l'email è stata inserita in una quarantena dal Mail Relay)
- esito dell'analisi delle policy, ovvero se l'email era in contrasto con alcune delle Policy implementate per l'invio
- esito dell'analisi degli allegati contenuti nella email e tipo di allegato

Analisi stato ricezione			
Quarantine	No		
Analisi Spam	is not spam	**Punteggio:** 2.40	**Test positivi:** INVALID_MSGID, RDNS_NONE
Analisi Malware	clean	**Dettagli:** Clean	
Reputazione mittente	**SPF check:** pass	**DKIM check:** none	**DMARC check:** none
Origine mittente	**Nazione:** FR	**Coordinates (approx.):** [2.3500,48.8600]	
Analisi Policy:	OK		
Analisi Allegati:	Num. 1	**Mimetype list:** application/x-msdownload	**Extension list:**

Nello stato di ricezione i dati visualizzati sono:

- esito delle analisi del sistema antispam, con punteggio di spam e test positivi. Se il punteggio è uguale o superiore al parametro "Livello spam" nella policy "Spam score policy", l'email viene considerata come probabile spam, se il punteggio è uguale o superiore al parametro "Livello highspam", l'email viene considerata certamente spam. Se invece l'email è compresa tra il "Livello spam" -1 e il "Livello spam" l'email viene considerata dubbia e la consegna viene ritardata (delayed email).
  Dopo il tempo "Ritardo email dubbie" il test antispam viene ri-eseguito, dando tempo alle blacklist ed altri database di aggiornarsi

- l’analisi del sistema anti-malware (virus, ransomware, trojan, ecc.) con i dettagli dell’esito (nell’esempio, Clean indica l’assenza di elementi pericolosi)
- l’analisi della reputazione del mittente con gli esiti del test SPF, DKIM e DMARC
- la nazione e le coordinate geografiche approssimative dell’origine dell’email (server che ha spedito l’email)
- esito dell’analisi delle policy, ovvero se l’email era in contrasto con alcune delle Policy implementate per la ricezione (tipicamente allegati pericolosi)
- esito dell’analisi degli allegati contenuti nell’email e tipo di allegato

Janusmail effettua diversi controlli antivirus mediante più di un sistema e usando diversi database di firme.
Nel campo details viene indicato quale database ha dato esito positivo (solamente il primo, in quanto Janusmail ottimizza i controlli e se un antivirus da esito positivo non perde tempo ad eseguire ulteriori controlli con altri).

Gli antivirus utilizzati sono

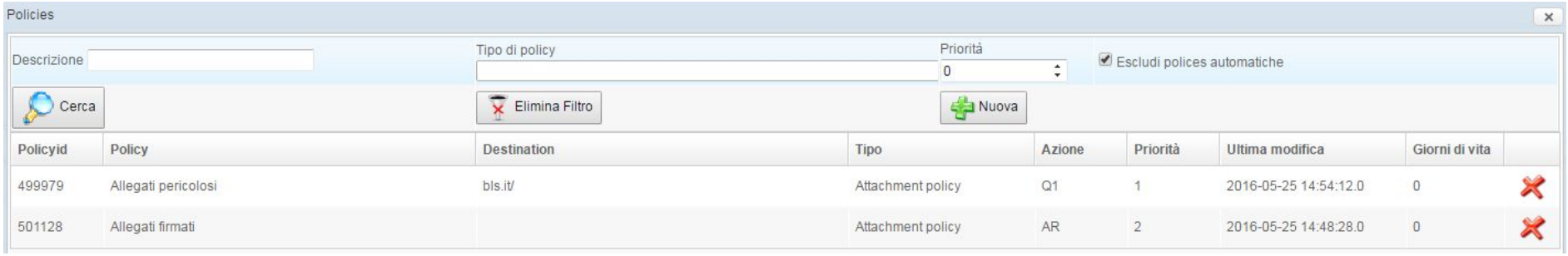
- **Clamav:** con tre diversi database di firme (quelli ufficiali con tasso di efficienza non superiore al 80%, SecuriteInfo e Sanesecurity lo aumentano ad oltre il 90%). In details troverete scritto “Infected“ e tra parentesi il database di firma che ha identificato il malware e la descrizione sintetica.
- **Sophos:** se avete attiva la licenza Sophos, in details troverete scritto “Infected” e tra parentesi “Sophos” e la descrizione sintetica del malware
- **Metadefender:** se avete attiva la licenza Strong security, in questo caso viene utilizzato un sistema multi-antivirus in parallelo che utilizza **ESET, Total Defense, Bitdefender** e **K7** quali motori antivirus, in details troverete scritto “Metadefender” e tra parentesi la descrizione sintetica del virus

POLICIES

Le POLICIES sono regole di accettazione ed esclusione delle email ricevute.

Una POLICY può essere generata automaticamente, quindi da meccanismi automatici del mailrelay, oppure manualmente, ovvero venire inserita dall'utente.

Per accedere alla schermata di gestione delle POLICIES, selezionare l'opzione dal menù funzioni.



La schermata che appare fornisce l'elenco delle Policies attive.
Le colonne contengono, nell'ordine, le seguenti informazioni:

- **Policyid**: Numero identificativo della Policy

- **Policy**: Il nome attribuito alla Policy.
  Se si tratta di una Policy automatica, il nome della Policy ne riassume le caratteristiche.
  Esempio: "whitelist from esempio1@esempiomail.it to user esempio2@esempiomail.it" è la dicitura standard delle Policy di aggiunta in Whitelist automatica.
  Vedremo nel paragrafo dedicato come vengono generate le Policies automatiche.

- **Destination**: Indica l'utente o il dominio per i quali è attiva la Policy

- **Tipo**: Indica la tipologia di Policy. Le tipologie e gli altri parametri sono descritti più avanti.

- **Azione**: Indica l'azione che il Mail Relay esegue sulla base della Policy impostata.

- **Priorità**: Definisce l'importanza della Policy nei confronti delle altre.

- **Ultima Modifica**: Indica la data e l'ora dell'ultima modifica effettuata alla Policy.

- **Giorni di Vita:** Indica per quanto la Policy rimarrà attiva.
  Questo indicatore esiste solamente nelle Policy automatiche, in quelle inserite manualmente risulterà sempre pari a 0 (cioè senza limite, quindi sempre attiva).

RICERCA POLICIES

Nella parte alta della schermata ci sono gli strumenti di ricerca delle Policies esistenti, nonché il tasto di creazione di Policies nuove.
La ricerca si esegue inserendo le voci desiderate nei vari campi e cliccando il tasto “cerca”.

Cliccando **Elimina Filtro** si eliminano gli effetti del filtro per Tipo di Policy.

Il campo **Priorità** permette di filtrare l’elenco in base alla priorità della Policy.

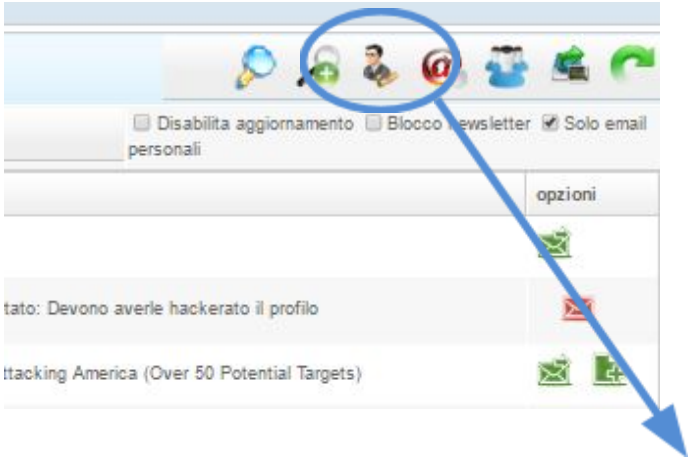
La spunta alla casella “**Escludi policies automatiche**” permette di vedere o escludere le Policies create automaticamente.

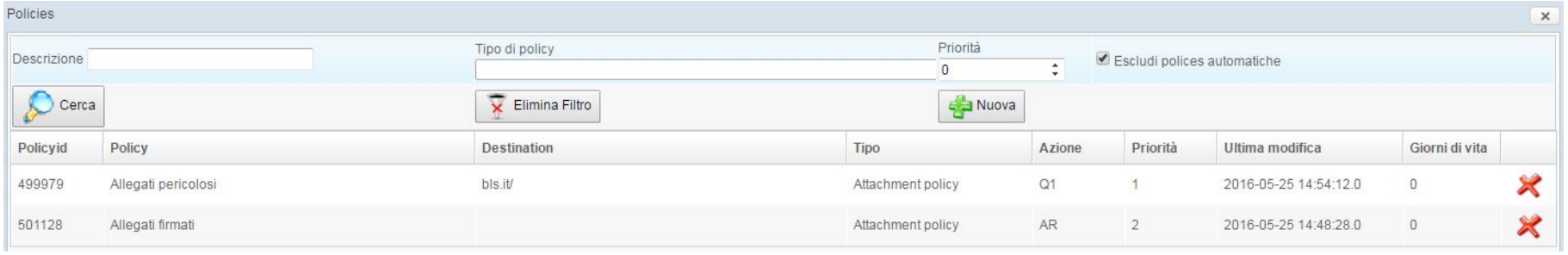
Tutti i filtri e la casella di ricerca sono sovrapponibili, ovvero è possibile inserire allo stesso tempo una priorità, un tipo di policy e una descrizione per ottenere i risultati che corrispondano a tutti i parametri.

INSERIMENTO MANUALE delle POLICIES

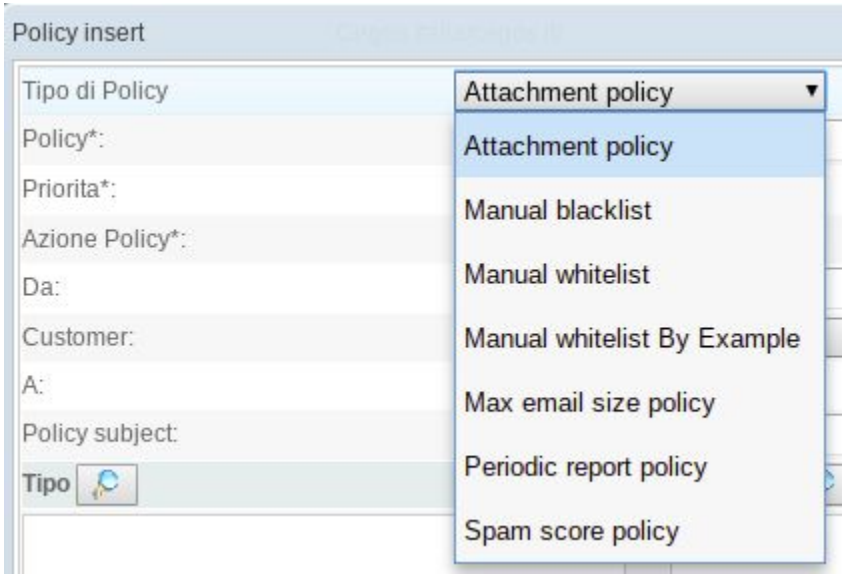
Le POLICIES possono venire inserite o eliminate solo dagli amministratori di Cliente o di Dominio.
L'amministratore di Cliente può decidere su quale dei suoi Domini impostarle.
Sia l'amministratore di Cliente che di Dominio possono impostare Policy sul singolo Utente.
Gli utenti non hanno diritto a impostare Policies, l'icona non è presente nelle loro Dashboard.

Per creare una nuova Policy si clicca il tasto "Nuova" nella schermata **POLICIES**, comparirà quindi la schermata **POLICY INSERT.**
Per eliminarle, basta cliccare l'icona a forma di "X" rossa a fianco di ogni Policy dell'elenco.





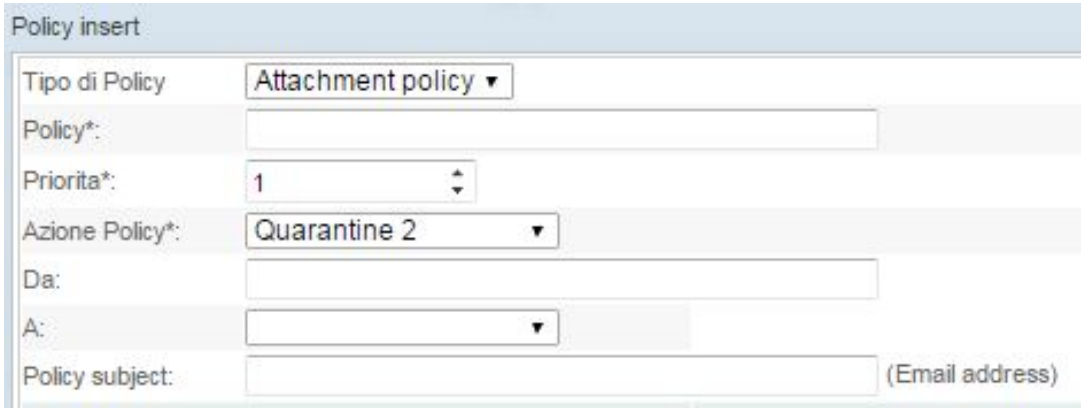
Il campo **Tipo di Policy** definisce la tipologia di policy:



Il **Tipo** può dunque essere:

- **Attachment policy** se la policy riguarda gli allegati
- **Manual blacklist** se si vuole aggiungere un indirizzo in Blacklist manualmente
- **Manual whitelist** se si vuole aggiungere un indirizzo in Whitelist manualmente
- **Manual whitelist by example** altra tipologia di whitelist, più flessibile
- **Max email size policy,** se si intende filtrare le mail in entrata e uscita in base alle dimensioni
- **Periodic report policy,** per schedulare l'invio periodico di report dettagliati sulle email filtrate da Janusmail
- **Spam score policy** se la policy riguarda la politica di classificazione delle email

Alcuni parametri sono comuni a tutte le Policy, e sono quelli indicati nella parte alta della schermata di inserimento.



- **POLICY,** è la descrizione della policy

- **PRIORITÀ,** molto importante per stabilire quale policy ha priorità rispetto ad un'altra.
  Infatti, quando le POLICIES intervengono, la gerarchia è stabilita dal livello di PRIORITÀ di ciascuna Policy.

  Si può, ad esempio, impostare una policy che permetta il passaggio di tutte le email con allegati firmati, e al contempo impostare una policy che imponga che le email con allegati pericolosi (ad es. file eseguibili) siano messe in quarantena.
  La prima Policy, avendo un'importanza bassa, dovrà avere priorità bassa, ad es. 2, mentre la seconda, essendo molto importante per la sicurezza, dovrà avere priorità elevata, ad es. 8.
  In questo esempio, un'email che avesse un allegato firmato ma potenzialmente pericoloso verrebbe accettata dalla prima Policy ma bloccata dalla seconda.
  Essendo quest'ultima dotata di priorità superiore, l'email sospetta verrebbe bloccata.

- **AZIONE POLICY** indica quale azione la Policy debba effettuare.
  Può essere:
  - **Allow Relay** (AR) che permette all'email di passare.
    Una categoria fra **Q1** e **Q9**, che indica in quale **Quarantena** conservare l'email in attesa.
    Le email in Quarantena possono essere rilasciate:
    - Tutte, dall'amministratore del cliente (quindi dalla Q1 alla Q9)
    - Dalla Q7 in giù dall'amministratore del dominio (quindi dalla Q1 alla Q7)
    - Dalla Q5 in giù dall'utente (quindi dalla Q1 alla Q5)
  - **Discard Email (DE)** che indica di scartare l'email.

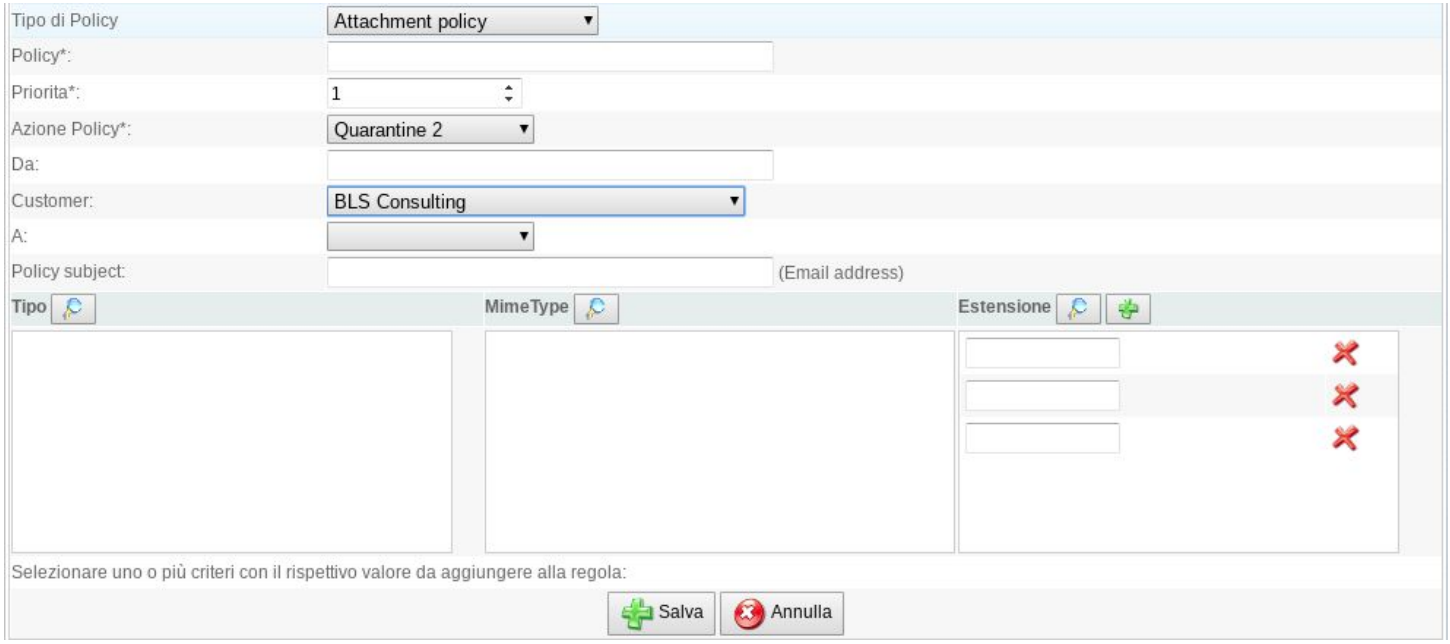
- **DA** indica l'indirizzo da cui l'email proviene.
  La policy verrà applicata alle email provenienti da quell'indirizzo.
  Se questo campo viene lasciato vuoto, vale per tutte le email che arrivano al Mail Relay.

- **A** indica il dominio verso cui l'email è indirizzata.
  Dall'elenco a tendina si può scegliere il dominio interessato tra tutti quelli che si hanno in gestione.
  Se si lascia vuoto questo campo, la Policy sarà valida per tutti i domini del cliente.

- **Policy Subject** è l'indirizzo email destinatario cui si applica la policy.
  Se questo campo viene lasciato vuoto, la policy viene applicata a tutto il dominio indicato al campo "**A**", o a tutte le email del cliente se il campo **"A"** non è stato specificato

ATTACHMENT POLICY

Le policy di questo tipo permettono di impostare regole sulla tipologia di allegati, i quali possono essere identificati per “Tipo”, “Mime Type” o “Estensione”.

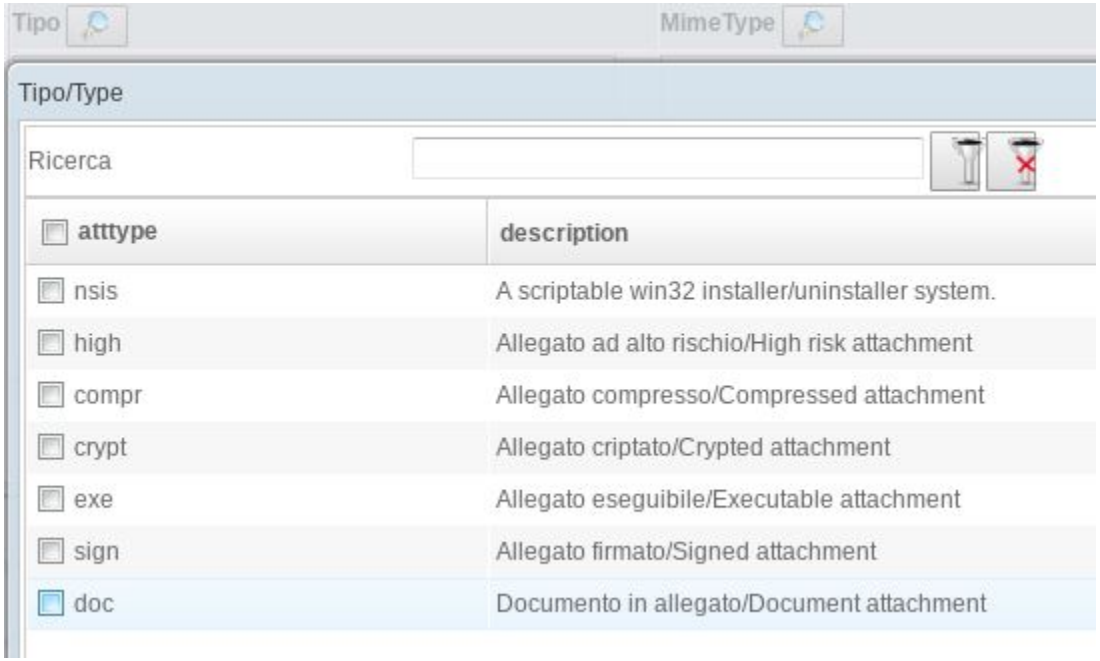


Janusmail implementa oltre 400 sistemi per identificare gli allegati nelle email.

Esistono infatti numerosi standard per allegare i files alle email, e vengono inoltre usate moltissime tecniche di elusione per mascherare la presenza di allegati all’interno delle email.

Se l’allegato è un file compresso, il controllo degli allegati viene esteso anche al contenuto del file compresso (Janusmail riconosce decine di sistemi di compressione).

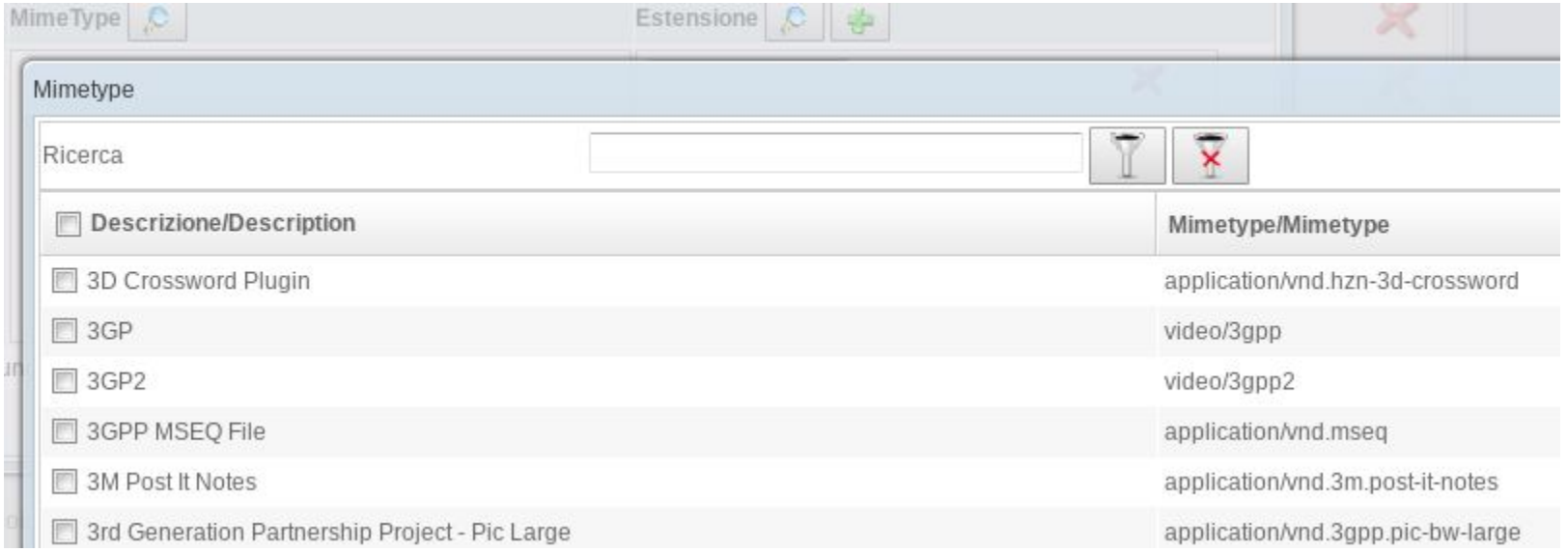
Il **filtro per "Tipo"** permette di identificare molto semplicemente le tipologie di allegato scelte tra le opzioni indicate:



Janusmail è in grado, con diversi meccanismi "intelligenti", di identificare la tipologia di allegato, ad esempio la tipologia "high", ovvero allegati ad alto rischio.

È inoltre in grado di identificare oltre 100 tipologie di file (Mime type, vedi in seguito) o estensioni di file ritenuti pericolosi.

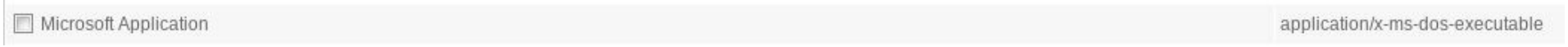
Il **filtro per "Mime Type"** permette filtrare per categoria/sottocategoria Mime (standard che identifica la tipologia di allegati):



Janusmail riconosce gli allegati non solo in base all'estensione, ma identificando il reale formato e quindi il tipo Mime.

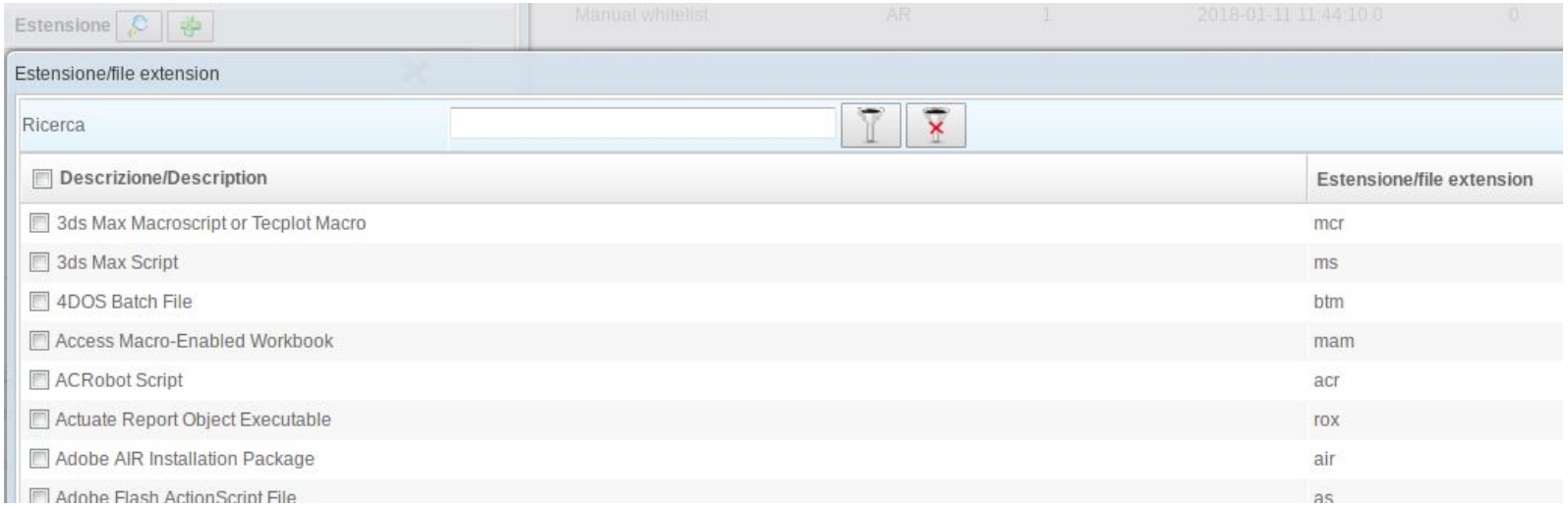
Ad esempio, un file eseguibile DOS/Windows per definizione inizia con i caratteri "MZ" (in altre parole un qualsiasi file che inizia per MZ verrebbe eseguito sotto Microsoft Windows), ma potrebbe avere una estensione completamente diversa, ad es. ".txt" (tipico sistema di elusione dei controlli).

Janusmail riconosce il file dal contenuto e lo classifica come:



indipendentemente dall'estensione del file.

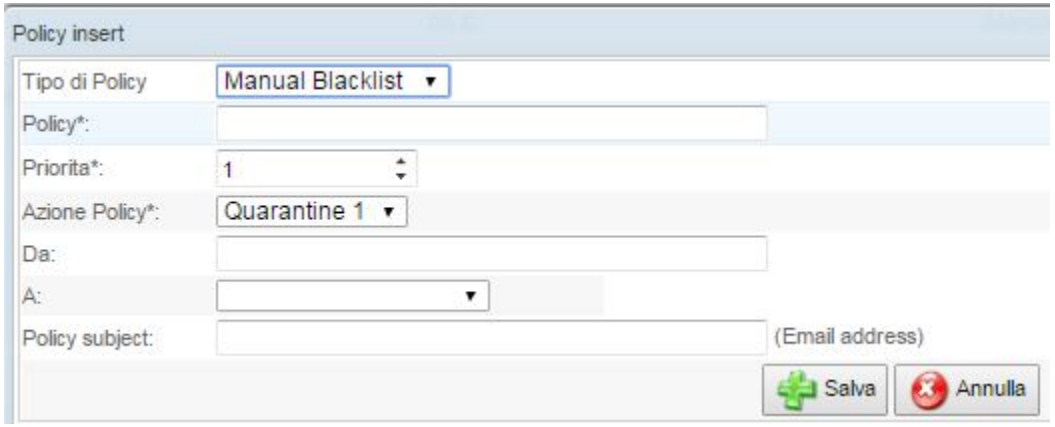
Il **filtro per "Estensione"** permette infine filtrare per l'estensione dell'allegato, è possibile indicare manualmente una estensione (inserendola nei campi sottostanti) o selezionarla dalla tabella delle principali estensioni (cliccando sul tasto lente di ingrandimento):



MANUAL BLACKLIST

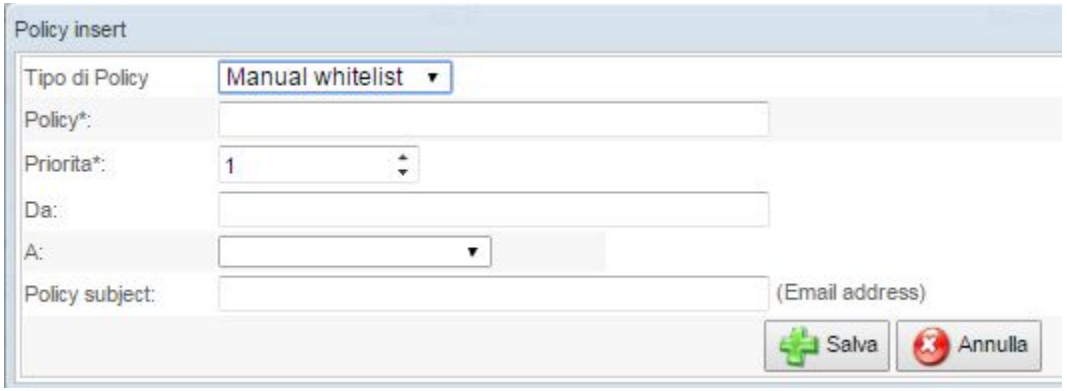
Questo tipo di policy serve a bloccare le email in base al mittente e al/ai destinatari.

Dopo aver assegnato un **Nome** alla Policy e averne impostato la **Priorità,** si sceglie tramite **Azione Policy** se eliminarle del tutto o inviarle a una quarantena.
Gli altri campi **DA, A e Policy Subject** mantengono le stesse caratteristiche indicate nel capitolo **Inserimento Manuale delle Policies**.



MANUAL WHITELIST

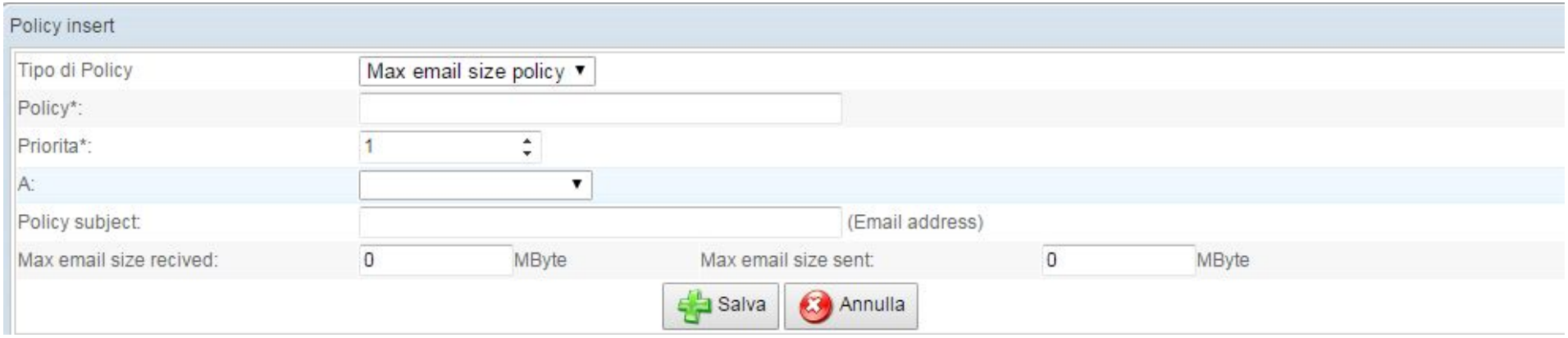
Questo tipo di policy serve a evitare che un'email venga bloccata.
È sufficiente assegnare un **Nome** alla Policy e impostarne la **Priorità**.
Gli altri campi, **DA, A e Policy Subject,** mantengono le stesse caratteristiche indicate nel capitolo **Inserimento Manuale delle Policies**.



MAX EMAIL SIZE POLICY

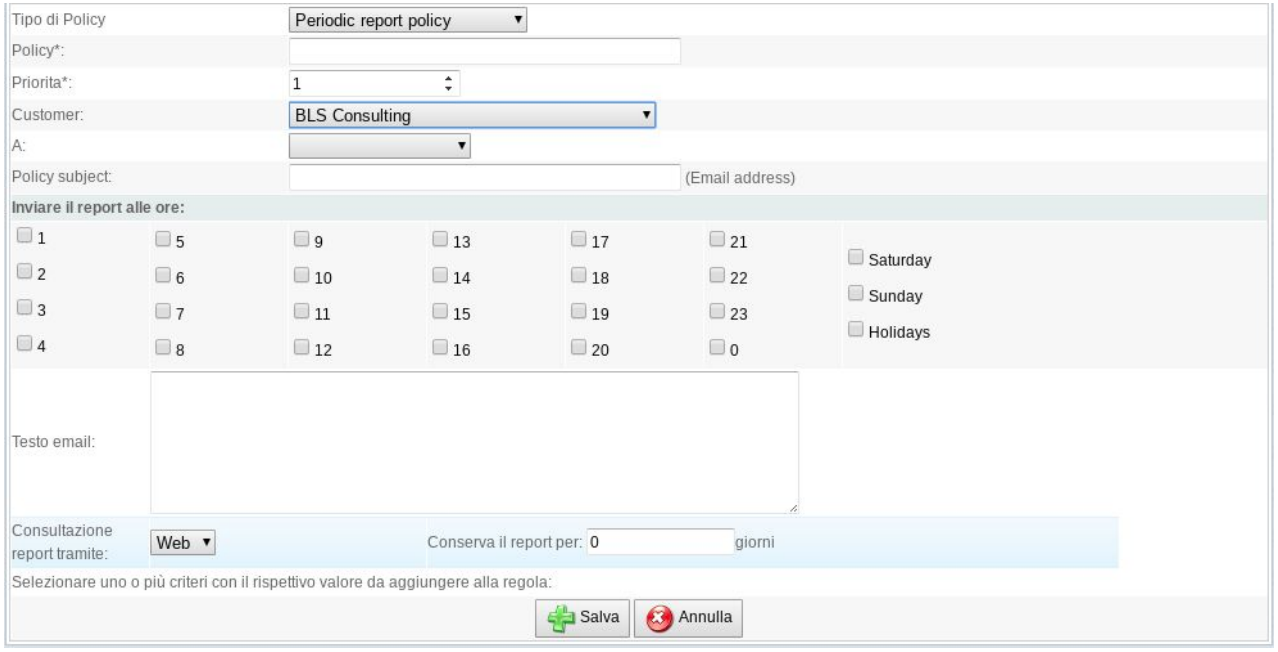
Questa Policy serve a impedire la ricezione o l'invio di email di dimensione troppo elevata.
Nei campi **Max email size received** e **Max email size sent** si impostano le dimensioni oltre le quali le email non verranno accettate, o nel caso di email in uscita, inviate.

Il mittente riceverà immediatamente una notifica che spiegherà l'impossibilità di spedire l'email.



PERIODIC REPORT POLICY

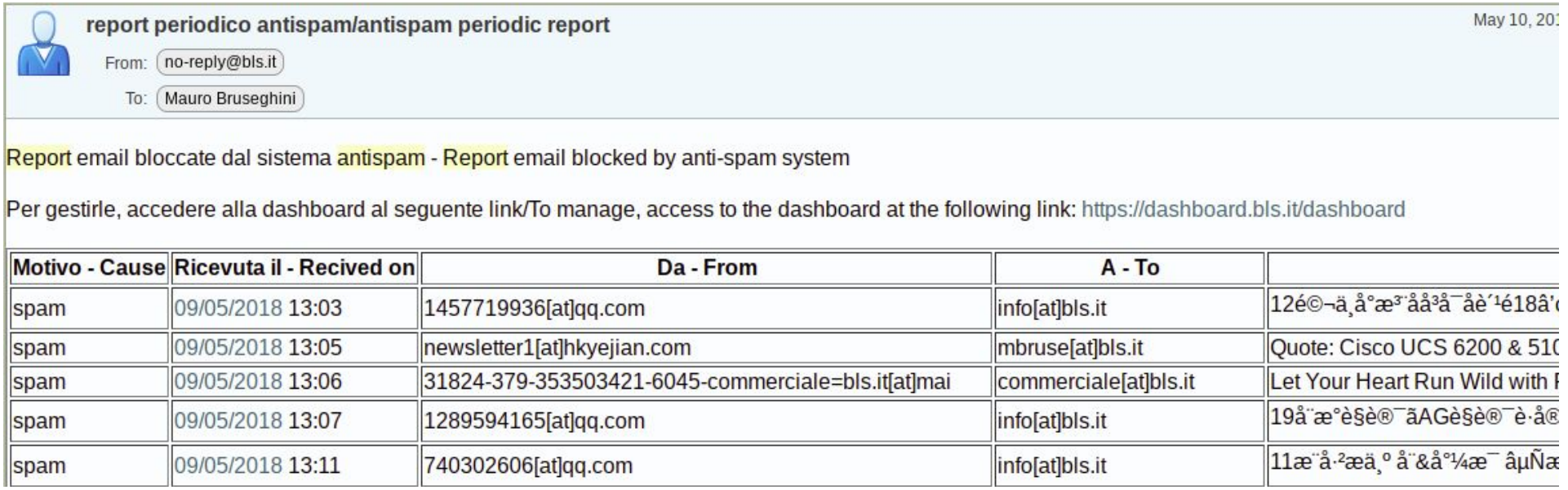
Con questa Policy si configura l'invio periodico di un Report Statistico sulle email inviate e ricevute dall'utente, dai suoi alias e dalle liste in cui il suo indirizzo è presente.
Il Report verrà inviato in orari configurabili nella policy spuntando la casella corrispondente.
Si può inoltre scegliere di ricevere il report anche nei giorni festivi, spuntando le relative caselle **Saturday**, **Sunday** o **Holidays**, sempre nelle ore impostate.



È possibile personalizzare il testo della email inviata, lasciare vuoto il parametro "Testo email" per un testo standard predefinito.

È poi possibile selezionare se il report è consultabile direttamente nell'email oppure via web.

Nel caso di consultazione via email, nel corpo dell'email è riportato l'elenco delle email bloccate:



report periodico antispam/antispam periodic report

May 10, 20

From: no-reply@bls.it

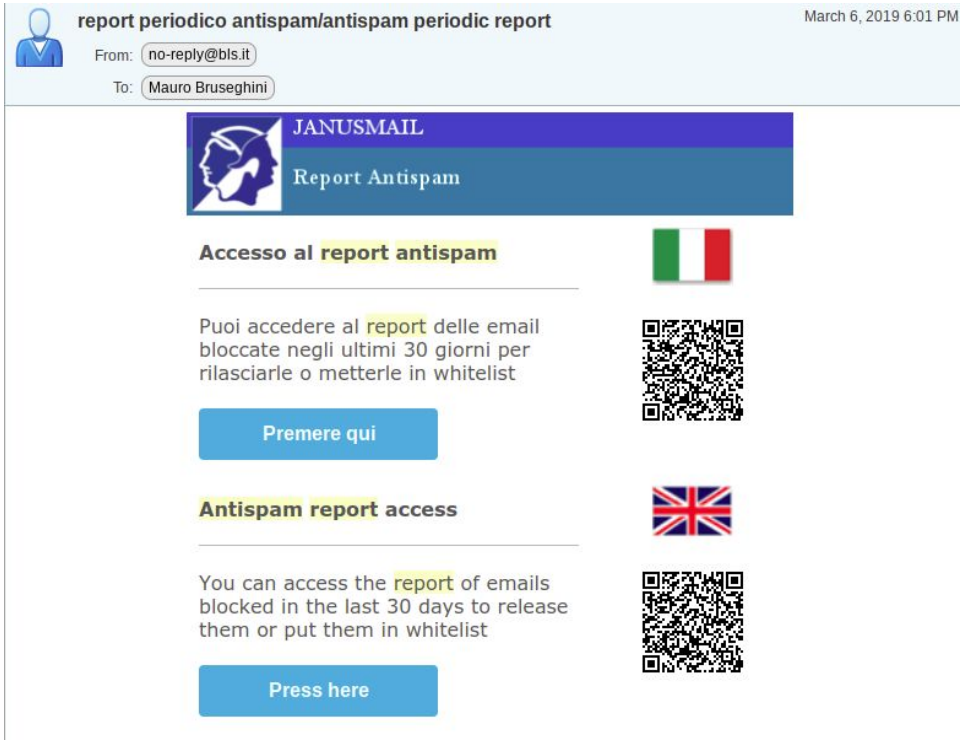
To: Mauro Bruseghini

Report email bloccate dal sistema antispam - Report email blocked by anti-spam system

Per gestirle, accedere alla dashboard al seguente link/To manage, access to the dashboard at the following link: https://dashboard.bls.it/dashboard

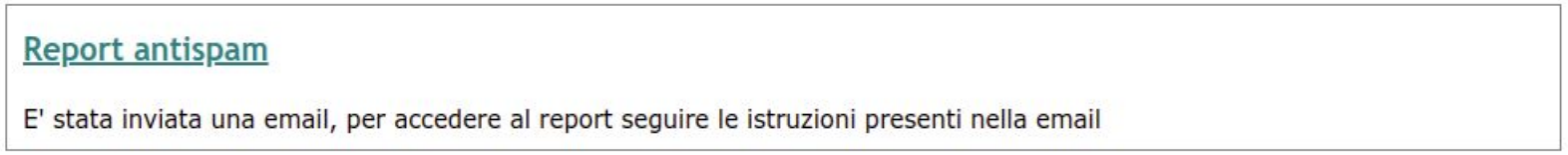
Motivo - Cause	Ricevuta il - Recived on	Da - From	A - To	
spam	09/05/2018 13:03	1457719936[at]qq.com	info[at]bls.it	12é©¬ä¸å°æ³¨åå³å¯¨è´¹é18â'(
spam	09/05/2018 13:05	newsletter1[at]hkyejian.com	mbruse[at]bls.it	Quote: Cisco UCS 6200 & 51(
spam	09/05/2018 13:06	31824-379-353503421-6045-commerciale=bls.it[at]mai	commerciale[at]bls.it	Let Your Heart Run Wild with F
spam	09/05/2018 13:07	1289594165[at]qq.com	info[at]bls.it	19å¨æ°è§è®¯ãAGè§è®¯è·å®
spam	09/05/2018 13:11	740302606[at]qq.com	info[at]bls.it	11æ¨å·²æä¸ºå¨&å°¼æ¯ âµÑæ

Nel caso di consultazione via web verrà inviata una email che permetterà di accedere al report via web:



È anche possibile accedere al report da Smartphone usando il QR Code.

La prima volta che si accede al report antispam da un PC o uno smartphone viene visualizzato quanto segue:

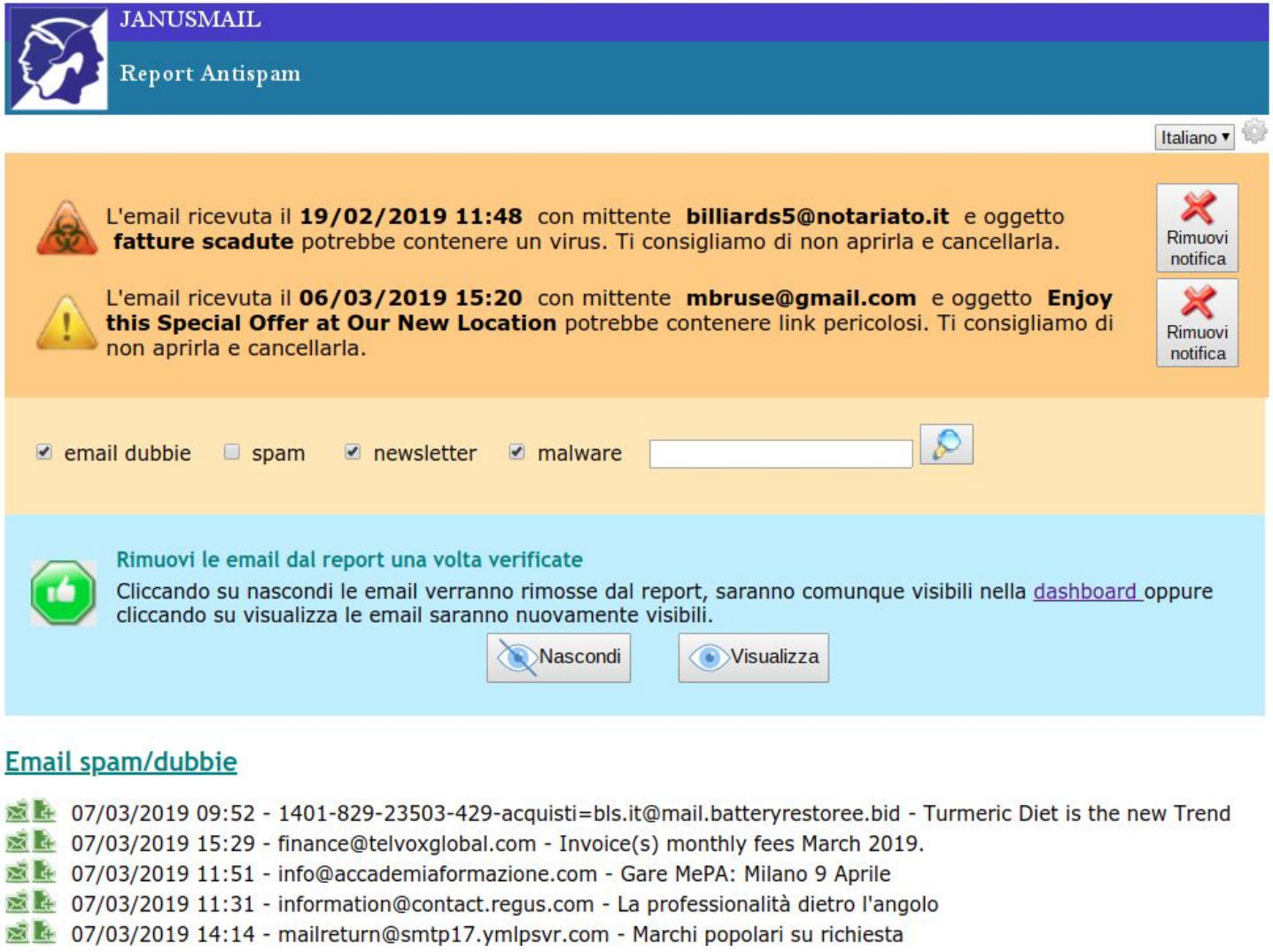


ed inviata una email per confermare l'accesso:

Premendo questo pulsante sarà possibile accedere solo a questo report dal PC che si sta usando, per visualizzare un altro report sarà necessario ripetere questa procedura.

Premendo questo pulsante sarà possibile accedere a questo report ed ai successivi report da questo pc senza dovere ripetere questa procedura. Utilizzare questa opzione dal proprio PC o smartphone. Questa opzione comporta l'uso di un cookie memorizzato sul browser del PC/smartphone utilizzato per riconoscere l'utente.

Questo è un esempio del report antispam via web:

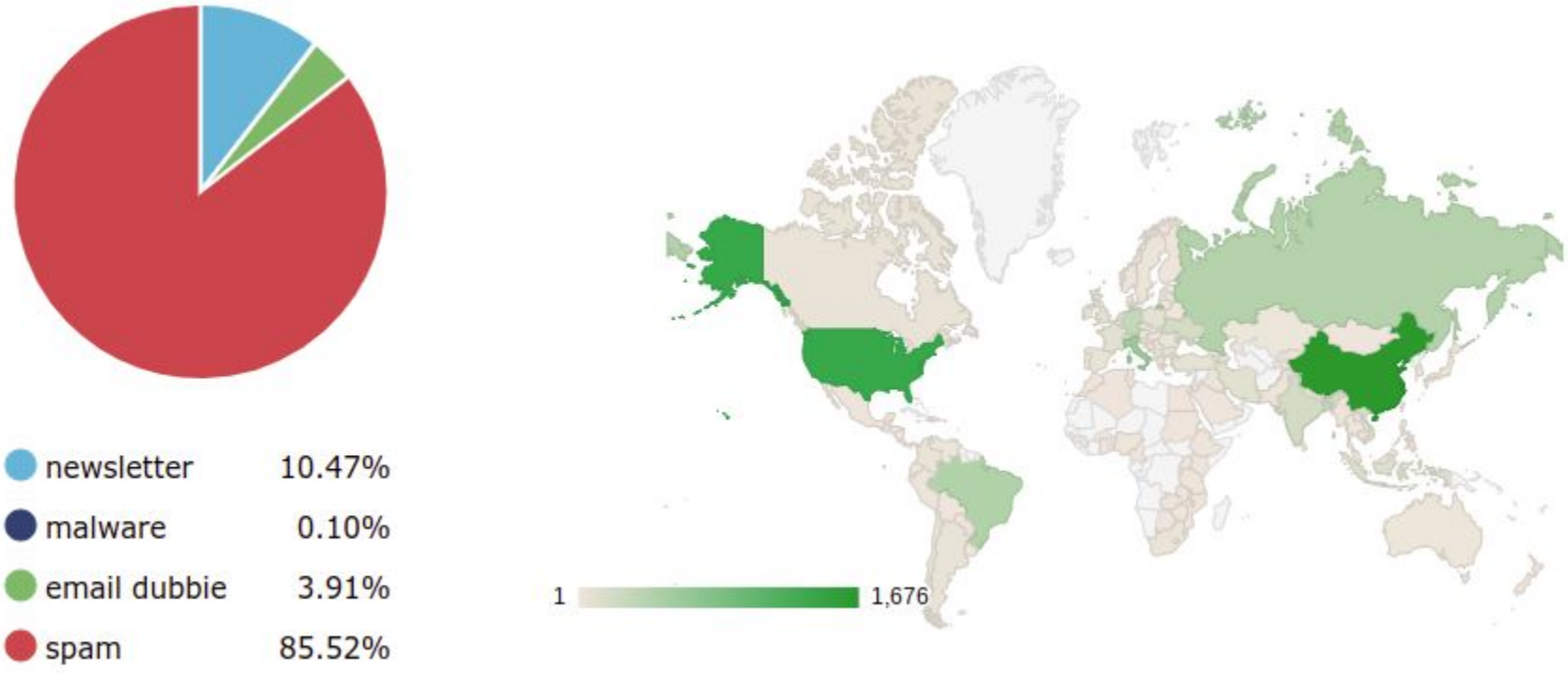


È possibile scegliere la lingua in cui è visualizzato il report direttamente dall'email o successivamente:

Cliccando sulla rotellina è possibile personalizzare il formato del report, questa scelta verrà memorizzata per il singolo utente:

Le scelte possibili sono:

Spuntando “visualizzazione grafici” verranno visualizzati i grafici statistici delle email bloccate negli ultimi 30 giorni:



Spuntando “email suddivise per mittente” le email verranno raggruppate per mittente e se il numero è elevato (superiore a 10) il blocco di email non viene visualizzato, se non premendo sul mittente. Se invece non viene spuntata, le email vengono visualizzate in sequenza.

La prima parte del report visualizza, se necessario, delle notifiche:

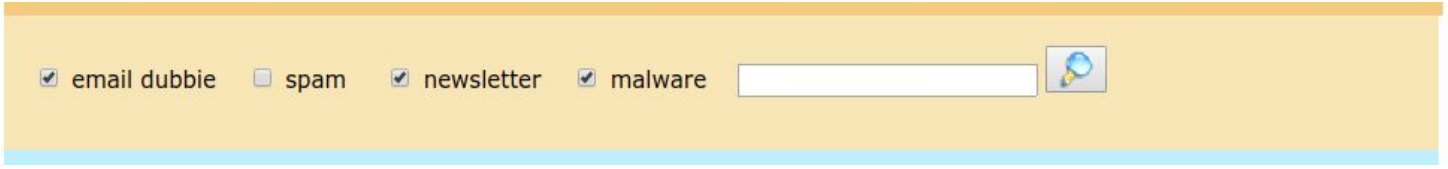
Le notifiche possono essere di diverso tipo e sono precedute da un'icona specifica:

è una notifica di una email già consegnata e contenente un possibile virus

è una notifica di una email già consegnata contenente dei link a siti pericolosi (URL)

Dopo aver verificato quanto notificato è possibile cliccare sul pulsante "Rimuovi notifica", quindi la notifica non verrà più visualizzata.

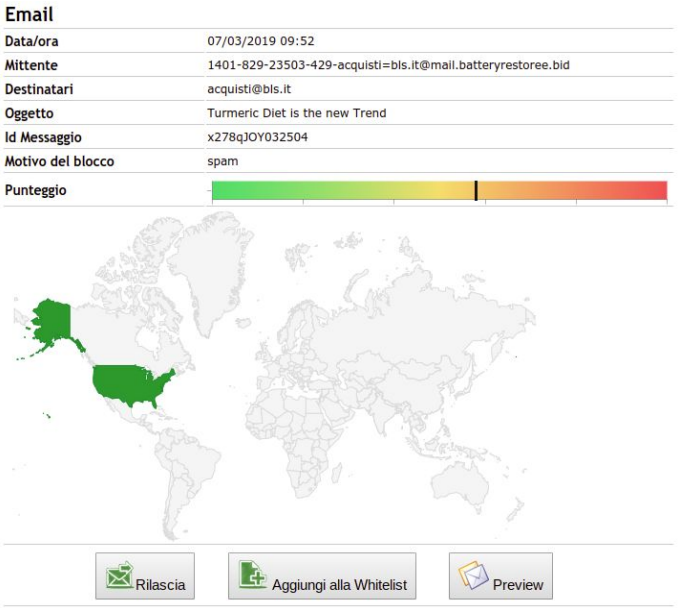
La sezione seguente permette scegliere quali email visualizzare nel report:



Spuntare la tipologia per email da visualizzare, eventualmente inserire nel campo di ricerca il mittente, l'oggetto (anche parzialmente) e premere l'icona di ricerca.

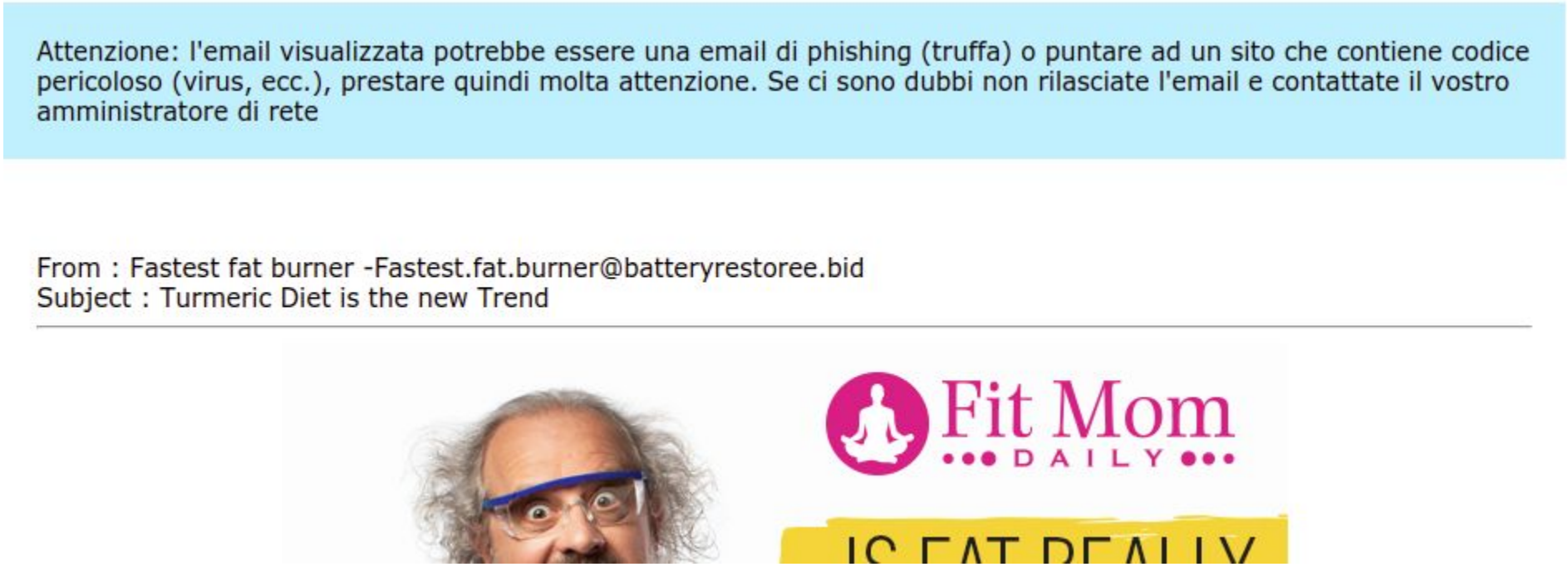
Successivamente vengono visualizzate le email bloccate divise per tipologia:

Cliccando su una email vengono ne visualizzati i dettagli:



Cliccando sulle icone a inizio riga o sui pulsanti in coda alla pagina di dettaglio è possibile rilasciare l'email o aggiungerla in whitelist e quindi rilasciarla.

Il pulsante Preview permette di visualizzare l'email (se non è ritenuta pericolosa) per decidere se rilasciarla:



Dopo aver verificato le email nel report ed averle eventualmente rilasciate o aggiunte in whitelist consigliamo di “nasconderle” dai successivi report.
Così facendo nel prossimo report verranno visualizzate solo le email arrivate nel frattempo e non di nuovo tutte.

Per fare questo cliccare sul pulsante “Nascondi”:

Cliccando su “Visualizza” si annulla l’effetto di “Nascondi” e verranno visualizzate di nuovo tutte le email bloccate nell’ultimo mese.

SPAM SCORE POLICY

Questo tipo di policy permette di impostare i parametri del sistema antispam.

I parametri principali sono il “Livello spam” e il “Livello Highspam”.
Se il punteggio spam calcolato su una email è inferiore al **Livello Spam**, l’email non sarà considerata spam.
Se il punteggio è compreso tra il livello **SPAM** e il livello **HIGHSPAM**, sarà considerata probabile spam.
Se è superiore al livello **HIGHSPAM** sarà considerata sicuramente spam.

Negli ultimi due casi l’email sarà di default inserita nella **Quarantena Spam** (**QS**) da cui potrà essere rilasciata dall’amministratore o dai destinatari.
Il sistema utilizza le email con punteggio superiore al livello **HIGHSPAM** per apprendere come sono fatte le email di spam ricevute.

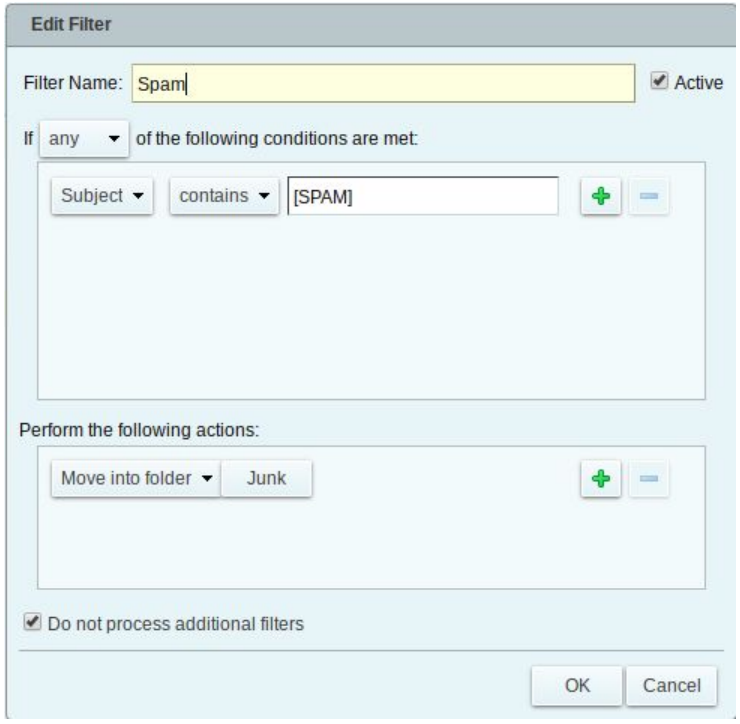
Se il punteggio spam è compreso tra “Livello spam” -1 e “Livello spam” allora la classificazione è dubbia, in questo caso la consegna della email viene ritardata (delayed emails). Dopo i minuti indicati nel parametro “Ritardo email dubbie” viene ripetuto il test antispam. Ciò permette alle blacklist e altri sistemi collaborativi di aggiornarsi. Se il punteggio sarà ancora dubbio l’email verrà comunque consegnata.

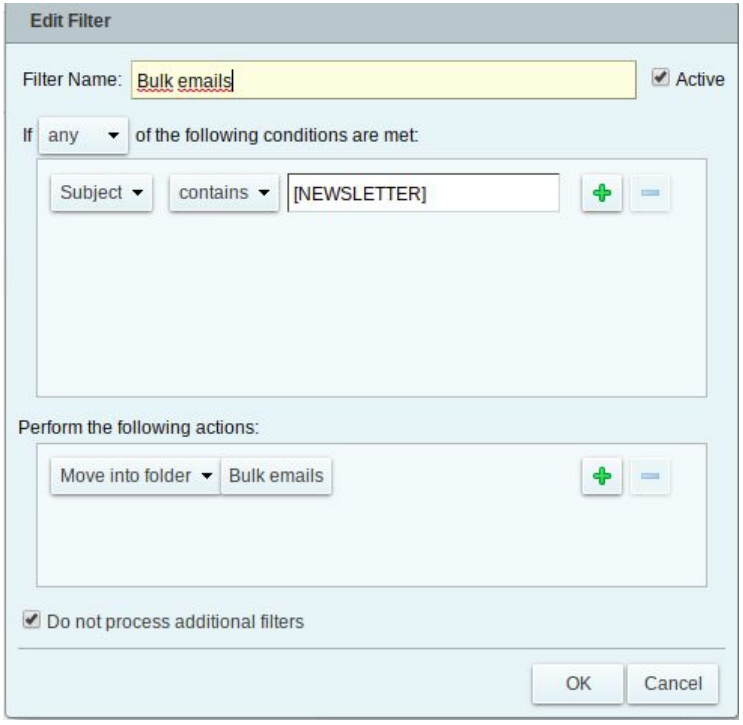
È possibile poi specificare se le Newsletter (bulk-emails) devono essere bloccate (per tutto il dominio), ogni utente potrà dalle proprie preferenze scegliere se riceverle.

L'ultimo parametro indica se la quarantena è attiva oppure no
Se la si disattiva, tutte le email non pericolose (quindi non quelle contenenti virus, allegati pericolose o classificate come scam) verranno consegnate agli utenti.

In questo caso però le email di spam avranno scritto nell'oggetto [SPAM] e le newsletter avranno scritto [NEWSLETTER], gli utenti potranno definire quindi dei filtri che spostano queste email in apposite cartelle.

Di seguito due esempi di filtri per Zimbra:



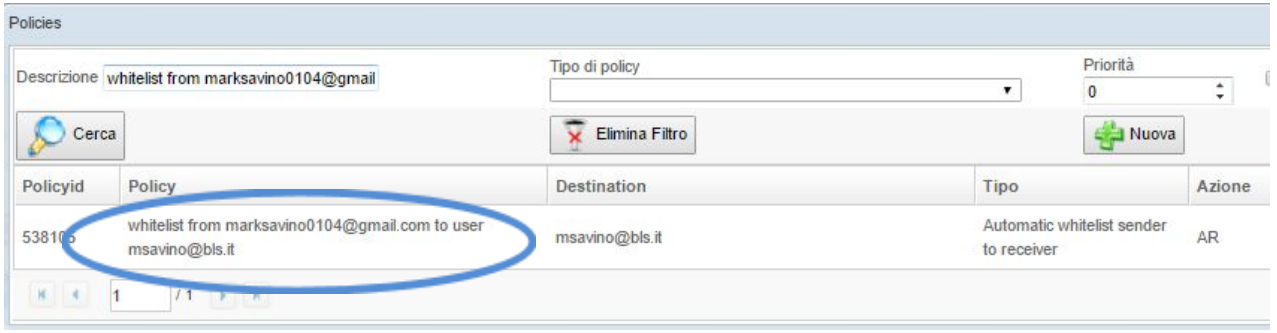


POLICIES AUTOMATICHE

Le Policies automatiche sono di due tipi: **Automatic Whitelist Sender to Receiver** e **Automatic Whitelist Domain Sender to Domain Receiver with not fail SPF**.
Queste due Policies sono native del sistema di **Mail Security** di **BLS**, e costituiscono un efficacissimo sistema per ridurre il problema dei **Falsi Positivi.**

Automatic Whitelist Sender to Receiver

Questa Policy si crea automaticamente ogni volta che viene inviata un'email da parte del cliente a un suo contatto.
L'indirizzo del contatto viene registrato dal sistema che, in futuro, permetterà alle email provenienti da quell'indirizzo di passare.
La Priorità di queste Policies è impostata di default a 5, in modo che eventuali altre Policies di sicurezza importanti possano comunque avere precedenza, mentre quelle di Spam non fermino le email con Policy di Whitelist automatica.
Nell'elenco delle Policies viene indicato, come nome della Policy, tra quali indirizzi questa è attiva.



Automatic Whitelist Domain Sender to Domain Receiver with not fail SPF

Anche questa Policy si crea automaticamente ogni volta che viene inviata un'email da parte del cliente a un suo contatto.
Il suo funzionamento è simile alla **Automatic Whitelist Sender to Receiver,** con la differenza che non sarà soltanto l'indirizzo del contatto a cui viene inviata l'email ad essere automaticamente inserito in una whitelist con priorità 5, ma l'intero suo dominio a patto che il **TEST SPF** effettuato su quel dominio non fallisca.

DURATA E SCADENZA DELLE POLICIES AUTOMATICHE

Come già accennato in precedenza, le Policies automatiche hanno una **scadenza**.

Scadono dopo 365 giorni, indicati nella colonna **Giorni di Vita,** dalla data di ULTIMA MODIFICA.
Per sapere se la Policy è ancora attiva, è sufficiente verificare se siano passati più o meno di 365 giorno da tale data.

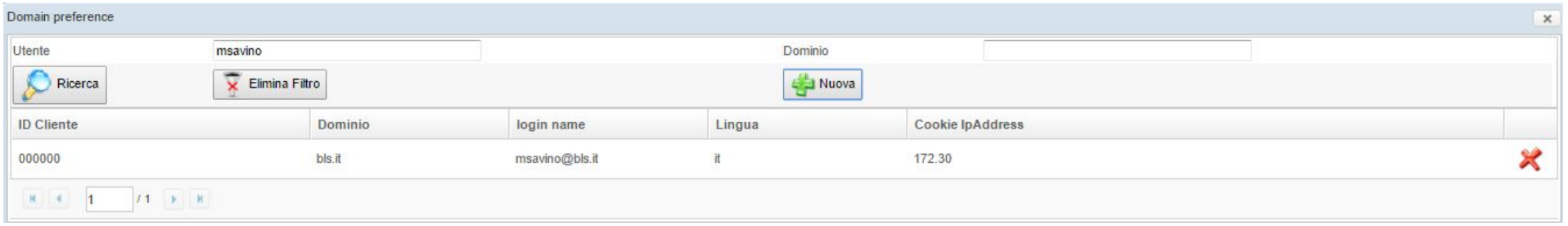
Policyid	Policy	Destination	Tipo	Azione	Priorità	Ultima modifica	Giorni di vita
146331	whitelist from esempio1@esmail.it to user mbruse@bls.it	mbruse@bls.it	automatic whitelist sender to receiver	AR	5	2016-02-08 15:20:15.0	365
471168	whitelist from esempio2@esmail.it to user mbruse@bls.it	mbruse@bls.it	automatic whitelist sender to receiver	AR	5	2016-04-14 11:22:44.0	365
42117	whitelist from esempio3@esmail.it to user mbruse@bls.it	mbruse@bls.it	automatic whitelist sender to receiver	AR	5	2016-05-04 17:23:01.0	365

La scadenza delle Policies è effettiva solo per quelle create automaticamente, NON per quelle create manualmente, per le quali i giorni di vita saranno sempre indicati come “0”.

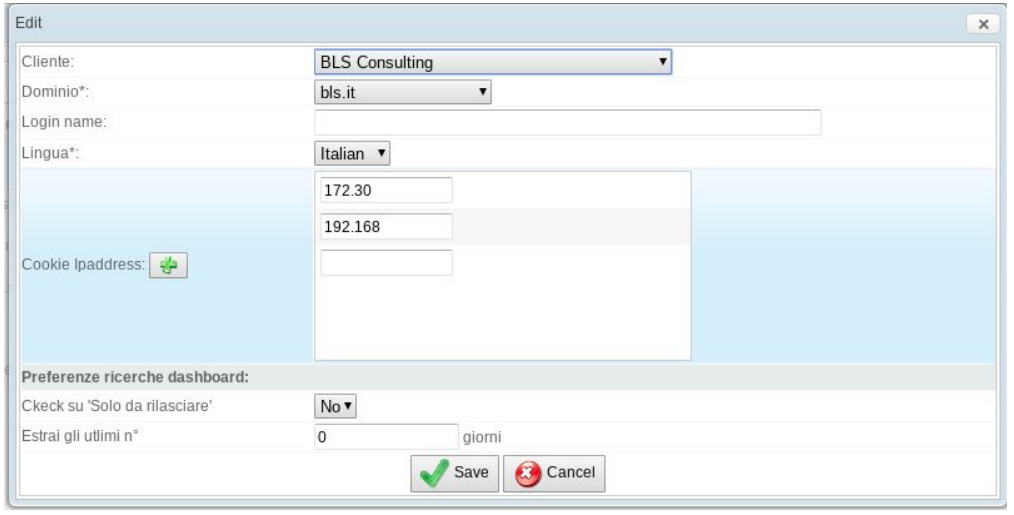
Il senso di questa funzione è evitare che delle Policies create per scambi di email saltuari vadano a intasare per lungo tempo le policies aziendali.

DOMAIN PREFERENCES

Da questa schermata è possibile configurare le proprie preferenze di dominio.
Per accedere cliccare sulla corrispondente opzione del menu funzioni.



Cliccando il tasto “NUOVA” si aggiunge una preferenza, ovvero si impostano alcuni parametri per tutti gli utenti di un dominio o per il singolo utente.



Impostare le preferenze per un dominio/utente specificando:

Cliente: cliente cui il Dominio appartiene

Dominio: il Dominio per cui si imposta la preferenza

Login Name: l'indirizzo email dell'utente. Se si lascia vuoto, varrà per tutti gli utenti del dominio

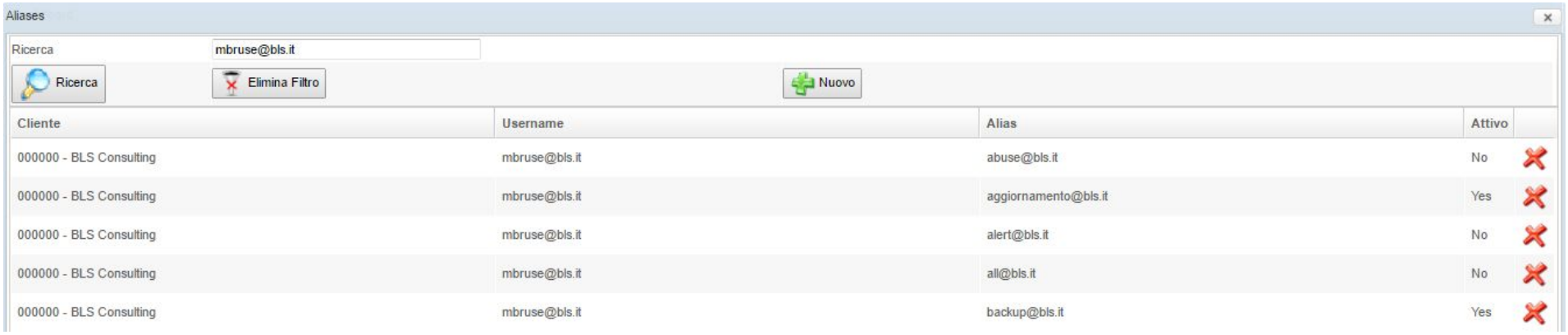
Lingua: con questo parametro si può impostare la lingua di default degli utenti del dominio

Cookie Ipaddress: gli indirizzi ritenuti sicuri, ovvero per i quali il Mail Relay riconoscerà il cookie e non chiederà le credenziali ad ogni accesso alla dashboard

Sotto "**Preferenze ricerche dashboard**" è possibile scegliere se la casella "**Solo da rilasciare**" è di default spuntata e nelle ricerche avanzate il numero dei giorni su cui verranno fatte le estrazioni.

GESTIONE ALIAS

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

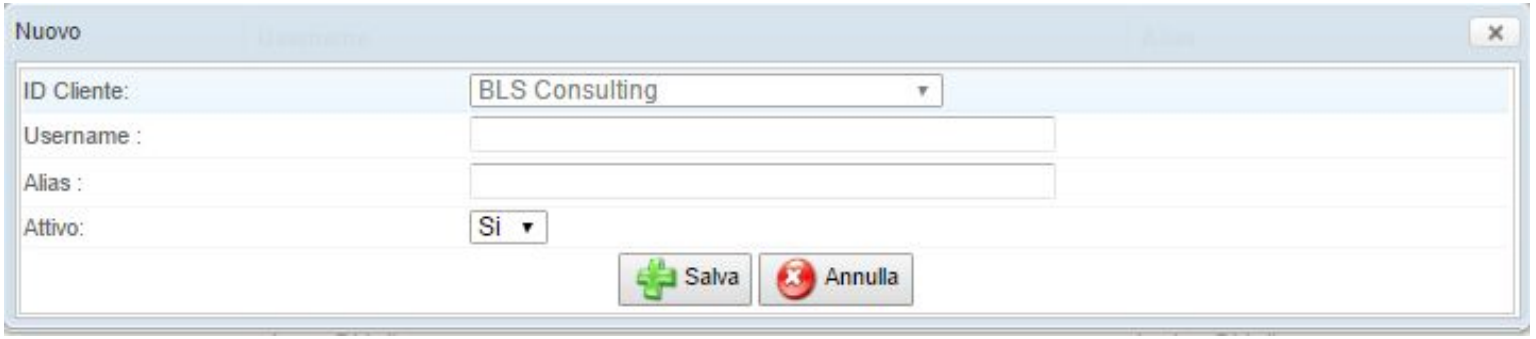


Da questa schermata è possibile visualizzare gli Alias e le liste di distribuzione cui ogni indirizzo email gestito dal Mail Relay è associato.
Le alias sono normalmente sincronizzate con quelle del proprio server di posta, è comunque possibile aggiungerlo manualmente.

Le alias vengono usate per:

- raggruppare i report antispam in modo da inviarne uno solo e non uno per ogni alias
- permettere ad un utente la gestione delle email inviate anche agli alias e alle liste di distribuzione
- permettere l'accesso alla dashboard con un'alias (solo se l'alias è attiva)

Cliccando “NUOVO” si aprirà la seguente schermata.



Da qui si configurano i vari campi:

Id cliente: il Cliente per cui si impostano gli Alias

Username: l’indirizzo email cui associare Alias o Lista

Alias: l’Alias o la Lista che si intende associare all’indirizzo email

Attivo: selezionando “SI”, si rende valido l’Alias o l’indirizzo della lista per accedere all’account Mail Relay dell’utente

SENT EMAIL MONITOR

Questa sezione offre una visualizzazione aggregata in tempo reale delle email inviate da ciascun Dominio appartenente al cliente.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Le varie colonne indicano il **Dominio, Data e Ora** dell'ultimo invio da quel Dominio, **Email Inviate**: il conteggio delle email inviate da quel dominio, **Invio Bloccato**: se l'invio per l'intero dominio è stato bloccato da un amministratore, **Invio temporaneamente bloccato**: se l'invio è stato bloccato dal sistema automatico di monitoraggio del volume delle email inviate, **Data/Ora del blocco**: quando è iniziato il blocco.

Le due icone alla fine di ciascuna riga permettono di accedere ad altre schermate che forniscono ulteriori dettagli sulle email inviate, la prima icona apre una finestra che mostra le stesse colonne del monitoraggio del traffico, ma organizzato per utente. La seconda icona apre una finestra che indica le ultime 50 email inviate dagli utenti del dominio.

Domini bloccati o contenenti utenti bloccati sono evidenziati in rosso, mentre domini temporaneamente bloccati o contenenti utenti temporaneamente bloccati sono evidenziati in giallo.

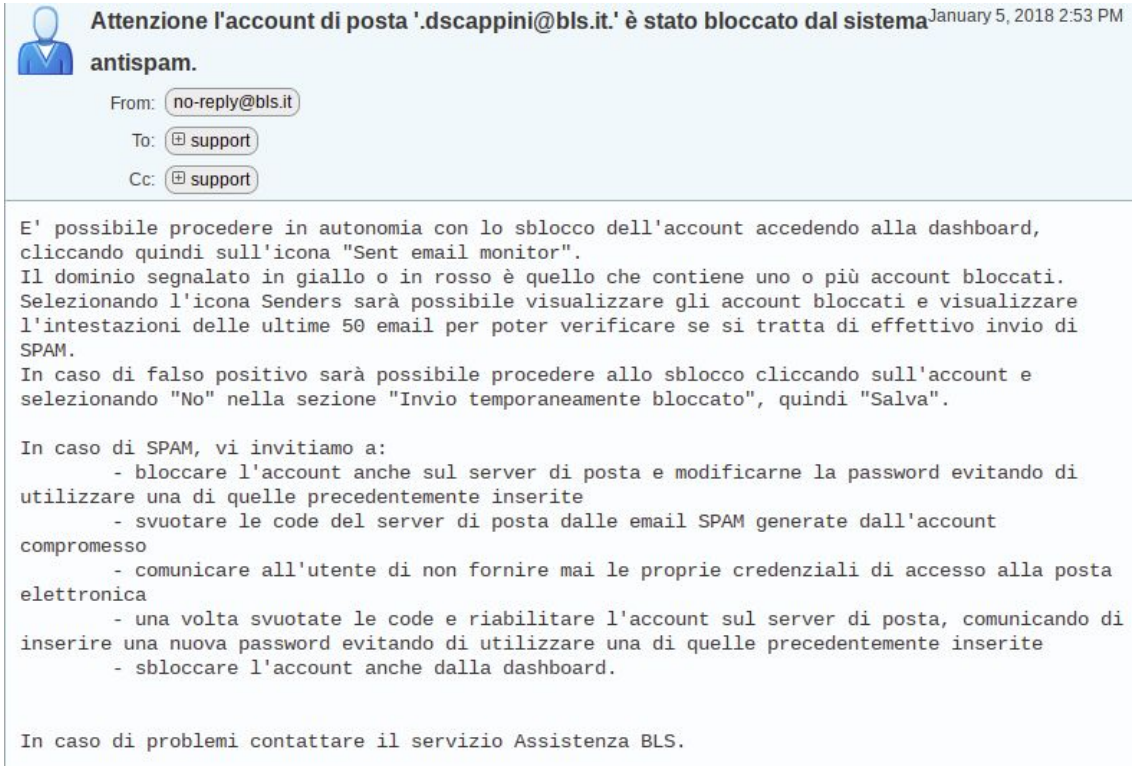
Cliccando su una riga viene aperta una finestra che permette di bloccare/sbloccare l'invio e definire i parametri che regolano il sistema automatico di monitoraggio del volume di email inviate.

Prestare molta attenzione all'uso di "Invio bloccato": infatti impostando questo parametro a "Yes" tutte le email inviate dall'utente dei dominio vengono bloccate e viene immediatamente segnalato al mittente l'impossibilità di recapitare l'email, attenzione: **l'email non verrà rispedita.**

Impostando invece il blocco temporaneo le email verranno tenute in coda e solo dopo un'ora verrà notificato all'utente che l'email non è stata ancora consegnata. Appena si sbloccherà l'account le email in coda verranno immediatamente consegnate.

Il sistema automatico di monitoraggio del volume di email inviate verifica che il numero di email/minuto o all'ora indicate non vengano superato.
Appena questi limiti vengono superati (per un uso improprio da parte dell'utente o più comunemente perché la casella ad insaputa dell'utente viene usata per inviare spam) viene impostato un blocco temporaneo.

Gli amministratori ricevono quindi una email con la notifica del problema con le istruzioni per sbloccare nuovamente l'account dopo aver risolto i problemi di sicurezza.



Attenzione l'account di posta '.dscappini@bls.it.' è stato bloccato dal sistema antispam. January 5, 2018 2:53 PM

From: no-reply@bls.it
To: support
Cc: support

```
E' possibile procedere in autonomia con lo sblocco dell'account accedendo alla dashboard,
cliccando quindi sull'icona "Sent email monitor".
Il dominio segnalato in giallo o in rosso è quello che contiene uno o più account bloccati.
Selezionando l'icona Senders sarà possibile visualizzare gli account bloccati e visualizzare
l'intestazioni delle ultime 50 email per poter verificare se si tratta di effettivo invio di
SPAM.
In caso di falso positivo sarà possibile procedere allo sblocco cliccando sull'account e
selezionando "No" nella sezione "Invio temporaneamente bloccato", quindi "Salva".

In caso di SPAM, vi invitiamo a:
        - bloccare l'account anche sul server di posta e modificarne la password evitando di
utilizzare una di quelle precedentemente inserite
        - svuotare le code del server di posta dalle email SPAM generate dall'account
compromesso
        - comunicare all'utente di non fornire mai le proprie credenziali di accesso alla posta
elettronica
        - una volta svuotate le code e riabilitare l'account sul server di posta, comunicando di
inserire una nuova password evitando di utilizzare una di quelle precedentemente inserite
        - sbloccare l'account anche dalla dashboard.


In caso di problemi contattare il servizio Assistenza BLS.
```

Nel caso di server **Zimbra**, e se la funzione è stata attivata, vengono bloccati contestualmente anche gli account.
In questo modo l'uso improprio della casella viene impedito e si evita l'accumulo di email nelle code del server **Zimbra**.

Cliccando sull'icona "Senders" verranno visualizzati i singoli utenti e se l'account Zimbra è stato bloccato:

Quindi oltre alle colonne già descritte per i domini, viene evidenziato se l'account Zimbra è stato bloccato.

Le tre icone a fine riga permettono di:

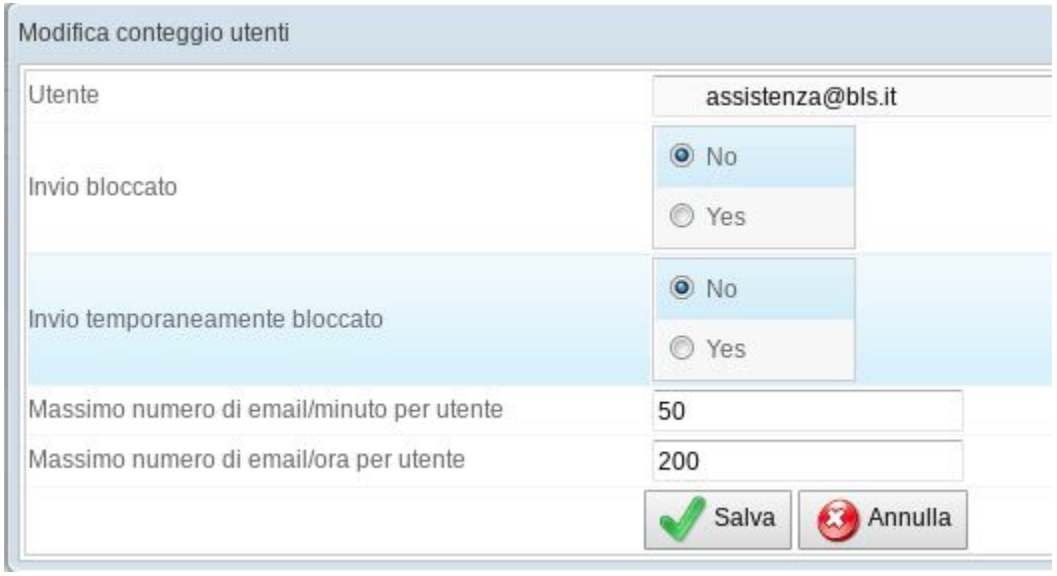
visualizzare le ultime 50 email, utile per verificare se si tratta di un uso improprio o di un falso positivo

bloccare o sbloccare l'account Zimbra

cambiare la password dell'account Zimbra

Utilizzando le ultime due icone sarà quindi possibile rimettere in sicurezza l'account Zimbra cambiando la password eventualmente compromessa e sbloccare l'account senza dover accedere alla console di gestione di Zimbra.

Anche nel caso degli utenti sarà possibile, cliccando su una riga, accedere alla schermata che permette il blocco/sblocco dell'invio e impostare parametri personalizzati per il sistema automatico di monitoraggio del volume di email inviate:



Prestare molta attenzione all'uso di "Invio bloccato".
Impostando questo parametro a "Yes" infatti tutte le email inviate dall'utente vengono bloccate e viene immediatamente segnalato al mittente l'impossibilità di recapitare l'email, attenzione: **l'email non verrà rispedita.**

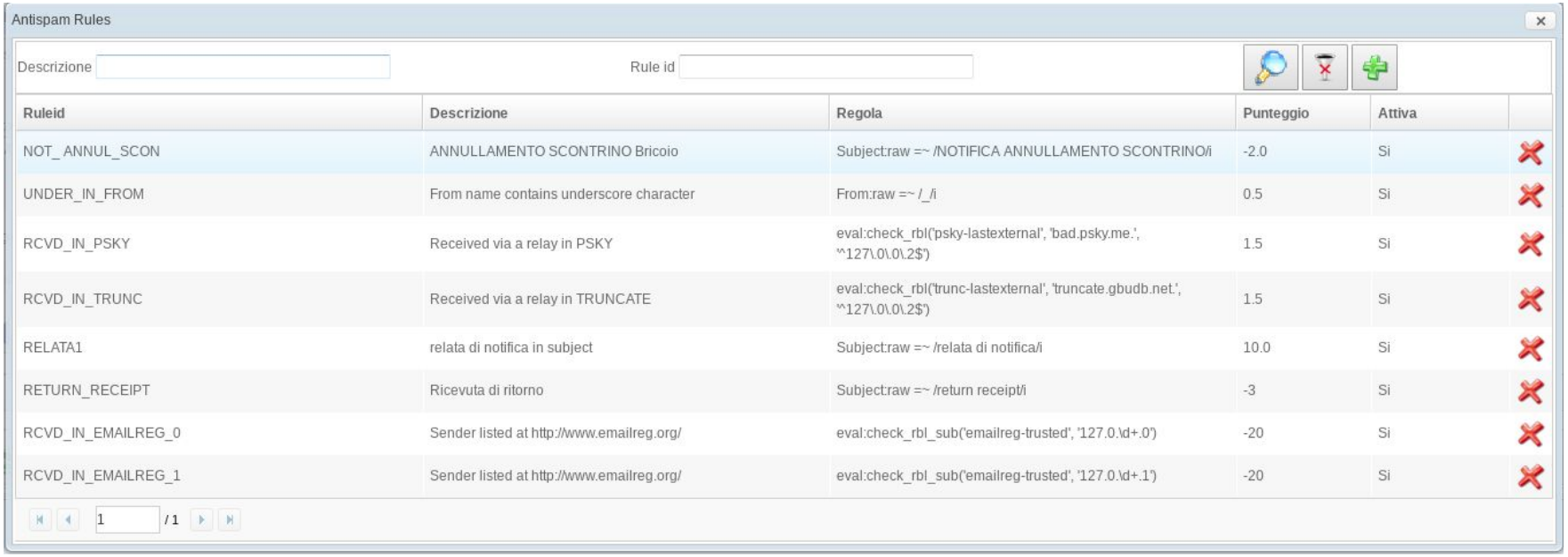
Impostando invece il blocco temporaneo, le email verranno tenute in coda e solo dopo un'ora verrà notificato all'utente che l'email non è stata ancora consegnata. Appena si sbloccherà l'account, le email in coda verranno immediatamente consegnate.

Il sistema automatico di monitoraggio del volume di email inviate verifica che il numero di email/minuto o all'ora indicate non vengano superate.
Appena questi limiti vengono superati (per un uso improprio da parte dell'utente o più comunemente perché la casella viene usata per inviare spam ad insaputa dell'utente) viene impostato un blocco temporaneo.

REGOLE ANTISPAM

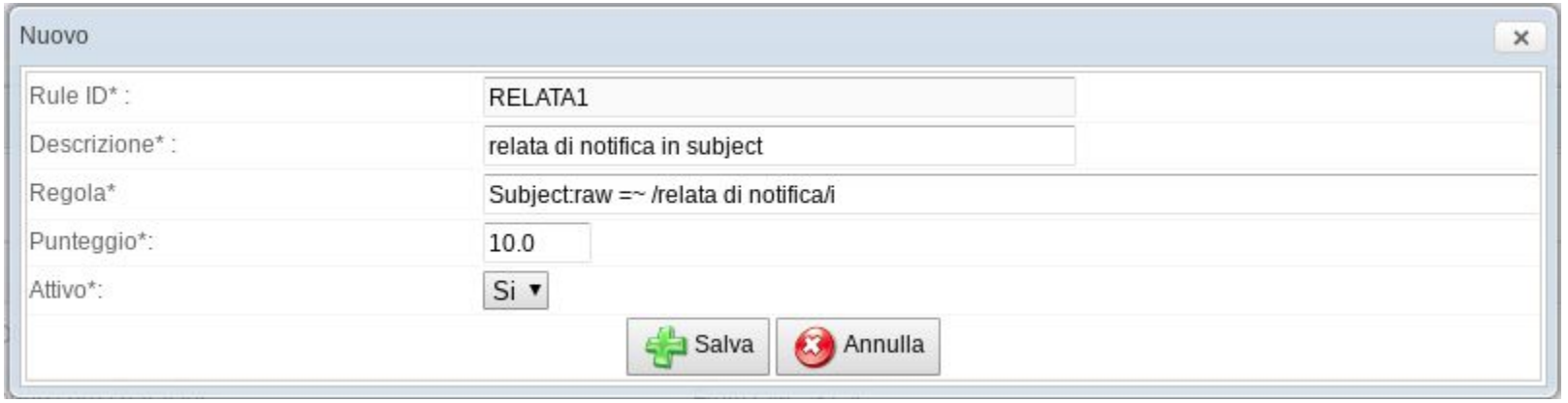
Con questa opzione è possibile personalizzare il punteggio del sistema antispam.
Questa opzione è disponibile solo per gli amministratori del cluster, in quanto le regole agiscono su tutti i clienti, domini e utenti del cluster.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.



Cliccando sull'icona "+" è possibile aggiungere una nuova regola, cliccando sulla croce rossa a fine riga si disattiverà la regola, cliccando direttamente su una regola è possibile modificarla.

Una regola deve essere identificata da un **Rule Id univoco**, e includere una descrizione della regola.



La regola segue in linea di massima questa sintassi:

parametro dell'email da valutare =~ (uguale e tilde) regular expression

Il parametro normalmente è: Subjectraw (oggetto della email) o Fromraw (mittente della email)

La regular expression più comune è quella usata per indicare una parola o frase contenuta nel parametro, la sintassi è:

/parola o frase/, se si aggiunge una "i" sta ad indicare che la ricerca è case insensitive, quindi non tiene conto delle maiuscole/minuscole.

Ad es. una regola che identifica le email che hanno nell'oggetto la frase "relata di notifica" si scriverà *Subjectraw =~ /relata di notifica/i*

Il punteggio si somma al punteggio valutato dal sistema antispam, può essere positivo o negativo.
Il livello normale per considerare una email come spam è 5 (impostabile con la policy Spam score policy descritta prima), quindi se si aggiunge 10 come in questo esempio è molto probabile che l'email verrà considerata spam, se si aggiunge 100 si avrà la certezza.
Analogamente, se il punteggio si imposta a -10 è molto probabile che l'email verrà fatta passare, con -100 sicuramente verrà fatta passare.

BILLING

Questa opzione visualizza il numero di caselle attive per singolo dominio e per un determinato mese.
Vengono valutate le caselle che hanno spedito email “Sender”, e quelle che le hanno ricevute “Receiver”.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Customer	Dominio	Anno/mese	Sender	Receiver	Total	Aggiornato il
000000 BLS Consulting	bls.it	2019/03	44	35	60	2019-03-08 00:04:45.0
000000 BLS Consulting	blscloud.com	2019/03	6	10	11	2019-03-08 00:04:45.0
000000 BLS Consulting	cloud-solutions.it	2019/03	1	2	2	2019-03-08 00:04:45.0

Cliccando sull’icona a fine riga viene visualizzato l’elenco delle caselle corrispondenti.

È possibile esportare l'elenco dei domini e dei domini suddivisi per cliente, con l'indicazione in questo caso delle opzioni commerciali attive (Strong security, Zimbra advanced, ecc.) e del numero di caselle licenziate:

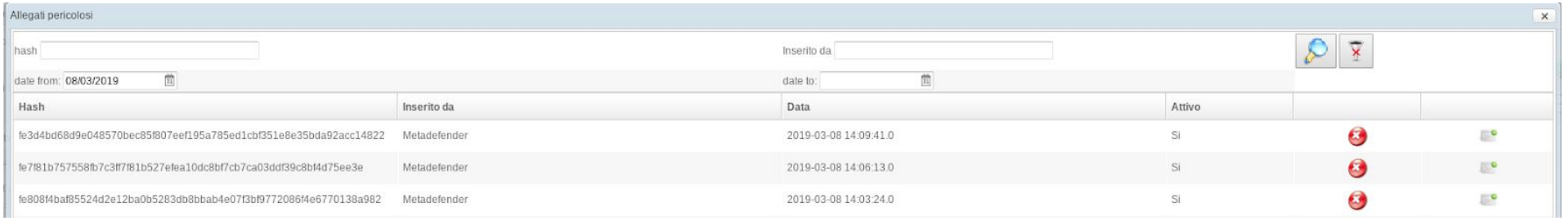
	A	B	C	D	E	F
1	**ELENCO ACCOUNT 201903**					
2						
3	Customer:	Expiry Date:	Mailbox licensed:	Options:		
4	BLS Consulting(000000)		50	Zimbra advanced- Strong security- Mass Mailing- Email archive		
5	Domain	Year/month	Sent	received	Total	Last Update
6	bls.it	201903	44	35	60	2019-03-08 00:04:45.0
7	blscloud.com	201903	6	10	11	2019-03-08 00:04:45.0
8	cloud-solutions.it	201903	1	2	2	2019-03-08 00:04:45.0
9	mail-solutions.it	201903	0	4	4	2019-03-08 00:04:42.0
10	zimbra-solutions.com	201903	0	5	5	2019-03-08 00:04:43.0
11	zimbra-solutions.it	201903	1	1	1	2019-03-08 00:04:45.0
12	Total:		66	57	97	
13						

Queste estrazioni sono utili per ri-addebitare il costo del servizio a clienti o altre aziende del gruppo.

ALLEGATI PERICOLOSI

Questa opzione permette accedere al database delle firme (hash SHA1) dei file pericolosi.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.



La colonna “Inserito da” indica la fonte della firma. Le firme possono venire segnalate dagli amministratori (da **dettaglio email** come illustrato nei paragrafi precedenti), e vengono inoltre aggiunte da Janusmail, che le ottiene costantemente da più fonti (mediamente **13000 firme a settimana**).

Le firme vengono usate in fase di ricezione di una nuova email: se un allegato ha una firma uguale ad una presente nel database, l’email viene bloccata come malware (virus) e nella descrizione viene indicato “hash” e fonte della firma.

Inoltre, se è attivo il modulo **Advanced security**, alla ricezione di una nuova firma vengono ricontrollate tutte le email ricevute fino a quel momento e, se la firma corrisponde, viene notificato all’utente mediante il report antispam (vedi paragrafo dedicato).Inoltre, se è attivo il modulo **Zimbra advanced,** l’email viene automaticamente spostata nella cartella “posta indesiderata” dopo pochi secondi.

Nel caso di falsi positivi (rari ma sempre possibili) si può disattivare la firma cliccando sull’apposita icona.

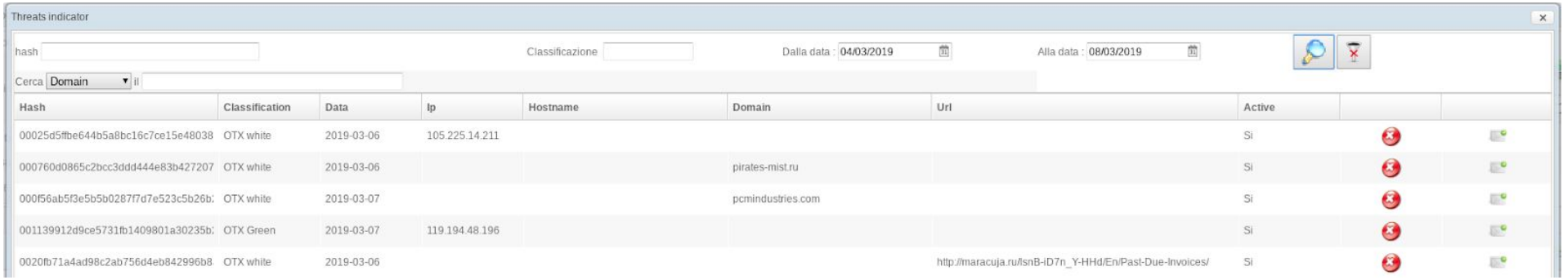
L’icona a forma di busta a fine riga permette visualizzare l’elenco delle email ricevute che contengono un allegato con la stessa firma. Mentre le quattro icone riportate sotto permettono visualizzare le analisi sulle pagine di metadefender, virustotal, joe sandbox e falcon sandbox.

L’uso di queste icone è già stato illustrato nel dettaglio email.

THREATS INDICATORS

Questa opzione permette di accedere al database degli indicatori di minaccia, cioè domini, nomi host, url e indirizzi ip coinvolti in attacchi di phishing o frodi, campagne di spam, diffusione di malware ecc...

Per accedere cliccare sulla corrispondente opzione del menu funzioni.



La colonna “Classification” indica la tipologia di minaccia, nel caso la minaccia non sia nota (ad esempio se per qualche motivo è riservata), viene indicato un livello di sensibilità dell’informazione secondo quanto indicato in questa pagina:

https://www.us-cert.gov/tlp

È possibile, per gli amministratori, segnalare una minaccia (da “dettaglio email” come già illustrato nel rispettivo paragrafo).
Inoltre, Janusmail recupera costantemente da diverse fonti nuovi indicatori (mediamente 9000 indicatori di minaccia a settimana).

Gli indicatori di minaccia vengono usati in fase di ricezione di una nuova email: se l’email contiene, nel corpo o negli allegati, uno o più di questi indicatori, viene calcolato un punteggio che determina il blocco dell’email se supera una determinata soglia (come **SCAM** se le minacce sono di tipo phishing, frode, coinvolte nella diffusione di malware, come **SPAM** se coinvolte in campagne di spam o come **NEWSLETTER** se sono presenti numerosi link di tipo ad/tracking, cioè usati per monitorare gli utenti per campagne marketing.)

Inoltre, se è attivo il modulo **Advanced security**, quando viene segnalato un nuovo URL pericoloso vengono controllate tutte le email ricevute fino a quel momento e se contengono l’URL viene notificata all’utente mediante report antispam (come già illustrato nel paragrafo dedicato).

Se inoltre è attivo il modulo **Zimbra advanced** l'email viene spostata nella posta indesiderata dopo pochi secondi.

Nel caso di falsi positivi (rari, ma sempre possibili) si può disattivare l'indicatore di minaccia cliccando sulla apposita icona.

L'icona a forma di busta a fine riga permette di visualizzare l'elenco delle email ricevute che contengono un allegato con lo stesso indicatore di minaccia.

DMARC REPORT

Il report DMARC raccoglie le informazioni inviate da server che hanno ricevuto email dai vostri domini, sia che siano state spedite da vostri utenti, sia che siano email di spam o phishing che usano impropriamente i vostri indirizzi email.

Quindi ad es. se voi inviate delle email ad un destinatario che usa Google Gmail, i server di Google vi invieranno periodicamente dei report statistici via email indicando il numero di email ricevute, da che server e se queste email sono ricevute da server compliant con SPF e firmate correttamente con DKIM.

Si può usare questo strumento per analizzare i dati ricevuti e sistemare la configurazione per attivare le policy DMARC.

Per poter ricevere i report DMARC è necessario impostare un record DNS appropriato:

_dmarc.bls.it IN TXT v=DMARC1; p=none; pct=100; rua=mailto:dmarc873245@bls.it; sp=none; aspf=r;

i principali parametri sono:

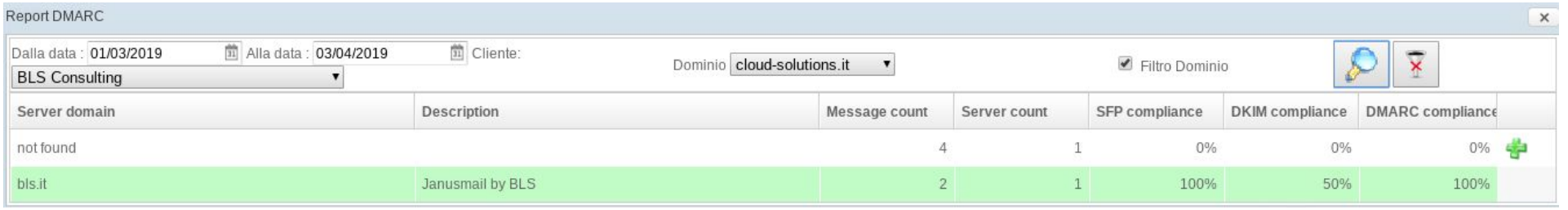
p=none che indica che la policy di fatto non è attivata, ma permette ricevere le informazioni per poi attivare la policy

rua=mailto:dmarc873245@bls.it indica l'email a cui inviare le informazioni

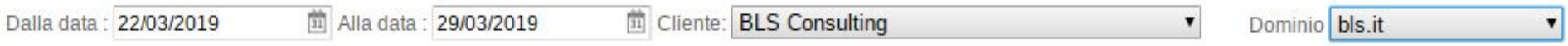
L'email da indicare è sempre quella indicata, ma va autorizzata la ricezione, chiedere al nostro servizio assistenza di essere autorizzati.

Le informazioni arriveranno periodicamente e saranno accessibili mediante questa funzione.

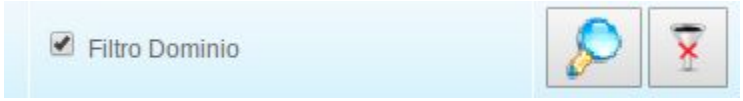
Per accedere cliccare sulla corrispondente opzione del menu funzioni.



Selezionare il periodo e il dominio da analizzare:



Si possono filtrare solo i record che hanno come dominio quello selezionato:



ciò riduce i dati da analizzare ma consigliamo successivamente di ripetere l'analisi senza filtro.

Questo è un esempio di report:

Server domain	Description	Message count	Server count	SFP compliance	DKIM compliance	DMARC compliance	
bls.it	Janusmail by BLS	462	2	98%	75%	100%	
not found		320	2	0%	0%	0%	
sparkpostmail.com	massmailing Sparkpost	221	1	0%	100%	100%	
aruba.it	forwardes Aruba	36	14	0%	30%	30%	
musvc.com	massmailing MailUp	4	4	0%	100%	100%	
imanpack.it		4	1	0%	0%	0%	
tin.it		2	1	0%	0%	0%	
seeweb.it	hosting web & mail	2	1	0%	100%	100%	
outlook.com	forwarders Microsoft Office 365	1	1	0%	100%	100%	

I server mittenti vengono raggruppati per dominio (l'indirizzo ip del server mittente viene risolto e viene estratto il dominio), per ogni dominio vengono riportati il numero totale di email inviate, il numero di server, la percentuale di server compliant con SPF, DKIM e DMARC.

Nel campo description è indicato la tipologia di server:

Janusmail by BLS: indica i server utilizzati dal nostro sistema di mail security

massmailing _____: indica i server utilizzati per spedire bulk email (newsletter)

forwarders _____: indica i server che hanno rigirato (forward) le email ai vostri server

Le righe sono evidenziate in colori diversi utili per evidenziare a colpo d'occhio tipi diversi di server.

Gli amministratori possono cliccare sul tasto "+" per aggiungere una descrizione e scegliere il colore con cui evidenziare la riga.

Cliccando su una riga verrà visualizzato il dettaglio dei server:

Server ip add	PTR	Message cou	SPF result	SPF domain	SPF policy evaluated	DKIM result	DKIM domain	DKIM policy evaluated	Reporters
91.196.64.11	smtpout005.bls.it.	338	pass	cegos.it	pass	pass	cegos.it	pass	beiersdorf.com, linkedin.com, google.com, mmc.com, esa2.lyondellbasell.iphmx.com, mail1.magna.com, sercoglobal.com, bmwgroup.com, bp.local, dhl.com, airfrance.fr
91.196.64.11	smtpout005.bls.it.	112	pass	cegos.it	pass	fail	cegos.it	fail	google.com

Le righe evidenziate in verde sono compliant con SPF o DKIM e considerate valide per DMARC (si dice che i domini sono allineati)

Le righe non evidenziate in verde sono anomale e vanno analizzate. E' possibile che:

- non sia impostato correttamente l'SPF (se l'SPF domain corrisponde e l'SPF result è uguale a fail o softfail)

SPF result	SPF domain
softfail	bls.it

- il server non firma correttamente con il protocollo DKIM (se il DKIM domain corrisponde e DKIM result è uguale a fail) o più probabile la firma non è valida in quanto firmata da un server non autorizzato che non dispone della chiave privata corretta

DKIM result	DKIM domain
fail	bls.it

- il server non firma con il protocollo DKIM (se il DKIM domain e DKIM result sono vuoti)

DKIM result	DKIM domain

L'SPF o il DKIM possono superare il test ma il dominio può non corrispondere (si dice che non è allineato):

SPF result	SPF domain	SPF policy evaluated
pass	preferredone.com	fail

DKIM result	DKIM domain	DKIM policy evaluated
pass	aseaps2019.com	fail

In questo caso si può trattare di una email ruotata (forwarded) da un altro server o può essere una truffa.

Se l'SPF non è impostato correttamente o le email non sono firmate con DKIM vanno sistemati per rendere compliant la policy, ad es.:

Server ip add	PTR	Message cou	SPF result	SPF domain	SPF policy evaluated	DKIM result	DKIM domain	DKIM policy evaluated
5.144.171.59	vm2737.cloud.seeweb.it.	2	pass	q360.it	fail	pass	cegos.it	pass

In questo caso le email provengono da un server in hosting, il DKIM è compliant e allineato è sufficiente per attivare la policy DMARC.

In quest'altro caso l'SPF non è compliant e neanche il DKIM quindi almeno uno dei due va sistemato:

Server ip address	PTR	Message cou	SPF result	SPF domain	SPF policy evaluated	DKIM result	DKIM domain	DKIM policy evaluated
62.149.158.245	smtpcmd01-d.aruba.it.	6	softfail	cegos.it	fail	fail	cegos.it/aruba.it	fail

Se analizziamo il record SPF notiamo che il server indicato non è elencato:

```
v=spf1 ip4:91.196.64.115 ip4:5.144.169.194 ip4:37.9.236.186 include:sparkpostmail.com ~all
```

Basta quindi aggiungere al record SPF l'indirizzo del server per renderlo compliant:

```
v=spf1 ip4:91.196.64.115 ip4:5.144.169.194 ip4:37.9.236.186 ip4:62.149.158.245 include:sparkpostmail.com ~all
```

Notare che vanno sistemati i server che per qualche motivo devono spedire le email (chiamiamoli server autorizzati) del vostro dominio, i server che invece sono utilizzate per spedire spam o email di phishing non vanno ovviamente resi compliant.

Una volta sistemati tutti i server autorizzati è possibile attivare una policy DMARC, es.:

_dmarc.bls.it IN TXT v=DMARC1; p=reject; pct=100; rua=mailto:dmarc873245@bls.it; sp=none; aspf=r;

Come si vede la policy è impostata per rifiutare le email da server non autorizzati (p=reject).

Quindi se si attiva questa policy, le email con il dominio bls.it verranno scartate se provenienti da server non autorizzati.

Una volta impostata la policy DMARC lo strumento è molto utile per identificare eventuali truffe che utilizzano i vostri indirizzi email.

Questo è un esempio:

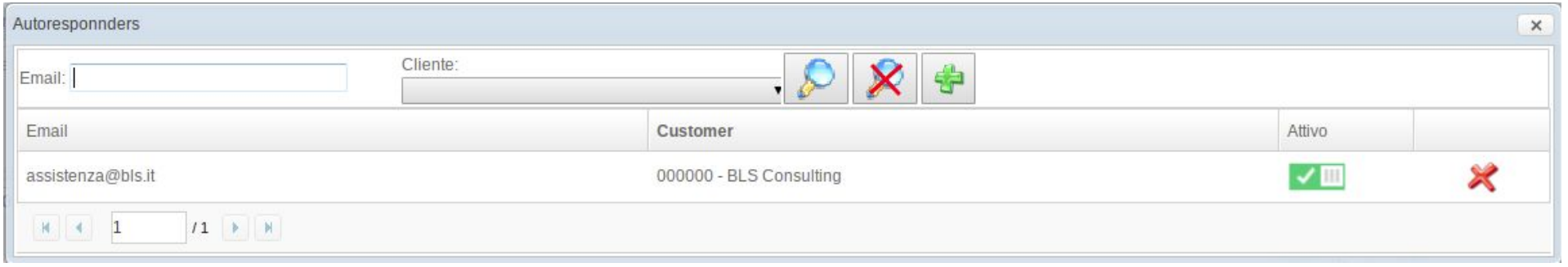
Server ip add	PTR	Message cou	SPF result	SPF domain	SPF policy evaluated	DKIM result	DKIM domain	DKIM policy evaluated
79.7.70.130	s1.imanpack.it.	4	softfail	cegos.it	fail	fail	cegos.it	fail

Come si vede sono state spedite 4 email da un server non compliant con il record SPF e firmate in modo non valido con DKIM, quindi si tratta probabilmente di email di phishing che usano il dominio indicato.

AUTORESPONDERS

Questa opzione permette di specificare le caselle email su cui è attivo un sistema di risposta automatica.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.



Una delle funzioni già descritte in precedenza di Janusmail sono le whitelist automatiche, ovvero l'aggiunta automatica in whitelist del destinatario di un'email, che determina che le risposte di tale destinatario non verranno bloccate dal sistema antispam indipendentemente dal contenuto e dal server di provenienza.

Questo vale anche per le risposte automatiche, quindi se è attivo un sistema di risposta automatica su una casella, il mittente di ogni email spedita alla casella verrà aggiunto alla whitelist.

Per ovviare a questo inconveniente, è possibile specificare in questa tabella gli indirizzi email su cui è attiva una funzione di risposta automatica.
Le email provenienti da questi indirizzi verranno in questo modo escluse dal sistema delle whitelist automatiche.

Non è necessario specificare le caselle su cui si attiva la funzionalità di fuori ufficio, queste email verranno riconosciute automaticamente e escluse dal sistema di whitelist automatiche.

MASS MAILING

Le funzioni descritte di seguito fanno parte del modulo Mass mailing, questo modulo permette inviare email transazionali o di marketing (bulk email, newsletter) garantendo la massima consegnabilità possibile.

A differenza delle email tradizionali hanno un sistema di spedizione completamente diverso basato sui seguenti principi:

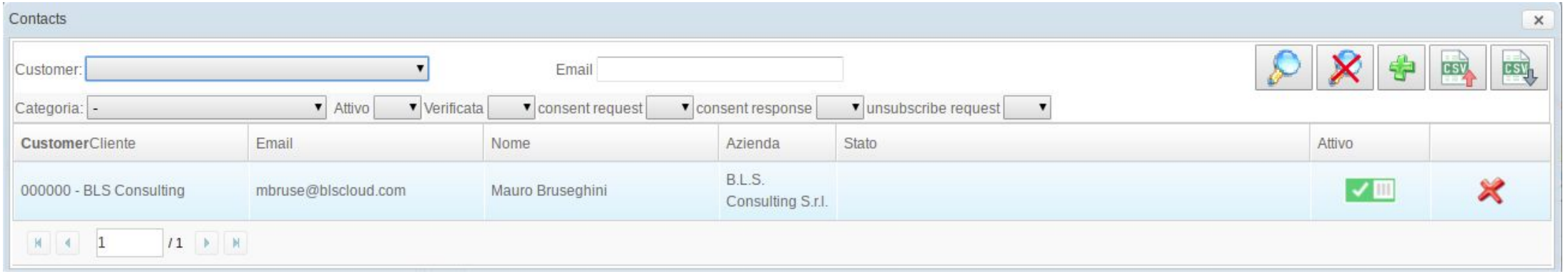
1) ogni email ha un singolo destinatario, in pratica ogni email è unica, ovviamente è possibile inviare ad una lista di destinatari (lista di distribuzione) ma per ogni destinatario verrà generata una email unica
2) le email vengono inviate un numero limitato di volte, quindi in caso di problemi il sistema non continuerà a tentare di consegnare l'email per giorni, ma proverà solo un numero predefinito di volte
3) ogni destinatario viene controllato prima di inviargli una email, quindi se ha richiesto di non ricevere più email la spedizione verrà bloccata
4) in caso di problemi non verranno generate email di risposta multiple (bounce email) bensì alla conclusione della spedizione il mittente riceverà un report sullo stato di consegna delle email alla lista di distribuzione
5) nelle email è possibile aggiungere un link per richiedere la cancellazione dalla lista di distribuzione (unsubscribe link)

Questa modalità di spedizione favorisce la consegnabilità delle email, senza pregiudicare la reputazione del mittente.

CONTATTI

Questa opzione permette gestire il database dei contatti comune a tutte le liste di distribuzione.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

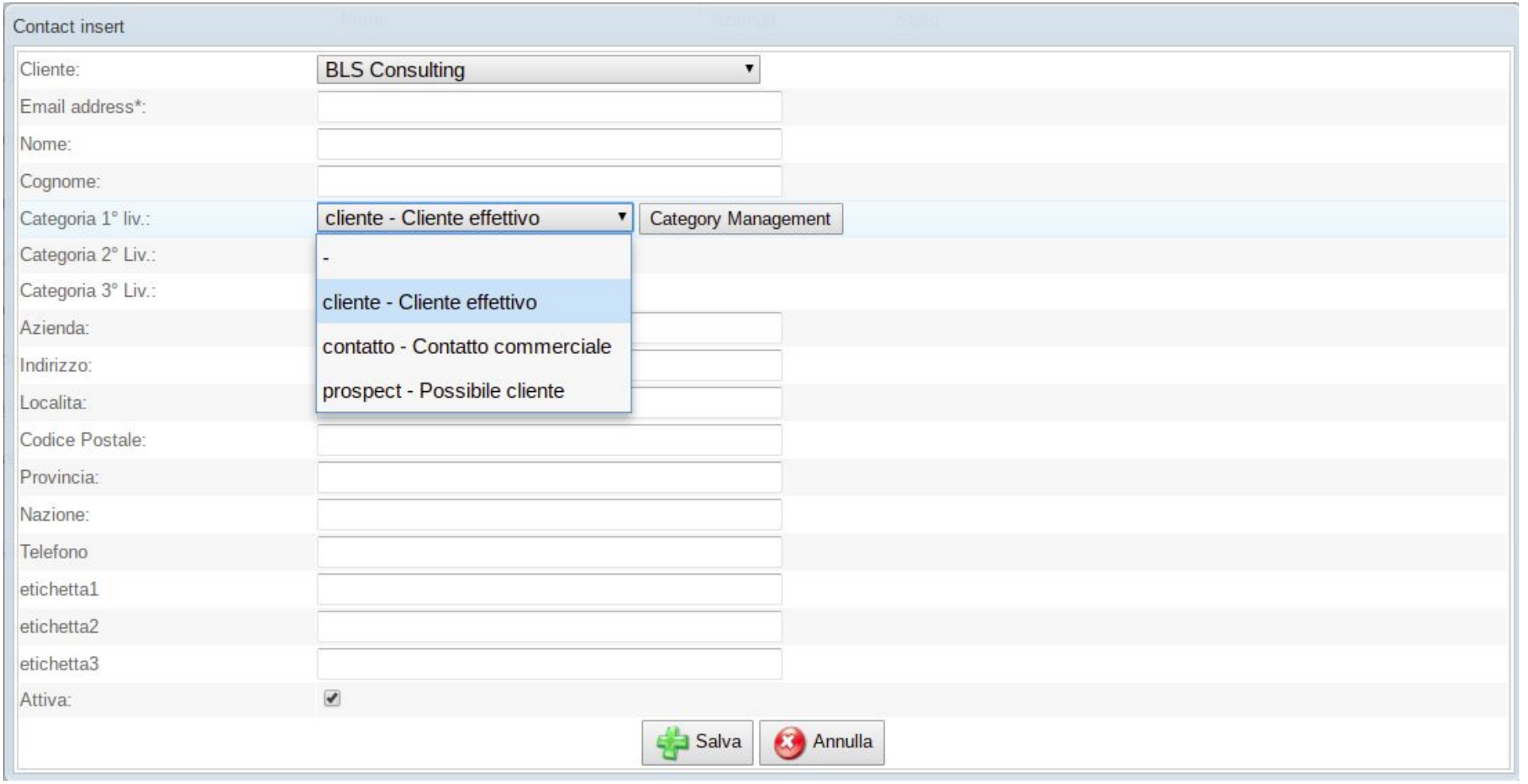


Le ultime tre icone in alto a destra permettono rispettivamente:

- inserire un nuovo contatto
- importare i contatti da un file in formato CSV
- esportare i contatti in formato CSV

Se un contatto viene disattivato non verranno inviate email anche se presente in una lista di distribuzione.

E’ possibile associare un contatto ad una categoria, ciò permetterà creare velocemente liste di distribuzione estraendo tutti i contatti di una determinata categoria:

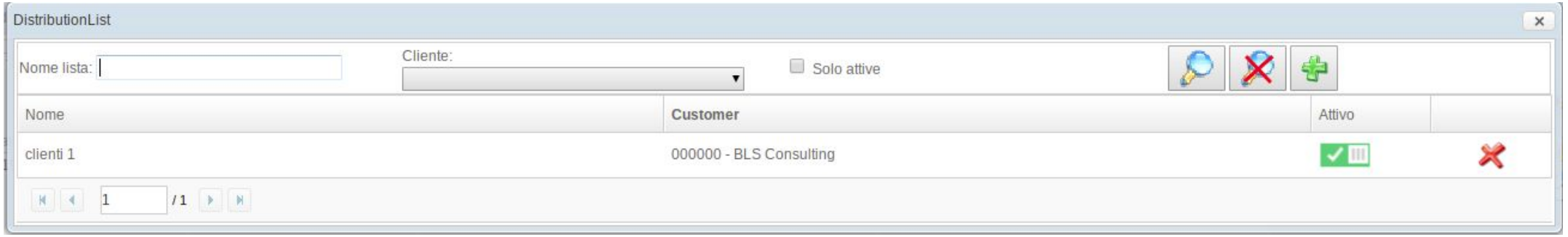


Le categorie sono gerarchiche su tre livelli, è comunque possibile specificare dei valori solo per il primo livello od i primi due.

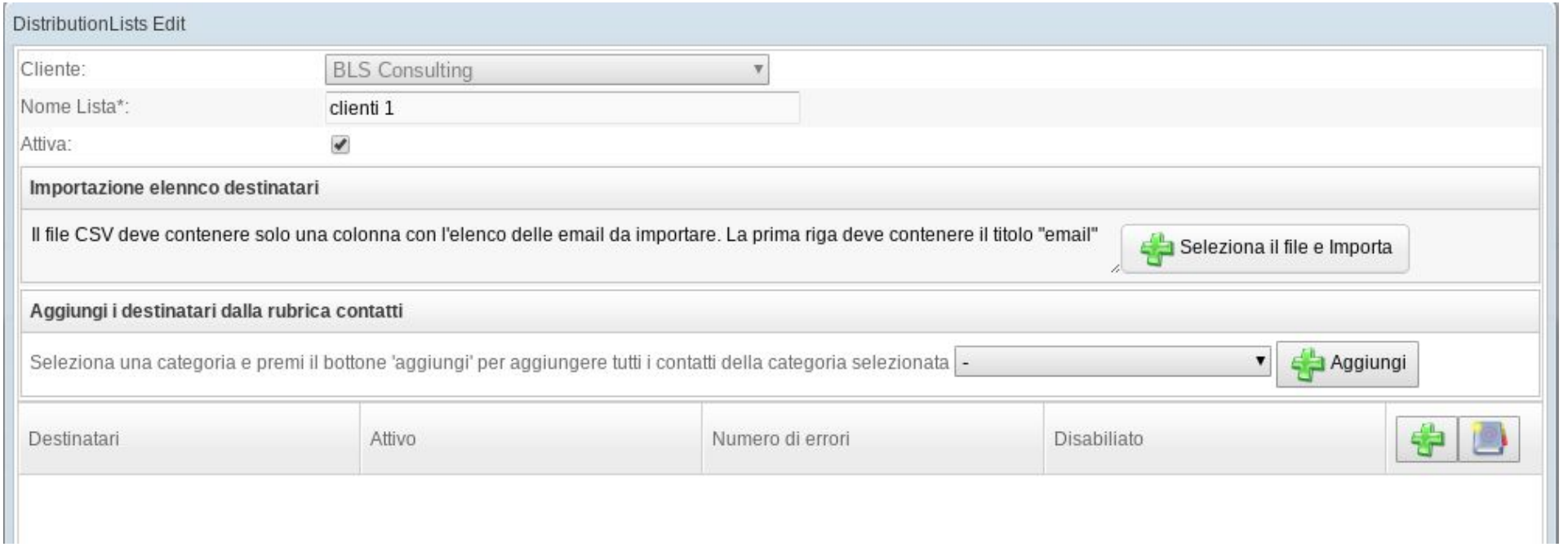
LISTE DI DISTRIBUZIONE

Questa opzione permette gestire le liste di distribuzione.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.



Cliccando sull'icona + è possibile aggiungere una lista di distribuzione, viene quindi visualizzata la pagina che permette aggiungere l'elenco dei destinatari della lista di distribuzione con diverse modalità, come illustrato nella prossima pagina.



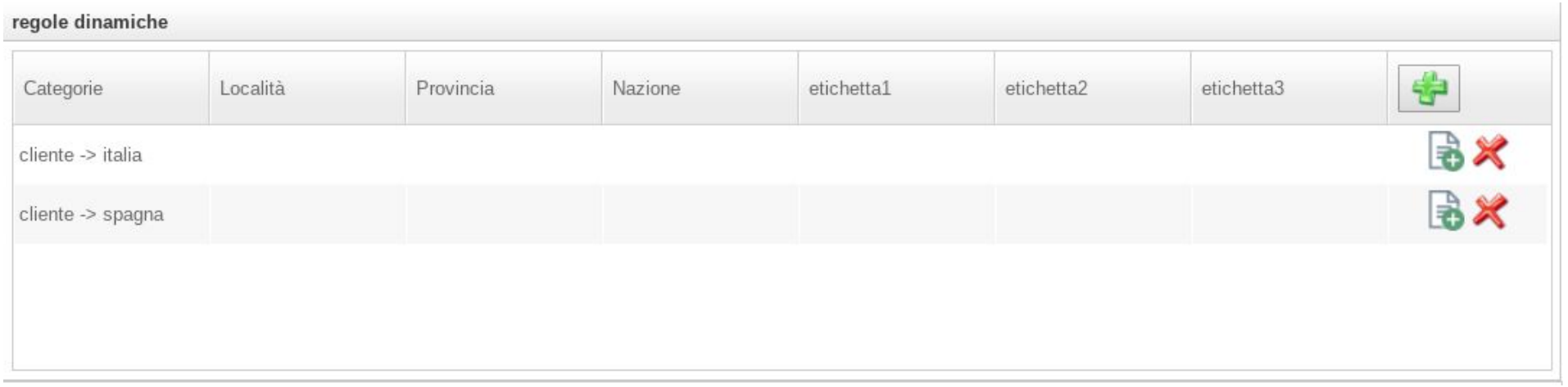
Cliccando su “Seleziona il file e importa” è possibile importare la lista dei destinatari da un file in formato CSV.

E’ anche possibile importare i destinatari dal database dei contatti selezionando la categoria e cliccando su “Aggiungi”.

Cliccando sull’icona “+” è possibile aggiungere un singolo destinatario nella lista.

Cliccando sull’icona Rubrica è possibile selezionare i destinatari dal database dei contatti.

E’ anche possibile specificare delle regole dinamiche per il popolamento della lista di distribuzione:



Queste regole verranno usate per estrarre i dati dal database dei contatti quando inizia la spedizione di una newsletter.

Nell’esempio sopra sono selezionati i clienti di Italia e Spagna.

EMAIL TEMPLATE

Questa opzione permette gestire i modelli di email da spedire con la funzionalità di mass mailing.

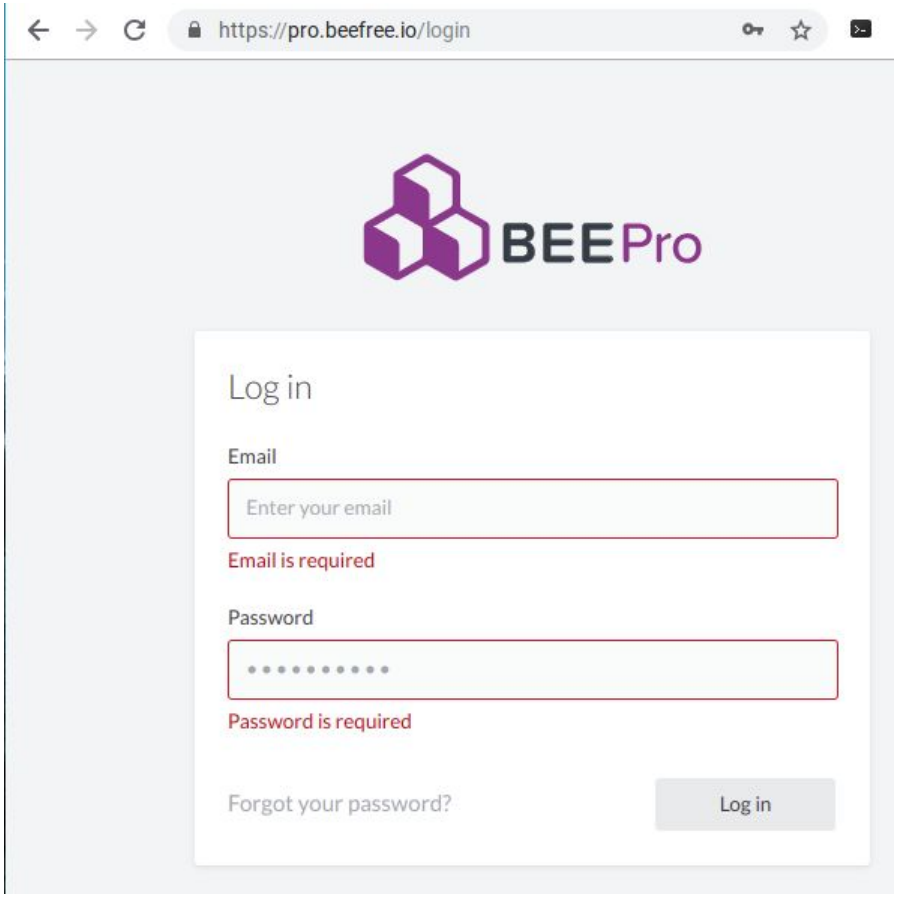
Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Cliccando sull'icona + è possibile aggiungere un nuovo modello (template) di email. L'email va scritta in HTML o più semplicemente utilizzare il servizio BeePro per costruire il modello.

Cliccando sull'icona BeePro new project si accede direttamente alla creazione di un nuovo progetto, mentre cliccando su BeePro projects si accede alla gestione dei progetti, l'uso di questo sistema è illustrato di seguito.

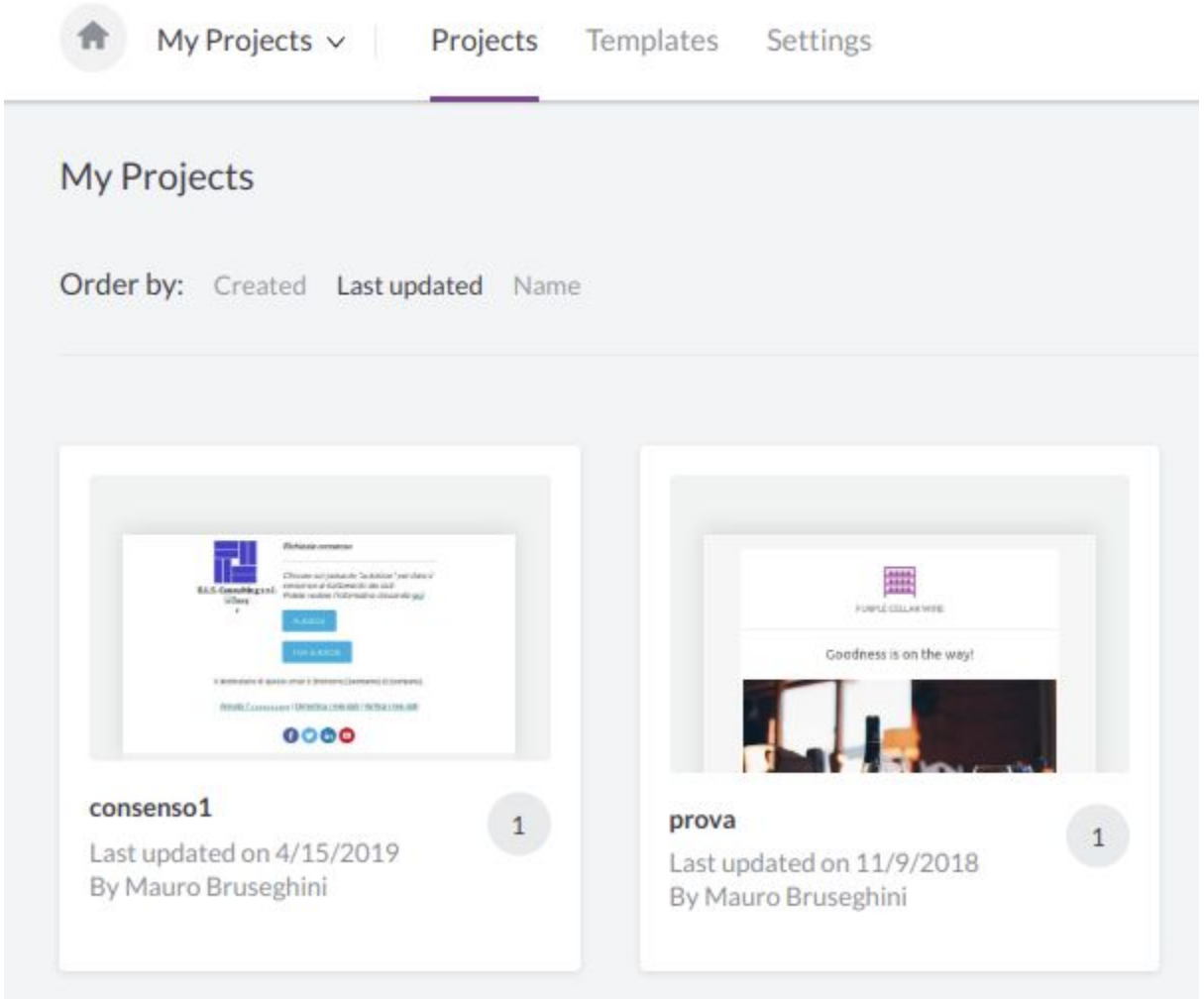
Per accedere a BeePro utilizzare un browser e aprire la seguente pagina:

https://pro.beefree.io



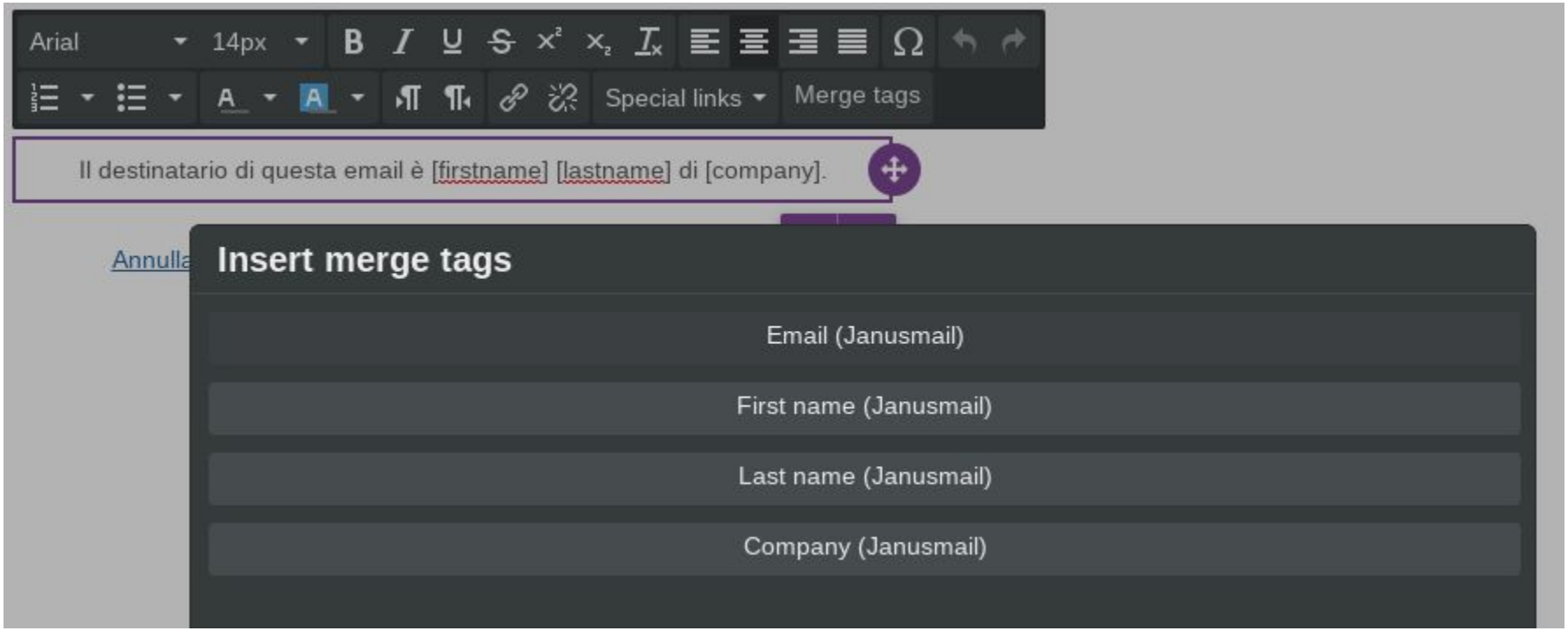
Inserire quindi l'email e la password per accedere.

Verranno quindi visualizzati i progetti inseriti:



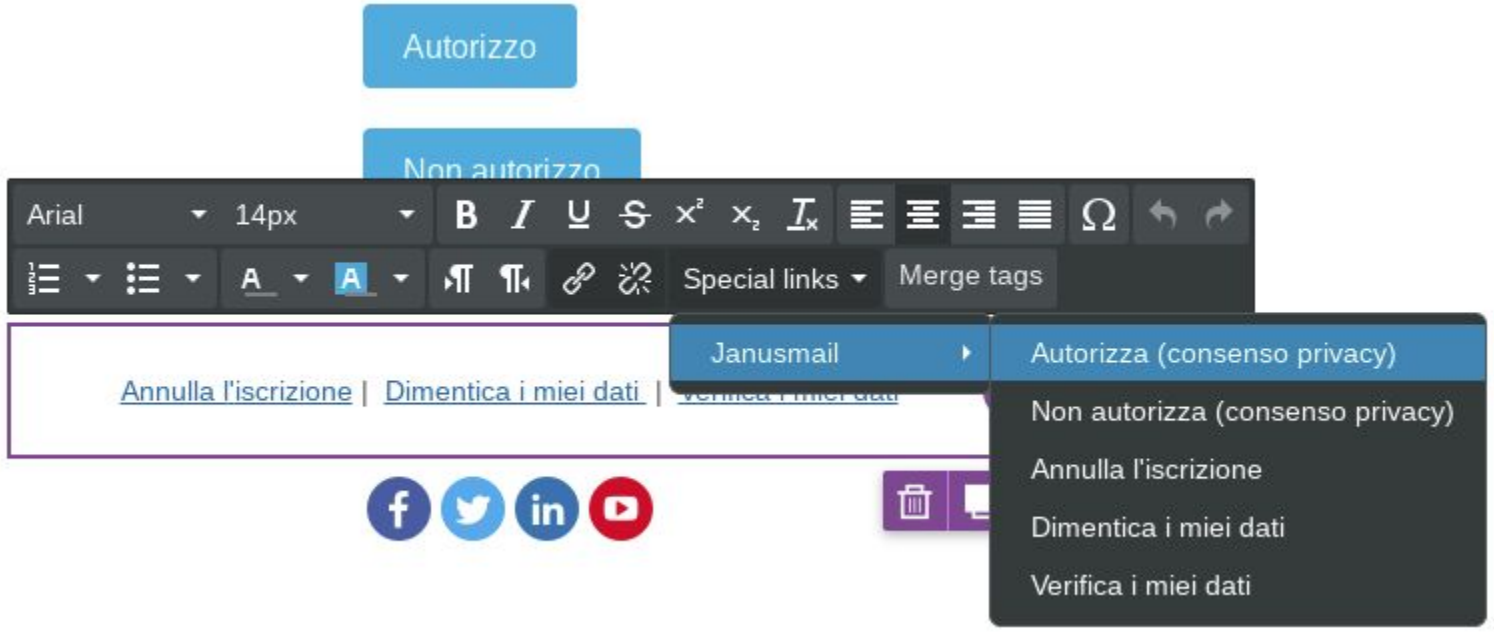
Cliccando su “Create a new project” verrà creato un nuovo progetto contenente uno o più messaggi (modelli di email)

Nei messaggi si possono inserire dei campi (con la funzione Merge tags) che verranno sostituiti con i dati anagrafici del destinatario presi dal database dei contatti:



In questo modo è possibile personalizzare l'email inserendo nel testo l'indirizzo email del destinatario, il nome, il cognome o la ragione sociale dell'azienda.

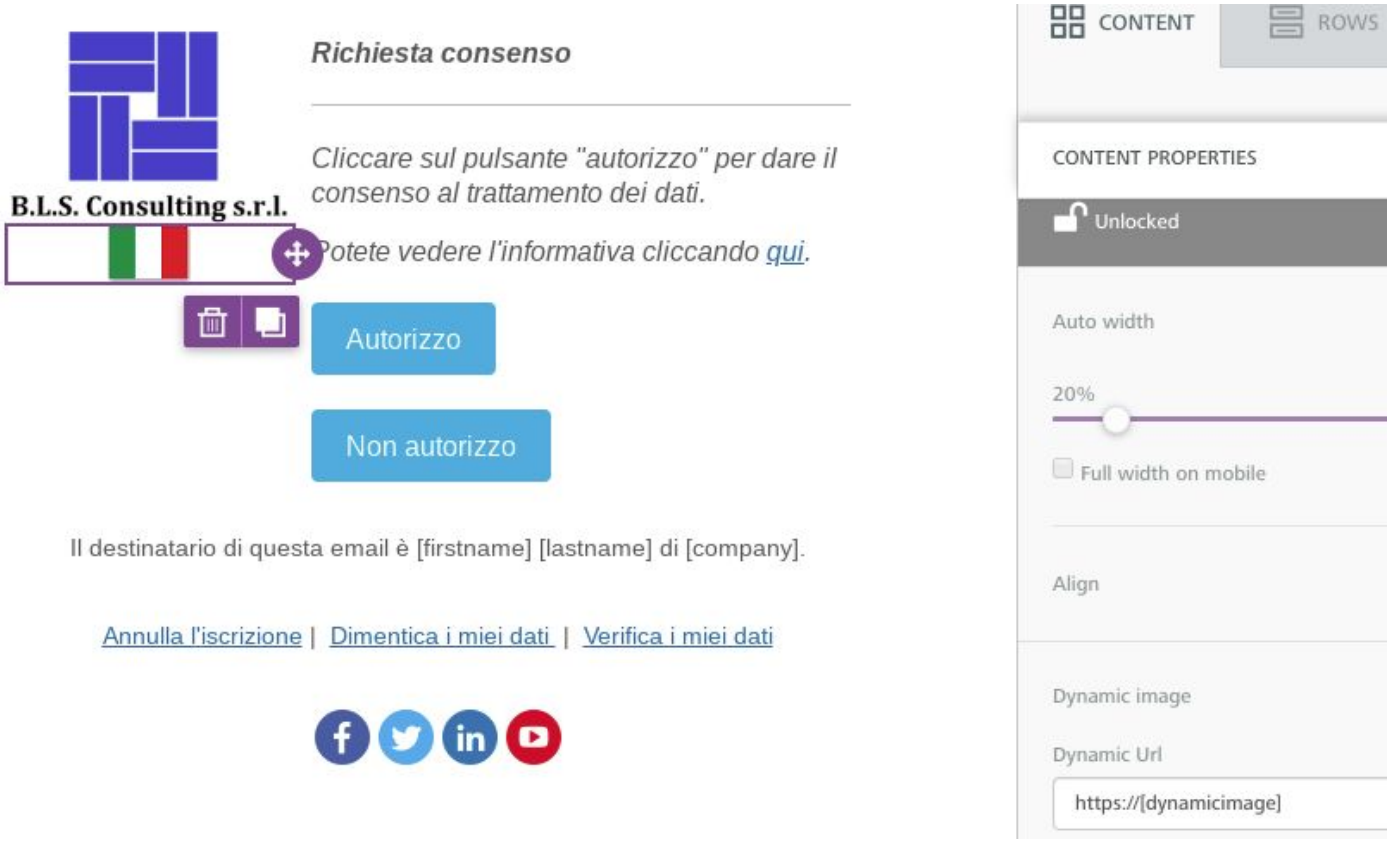
Inoltre si possono aggiungere dei link (con la funzione special links) che attivano diverse funzionalità:



Le funzioni sono:

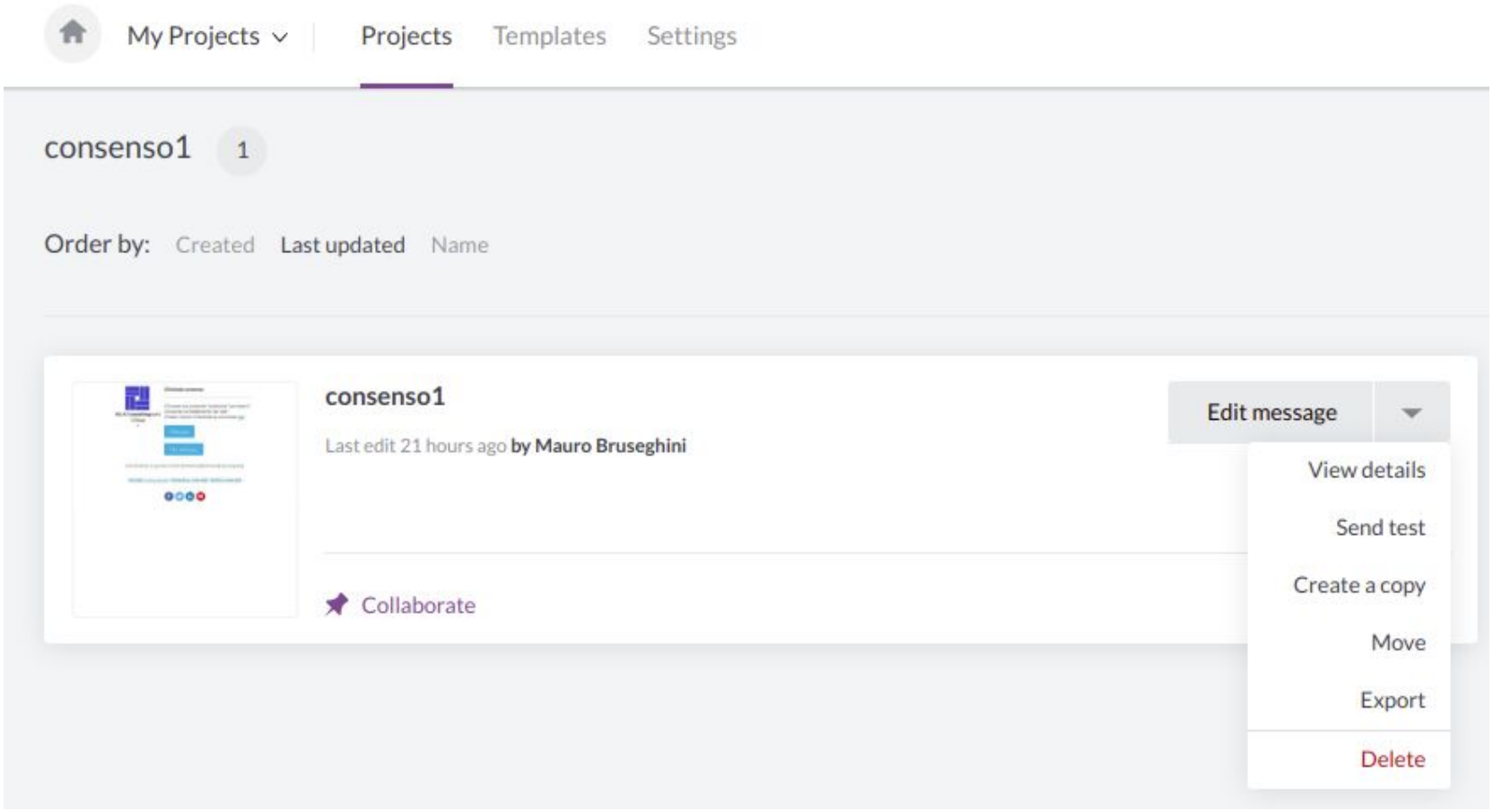
- autorizza: da usare per link o pulsanti per autorizzare il trattamento dei dati (consenso privacy/GDPR), se il destinatario clicca su questo link/pulsante verrà memorizzata la data, l'ora e l'indirizzo IP di chi autorizza il consenso
- non autorizza: da usare per link o pulsanti per non autorizzare il trattamento dei dati (consenso privacy/GDPR), se il destinatario clicca su questo link/pulsante verrà memorizzata l'opposizione al trattamento nel database dei contatti
- annulla iscrizione: permette inserire un link per richiedere la cancellazione dalla newsletter
- dimentica i miei dati: permette inserire un link per richiedere la cancellazione dei propri dati (diritto all'oblio)
- verifica i miei dati: permette inserire un link per richiedere la verifica dei propri dati (verrà inviata una email con la richiesta al responsabile privacy dell'azienda)

E’ inoltre possibile aggiungere un’ immagine (che nelle email inviate risulterà invisibile) chiamata “dynamic image”:



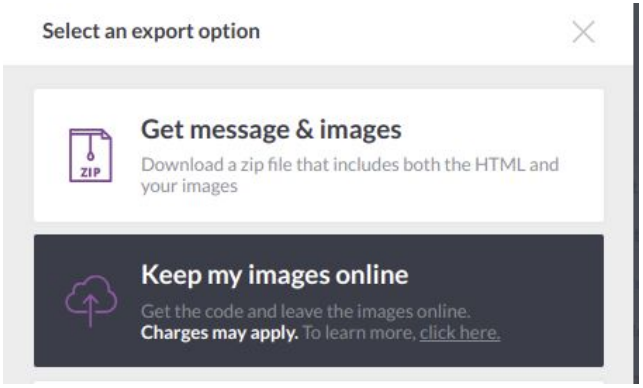
Nell’esempio è evidenziata con la bandiera italiana, specificare nel campo Dynamic Url: https://[dynamicimage]

Inserire questa immagine è utilissimo, in quanto verrà visualizzata appena l’utente visualizza l’email, Janusmail memorizza quindi quando un utente legge effettivamente l’email e non solo se l’ha ricevuta.

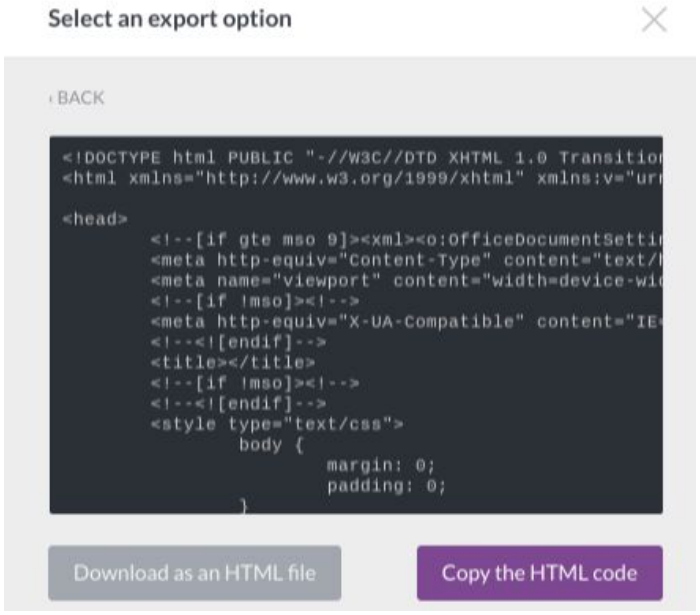


Le opzioni permettono:

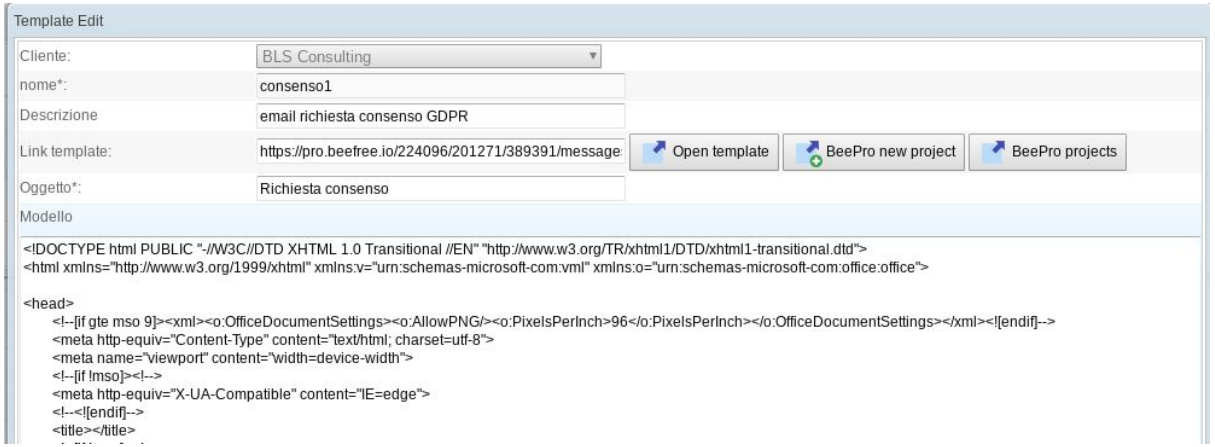
- editare il messaggio. creare una copia, muoverlo in un altro progetto, cancellarlo
- inviare una email di test con questo messaggio
- esportarlo, usare l'opzione di esportazione "Kepp my images online"



Questa opzione permette mantenere online le immagini inserite nella email, contribuendo a mantenere contenuta la dimensione dell'email favorendone la consegnabilità. Cliccare quindi su "Copy the HTML code":

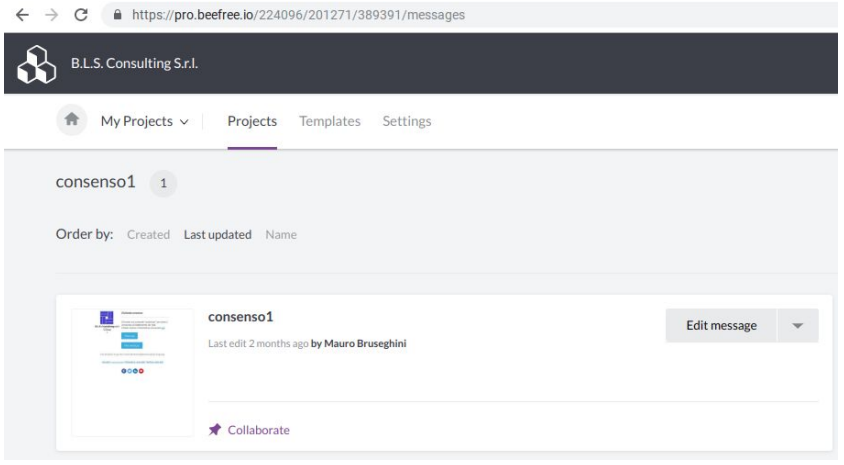


Incollare quindi il codice HTML nel template nel campo Modello:



Incollare anche il link al template nel campo Link template, cliccando poi su Open template si potrà andare direttamente in gestione del modello su BeePro.

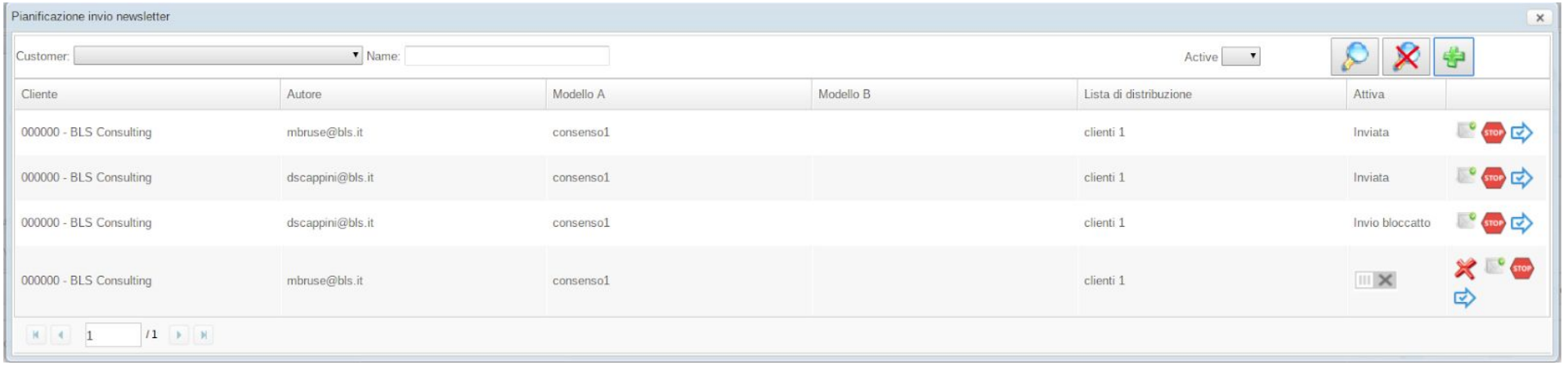
Il link da copiare è l'url visualizzato nel browser per la pagina seguente:



SCHEDULAZIONE EMAIL

Questa opzione permette schedulare l'invio delle email di tipo mass mailing.

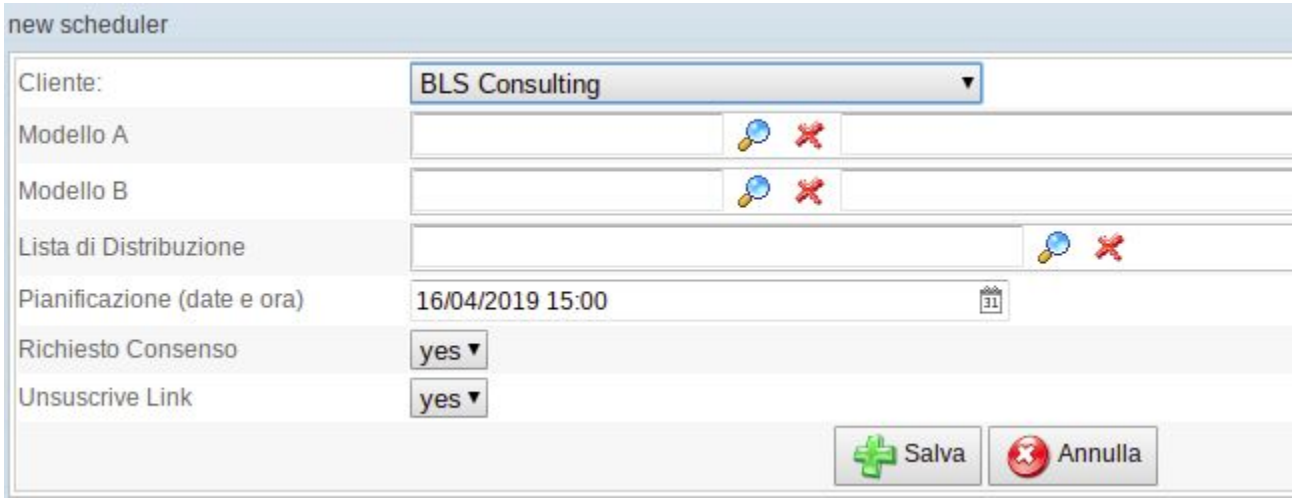
Per accedere cliccare sulla corrispondente opzione del menu funzioni.



Cliccando sull'icona + è possibile aggiungere una nuova schedulazione.

A fine di ogni riga sono presenti le icone per:

- vedere lo stato di di spedizione di una newsletter
- bloccare immediatamente l'invio di una spedizione in corso
- inviare una email di test a dei destinatari selezionati



Selezionare quindi un modello (email template), è possibile specificarne due (modello A e B), se se ne specificano due metà delle email verranno spedite con un modello e metà con l'altro. Sarà quindi possibile valutare l'efficacia dei due modelli di email verificando quanti destinatari si "convertiranno" con un modello e quanti con l'altro.

Selezionare quindi la lista di distribuzione a cui inviare l'email e la data/ora di inizio spedizione.

Se poi il flag "Richiesto consenso" viene posto uguale a yes, le email verranno inviate solo ai contatti che avranno espresso il consenso.

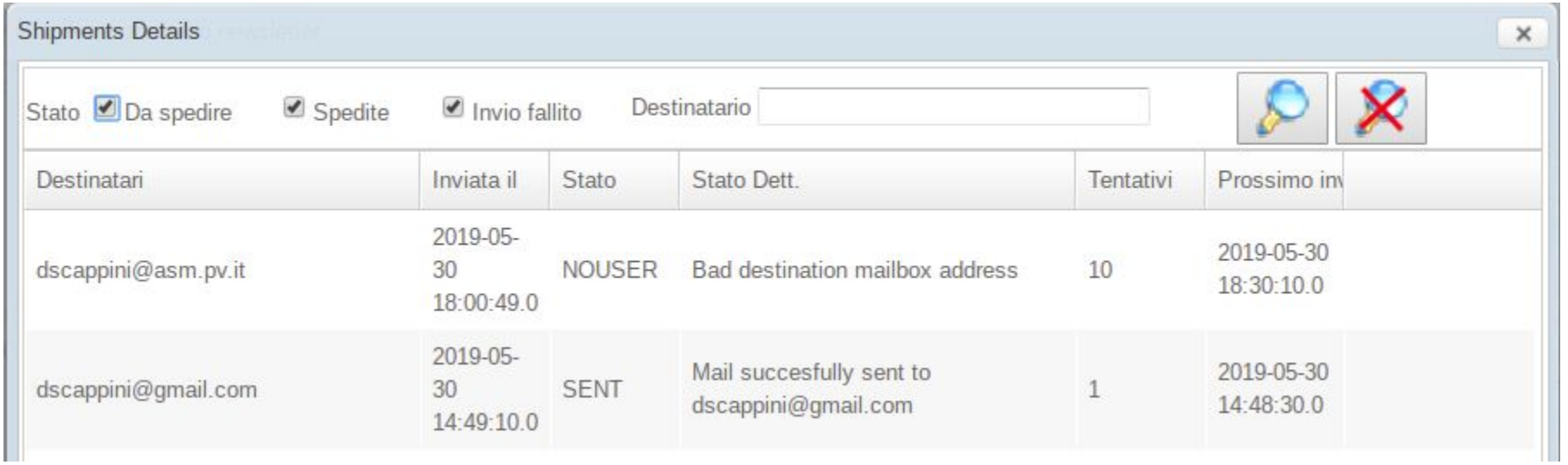
Se viene messo a yes il flag Unsuscribe Link, nell'intestazione della email (headers) verrà aggiunti il link per permettere l'annullamento dell'iscrizione alla newsletter.

Ovviamente questi due flag vanno impostati in base al tipo di email da inviare, ad es.:

- per una email di richiesta consenso privacy/GDPR andranno posti entrambi a no
- per una email di marketing andrà posto a yes il flag "Richiesto consenso" e a no il flag "Unsubscribe Link"
- per una newsletter andranno posti entrambi a yes

A conclusione della spedizione delle email alla lista di distribuzione verrà inviato al mittente una email che permette accedere al report delle spedizioni.

Cliccando sull'incona "sent status" verrà visualizzato l'elenco dei destinatari e lo stato di consegna:



Sarà possibile selezionare spuntando le apposite caselle:

- le email ancora da spedire
- le email già spedite
- le email che hanno avuto problemi di spedizione

STATISTICHE

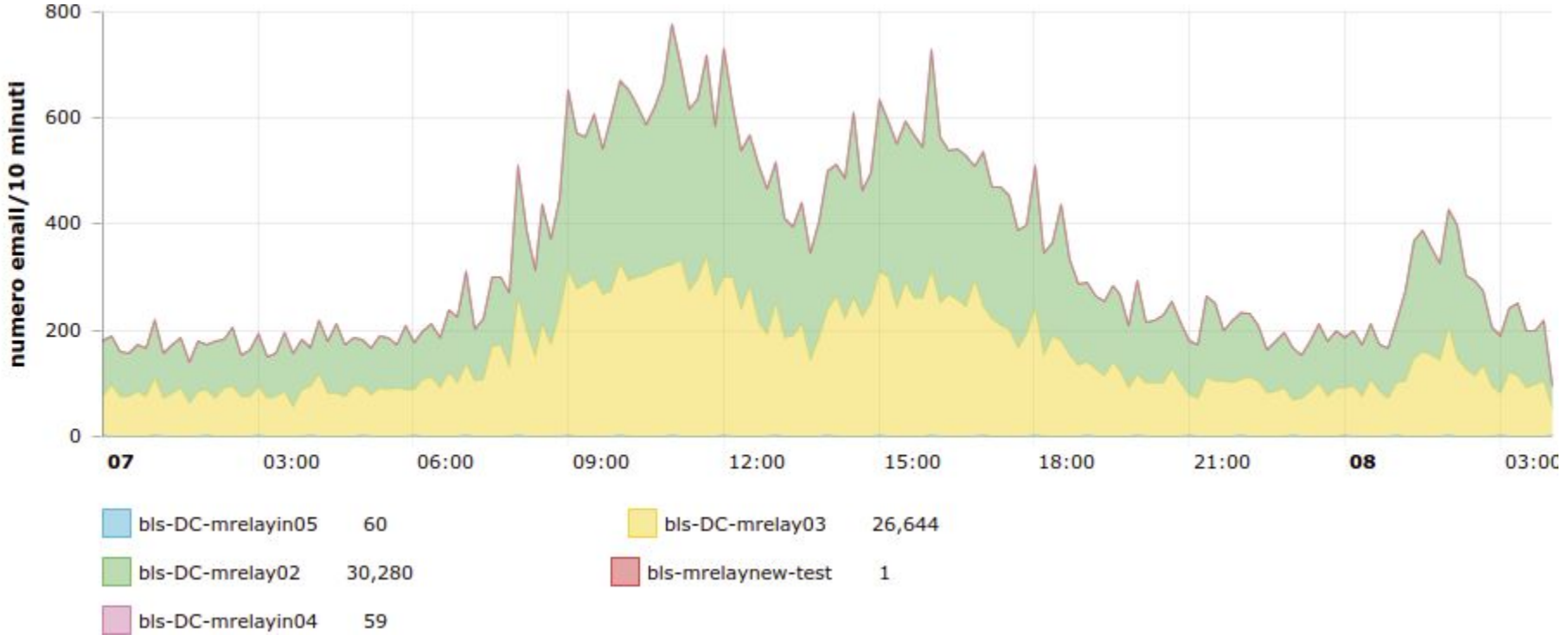
Janusmail dispone di diversi sistemi di statistiche per monitorare il funzionamento del sistema.
Queste funzioni sono disponibili per gli amministratori dei server e quindi esulano da questo manuale.

È però possibile, per un amministratore dei server, attivare l'invio giornaliero delle statistiche agli amministratori dei clienti.

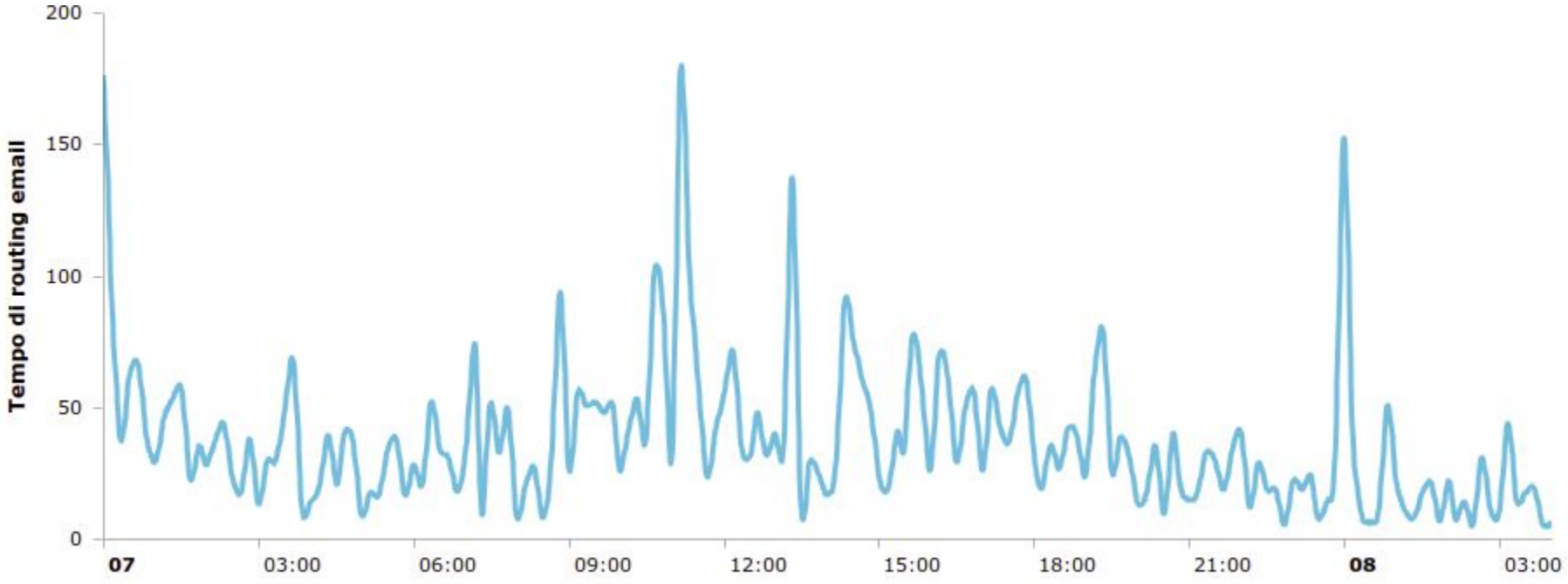
L'email viene spedita poco dopo le 4:00 e riporta sia le statistiche delle ultime 24 ore sia le statistiche dell'ultima settimana. Segue un esempio di email:

Le statistiche comprendono i seguenti grafici:

Volume di email gestite ogni 10 minuti (report giornaliero) od ogni ora (report settimanale) per mailrelay

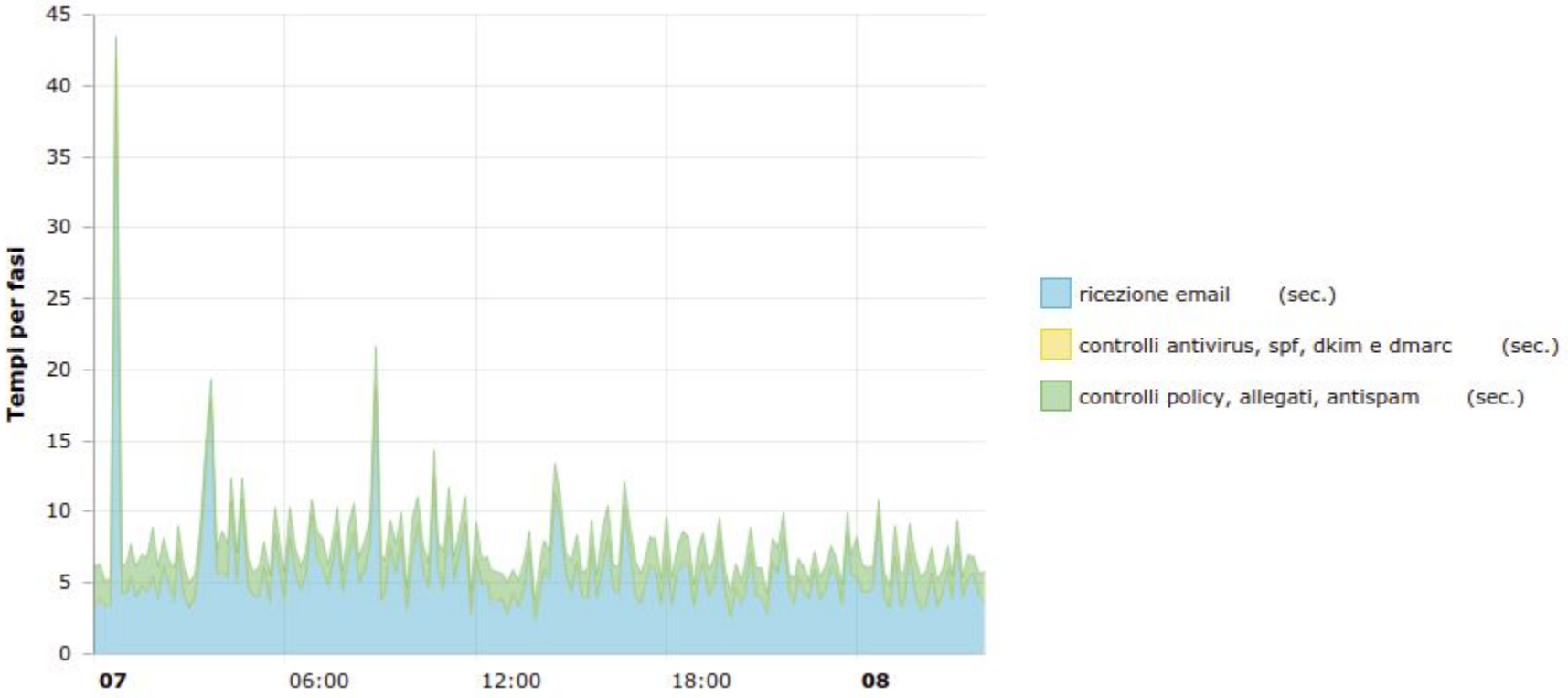


Tempo medio di routing (in secondi) del messaggio di email



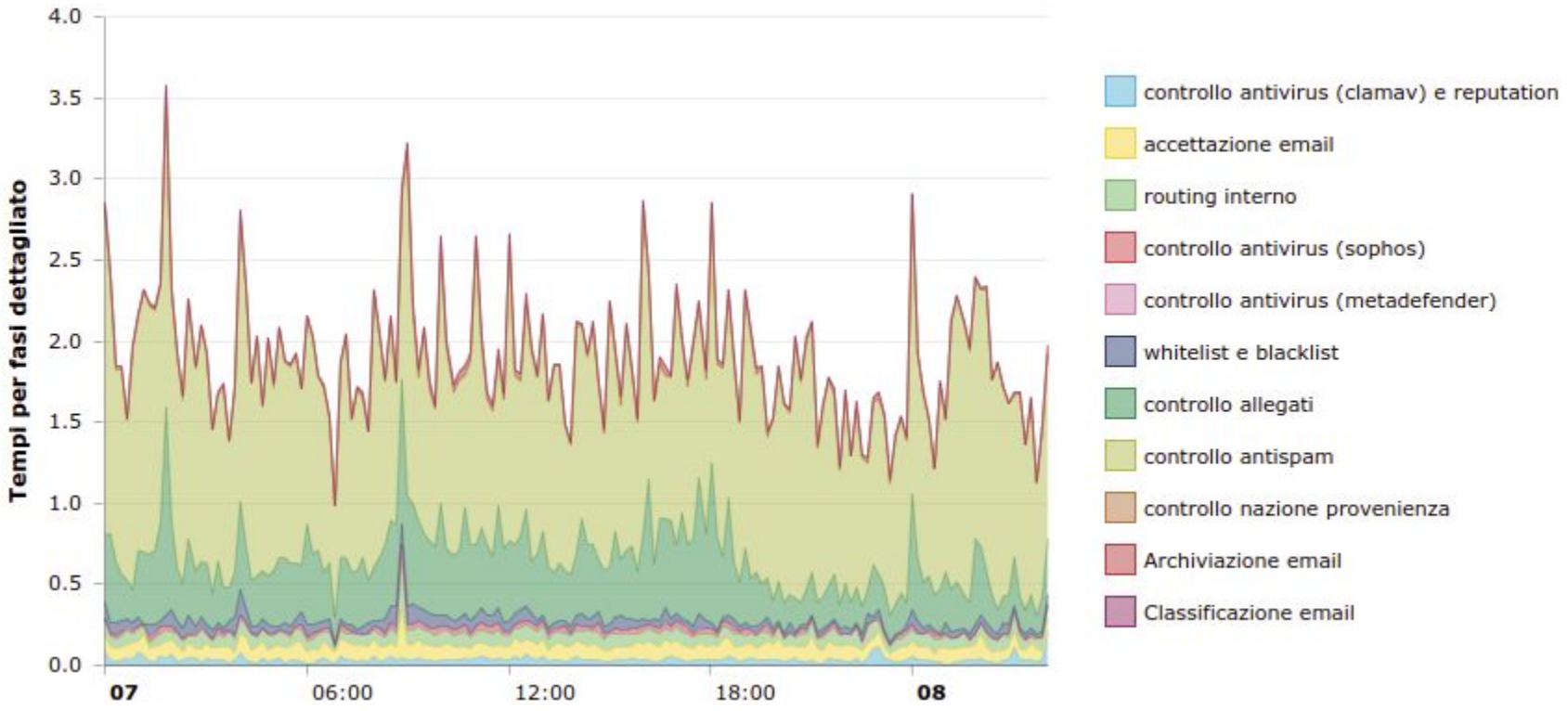
Indica il tempo complessivo, comprensivo del tempo di ricezione, analisi e consegna al server di destinazione.

Tempo suddiviso per macro fasi in secondi



Janusmail inizia a processare l'email mentre viene consegnata (azzurro), poi esegue una prima serie di controlli (giallo), salva l'email in coda e quindi esegue i controlli che richiedono più tempo di elaborazione (verde).

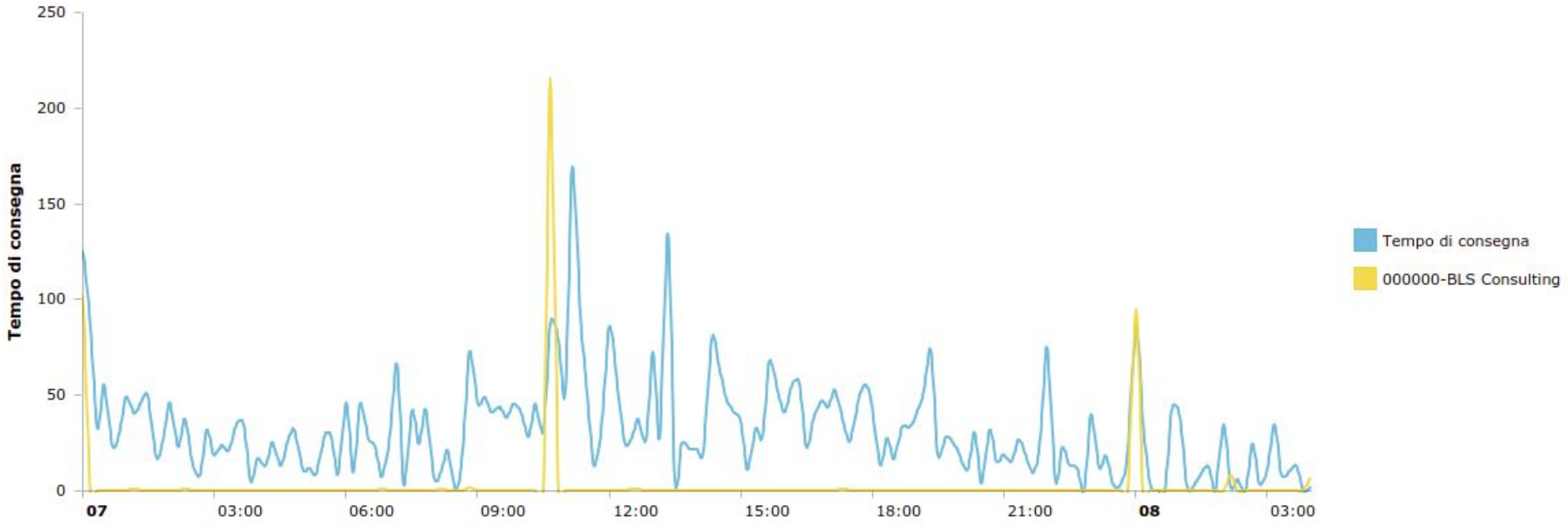
Tempo di elaborazione dettagliato per fasi in secondi



Se il server si sovraccarica, normalmente aumentano le fasi di controllo antivirus e antispam.

Un aumento molto limitato nel tempo della sola fase di controllo antivirus clamav o dell'antispam possono significare un aggiornamento delle firme in corso e conseguente interruzione momentanea del servizio (normalmente di qualche decina di secondi.)

Tempo di consegna in secondi



In azzurro è indicato il tempo medio di consegna per tutti i clienti.
Se ci sono problemi di consegna (tempi superiori ai 15 minuti di una email) viene riportato anche il grafico del cliente (in questo caso il nostro) per indicare una anomalia di consegna.

Normalmente le anomalie di consegna sono dovute a problemi di raggiungibilità del server di posta di destinazione causati da backup in corso, interruzione di servizio o per mancanza di connettività.

SOMMARIO