

Manuale Mail Sicura

Guida pratica per utenti

Informazioni documento	Autore	Omitech
	Data	24/01/2023
	Modello	MSP_documentazione_102020
	Nome file	Manuale_MailSicura_Users
	Stato	chiuso
Il presente documento è registrato all'emissione, dall'operatore, nel software documentale Omitech srl		

Sommario

1. Dashboard e credenziali di accesso.....	4
2. Home.....	4
View Msg Body.....	5
Msg Release.....	5
Data.....	5
Time.....	5
Sender.....	5
Recipient.....	5
Subject.....	5
Score.....	5
Soglie default del filtro antispam Mail Sicura.....	5
Status.....	6
3. Ricerca dei messaggi in Quarantena (Quarantine).....	7
4. Lists.....	8
5. Report.....	8
6. User Settings.....	9
7. FAQ.....	10

Storico documento

Data	Autore	Note

Allegati documento

File	Titolo	Note

1. Dashboard e credenziali di accesso

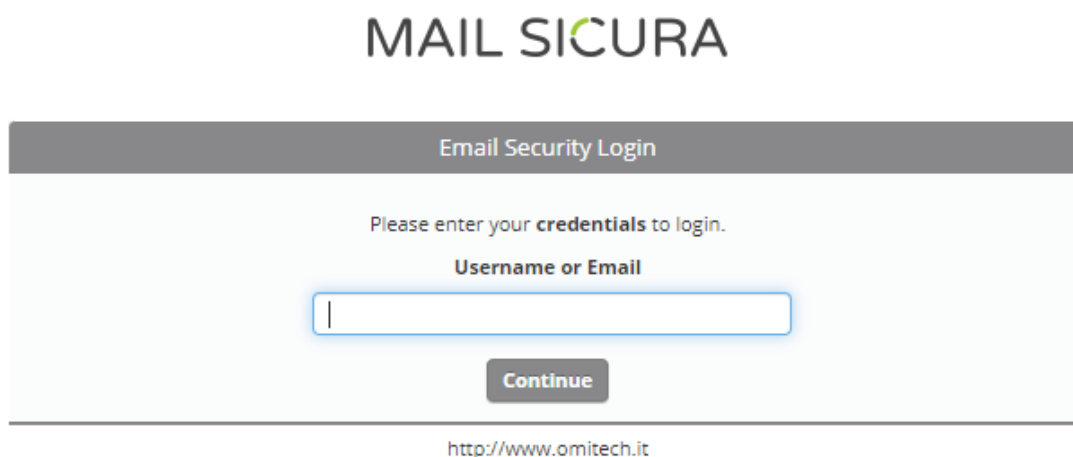
Gli utenti che hanno sottoscritto il servizio di posta OT-MAIL, possono gestire le impostazioni antispam accedendo al portale di MAIL SICURA raggiungibile al seguente link:

<https://mgw.ot-mail.it>

Per tutti gli altri utenti, il servizio MAIL SICURA sarà raggiungibile a uno dei seguenti link e verrà comunicato in fase di attivazione del servizio:

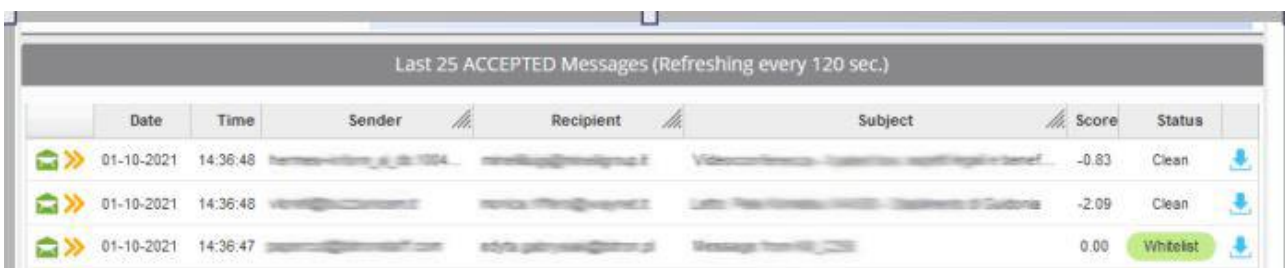
<https://mailsicura.ot-mail.it>

<https://ms02.ot-mail.it>



2. Home

La sezione **Home** riporta gli ultimi 25 messaggi ricevuti, la pagina si aggiorna di default ogni 120 secondi, la sezione **Quarantena** visualizza tutti i messaggi in quarantena degli ultimi 30 giorni. La pagina in entrambe le sezioni è composta da 8 colonne:



Last 25 ACCEPTED Messages (Refreshing every 120 sec.)							
	Date	Time	Sender	Recipient	Subject	Score	Status
	01-10-2021	14:36:48	sender@domain.it	recipient@domain.it	Subject of the message	-0.83	Clean
	01-10-2021	14:36:48	sender@domain.it	recipient@domain.it	Subject of the message	-2.09	Clean
	01-10-2021	14:36:47	sender@domain.it	recipient@domain.it	Subject of the message	0.00	Whitelisted

View Msg Body

Cliccando sulla lettera verde si potrà leggere la mail e compiere alcune azioni basilari, rispondere inoltrare, scaricare la mail in formato eml, rilasciare il messaggio e infine aggiungere o rimuovere il mittente in black o white list. Questa funzionalità ritorna molto utile per leggere in anteprima eventuali mail sospette bloccate in quarantena.

Msg Release

Cliccando su *Msg Release* in corrispondenza del messaggio, il messaggio originale verrà rilasciato e consegnato al destinatario/i.

Data

La data di composizione della mail.

Time

L'ora di composizione della mail.

Sender

L'indirizzo mail del mittente specificato nel campo from dell'intestazione del messaggio.

Recipient

L'indirizzo mail del destinatario.

Subject

Oggetto del messaggio.

Score

punteggio ottenuto dall'analisi antispam, questo punteggio determina la categorizzazione del messaggio riportato nella colonna successiva nel caso il mittente non sia inserito in una whitelist o blacklist.

Soglie default del filtro antispam Mail Sicura

<=0 <=4 la mail è pulita e verrà consegnata.

>4 <=10 la mail è considerata un probabile messaggio di spam, la mail verrà egualmente consegnata ma nell'oggetto verrà anteposta la stringa *?SPAM* e verrà salvata una copia nella quarantena.

>10 <=25 la mail è considerata *High Spam* e non verrà consegnata ma trattenuta nella quarantena fino al suo rilascio che deve essere eseguito manualmente dall'utente cliccando su *Msg Release* dalla scheda *Home* oppure direttamente dalla scheda *Quarantena*. I messaggi in quarantena più vecchi di 30 gg vengono automaticamente eliminati.

>25 la mail viene scartata e non sarà salvata o consegnata al destinatario.

È molto raro che un messaggio superi il punteggio di 25, superati i 20 punti le casistiche individuano al 99.9% spam certo di nessuna utilità.

Status

Clean

Clean: il messaggio è pulito, verrà consegnato ($\leq 0 \leq 4$)

Spam

Spam: il messaggio è considerato probabile spam, verrà consegnato ma anteposta nell'oggetto del messaggio la stringa *?SPAM* ($>4 \leq 10$).

High Spam

High Spam: il messaggio ha ottenuto un alto punteggio di spam ha un'altissima percentuale di probabilità di essere spam ($>10 \leq 25$), verrà trattenuto in quarantena fino al rilascio da parte dell'utente.

Whitelist

WhiteList: il punteggio antispam non ha nessuna influenza, la mail viene consegnata, la whitelist viene gestita dall'utente o dagli amministratori, le liste gestite dagli amministratori hanno precedenza su quella impostata dall'utente.

BlackList

BlackList: il punteggio antispam non ha nessuna influenza, la mail non viene consegnata ma trattenuta in quarantena, l'utente può rilasciarla cliccando su *Msg Release*.

QuickSand

QuickSand: il messaggio indifferentemente dal punteggio antispam contiene un allegato di tipo Microsoft Office o pdf, sono previste diverse azioni a seconda del contenuto attivo individuato all'interno dell'allegato:

- Allegato con contenuto attivo ritenuto sicuro: il messaggio viene consegnato con allegato originale.
- Allegato con contenuto attivo di tipo sospetto o indeterminato: Mail Sicura quando possibile rimuove il contenuto attivo sospetto o indeterminato, altrimenti quando non ci riesce blocca il documento originale in quarantena. La mail verrà consegnata in ogni caso con l'allegato modificato senza il contenuto attivo, oppure verrà consegnata senza allegato nel caso non sia stato possibile rimuoverlo. Nel caso non si riesca ad aprire l'allegato, l'utente dovrà rilasciare il messaggio originale dalla quarantena (*Msg Release*) >>

- Allegato con contenuto attivo e criptato: il contenuto non può essere analizzato perché criptato perciò di default Mail Sicura blocca l'allegato in quarantena, potrà essere sbloccato dalla quarantena dall'utente cliccando su *MsgRelease*. >>>
Questo tipo di allegato è molto pericoloso perché comunemente utilizzato per inviare documenti con dati sensibili (buste paga, analisi mediche, etc), alcune minacce tra cui virus o messaggi di phishing sfruttano questa vulnerabilità consapevoli che una mail criptata non può essere analizzata. Molti utenti sottovalutano questo rischio chiedendo di modificare il filtro per fare in modo che consegni egualmente il documento originale. A nostro avviso e forte raccomandazione è invece opportuno che l'utente o l'amministratore di dominio acceda alla propria Dashboard di Mail Sicura, visioni in anteprima il messaggio (*Msg Details*) e una volta riconosciuto come attendibile, lo rilasci dalla quarantena (*Msg Release*). In alternativa è consigliabile chiedere al mittente di inviare i messaggi di posta in chiaro su connessione TLS se non strettamente necessario che il messaggio sia criptato end to end.

3. Ricerca dei messaggi in Quarantena (Quarantine)

È possibile cercare i messaggi in quarantena, non più vecchi di 30 giorni, nella sezione *Quarantine*. I parametri di ricerca presenti sono classici, ad eccezione dell'ultimo che consente di restringere il campo di ricerca definendo la ragione del blocco in quarantena.

MAIL SICURA

Home Reports Lists Quarantine User Settings

Quarantine Management

From this section you can manage your quarantined messages.

Quarantined Messages

Export Search Help

Date	Time
29-09-2021	09:13:50
29-09-2021	03:28:09
28-09-2021	12:17:53
28-09-2021	09:22:32
28-09-2021	04:26:03

Search

Refine your search with the filter below. Filter is set on exact match:

From Date (yyyy-mm-dd): 2021-09-22

To Date (yyyy-mm-dd): 2021-09-29

Subject:

Sender Email:

Recipient Email:

Block Reason: All Messages

Search Reset Search

Score	Status	Delivery
0.00	BlackList	-
20.58	High Spam	-
19.29	High Spam	-
19.68	High Spam	-
29.14	High Spam	-

4. Lists

Lists permette all'utente di gestire le proprie liste di indirizzi mail da cui accettare o rifiutare messaggi indifferentemente dal fatto che la mail sia considerata dal motore antispam, clean, spam o high spam. Nella lista Spam Whitelist di norma si inseriscono tutti gli indirizzi mail attendibili da cui sono state ricevute mail identificate come spam, mentre nelle Blacklist gli indirizzi mail dei mittenti per i quali vogliamo che le mail vengano non recapitate e trattenute in quarantena. Nelle liste Spam Whitelist e Spam Blacklist saranno presenti tutti gli indirizzi mail popolati autonomamente a seconda delle segnalazioni dell'utente tramite *Msg Details* o segnalati cliccando il link di segnalazione presente in ogni mail ricevuta scansionata da Mail Sicura o inseriti manualmente dall'utente direttamente nella lista.

Importante:

- Per l'utente è possibile inserire nelle liste solamente indirizzi mail completi.
- Se un indirizzo mail è inserito in entrambe le liste, ha precedenza la lista Spam Whitelist.
- Le liste hanno efficacia solamente per modificare il filtro antispam, tutti gli altri filtri di controllo hanno la precedenza tra cui Antivirus Content filter (controllo allegati), Quick Sand e Url Sand, perciò è possibile che una mail venga egualmente bloccata in quarantena nonostante l'utente abbia inserito in Spam Whitelist l'indirizzo mail del mittente.

5. Report

Questa sezione permette di creare dei Reports personalizzati, configurando diversi parametri tramite l'aggiunta di filtri: *Add New Filter*.

Ad esempio, per estrarre tutte le mail ricevute oggi da uno specifico mittente, avrò bisogno di aggiungere due filtri.

- Primo filtro:
 - Field: Day
 - Filter Expression: is Equal
 - Value: Today
- Secondo filtro
 - Next filter: And
 - Field: From Address
 - Filter Expression: "is equal to" oppure "contains"

- Value: <indirizzo del mittente> (digitare l'indirizzo del mittente)

Dopo averli aggiunti potrò visionarli e gestirli da *Active Filters*.

Subito a destra nel riquadro *Filter Results* potrò visionare i risultati e visualizzare i messaggi estratti cliccando su *Message Listing*.

6. User Settings

Se consentito dall'amministratore di dominio, l'utente può modificare alcuni parametri riguardanti il proprio profilo utente di Mail Sicura.

- **Full name:** nome visualizzato dell'utente spesso coincide con l'indirizzo mail
- **Spam checks:** permesso di gestione Spam. L'amministratore può permettere o meno di far gestire lo spam all'utente
- **Spam Score e HiSpam:** soglia per l'individuazione e categorizzazione di una mail di spam o High Spam (si consiglia di non modificare e lasciare vuoti i due parametri).
- **Quarantine Report:** se spuntato consente di ricevere o meno il report giornaliero delle mail in quarantena
- **Quarantine Email:** l'indirizzo del destinatario a cui recapitare il Report giornaliero dei messaggi in quarantena, di default viene configurato l'indirizzo e-mail principale dell'utente
- **Quarantine Msg Preview:** consente di leggere in anteprima i messaggi in quarantena
- **Schedule Delivery at, Additional delivery:** per recapitare il report giornaliero della quarantena più volte al giorno in orari diversi
- **Two factor Authentication:** permette di attivare l'autenticazione a due fattori con l'ausilio di Google Authenticator o FreeOTP

7. FAQ

- ***Che tipo di allegati vengono bloccati da Mail sicura?***

Se non diversamente specificato dall'amministratore di dominio, Mail Sicura blocca gli allegati protetti da password, criptati, con contenuto attivo non riconosciuto come sicuro del tipo Microsoft Office o pdf e con le seguenti estensioni.

.ade .adp .ani .b64 .bat .bhx .cab .cdxml .ceo .cer .chm .cmd .cnf .cnt .com .cpl .crt .cur .der .diagcab .dll .exe .fdf .grp .hpj .hqx .hta .ico .img .ins .iqy .iso .isp .its .jar .jnlp .job .jse? .lha .lib .lnk .lzh .mad .maf .mag .mam .maq .mar .mas .mat .mau .mav .maw .mcf .mda .mde .mdz .mhtml .mim .mobileconfig .msc .msi .msp .mst .msu .oft .pif .pl .prf .printerexport .ps1 .ps1xml .ps2 .ps2xml .pscd1 .pscd2 .psdm1 .pssc .pst .py .pyc .pyo .pyw .pyz .pyzw .reg .scf .scr .sct .settingcontent-ms .shb .shs .sys .theme .udl .uue .vbe .vbp .vbs .vhd .vmdk .vsmacros .vss .vst .vsw .vxd .webpnp .website .ws .wsb .wsc .wsf .wsh .xbap .xll .xnk .xxe

- ***Come funziona la funzione sandbox che analizza ogni link all'interno della mail?***



Si tratta del componente di Sandboxing Urlsand, che scansiona in tempo reale la pagina di destinazione, nel caso venga rilevato un potenziale rischio per la sicurezza ne impedirà l'accesso all'utente.

- ***Non ricevo messaggi con allegati criptati o protetti da password, come posso risolvere il problema?***

Gli allegati criptati o protetti da password non possono essere esaminati dagli antispam e antivirus, perciò vengono trattenuti in quarantena come non sicuri, solitamente interviene il filtro Quicksand. L'utente può comunque rilasciarli dalla pagina quarantena. Per maggiori dettagli vedere [paragrafo Status](#)