DIGIWAY

PEC MANAGER

GUIDA INSTALLAZIONE

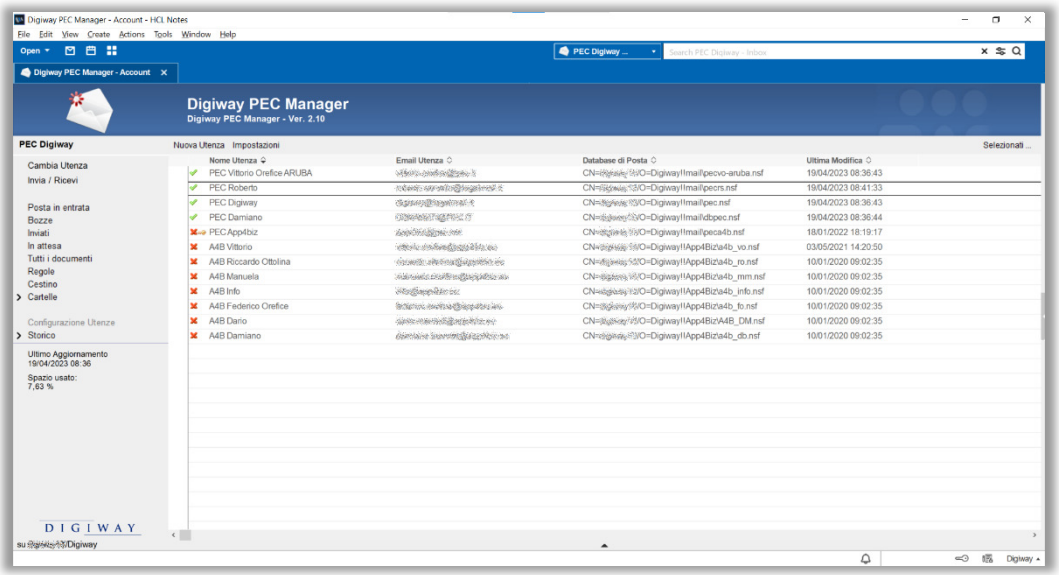
DIGIWAY srl
www.digiway.it info@digiway.it
Via C. Battisti, 2 – 20081 - Abbiategrasso (MI) Tel +39 02 87158030 Fax +39 02 70030800
Sede Legale Via Valsesia, 50 20152 Milano P.Iva 13383650150 PEC Digiway@legalmail.it
Capitale Sociale 10.500 € i.v.Iscrizione REA N° MI-1645521 – Reg. Imp. N° MI-2001-94354

INDICE DEI CONTENUTI

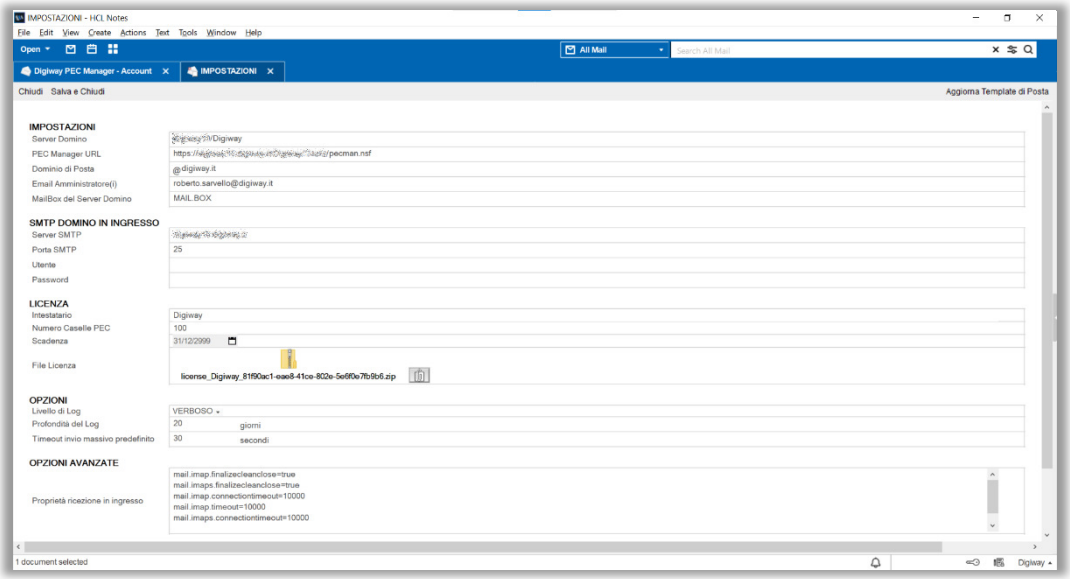
PREMESSA

Digiway PEC Manager è costituito da un'applicazione Domino che rappresenta l'interfaccia utente unica alle caselle PEC, indifferentemente per l'accesso da client Notes, Web browser o Tablet/Smartphone.

Dalla stessa interfaccia, gli utenti dotati del ruolo [Admin], possono accedere alla vista Configurazione Utenze dalla quale è possibile eseguire la configurazione delle caselle PEC ed accedere alle Impostazioni generali dell'applicazione; per gli stessi utenti sarà disponibile la vista Storico contenente il log degli eventi principali e degli eventuali errori.

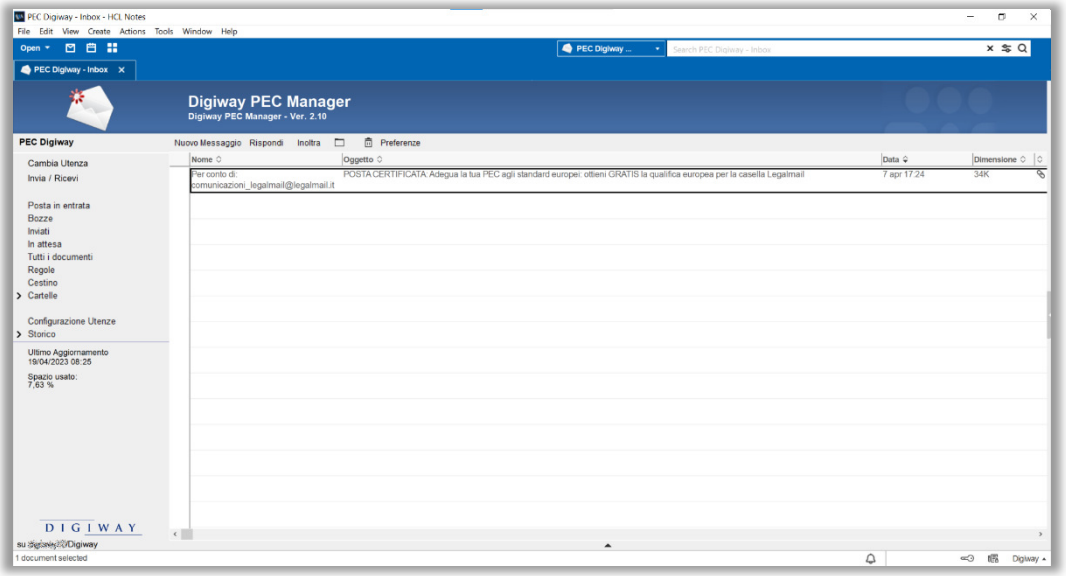


Le mail ricevute nelle singole caselle sono contenute in database di posta custom separati, che vengono acceduti mediante Digiway PEC Manager. Il template usato da questi database di posta è contenuto in Digiway PEC Manager e vi si può accedere dalle Impostazioni generali dell'applicazione.



Lo scambio di mail sia in ingresso che in uscita è gestito da un agente Domino (**PEC MANAGER**) che viene eseguito automaticamente ogni 5 minuti.

I messaggi in uscita vengono letti dalla vista **In attesa** delle singole caselle, viene contattato il server SMTP configurato nella relativa utenza, inviati e spostati nella vista **Inviati**. Se occorre un invio immediato (senza attendere la schedulazione dell'agente Domino), l'utente può cliccare su **Invia / Ricevi**, presente nel navigatore di Digiway PEC Manager.



Per quanto riguarda i messaggi in ingresso, l'agente **PEC MANAGER** contatta il server IMAP, scarica i messaggi non ancora ricevuti e li consegna al server Domino mediante il servizio SMTP del server stesso[1], definito nelle Impostazioni generali di PEC Manager. Il server Domino riceve questi messaggi e li inoltra al mailin database configurato per la relativa casella PEC.

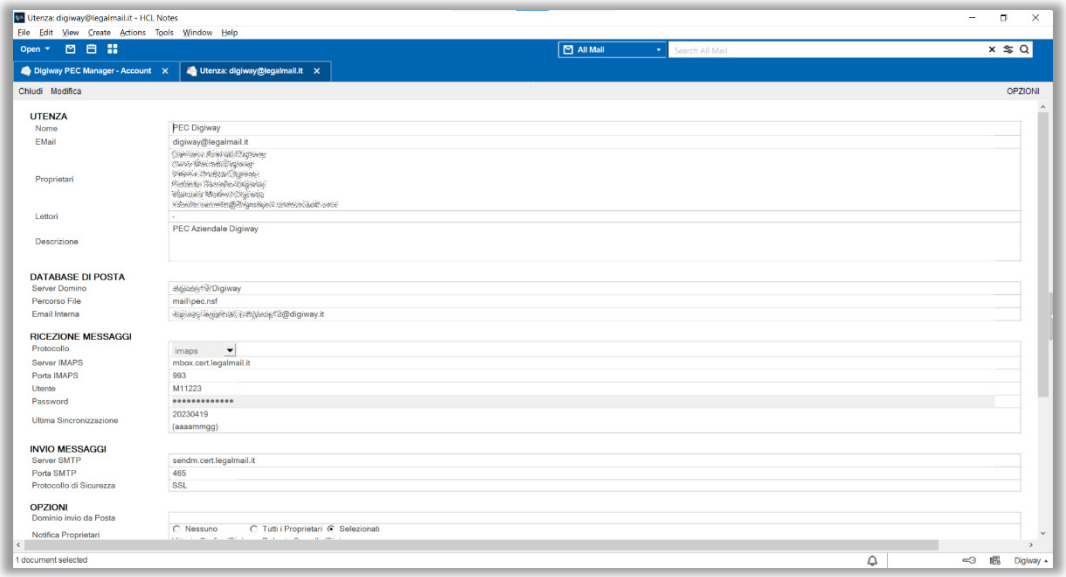
Questi mailin database verranno configurati automaticamente alla creazione della singola utenza o mediante una procedura apposita (**Installa Utenza**) presente nel modulo di configurazione delle singole caselle PEC.

I criteri con cui vengono prelevati i messaggi dal fornitore di PEC sono i seguenti:

- Inizialmente vengono letti tutti i messaggi presenti nella casella PEC. Nel caso alcuni messaggi siano posizionati in cartelle diverse dalla "inbox", questi vengono posizionati nelle medesime cartelle anche nella casella di PEC Manager; a regime il posizionamento dei messaggi nelle cartelle viene pilotato da PEC Manager mediante un agente apposito (**FOLDER MANAGER**).
- A regime vengono verificati i messaggi delle ultime 24 ore e, nel caso uno o più di questi non sia già presente nella casella di PEC Manager, viene scaricato e posizionato nella relativa cartella.

Nel caso si vogliano verificare nuovamente tutti i messaggi presenti nella casella del fornitore PEC, è possibile mediante una procedura apposita (Reset Ultima Sincronizzazione) presente nel modulo di configurazione delle singole caselle PEC.

[1] **Per questo motivo, occorre che il server Domino su cui si installa Digiway PEC Manager abbia configurato il servizio SMTP. Verificare la documentazione HCL per approfondimenti.**



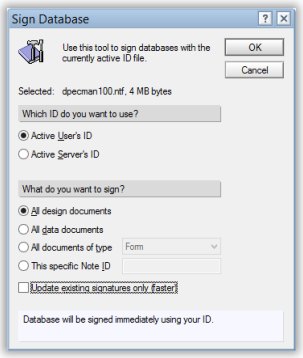
Nell'applicazione sono inoltre presenti altri quattro agenti:

- **NOTIFY OWNERS**: schedulato ogni ora, notifica i proprietari delle caselle dell'arrivo di nuovi messaggi, se questa opzione è configurata nella singola utenza PEC.
- **LOG MANAGER**: schedulato una volta al giorno (alle 01:00), provvede a notificare all'amministratore di PEC Manager (definito nelle Impostazioni generali dell'applicazione) della presenza di errori nel log, presenti nella vista Storico.
- **FOLDER MANAGER**: schedulato ogni ora, sincronizza le cartelle del provider con quelle di PEC Manager.
- **NOTIFY FAILURES:** invio le notifiche di errore agli owner della casella dovuti alla mancata autorizzazione del provider nell'accedere alla casella. In questo caso, l'utente ha a disposizione un bottone nell'interfaccia di PEC Manager che gli consente di modificare la password e ritentare l'accesso alla casella.

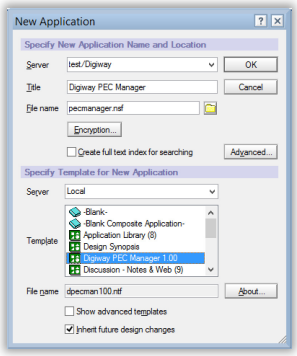
PRIMA INSTALLAZIONE

Eseguire le seguenti operazioni:

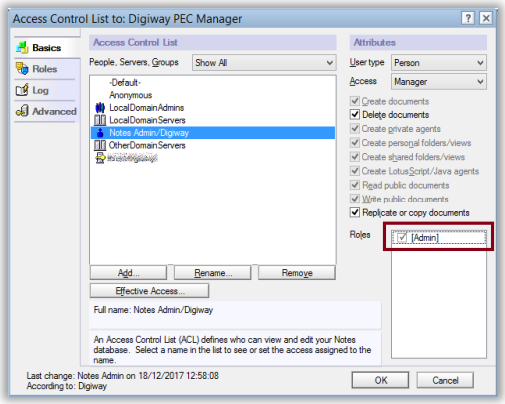
1. Firmare il template Digiway PEC Manager con un id di amministrazione del server Domino. L'utenza associata deve avere configurata la posta sullo stesso server di installazione di PEC Manager. In alternativa, è possibile inserire nel notes.ini del server il parametro `AMgr_DisableMailLookup=1`:



2. Creare il database **Digiway PEC Manager** (ad es. `pecmanager.nsf`) sul server Domino che si intende utilizzare come gestore delle caselle PEC, usando l'ultima versione di template fornito da Digiway:



3. Assegnare all'utente di amministrazione dell'applicazione il livello d'accesso **Manager** e ruolo **[Admin]**:



IMPOSTAZIONI GENERALI

Entrare nell'applicazione Digiway PEC Manager e cliccare sul bottone **Impostazioni**. Nel modulo di configurazione che si apre, inserire i seguenti dati:

Server Domino	Inserire il nome del server Domino sul quale è installato l'applicazione Digiway PEC Manager o confermare il valore presentato di default.
Dominio di Posta	Inserire il dominio internet di posta elettronica gestito dal server Domino. Ad es. `digiway.it`
Email Amministratore(i)	Una o più email (separate da virgola) che verranno notificate una volta al giorno di eventuali errori emersi durante le attività di PEC Manager. La notifica viene generata dall'agente LOG MANAGER.
Mailbox del Server Domino	Inserire il percorso al file di mailbox usato dal server Domino per distribuire i normali messaggi posta elettronica o lasciare il valore di default MAIL.BOX.

Server SMTP	Nome di host del server Domino al quale risponde internamente il servizio SMTP di posta elettronica. Ad es. `localhost`
Porta SMTP	Numero di porta alla quale risponde il servizio SMTP del server Domino. Ad es. 25
Utente	Inserire un eventuale nome utente per accedere al servizio SMTP del server Domino
Password	Inserire l'eventuale password per accedere al servizio SMTP del server Domino

File Licenza	Allegare il file ZIP consegnato da Digiway, contenente le informazioni di licenza del prodotto. Contattare Digiway per ottenere il file. Una volta allegato il file corretto di licenza, in questa sezione saranno visibili le informazioni di licenza (Intestatario della licenza, numero massimo di caselle PEC gestibili e data di scadenza della licenza)

Livello di Log	A scelta tra NESSUNO, MESSAGGI, VERBOSO e DEBUG, permette di selezionare il livello di log delle attività di Digiway PEC Manager, visibili nella vista Storico. Se non occorre una tracciatura dettagliata delle attività, lasciare il valore su MESSAGGI.
Profondità del Log	Numero di giorni dopo i quali i documenti di Log vengono automaticamente cancellati.
Time-out invio massivo predefinito	Indica il time-out di default che viene assegnato ai nuovi account di PEC. Per ogni account è possibile ridefinire tale valore

Proprietà ricezione in ingresso	Elenco di proprietà avanzate della libreria JavaMail che è possibile personalizzare (vedi paragrafo *Proprietà JavaMail* per

	l'elenco completo delle proprietà che è possibile impostare). Nel caso non ci sia alcun problema, lasciare le impostazioni presenti di default.
N° tentativi in ricezione prima di tornare errore	Indica il numero di tentativi che PEC Manager deve eseguire quando contatta il provider prima di tornare un errore. Server per evitare che un momentaneo timeout di connessione produca sistematicamente un errore nel log di PEC Manager.
Ritardo tra tentativi successivi	Collegato al campo precedente, indica a PEC Manager quanti secondi deve attendere prima di eseguire un nuovo tentativo di connessione con il provider.
Intervallo di manutenzione	Se l'apposito flag è impostato, permette di inserire un intervallo orario nel quale gli agenti schedulati sul server non vengono eseguiti. Utile quando quell'intervallo è usato dai sistemi per eseguire altre attività sul server, quali il backup dei dati.
Esclusione delle rubriche contenenti contatti interni	È possibile sccegliere o inserire una o più rubriche del server Domino che devono essere escluse nel ricercare indirizzi interni durante l'invio di una PEC, ovvero quegli indirizzi per i quali l'invio non viene eseguito tramite il provider, ma come una normale mail interna.

All'interno delle Impostazioni è presente un bottone **Aggiorna Template di Posta** che consente di caricare un nuovo template delle caselle PEC ed aggiornare automaticamente il design di tutte le caselle configurate.

CONFIGURAZIONE ACCOUNT

Dopo avere salvato le Impostazioni di Digiway PEC Manager, è possibile configurare le utenze PEC. Dalla vista Configurazione Utente, per ogni casella da configurare, cliccare il bottone **Nuova Utenza** ed inserire i seguenti dati:

UTENZA	
Nome	Inserire un nome rappresentativo che si vuole assegnare alla casella PEC (ad es. **PEC Marketing**). Tale nome sarà sia il nome del mailin database che il titolo della casella creati automaticamente dalla procedura di installazione.
Email	Indirizzo di email della casella PEC. Ad es. `pec-marketing@legalmail.it`
Proprietari	Inserire o selezionare i nomi degli utenti o gruppi Domino che hanno diritto ad gestire la casella PEC con la possibilità di ricevere ed inviare messaggi.
Lettori	Inserire o selezionare i nomi degli utenti o gruppi Domino che hanno accesso di sola lettura alla casella PEC.
Descrizione	Inserire opzionalmente una breve descrizione della casella PEC. Quanto scritto diventerà anche la Descrizione del mailin database.

DATABASE DI POSTA	
Server Domino	Inserire il server Domino sul quale attestare la casella PEC.
Percorso File	Inserire il percorso del database (mailin database) che conterrà i messaggi della casella PEC. Ad es. `pec\pecmarketing.nsf`
Hostname	Nel caso in cui la casella PEC si trovi su un server diverso da quello di PEC Manager, inserire l'URL del server ospitante la casella. Ad es. https://mail.digiway.it
Email interna	In automatico verrà prodotto una email interna basata sull'indirizzo di Email della casella PEC e sul dominio di posta configurato nelle Impostazioni generali dell'applicazione. Ad es. `pec-marketing-legalmail.it@digiway.it`

RICEZIONE MESSAGGI	
Protocollo	Scelta tra IMAP, IMAPS, POP3 e POP3S. Verificare la documentazione del fornitore della casella PEC.
Server	Inserire il nome di host del server di posta per la ricezione IMAP o POP, a seconda del Protocollo su scelto. Verificare la documentazione del fornitore della casella PEC.
Porta	Inserire il numero di porta per l'accesso al server di posta, a seconda del Protocollo su scelto. Solitamente queste porte sono 143 per IMAP, 993 per IMAPS, 110 per POP3 e 995 per POP3S. Verificare la documentazione del fornitore della casella PEC.
Utente	Utente per accedere alla casella PEC.
Password	Password per accedere alla casella PEC. Quando la password viene cambiata dall'interfaccia web del provider, l'utente avrà

	a disposizione nel navigatore di PEC Manager un bottone che gli consente di impostare la nuova password anche in PEC Manager.
Ultima Sincronizzazione	Contiene la data dell'ultima lettura dei messaggi nella casella PEC. Questo campo viene gestito automaticamente dall'agente di sincronizzazione della casella.

INVIO MESSAGGI	
Server SMTP	Inserire il nome di host del server di posta per l'invio mediante il protocollo SMTP. Verificare la documentazione del fornitore della casella PEC.
Porta SMTP	Inserire il numero di porta per l'invio di posta mediante il protocollo SMTP. Solitamente questa porta è la 25 o 465. Verificare la documentazione del fornitore della casella PEC.
Protocollo di Sicurezza	Scelta tra NESSUNO, SSL o TLS. Verificare la documentazione del fornitore della casella PEC.

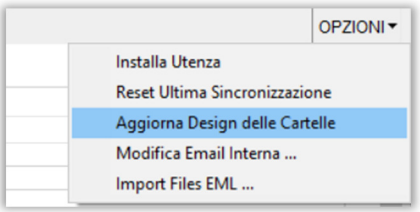
OPZIONI	
Dominio invio da Posta	A scelta fra i domini definiti nella directory del server Domino. Se valorizzato, sarà possibile inviare una PEC dalla casella personale degli utenti, aggiungendo questo dominio all'indirizzo PEC di destinazione. Ad es. `digiway@legalmail.it@DOMINIOPEC`
Notifica Proprietari	Scelta tra: • Nessuno: all'arrivo di nuovi messaggi, non verrà inviata alcuna notifica. • Tutti: tutti gli utenti (o gruppi) su definiti come 'Proprietari' verranno notificati dell'arrivo dei nuovi messaggi. • Selezionati: operando questa scelta, appare un ulteriore campo nel quale scegliere alcuni dei proprietari che verranno notificati dell'arrivo dei nuovi messaggi.
Notificare	• Tutti i messaggi: verranno inviate le notifiche di tutti i messaggi ricevuti nella casella PEC. • Solo PEC: le notifiche riguarderanno solo i messaggi PEC. Non verranno notificate le ACCETTAZIONI e le CONFERME.
Sincronizzazione Letti con Provider	Scelta tra: • Sincronizza Messaggi Letti: i messaggi vengono impostati come letti nella casella PEC del fornitore solo quando vengono letti dall'utente in PEC Manager. L'impostazione sulla casella PEC del fornitore verrà eseguita alla sincronizzazione delle email successiva alla lettura dei messaggi. • Non Sincronizzare Messaggi Letti: i messaggi nella casella PEC non vengono mai impostati come letti, a meno che non vengano letti dalla webmail della casella PEC stessa. • Rende Letti in fase di Scarico: i messaggi vengono automaticamente impostati come letti quando PEC Manager li scarica dalla casella PEC del fornitore.

Gestione dei Letti di Notes	Scelta tra: Rispetto dei Messaggi Letti degli Altri Proprietari: quando un utente legge un messaggio, gli altri utenti trovano il messaggio inalterato. Imposta a Letto alla prima Apertura a Tutti i Proprietari: quando un utente legge un messaggio, gli altri utenti vedono il messaggio come Letto. Imposta a Letto alla prima Apertura ai Selezionati: operando questa scelta, appare un ulteriore campo nel quale scegliere alcuni dei proprietari; quando un utente legge un messaggio, solo gli utenti selezionati vedono il messaggio come Letto.
Cartelle	Se viene selezionato, un agente automatizzato sposterà i messaggi presenti sul provider nelle stesse cartelle in cui si trovano in PEC Manager. Indicare il prefisso delle cartelle IMAP (lasciare il valore di default INBOX, a meno di provider particolari che usino uno standard diverso).
Gestione Cancellazioni	Scelta tra: • Nessuna gestione. I messaggi cancellati rimangono nel cestino: i messaggi cancellati rimangono per sempre nella vista cestino della casella PEC. • Esegui cancellazioni sul server dopo: operando questa scelta, appare un altro campo in cui inserire il numero di giorni dopo il quale i documenti nel cestino vengono definitivamente rimossi, anche nella casella del fornitore PEC.
Time-out invio massivo	Indica il time-out che deve essere gestito negli invii massivi dei messaggi PEC, ovvero la pausa che deve essere inserita tra un invio e l'altro, per evitare di ricevere errori dal fornitore della PEC ("`too many messages`").
Debug	Scelta tra SI e NO. Nel caso in cui ci siano problemi nella sincronizzazione dei messaggi, è possibile impostare questo campo a SI e verificare sulla console del server Domino quali sono i messaggi di errore specifici.

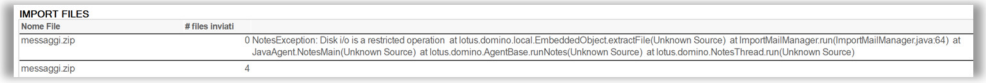
Quando il modulo è completato e salvato la prima volta, viene automaticamente attivata procedura di installazione dell'utenza che prevede:

- La creazione del mailin database all'interno della Domino Directory. L'utente che sta eseguendo questa operazione deve avere le giuste abilitazioni per poter completare l'operazione.
- La creazione della casella PEC con gli attributi di Server e Percorso su specificati, usando il template di posta presente all'interno delle Impostazioni generali di Digiway PEC Manager. Anche per questa operazione, l'utente deve possedere le corrette abilitazioni.

All'interno del modulo di configurazione dell'utenza è presente un bottone OPZIONI che prevede alcune scelte:



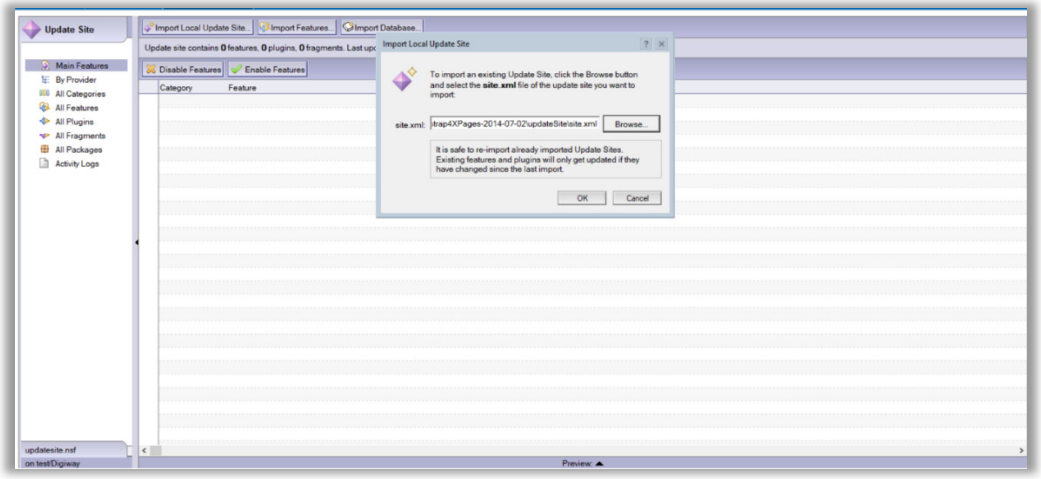
- **Installa Utenza**: viene ripetuta la procedura di installazione dell'utenza sopra descritta.
- **Reset Ultima Sincronizzazione**: nel caso occorra leggere tutte o parte delle mail dal fornitore della casella PEC, occorre prima resettare la data di Ultima Sincronizzazione. Prima di procedere, viene richiesto se si vuole resettare completamente questa data o riportarla ad uno specifico valore. Attenzione: nel caso la casella contenga molte mail, la successiva sincronizzazione dei messaggi potrebbe durare molto a lungo.
- **Aggiorna Design delle Cartelle:** nel caso in cui il design della Posta in Entrata venga modificato, questa operazione permette di impostare lo stesso design anche sulle altre cartelle già presenti nella casella di PEC Manager.
- **Modifica Email Interna:** permette di modificare la Email Interna alla quale la casella PEC riceve messaggi internamente all'ambiente Domino.
- **Import Files EML:** nel caso in cui si abbiano a disposizione messaggi PEC conservati esternamente al provider PEC, è possibile caricare questi messaggi nella casella PEC. Occorre disporre di un file ZIP che contiene questi messaggi in formato EML ed indicare a questa operazione un'eventuale cartella in cui inserire questi messaggi. Un apposito log elencherà le operazioni di import eseguite, con il numero di dei files inviati e gli eventuali log/errori risultanti dall'import:



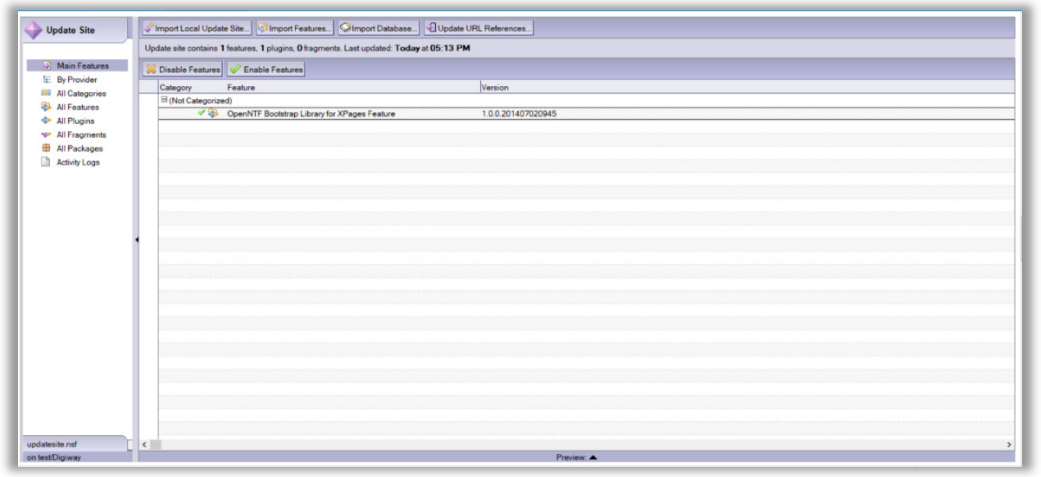
FRUIZIONE DA BROWSER

Per una corretta visualizzazione di Digiway PEC Manager da browser, occorre installare alcuni plugin sul server Domino che lo ospita. Per installare questi plugin, occorre avere un **Update Site** configurato sul medesimo server. Verificare la documentazione HCL per le modalità di installazione dell'Update Site.

All'interno dell'Update Site, importare un Local Update Site, specificando il file `site.xml` contenuto nella cartella `updateSite` del package **Bootstrap4XPages** fornito da Digiway:



Terminato l'import, l'Update Site mostrerà le nuove feature caricate, come mostra la figura seguente:



Perché il server Domino possa prendere in carico queste nuove feature, occorre eseguire un riavvio del task http del server.

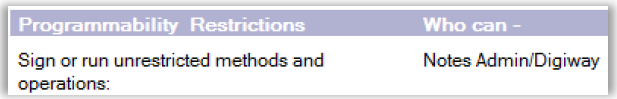
GESTIONE SICUREZZA

Digiway PEC Manager gestisce l'invio e la ricezione delle mail mediante un agente (**PEC MANAGER**) schedulato sul server Domino ogni 5 minuti. Alla sua prima esecuzione si potrebbero ricevere alcuni errori dovuti alla mancanza di alcune impostazioni sul server Domino.

Nel caso si riceva un errore tipo:

```
AMgr: Agent 'PEC MANAGER|PEC_MGR' in 'pecmanager.nsf' does not have proper execution
access, cannot be run
```

Significa che l'utente con cui si è firmato il template di Digiway PEC Manager non ha sufficienti diritti per eseguire questo agente. Per correggere la situazione occorre inserire il nome di questo utente Domino (o del gruppo di cui fa parte) nelle impostazioni del server Domino (*Sign or run unrestricted methods and operations*). Verificare la documentazione HCL per approfondimenti.



Se la console del server Domino riporta un errore tipo:

```
AMgr: Agent ('PEC MANAGER|PEC MGR' in 'pecmanager.nsf') error message:
java.lang.SecurityException: non è permesso accedere alle proprietà del sistema
AMgr: Agent ('PEC MANAGER|PEC_MGR' in 'pecmanager.nsf') error message:   at
lotus.notes.AgentSecurityManager.checkPropertiesAccess(Unknown Source)
```

Allora occorre modificare le abilitazioni sulla Java Virtual Machine del server Domino. Creare o aprire se già presente il file `java.pol` nella cartella del server Domino `<Domino>\jvm\lib\security\`

Ed aggiungere la direttiva:

```
grant {
     permission java.security.AllPermission;
};
```

Dalla versione 11 di Domino, la posizione ed il nome di questo file sono diverse. Per Windows, la cartella di default è `C:\Windows\System32\config\systemprofile` ed il nome file è `.java.policy`. Verificare la documentazione per la specifica versione del server Domino installato.

Inoltre, le funzionalità di ricezione e invio dei messaggi si basa sul toolkit Javamail; il server Domino è dotato di questa libreria di funzioni, ma per far funzionare Digiway PEC Manager in maniera ottimale, occorre installare una versione più recente di Javamail.

Per questo motivo, copiare il file `javax.mail.jar` fornito da Digiway nella cartella `Domino\jvm\lib\ext` del server Domino.

Perché le suddette modifiche abbiano effetto, occorre riavviare il server Domino.

Alcuni fornitori di PEC, come Aruba, potrebbero utilizzare un certificato SSL non contemplato dal server Domino. In questo caso lo storico degli eventi di PEC Manager potrebbe riportare un errore come:

```
PecManager - org.apache.commons.mail.EmailException: Sending the email to the
following server failed : smtps.pec.aruba.it:465
      at org.apache.commons.mail.Email.sendMimeMessage(Email.java:1469)
      at it.digiway.pec.OutboundEmail.sendEmail(OutboundEmail.java:173)
      at PecManager.run(PecManager.java:55)
      at JavaAgent.NotesMain(JavaAgent.java:10)
      at lotus.domino.AgentBase.runNotes(Unknown Source)
      at lotus.domino.NotesThread.run(Unknown Source)
Caused by: javax.mail.MessagingException: Could not connect to SMTP host:
smtps.pec.aruba.it, port: 465;
  nested exception is:
      javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.h: No trusted
certificate found
      at com.sun.mail.smtp.SMTPTransport.openServer(SMTPTransport.java:2196)
      at com.sun.mail.smtp.SMTPTransport.protocolConnect(SMTPTransport.java:726)
      at javax.mail.Service.connect(Service.java:388)
      at javax.mail.Service.connect(Service.java:246)
      at javax.mail.Service.connect(Service.java:195)
      at javax.mail.Transport.send0(Transport.java:254)
      at javax.mail.Transport.send(Transport.java:124)
      at org.apache.commons.mail.Email.sendMimeMessage(Email.java:1459)
      ... 5 more
Caused by: javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.h: No trusted
certificate found
      at com.ibm.jsse2.k.a(k.java:17)
      at com.ibm.jsse2.at.a(at.java:851)
      at com.ibm.jsse2.D.a(D.java:333)
      at com.ibm.jsse2.D.a(D.java:113)
      at com.ibm.jsse2.E.a(E.java:79)
      at com.ibm.jsse2.E.a(E.java:107)
      at com.ibm.jsse2.D.r(D.java:610)
      at com.ibm.jsse2.D.a(D.java:372)
      at com.ibm.jsse2.at.a(at.java:558)
      at com.ibm.jsse2.at.i(at.java:73)
      at com.ibm.jsse2.at.a(at.java:357)
      at com.ibm.jsse2.at.startHandshake(at.java:723)
      at com.sun.mail.util.SocketFetcher.configureSSLSocket(SocketFetcher.java:619)
      at com.sun.mail.util.SocketFetcher.createSocket(SocketFetcher.java:393)
      at com.sun.mail.util.SocketFetcher.getSocket(SocketFetcher.java:217)
      at com.sun.mail.smtp.SMTPTransport.openServer(SMTPTransport.java:2160)
      ... 12 more
Caused by: com.ibm.jsse2.util.h: No trusted certificate found
```

```
at com.ibm.jsse2.util.g.a(g.java:163)
at com.ibm.jsse2.util.g.b(g.java:33)
at com.ibm.jsse2.util.e.a(e.java:14)
at com.ibm.jsse2.aB.a(aB.java:79)
at com.ibm.jsse2.aB.a(aB.java:48)
at com.ibm.jsse2.aB.checkServerTrusted(aB.java:9)
at com.ibm.jsse2.E.a(E.java:5)
... 23 more
```

In questo caso occorre scaricare il certificato SSL del fornitore di servizio usando un'utilità come **openssl** (https://sourceforge.net/projects/openssl), mediante il seguente comando:

```
openssl s_client -connect smtps.pec.aruba.it:465 > aruba-smtp.cer
```

Il file scaricato (`aruba-smtp.cer`) potrà essere caricato nel file `cacerts` contenuto nella cartella `<DOMINO>\jvm\lib\security` usando l'utilità `keytool.exe` contenuta nella cartella `<DOMINO>\jvm\bin`. Aprire un prompt DOS sul server Domino ed invocare il seguente comando:

```
<DOMINO>\jvm\bin\keytool -import -alias aruba -file aruba-smtp.cer -
keystore <DOMINO>\jvm\lib\security\cacerts
```

dove:

`<DOMINO>` è la cartella in cui è installato il server Domino

`aruba` è un nome scelto liberamente come alias del certificato che si sta importando

`aruba-smtp.cer` è il nome del file contenente il certificato scaricato precedentemente con openssl.

Nelle versioni più recenti di Domino, l'utilità `keytool.exe` non è più disponibile ed occorre, quindi, utilizzare uno dei software equivalenti disponibili liberamente in rete, come KeyStore Explorer (https://keystore-explorer.org).

Al termine dell'installazione del certificato, occorre eseguire il riavvio del server Domino.

PROPRIETÀ JAVAMAIL

Note that if you're using the "imaps" protocol to access IMAP over SSL, all the properties would be named "mail.imaps.*".

Name	Type	Description
mail.imap.user	String	Default user name for IMAP.
mail.imap.host	String	The IMAP server to connect to.
mail.imap.port	int	The IMAP server port to connect to, if the connect() method doesn't explicitly specify one. Defaults to 143.
mail.imap.partialfetch	boolean	Controls whether the IMAP partial-fetch capability should be used. Defaults to true.
mail.imap.fetchsize	int	Partial fetch size in bytes. Defaults to 16K.
mail.imap.peek	boolean	If set to true, use the IMAP PEEK option when fetching body parts, to avoid setting the SEEN flag on messages. Defaults to false. Can be overridden on a per-message basis by the setPeek method on IMAPMessage.
mail.imap.ignorebodystructuresize	boolean	The IMAP BODYSTRUCTURE response includes the exact size of each body part. Normally, this size is used to determine how much data to fetch for each body part. Some servers report this size incorrectly in some cases; this property can be set to work around such server bugs. If this property is set to true, this size is ignored and data is fetched until the server reports the end of data. This will result in an extra fetch if the data size is a multiple of the block size. Defaults to false.
mail.imap.connectiontimeout	int	Socket connection timeout value in milliseconds. This timeout is implemented by java.net.Socket. Default is infinite timeout.
mail.imap.timeout	int	Socket read timeout value in milliseconds. This timeout is implemented by java.net.Socket. Default is infinite timeout.
mail.imap.writetimeout	int	Socket write timeout value in milliseconds. This timeout is implemented by using a java.util.concurrent.ScheduledExecutorService per connection that schedules a thread to close the socket if the timeout expires. Thus, the overhead of using this timeout is one thread per connection. Default is infinite timeout.
mail.imap.statuscachetimeout	int	Timeout value in milliseconds for cache of STATUS command response. Default is 1000 (1 second). Zero disables cache.
mail.imap.appendbuffersize	int	Maximum size of a message to buffer in memory when appending to an IMAP folder. If not set, or set to -1, there is no maximum and all messages are buffered. If set to 0, no messages are buffered. If set to (e.g.) 8192, messages of 8K bytes or less are buffered, larger messages are not buffered. Buffering saves cpu time at the expense of short term memory usage. If you commonly append very large messages to IMAP mailboxes you might want to set this to a moderate value (1M or less).
mail.imap.connectionpoolsize	int	Maximum number of available connections in the connection pool. Default is 1.
mail.imap.connectionpooltimeout	int	Timeout value in milliseconds for connection pool connections. Default is 45000 (45 seconds).
mail.imap.separatestoreconnection	boolean	Flag to indicate whether to use a dedicated store connection for store commands. Default is false.

mail.imap.allowreadonlyselect	boolean	If false, attempts to open a folder read/write will fail if the SELECT command succeeds but indicates that the folder is READ-ONLY. This sometimes indicates that the folder contents can'tbe changed, but the flags are per-user and can be changed, such as might be the case for public shared folders. If true, such open attempts will succeed, allowing the flags to be changed. The getMode method on the Folder object will return Folder.READ_ONLY in this case even though the open method specified Folder.READ_WRITE. Default is false.
mail.imap.auth.mechanisms	String	If set, lists the authentication mechanisms to consider, and the order in which to consider them. Only mechanisms supported by the server and supported by the current implementation will be used. The default is "PLAIN LOGIN NTLM", which includes all the authentication mechanisms supported by the current implementation except XOAUTH2.
mail.imap.auth.login.disable	boolean	If true, prevents use of the non-standard AUTHENTICATE LOGIN command, instead using the plain LOGIN command. Default is false.
mail.imap.auth.plain.disable	boolean	If true, prevents use of the AUTHENTICATE PLAIN command. Default is false.
mail.imap.auth.ntlm.disable	boolean	If true, prevents use of the AUTHENTICATE NTLM command. Default is false.
mail.imap.auth.ntlm.domain	String	The NTLM authentication domain.
mail.imap.auth.ntlm.flags	int	NTLM protocol-specific flags. See http://curl.haxx.se/rfc/ntlm.html#theNtlmFlags for details.
mail.imap.auth.xoauth2.disable	boolean	If true, prevents use of the AUTHENTICATE XOAUTH2 command. Because the OAuth 2.0 protocol requires a special access token instead of a password, this mechanism is disabled by default. Enable it by explicitly setting this property to "false" or by setting the "mail.imap.auth.mechanisms" property to "XOAUTH2".
mail.imap.proxyauth.user	String	If the server supports the PROXYAUTH extension, this property specifies the name of the user to act as. Authenticate to the server using the administrator's credentials. After authentication, the IMAP provider will issue the PROXYAUTH command with the user name specified in this property.
mail.imap.localaddress	String	Local address (host name) to bind to when creating the IMAP socket. Defaults to the address picked by the Socket class. Should not normally need to be set, but useful with multi-homed hosts where it's important to pick a particular local address to bind to.
mail.imap.localport	int	Local port number to bind to when creating the IMAP socket. Defaults to the port number picked by the Socket class.
mail.imap.sasl.enable	boolean	If set to true, attempt to use the javax.security.sasl package to choose an authentication mechanism for login. Defaults to false.
mail.imap.sasl.mechanisms	String	A space or comma separated list of SASL mechanism names to try to use.
mail.imap.sasl.authorizationid	String	The authorization ID to use in the SASL authentication. If not set, the authentication ID (user name) is used.
mail.imap.sasl.realm	String	The realm to use with SASL authentication mechanisms that require a realm, such as DIGEST-MD5.
mail.imap.sasl.usecanonicalhostname	boolean	If set to true, the canonical host name returned by InetAddress.getCanonicalHostName is passed to the SASL mechanism, instead of the host name used to connect. Defaults to false.

mail.imap.sasl. xgwtrustedapphack.enable	boolean	If set to true, enables a workaround for a bug in the Novell Groupwise XGWTRUSTEDAPP SASL mechanism, when that mechanism is being used. Defaults to true.
mail.imap.socketFactory	SocketFactory	If set to a class that implements the javax.net.SocketFactory interface, this class will be used to create IMAP sockets. Note that this is an instance of a class, not a name, and must be set using the put method, not the setProperty method.
mail.imap.socketFactory.class	String	If set, specifies the name of a class that implements the javax.net.SocketFactory interface. This class will be used to create IMAP sockets.
mail.imap.socketFactory.fallback	boolean	If set to true, failure to create a socket using the specified socket factory class will cause the socket to be created using the java.net.Socket class. Defaults to true.
mail.imap.socketFactory.port	int	Specifies the port to connect to when using the specified socket factory. If not set, the default port will be used.
mail.imap.usesocketchannels	boolean	If set to true, use SocketChannels instead of Sockets for connecting to the server. Required if using the IdleManager. Ignored if a socket factory is set. Defaults to false.
mail.imap.ssl.enable	boolean	If set to true, use SSL to connect and use the SSL port by default. Defaults to false for the "imap" protocol and true for the "imaps" protocol.
mail.imap.ssl.checkserveridentity	boolean	If set to true, check the server identity as specified by RFC 2595. These additional checks based on the content of the server's certificate are intended to prevent man-in-the-middle attacks. Defaults to false.
mail.imap.ssl.trust	String	If set, and a socket factory hasn't been specified, enables use of a MailSSLSocketFactory. If set to "*", all hosts are trusted. If set to a whitespace separated list of hosts, those hosts are trusted. Otherwise, trust depends on the certificate the server presents.
mail.imap.ssl.socketFactory	SSLSocketFactory	If set to a class that extends the javax.net.ssl.SSLSocketFactory class, this class will be used to create IMAP SSL sockets. Note that this is an instance of a class, not a name, and must be set using the put method, not the setProperty method.
mail.imap.ssl.socketFactory.class	String	If set, specifies the name of a class that extends the javax.net.ssl.SSLSocketFactory class. This class will be used to create IMAP SSL sockets.
mail.imap.ssl.socketFactory.port	int	Specifies the port to connect to when using the specified socket factory. If not set, the default port will be used.
mail.imap.ssl.protocols	string	Specifies the SSL protocols that will be enabled for SSL connections. The property value is a whitespace separated list of tokens acceptable to the javax.net.ssl.SSLSocket.setEnabledProtocols method.
mail.imap.ssl.ciphersuites	string	Specifies the SSL cipher suites that will be enabled for SSL connections. The property value is a whitespace separated list of tokens acceptable to the javax.net.ssl.SSLSocket.setEnabledCipherSuites method.
mail.imap.starttls.enable	boolean	If true, enables the use of the STARTTLS command (if supported by the server) to switch the connection to a TLS-protected connection before issuing any login commands. If the server does not support STARTTLS, the connection continues without the use of TLS; see the mail.imap.starttls.required property to fail if STARTTLS isn't supported. Note that an appropriate trust store must configured so that the client will trust the server's certificate. Default is false.

mail.imap.starttls.required	boolean	If true, requires the use of the STARTTLS command. If the server doesn't support the STARTTLS command, or the command fails, the connect method will fail. Defaults to false.
mail.imap.proxy.host	string	Specifies the host name of an HTTP web proxy server that will be used for connections to the mail server.
mail.imap.proxy.port	string	Specifies the port number for the HTTP web proxy server. Defaults to port 80.
mail.imap.proxy.user	string	Specifies the user name to use to authenticate with the HTTP web proxy server. By default, no authentication is done.
mail.imap.proxy.password	string	Specifies the password to use to authenticate with the HTTP web proxy server. By default, no authentication is done.
mail.imap.socks.host	string	Specifies the host name of a SOCKS5 proxy server that will be used for connections to the mail server.
mail.imap.socks.port	string	Specifies the port number for the SOCKS5 proxy server. This should only need to be used if the proxy server is not using the standard port number of 1080.
mail.imap.minidletime	int	Applications typically call the idle method in a loop. If another thread termiantes the IDLE command, it needs a chance to do its work before another IDLE command is issued. The idle method enforces a delay to prevent thrashing between the IDLE command and regular commands. This property sets the delay in milliseconds. If not set, the default is 10 milliseconds.
mail.imap.enableresponseevents	boolean	Enable special IMAP-specific events to be delivered to the Store's ConnectionListener. If true, IMAP OK, NO, BAD, or BYE responses will be sent as ConnectionEvents with a type of IMAPStore.RESPONSE. The event's message will be the raw IMAP response string. By default, these events are not sent. NOTE: This capability is highly experimental and likely will change in future releases.
mail.imap.enableimapevents	boolean	Enable special IMAP-specific events to be delivered to the Store's ConnectionListener. If true, unsolicited responses received during the Store's idle method will be sent as ConnectionEvents with a type of IMAPStore.RESPONSE. The event's message will be the raw IMAP response string. By default, these events are not sent. NOTE: This capability is highly experimental and likely will change in future releases.
mail.imap.throwsearchexception	boolean	If set to true and a SearchTerm passed to the Folder.search method is too complex for the IMAP protocol, throw a SearchException. For example, the IMAP protocol only supports less-than and greater-than comparisons for a SizeTerm. If false, the search will be done locally by fetching the required message data and comparing it locally. Defaults to false.
mail.imap.folder.class	String	Class name of a subclass of com.sun.mail.imap.IMAPFolder. The subclass can be used to provide support for additional IMAP commands. The subclass must have public constructors of the form public MyIMAPFolder(String fullName, char separator, IMAPStore store, Boolean isNamespace) and public MyIMAPFolder(ListInfo li, IMAPStore store)
mail.imap.closefoldersonstorefailure	boolean	In some cases, a failure of the Store connection indicates a failure of the server, and all Folders associated with that Store should also be closed. In other cases, a Store connection failure may be a transient failure, and Folders may continue to operate normally. If this property is true (the default), failures in the Store connection cause all associated Folders to be closed. Set this property to false to better handle transient failures in the Store connection.

mail.imap.finalizecleanclose	boolean	When the finalizer for IMAPStore is called, should the connection to the server be closed cleanly, as if the application called the close method? Or should the connection to the server be closed without sending any commands to the server? Defaults to false, the connection is not closed cleanly.
mail.imap.referralexception	boolean	If set to true and an IMAP login referral is returned when the authentication succeeds, fail the connect request and throw a ReferralException. Defaults to false.
mail.imap.compress.enable	boolean	If set to true and the IMAP server supports the COMPRESS=DEFLATE extension, compression will be enabled. Defaults to false.
mail.imap.compress.level	int	The compression level to be used, in the range -1 to 9. See the Deflater class for details.
mail.imap.compress.strategy	int	The compression strategy to be used, in the range 0 to 2. See the Deflater class for details.
mail.imap.compress.strategy	boolean	If true, always use "A" for the IMAP command tag prefix. If false, the IMAP command tag prefix is different for each connection, from "A" through "ZZZ" and then wrapping around to "A". Applications should never need to set this. Defaults to false.