



Guard
Manuale utente



Guard: Manuale utente

Data di pubblicazione mercoledì, 09. novembre 2016 Version 2.6.0

Diritto d'autore © 2016-2013 OX Software GmbH , Questo documento è proprietà intellettuale di OX Software GmbH

Il documento può essere copiato per intero o in parte, a condizione che ogni copia contenga la comunicazione del diritto d'autore. Le informazioni contenute in questo manuale sono state scritte con la massima attenzione. Tuttavia, non è possibile escludere completamente la presenza di qualche imprecisione. OX Software GmbH, gli autori e i traduttori non sono responsabili per i possibili errori e per le loro conseguenze. I nomi dei programmi e dell'hardware utilizzati in questo manuale potrebbero essere marchi registrati; essi sono utilizzati senza garanzia di libero utilizzo. OX Software GmbH segue generalmente le diciture convenzionali dei produttori. La riproduzione dei nomi, marchi, loghi, ecc. in questo manuale (anche senza contrassegni speciali) non giustifica l'assunzione che tali nomi siano liberamente utilizzabili (per la regolamentazione sui nomi e sui marchi).

Indice

1 Informazioni su questa documentazione	5
2 A cosa serve Guard?	7
3 Utilizzare Guard	9
3.1 Configurare <i>Guard</i>	10
3.2 Cifrare le comunicazioni di posta elettronica	11
3.2.1 Leggere i messaggi di posta cifrati	11
3.2.2 Inviare messaggi di posta cifrati	11
3.2.3 Come possono leggere un messaggio di posta cifrato i destinatari esteri?	12
3.3 Cifrare i file	13
3.3.1 Cifrare i file	13
3.3.2 Creare nuovi file cifrati	13
3.3.3 Aprire i file cifrati	13
3.3.4 Scaricare i file cifrati	14
3.3.5 Decifrare i file	14
3.4 Uscire da Guard	15
3.5 Impostazioni di Guard	16
3.5.1 Impostazioni di sicurezza di Guard	16
3.5.2 Impostazioni di cifratura PGP	17
3.5.3 Gestione delle chiavi	18
Indice analitico	21

1 Informazioni su questa documentazione

Le seguenti informazioni vi aiuteranno ad utilizzare al meglio questa documentazione.

- [A chi è destinata questa documentazione?](#)
- [Quali contenuti sono inclusi nella documentazione?](#)
- [Ulteriore aiuto](#)

A chi è destinata questa documentazione?

Questa documentazione è destinata agli utenti che desiderano utilizzare la cifratura per proteggere le loro comunicazioni di posta elettronica e i file dagli accessi non autorizzati.

Quali contenuti sono inclusi nella documentazione?

La documentazione include le seguenti informazioni:

- In [A cosa serve Guard?](#) sarà disponibile una breve descrizione di Guard.
- In [Utilizzare Guard](#) troverete le istruzioni per utilizzare Guard.

Questa documentazione descrive come lavorare con un'installazione e una configurazione tipica del groupware. La versione installata e la configurazione del proprio groupware potrebbero differire da quanto descritto qui.

Ulteriore aiuto

Una documentazione completa del groupware è disponibile nel Manuale utente di Groupware

2 A cosa serve Guard?

Guard è un componente di protezione del groupware che consente di cifrare messaggi di posta e file.

- Cifrare le proprie comunicazioni di posta elettronica con altri utenti o collaboratori esterni.
- Cifrare singoli file. Condividere i dati cifrati con altri utenti.
- Utilizzare le opzioni di sicurezza per definire il livello di cifratura.
- I dati cifrati sono protetti da password. Utilizzare la funzione di ripristino della password per proteggersi dalle conseguenze di uno smarrimento della password.

3 Utilizzare Guard

Scoprire come funziona l'applicazione *Guard*.

- [applicare](#) le impostazioni di base
- cifrare le [comunicazioni di posta elettronica](#)
- cifrare [file](#)
- [applicare](#) le impostazioni di sicurezza

3.1 Configurare *Guard*


Prima di poter utilizzare *Guard*, è necessario applicare alcune impostazioni di base.

- Prima di tutto, bisogna digitare la password di sicurezza di *Guard* che viene utilizzata per cifrare i dati e accedere ai dati cifrati.
- Digitare un indirizzo di posta elettronica secondario che sarà utilizzato se si dimentica la propria password di sicurezza di *Guard*. In questo caso, utilizzare la funzione per ripristinare la password di sicurezza di *Guard*. Una nuova password sarà inviata al proprio indirizzo di posta. Per motivi di sicurezza, è vivamente consigliato di digitare un indirizzo di posta elettronica secondario a tale scopo. Altrimenti, la nuova password viene inviata all'account di posta principale.


Sono disponibili due opzioni per configurare le impostazioni di base:

- Specificare le impostazioni di base **mentre** si utilizza per la prima volta la funzione di cifratura.
- Specificare le impostazioni di base nella pagina delle impostazioni **prima** di utilizzare la funzione di cifratura.

Come specificare le impostazioni di base quando si utilizza per la prima volta la funzione di cifratura:

1. Abilitare la funzione di cifratura quando si compone un messaggio di posta, cifrare un file o caricare un nuovo file facendo clic sull'icona **Cifra**  accanto al nome della cartella nell'albero delle cartelle.
2. Successivamente verrà richiesta l'immissione di una password di sicurezza di *Guard* e un indirizzo di posta elettronica secondario. Digitare i dati.

Come specificare le impostazioni di base quando si utilizza per la prima volta la cifratura:

1. Fare clic sull'icona **Menu di sistema**  a destra della barra dei menu. Fare clic su **Impostazioni** nel menu.
2. Fare clic su **Sicurezza di Guard** nella barra laterale.
Al primo avvio delle impostazioni di sicurezza di *Guard*, si aprirà la finestra *Crea chiavi di sicurezza di Guard*.
3. Nel campo **Password**, digitare la password che si desidera utilizzare la cifrare i propri dati.
Confermare la password nel campo **Verifica** digitandola nuovamente.
4. Nel campo **Digita il nuovo indirizzo di posta secondario**, digitare l'indirizzo di posta utilizzato per ricevere la password temporanea per il ripristino della propria password di sicurezza di *Guard*.
5. Fare clic su **OK**.

3.2 Cifrare le comunicazioni di posta elettronica


Sono disponibili le seguenti opzioni:

- [Leggere i messaggi di posta cifrati](#)
- [Inviare messaggi di posta cifrati](#)
- [Come possono leggere un messaggio di posta cifrato i destinatari esterni?](#)

3.2.1 Leggere i messaggi di posta cifrati

Per poter leggere un messaggio di posta cifrato, è richiesta almeno la password di sicurezza di Guard. Il mittente di un messaggio di posta cifrato può proteggere il messaggio con una password aggiuntiva.

Come leggere un messaggio di posta cifrato:

1. Selezionare un messaggio con l'icona *Cifrato* . Nella vista dettagliata, la notifica *Messaggio sicuro, digita la password di Guard.* sarà visualizzata.
Nota: Se, dopo aver utilizzato Guard l'ultima volta, si imposta che Guard dovrebbe ricordare la password di protezione, il messaggio è visualizzato immediatamente, in base all'impostazione.
2. Digitare la password di sicurezza di Guard.
È possibile specificare quanto tempo dovrebbe essere memorizzata la password di sicurezza da parte di Guard. Per fare ciò, abilitare **Mantieni il mio accesso a Guard**. Selezionare un valore dall'elenco.
3. Fare clic su **OK**. Il contenuto è mostrato in testo semplice.
Se il messaggio ha allegati, sono visualizzate funzioni per utilizzare le versioni decifrate o cifrate degli allegati.


Nota: è possibile rispondere a questo messaggio di posta o inoltrarlo solo se si utilizza un messaggio cifrato.

3.2.2 Inviare messaggi di posta cifrati

Sono disponibili le seguenti opzioni:

- Inviare un messaggio di posta cifrato. Solo voi e i destinatari potrete leggere il contenuto del messaggio.
Avviso: quando si invia una bozza di messaggio cifrato, la bozza sarà eliminata una volta inviata dalla cartella *Bozze*.
- Inviare un messaggio di posta elettronica con una firma. La firma assicura che il destinatario sia in grado di riconoscere che il contenuto del messaggio sia stato modificato durante il trasporto.
- inviare un messaggio di posta cifrato con una firma.

Come inviare un messaggio di posta cifrato:

1. Comporre un messaggio di posta nell'applicazione *Posta elettronica*.
Nella pagina *Componi*, fare clic su l'icona **Cifra**  in alto a destra.
È possibile fare clic anche su **Sicurezza** sotto l'oggetto. Abilitare **Cifra**.
Le icone accanto ai destinatari indicano se il messaggio può essere cifrato per questo destinatario. Se passando su un'icona, sarà visualizzata una descrizione.
2. Per visualizzare le opzioni aggiuntive, fare clic su **Sicurezza**. È possibile attivare le seguenti opzioni:
Per aggiungere una firma al messaggio di posta, abilitare **Firma**.
Nel caso in cui il client di posta elettronica del destinatario non supporti PGP, il messaggio dovrebbe essere comunque leggibile, abilitare **Usa PGP in linea**. Se si utilizza questa impostazione, è possibile inviare messaggi di posta in formato html.
Per consentire al destinatario di un messaggio di inviare una risposta cifrata, il destinatario deve avere la vostra chiave pubblica. È possibile inviare la chiave pubblica come allegato. Per fare ciò, abilitare **Allega la mia chiave**.
3. Fare clic su **Invio cifrato**.
Quando si invia a destinatari esterni, viene visualizzata una finestra che consente di inviare [note per aprire il messaggio di posta cifrato \[12\]](#) ai destinatari esterni.
Quando inizialmente si invia un messaggio di posta elettronica cifrato a un destinatario esterno, quest'ultimo riceverà un allegato di posta elettronica con la vostra chiave pubblica.

3.2.3 Come possono leggere un messaggio di posta cifrato i destinatari esterni?

È inoltre possibile inviare messaggi di posta elettronica cifrati a destinatari esterni che non sono utenti del groupware. Quando si aggiunge un destinatario esterno, Guard controlla se una chiave pubblica è disponibile per il destinatario. In base al risultato, Guard utilizza diverse procedure per l'invio del messaggio cifrato.

- Se esiste una chiave pubblica per il destinatario:
 - Il messaggio viene inviato cifrato con questa chiave. Il destinatario può leggere il messaggio con la sua chiave privata.
 - Per permettere al destinatario di inviare una risposta cifrata, la propria chiave pubblica è inviata come allegato. Il nome dell'allegato è `public.asc`. Il destinatario può importare questa chiave nel suo client di posta elettronica.
- Se non esiste una chiave pubblica per il destinatario:
 - Se l'utente esterno ha già un account ospite, riceverà un messaggio di posta con il collegamento alla pagina di accesso del proprio account ospite. Dopo aver eseguito l'accesso, potrà leggere il messaggio cifrato nella pagina degli ospiti. Può inviare una risposta cifrata da questa pagina.
 - Se non c'è alcun account ospite, sarà creato un account ospite. Il destinatario esterno riceverà un messaggio di posta con un collegamento alla pagina degli ospiti e una password creata automaticamente. L'utente eseguirà l'accesso dalla pagina degli ospiti. Potrà quindi creare una propria password.
In base alla configurazione, la password creata automaticamente e il collegamento alla pagina degli ospiti sono inviati in messaggi separati.
 - In base alla configurazione del groupware, i messaggi di posta dell'account ospite sono eliminati dopo un numero specifico di giorni. Affinché tali messaggi siano ancora disponibili, il messaggio con il collegamento alla pagina degli ospiti contiene un allegato con il messaggio cifrato. Il nome dell'allegato è `encrypted.asc`. Questo allegato può essere caricato e letto nella pagina degli ospiti.

3.3 Cifrare i file

Sono disponibili le seguenti opzioni:



- Cifrare i file
- Creare nuovi file cifrati
- Aprire i file cifrati
- Scaricare i file cifrati
- Decifrare i file

3.3.1 Cifrare i file

Quando si cifra un file, solo l'ultima versione di questo file sarà cifrata. Tutte le altre versioni saranno eliminate.

Come cifrare un file:

Avviso: se si cifra un file, tutte le versioni di questo file saranno eliminate, eccetto la versione attuale. Se si vuole conservare una versione più datata, salvarla prima di cifrare il file.

1. Selezionare uno o più file nell'applicazione *File*. Fare clic sull'icona **Azioni**  nella barra degli strumenti. Fare clic su **Cifra** nel menu.
È possibile anche utilizzare l'icona **Azioni**  nel *Visualizzatore*. Fare clic su **Cifra** nel menu.
2. Se il file contiene più versioni, sarà visualizzata la finestra *Cifra i file*. Confermare che si desidera cifrare il file ed eliminare tutte le versioni precedenti facendo clic su **OK**.
Se il file contiene solo una versione, il file è cifrato senza ulteriori richieste.

3.3.2 Creare nuovi file cifrati

È possibile creare un nuovo file cifrato caricando un file locale con la cifratura.

Come creare un nuovo file cifrato:


1. Nell'applicazione *File*, selezionare la cartella nell'albero delle cartelle
Nota: aprire una cartella per la quale si dispone dei permessi appropriati per creare oggetti.
2. Fare clic su **Nuovo** nella barra degli strumenti. Fare clic su **Aggiungi e cifra file locale**.
3. Selezionare uno o più file nella finestra *Carica file*.
Fare clic su **Apri**. L'area di visualizzazione mostra lo stato di avanzamento corrente.
Per annullare il processo, fare clic su **Dettagli file** in basso a destra dell'area di visualizzazione. Fare clic su **Annulla** accanto al nome del file nella finestra *Avanzamento del caricamento*.

Suggerimento: è possibile creare un nuovo file cifrato anche trascinando un file dal proprio desktop alla finestra dell'applicazione *File* e rilasciandolo nella parte superiore.

3.3.3 Aprire i file cifrati

È possibile aprire e leggere un file cifrato. Il file rimane cifrato sul server.



Come aprire un file cifrato:

1. Nell'applicazione *File*, selezionare un file cifrato nell'area di visualizzazione. Fare clic sull'icona **Vista**  nella barra degli strumenti.
2. Si aprirà la finestra *Digita la password di sicurezza di Guard*. Digitare la password di sicurezza di Guard. È possibile specificare per quanto tempo Guard dovrebbe memorizzare la password di sicurezza. Per fare ciò, abilitare **Ricorda password**. Selezionare un valore dall'elenco. Fare clic su **OK**.

3.3.4 Scaricare i file cifrati

È possibile scaricare un file cifrato per leggere localmente leggerla o modificarla. Il file rimane cifrato sul server.


Come scaricare un file cifrato:

1. Nell'applicazione *File*, selezionare un file cifrato nell'area di visualizzazione. Fare clic sull'icona **Vista**  nella barra degli strumenti.
Nota: facendo clic invece su **Scarica** nella finestra a comparsa, il file scaricato rimane cifrato.
2. Si aprirà la finestra *Digita la password di sicurezza di Guard*. Digitare la password di sicurezza di Guard. È possibile specificare per quanto tempo Guard dovrebbe memorizzare la password di sicurezza. Per fare ciò, abilitare **Ricorda password**. Selezionare un valore dall'elenco. Fare clic su **OK**.
3. È possibile anche selezionare l'icona **Azioni**  nel visualizzatore. Fare clic su **Scarica decifrato**.

3.3.5 Decifrare i file

È possibile rimuovere la cifratura di un file decifrandolo.

Come decifrare un file:


1. Nell'applicazione *File*, selezionare un file cifrato nell'area di visualizzazione. Fare clic sull'icona **Azioni**  nella barra degli strumenti. Fare clic su **Rimuovi cifratura** nel menu.
2. Si aprirà la finestra *Digita la password di sicurezza di Guard*. Digitare la password di sicurezza di Guard. È possibile specificare per quanto tempo dovrebbe essere valida la password di sicurezza di Guard. Per fare ciò, abilitare **Ricorda password**. Selezionare un valore dall'elenco. Fare clic su **OK**.

3.4 Uscire da Guard

È possibile uscire da Guard senza chiudere il groupware. Per aprire un messaggio di posta cifrato, file o cartella, è necessario digitare nuovamente la password di sicurezza di Guard.

Nota: questa funzionalità è disponibile solo se si abilita **Ricorda password** quando si apre un messaggio di posta o un file cifrato.

Come uscire da Guard:

1. Fare clic sull'icona **Menu di sistema**  a destra della barra dei menu.
2. Fare clic su **Esci da Guard** nel menu.

3.5 Impostazioni di Guard

Esistono le seguenti opzioni:


- Per poter gestire la propria password di sicurezza di Guard, utilizzare le impostazioni di sicurezza di Guard.
- Per modificare le impostazioni predefinite per l'invio di messaggi di posta sicuri, utilizzare le [Impostazioni di cifratura di PGP](#).
- È possibile [gestire le proprie chiavi PGP](#).

3.5.1 Impostazioni di sicurezza di Guard


Esistono le seguenti opzioni:

- [cambiare](#) la password di sicurezza di Guard
- Nel caso in cui si smarrisca la password di sicurezza di Guard, è possibile richiedere una password di sicurezza di Guard [ripristinando](#) la Guard password di sicurezza.
- [cambiare](#) l'indirizzo di posta elettronica secondario


Come cambiare la password di sicurezza di Guard

1. Fare clic sull'icona **Menu di sistema**  a destra della barra dei menu. Fare clic su **Impostazioni** nel menu.
2. Nella barra laterale, fare clic su **Sicurezza di Guard**.
3. Nel campo **Digita la password di sicurezza di Guard** sotto *Password*, digitare la password utilizzata fino a quel momento per cifrare i propri dati.
Nel campo **Digita la nuova password di sicurezza di Guard**, digitare la password che si desidera utilizzare da quel momento in poi.
Confermare la password nel campo **Verifica la nuova password di sicurezza di Guard** digitandola nuovamente.
4. Fare clic su **Cambia la password di sicurezza di Guard**.

Come ripristinare la password di sicurezza di Guard:

1. Fare clic sull'icona **Menu di sistema**  a destra della barra dei menu. Fare clic su **Impostazioni** nel menu.
2. Nella barra laterale, fare clic su **Sicurezza di Guard**.
3. Fare clic su **Ripristina la password di sicurezza di Guard**. Una nuova password sarà inviata all'indirizzo di posta secondario.
Se non è stato digitato un indirizzo di posta secondario, la nuova password sarà inviata all'indirizzo di posta principale.
4. Questa nuova password è ora la propria password di sicurezza di Guard. È consigliabile [cambiare](#) immediatamente questa password.

Come modificare il proprio indirizzo secondario di posta elettronica per ripristinare la password di cifratura:

1. Fare clic sull'icona **Menu di sistema**  a destra della barra dei menu. Fare clic su **Impostazioni** nel menu.
2. Nella barra laterale, fare clic su **Sicurezza di Guard**.
3. Digitare la password per cifrare i propri dati nel campo **Digita la password di sicurezza di Guard** sotto *Indirizzo di posta secondario*.
Nel campo **Digita il nuovo indirizzo di posta secondario**, digitare l'indirizzo di posta utilizzato per ricevere la password temporanea per il ripristino della propria password di sicurezza di Guard.
Fare clic su **Cambia indirizzo**.

3.5.2 Impostazioni di cifratura PGP

Le impostazioni di cifratura di PGP specificano le impostazioni preimpostate che sono disponibili quando si compongono messaggi di posta elettronica. Quando si compone un nuovo messaggio di posta, le impostazioni predefinite possono essere modificate prima di inviare il messaggio.

Come modificare le impostazioni di cifratura PGP:

1. Fare clic sull'icona **Menu di sistema** a destra della barra dei menu. Fare clic su **Impostazioni** nel menu.
2. Selezionare la voce **Sicurezza di Guard** nella barra laterale. Fare clic su **Impostazioni avanzate**.
3. Modificare un'impostazione in *Impostazioni di cifratura PGP*.

Sono disponibili le seguenti impostazioni.

Utilizzare in modo predefinito la cifratura quando si compone un messaggio di posta

Definisce se un nuovo messaggio di posta elettronica deve essere cifrato con PGP in modo predefinito.

Firmare in modo predefinito i messaggi di posta in uscita

Definisce se un nuovo messaggio di posta elettronica deve essere cifrato con PGP in modo predefinito.

Abilitare le funzionalità avanzate di PGP

Definisce se funzionalità di PGP, come la gestione delle chiavi, devono essere visualizzate.

Utilizzare PGP in linea in modo predefinito per i nuovi messaggi

Per mostrare questa impostazione, abilitare la casella di selezione **Abilita funzionalità avanzate di PGP**.


Specifica se la cifratura PGP deve avvenire in linea. Utilizzare queste impostazioni solo se il client di posta elettronica del destinatario non supporta PGP, il messaggio dovrebbe essere comunque leggibile. Se si utilizza questa impostazione, non è possibile inviare messaggi di posta in formato HTML.

3.5.3 Gestione delle chiavi

Per inviare o ricevere messaggi cifrati, le funzioni di gestione delle chiavi non sono normalmente richieste. Tali funzioni possono essere utilizzate comunque per le seguenti esigenze:

- Si desidera utilizzare le proprie chiavi PGP di Guard in altri client di posta elettronica, ad es. nei client di posta locali.
- Si dispone di chiavi PGP da altre applicazioni. Si desidera utilizzare tali chiavi in Guard.
- Si dispone della chiave pubblica di un collaboratore esterno. Per leggere i messaggi cifrati di questo collaboratore esterno senza avere accesso a un server di chiavi, si vuole importare la chiave pubblica del collaboratore in Guard..
- Si vuole fornire la propria chiave pubblica a un destinatario per dargli accesso in lettura ai propri messaggi cifrati senza la necessità di accedere a un server di chiavi.

Come aprire la pagina per la gestione delle proprie chiavi:

1. Fare clic sull'icona **Menu di sistema**  a destra della barra dei menu. Fare clic su **Impostazioni** nel menu.
2. Selezionare la voce **Sicurezza di Guard** nella barra laterale. Fare clic su **Impostazioni avanzate**. Attivare **Abilita funzionalità avanzate di PGP**.

La pagina contiene i seguenti elementi.

- Opzioni per modificare le [impostazioni predefinite Guard](#)
- La sezione *Le tue chiavi*. Contiene funzioni per gestire le tue chiavi PGP private e pubbliche. Le proprie chiavi saranno visualizzate sotto *Il tuo elenco di chiavi*. L'elenco delle chiavi contiene due chiavi:
 - Una chiave principale. Tra le altre cose, questa chiave è utilizzata per firmare i propri messaggi di posta elettronica.
 - Una sottochiave. Questa chiave è utilizzata per cifrare e decifrare i messaggi di posta e i file. La distinzione tra chiave principale e sottochiave è una delle caratteristiche della tecnologia di cifratura di PGP. Ogni chiave principale e ogni sottochiave contiene una chiave pubblica e una chiave privata. In base alle esigenze, Guard utilizza automaticamente la relativa chiave.
- La sezione *Chiavi pubbliche*. Visualizza le chiavi pubbliche condivise da voi o da altri utenti. Se la chiave pubblica di un utente è mostrata nell'elenco, è possibile assumere che questo utente sia in grado di decifrare i messaggi di posta cifrati a lui inviati.
- Le chiavi scadute sono visualizzate in rosso.

Sono disponibili le seguenti funzioni.

- [scaricare](#) la propria chiave pubblica
- [inviare la propria chiave pubblica tramite posta elettronica](#)
- [aggiungere nuove chiavi](#) alle chiavi esistenti caricando le chiavi locali o creare nuove chiavi di Guard
- [trasformare una chiave in chiave corrente](#)
- [mostrare i dettagli](#) di una chiave
- [eliminare](#) una chiave
- [scaricare](#) la propria chiave privata
- [aggiungere un ulteriore account di posta](#) a una chiave
- [caricare](#) la chiave pubblica di un collaboratore esterno

Come scaricare la propria chiave pubblica:

1. Nelle impostazioni, [aprire](#) la pagina di gestione delle chiavi.
2. Fare clic su **Scarica chiave pubblica PGP** in *Le tue chiavi*.

Come inviare la propria chiave pubblica tramite posta elettronica:

1. Nelle impostazioni, [aprire](#) la pagina di gestione delle chiavi.
2. Fare clic su **Invia la tua chiave pubblica PGP tramite posta** in *Le tue chiavi*.

Come aggiungere una nuova chiave alle proprie chiavi:

1. Nelle impostazioni, [aprire](#) la pagina di gestione delle chiavi.
2. Fare clic sull'icona **Aggiungi+** accanto a *Elenco delle tue chiavi* sotto *Le tue chiavi*. Si aprirà la finestra *Aggiunta chiavi*.
3. Sono disponibili le seguenti opzioni:
 - Per aggiungere una chiave privata, fare clic su **Carica chiave privata**. Selezionare un file contenendo una chiave privata. Si aprirà la finestra *Carica chiavi private*.
Per caricare la nuova chiave, digitare la propria password di sicurezza Guard. Digitare una nuova password per la nuova chiave.
 - Per aggiungere una chiave pubblica, fare clic su **Carica solo la chiave pubblica**. Selezionare un file contenente una chiave pubblica.
 - Per creare una nuova coppia di chiavi, fare clic su **Creare nuove chiavi**. Si aprirà la finestra *Creare chiavi di sicurezza di Guard*.
Digitare una password per la nuova chiave. Confermare la password.
La nuova chiave consiste di una chiave principale e di una sottochiave corrispondente.
La nuova chiave sarà inserita in cima alla propria lista di chiavi. La nuova chiave diventerà la chiave corrente.


Come rendere una chiave la chiave corrente:

È possibile utilizzare questa funzione se il proprio elenco di chiavi contiene più di una chiave principale e di una sottochiave. Da questo momento, la chiave corrente sarà utilizzata per la cifratura.


1. Nelle impostazioni, [aprire](#) la pagina di gestione delle chiavi.
2. Sotto *Il tuo elenco di chiavi*, fare clic sulla casella di selezione accanto a una chiave sotto **Corrente**. Se si trasforma una chiave principale nella chiave corrente, anche la sottochiave corrispondente sarà marcata come corrente, e viceversa.

Come mostrare i dettagli di una chiave:

È possibile ottenere i dettagli per le chiavi. I dettagli di una chiave sono particolarmente utili per gli utenti che hanno conoscenze di PGP.


1. Nelle impostazioni, [aprire](#) la pagina di gestione delle chiavi.
2. Fare clic sull'icona **Dettagli**  accanto a una chiave sotto *Elenco delle tue chiavi*. Si aprirà la finestra *Dettagli chiave*. Per visualizzare le firme delle chiavi, fare clic su **Firme**.

Come eliminare una chiave:

1. Nelle impostazioni, [aprire](#) la pagina di gestione delle chiavi.
2. Fare clic sull'icona **Elimina**  accanto a *Elenco delle tue chiavi* sotto *Le tue chiavi*. Si aprirà la finestra *Elimina chiave privata*.
3. Sono disponibili le seguenti opzioni:
 - Per revocare una chiave privata, fare clic su **Revoca**.
Digitare la password della chiave privata. Se richiesto, selezionare un motivo per la revoca della chiave.
Fare clic su **Revoca**.
 - Per eliminare una chiave privata, fare clic su **Elimina**.
Digitare la password della chiave privata.
Fare clic sul pulsante **Elimina**.Se si elimina una chiave principale, sarà eliminata anche la sottochiave corrispondente.


Come scaricare la propria chiave privata:

Attenzione: lo scaricamento di una chiave privata sulla propria macchina può essere un rischio di sicurezza. Assicurarsi che nessun altro possa accedere alla propria chiave privata.

1. Nelle impostazioni, [aprire](#) la pagina di gestione delle chiavi.
2. Fare clic sull'icona **Scarica**  accanto a una chiave nell'elenco delle chiavi private sotto *Le tue chiavi*.

Come aggiungere un ulteriore account di posta a una chiave:

Quando si aggiungono ulteriori ID utente a una chiave, è possibile utilizzare la chiave per più account di posta elettronica.

1. Nelle impostazioni, [aprire](#) la pagina di gestione delle chiavi.
2. Fare clic sull'icona **Modifica**  accanto a *Elenco delle tue chiavi* sotto *Le tue chiavi*. Si aprirà la finestra *Aggiunta ID utente*.
3. Digitare un nome per l'ID utente. Digitare l'indirizzo di posta elettronica che si desidera utilizzare per questa chiave.
Digitare la propria password per questa chiave.
Fare clic su **OK**.

Come caricare la chiave pubblica di un collaboratore esterno:

1. Nelle impostazioni, [aprire](#) la pagina di gestione delle chiavi.
2. Fare clic sull'icona **Aggiungi+** accanto a *Elenco delle tue chiavi pubbliche PGP* sotto *Le tue chiavi*. Selezionare un file che contiene una chiave pubblica.

Indice analitico

A

Aprire i file cifrati, 13

C

Cambiare la password, 16

Cifrare

Comunicazioni di posta elettronica, 11

creare nuovi file cifrati, 13

File, 13

Cifrare i file, 13

Cifrare le comunicazioni di posta elettronica, 11

Creare nuovi file cifrati, 13

D

Decifrare i file, 14

Documentazione, 5

F

File cifrati

Aprire, 13

decifrare, 14

scaricare, 14

G

Guard, 7, 9

configurazione, 10

Gestione delle chiavi, 18

Impostazioni, 16

Impostazioni di cifratura PGP, 17

impostazioni di sicurezza, 16

uscire, 15

I

Impostazioni di Guard

Cambiare password, 16

Ripristinare la password, 16

Impostazioni PGP di Guard di Guard

Abilitare le funzionalità avanzate di PGP, 17

Firmare in modo predefinito i messaggi di posta in uscita, 17

Utilizzare in modo predefinito la cifratura quando si compone un messaggio di posta, 17

Utilizzare PGP in linea in modo predefinito per i nuovi messaggi, 17

M

Messaggi di posta cifrati

accessi per destinatari esterni, 12

bloccare, 11

inviare, 11

leggere, 11

R

Ripristinare la password, 16

S

Scaricare i file cifrati, 14

U

Uscire

Cambiare password, 15

