Guard

Manuale utente

Guard: Manuale utente

Data di pubblicazione mercoledì, 23. marzo 2016 Version 2.2.0

Indice

1 Informazioni su questa documentazione

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

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 funzione 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 all'intestazione.
2. Successivamente sarà richiesto di digitare la 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. Nella barra laterale, fare clic su **Impostazioni di sicurezza di Guard**.

   Quando si selezionano inizialmente le impostazioni di sicurezza di Guard, si aprirà la finestra *Crea le 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
- Accesso per destinatari esterni

3.2.1 Leggere i messaggi di posta cifrati

Per poter leggere un messaggio di posta cifrato, almeno la password di sicurezza di Guard è richiesta. 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, durante l'ultimo utilizzo di Guard, si è scelto di far memorizzare la password di sicurezza, il messaggio di posta è visualizzato immediatamente, in base all'impostazione.

2. Digitare la password di sicurezza di Guard.

   È possibile specificare per quanto tempo dovrebbe essere memorizzata la password di sicurezza. 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 il destinatario 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 un nuovo messaggio*, fare clic su l'icona **Cifra** in alto a destra.

   È possibile fare clic anche su **Sicurezza** sotto l'oggetto. Abilitare **Cifra**.

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.

3. Fare clic su **Invio sicuro**.

   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.

3.2.3 Accesso per destinatari esterni

È possibile anche inviare messaggi di posta cifrati a destinatari esterni che non sono utenti del groupware. Quando si invia per la prima volta un messaggio cifrato a un destinatario esterno, si verifica ciò che segue:

- Un account speciale viene configurato automaticamente per il destinatario esterno.
- Si specifica se il destinatario esterno deve ricevere una notifica creata automaticamente del messaggio cifrato o una notifica personalizzata.
- Il destinatario esterno riceve un messaggio di posta con la notifica e una password generata automaticamente.

  In base alla configurazione del groupware, è possibile inviare un PIN di 4 cifre al destinatario per proteggere la password creata.
- Il destinatario esterno riceve un messaggio di posta con un collegamento alla pagina di accesso per l'account speciale.
- Il destinatario esterno digita la password generata automaticamente nella pagina di accesso.

  Poi, il destinatario deve cambiare la password generata automaticamente. Per poter ripristinare l'account in caso di smarrimento della password, deve essere specificata una domanda di sicurezza e la rispettiva risposta.

  Il messaggio di posta cifrato viene visualizzato.
- Il destinatario esterno può inviare una risposta cifrata al messaggio.

Quando si invia il messaggio cifrato successivo a questo destinatario esterno, si verifica ciò che segue:

- Il destinatario esterno riceve un messaggio con un collegamento alla pagina di accesso per l'account speciale.
- Nella pagina di accesso, il destinatario digita la password configurata al momento della ricezione di un messaggio cifrato.

  Se il destinatario non ricorda la password, può essere richiesta una nuova password. Per fare ciò, è necessario rispondere correttamente alla domanda di sicurezza.

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 selezionare 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. Nella finestra *Digita la password di sicurezza di Guard*, digitare la password di sicurezza di Guard.
   È possibile specificare per quanto tempo dovrebbe essere memorizzata 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 cifrare 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. Nella finestra *Digita la password di sicurezza di Guard*, digitare la password di sicurezza di Guard.
   È possibile specificare per quanto tempo dovrebbe essere memorizzata 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. Nella 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 Disconnettersi 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 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 predefinite di Guard.
- 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
- Se si dimentica la password di sicurezza di Guard, è possibile richiedere l'invio di una password temporanea al proprio indirizzo di posta elettronica ripristinando la password di sicurezza di Guard.
- 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 in precedenza per cifrare i propri dati.

   Nel campo **Digita la nuova password di sicurezza di Guard**, digitare la password che si desidera utilizzare per cifrare i propri dati da quel momento in avanti.

   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 di posta**.

3.5.2 Impostazioni predefinite di Guard

Le impostazioni predefinite 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 predefinite:

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 PGP di Guard**.
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.

PGP usa PGP in linea in modo predefinito per compatibilità

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 ottengono chiavi PGP da altre applicazioni PGP. 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 PGP di Guard**.

La pagina contiene i seguenti elementi.

- Opzioni per modificare le Impostazioni predefinite di Guard.
- La sezione *Le tue chiavi*. Contiene funzioni per gestire le tue chiavi PGP private e pubbliche.
- 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.

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 creando nuove chiavi di Guard
- scaricare la propria chiave privata
- 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** + . 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 password di sicurezza di 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 **Crea nuove chiavi**. Si aprirà la finestra *Crea chiavi di sicurezza di Guard*.

     Digitare una password per la nuova chiave. Confermare la password.

   La nuova chiave sarà inserita sotto *Elenco chiavi*.

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** .

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** + . Selezionare un file che contiene una chiave pubblica.

Indice analitico