Guard

Benutzeranleitung

Guard: Benutzeranleitung

Veröffentlicht Mittwoch, 09. November 2016 Version 2.6.0

Inhaltsverzeichnis

1 Über diese Dokumentation

Die folgenden Informationen helfen Ihnen beim Umgang mit der Dokumentation.

An wen richtet sich diese Dokumentation?

Diese Dokumentation richtet sich an Benutzer, die ihre E-Mail Kommunikation und ihre Dateien vor unbefugtem Zugriff schützen möchten, indem sie diese verschlüsseln.

Welche Inhalte umfasst diese Dokumentation?

In dieser Dokumentation finden Sie die folgenden Informationen:

- In *Wozu dient Guard ?* finden Sie eine kurze Beschreibung von Guard .
- In *Die Verwendung von Guard* finden Sie Anleitungen zur Verwendung von Guard .

Diese Dokumentation beschreibt den Umgang mit einer typischen Installation und Konfiguration der Groupware. Die Installation und Konfiguration, mit der Sie arbeiten, kann davon abweichen.

Welche sonstigen Hilfen sind verfügbar?

Eine ausführliche Dokumentation der Groupware finden Sie in der Groupware Benutzeranleitung.

2 Wozu dient Guard ?

Mit Guard verwenden Sie innerhalb der Groupware eine Sicherheitslösung zur Verschlüsselung von E-Mails und Dateien.

- Verschlüsseln Sie Ihre E-Mail-Kommunikation mit anderen Benutzern oder mit externen Partnern.
- Verschlüsseln Sie einzelne Dateien. Teilen Sie die verschlüsselten Daten mit anderen Benutzern.
- Bestimmen Sie mit Hilfe von Sicherheitsoptionen den Grad der Verschlüsselung.
- Für den Zugriff auf Ihre verschlüsselten Daten ist ein Passwort erforderlich. Schützen Sie sich vor den Folgen eines Passwortverlusts, indem Sie die Funktion zum Zurücksetzen des Passwortes aktivieren.

3 Die Verwendung von Guard

Erfahren Sie, wie Sie mit *Guard* arbeiten.

- Grundeinstellungen vornehmen
- Verschlüsseln der E-Mail Kommunikation
- Verschlüsseln von Dateien
- Sicherheitseinstellungen vornehmen

3.1 Die *Guard* Einrichtung

Bevor Sie *Guard* verwenden können, müssen Sie einige Grundeinstellungen vornehmen.

- Sie bestimmen ein Guard-Sicherheitspasswort, um Daten verschlüsseln zu können und um auf verschlüsselte Daten zugreifen zu können.
- Sie geben eine sekundäre E-Mail-Adresse an, für den Fall dass Sie Ihr Guard-Sicherheitspasswort verlieren sollten. In diesem Fall verwenden Sie die Funktion zum Zurücksetzen des Guard-Sicherheitspassworts. Diese Funktion sendet Ihnen ein Ersatzpasswort. Aus Sicherheitsgründen wird dringend empfohlen, hierfür eine sekundäre E-Mail-Adresse anzugeben. Andernfalls erhalten Sie das Ersatzpasswort an Ihren primären E-Mail-Account.

Um die Grundeinstellungen vorzunehmen, haben Sie zwei alternative Möglichkeiten:

- Sie bestimmen die Grundeinstellungen, während Sie das erste Mal eine Verschlüsselungsfunktion verwenden.
- Sie bestimmen die Grundeinstellungen mit Hilfe der Groupware Einstellungen, bevor Sie die Verschlüsselungsfunktionen verwenden.

So bestimmen Sie die Grundeinstellungen während der erstmaligen Verwendung einer Verschlüsselungsfunktion:

1. Aktivieren Sie beim Schreiben einer E-Mail, beim Verschlüsseln einer Datei oder beim Hochladen einer neuen Datei die Verschlüsselungsfunktion, indem Sie das Symbol **Verschlüsseln** anklicken.
2. Sie werden nacheinander dazu aufgefordert, ein Guard Sicherheitspasswort und eine sekundäre E-Mail-Adresse anzugeben. Geben Sie diese Daten ein.

So bestimmen Sie die Grundeinstellungen vor der erstmaligen Verwendung einer Verschlüsselung:

1. Klicken Sie in der Menüleiste rechts auf das Symbol **Systemmenü** . Klicken Sie im Menü auf **Einstellungen**.
2. Klicken Sie in der Seitenleiste auf **Guard-Sicherheit**.

   Wenn Sie zum ersten Mal die Guard-Sicherheitseinstellungen wählen, öffnet sich das Fenster *Guard-Sicherheitsschlüssel erstellen*.
3. Geben Sie in **Passwort** das Passwort ein, das Sie für die Verschlüsselung Ihrer Daten verwenden möchten.

   Geben Sie in **Bestätigen** das gleiche Passwort nochmal ein.
4. Geben Sie in **Sekundäre E-Mail-Adresse eingeben** die E-Mail-Adresse ein, an die ein temporäres Passwort gesendet wird, mit dessen Hilfe Sie Ihr Guard-Sicherheitspasswort bei Bedarf zurücksetzen können.
5. Klicken Sie auf **OK**.

3.2 E-Mail Kommunikation verschlüsseln

Sie haben folgende Möglichkeiten:

- Verschlüsselte E-Mails lesen
- Verschlüsselte E-Mails senden
- Wie lesen externe Empfänger eine verschlüsselte E-Mail?

3.2.1 Verschlüsselte E-Mails lesen

Um eine verschlüsselte E-Mail zu lesen, benötigen Sie mindestens das Guard Sicherheitspasswort. Der Absender der verschlüsselten E-Mail kann festlegen, dass Sie ein zusätzliches Passwort zum Lesen der E-Mail benötigen.

So lesen Sie eine verschlüsselte E-Mail:

1. Klicken Sie in der Liste auf eine E-Mail, bei der das Symbol *Verschlüsselt* angezeigt wird. In der Detailansicht wird die Meldung *Sichere E-Mail. Geben Sie Ihr Sicherheitspasswort ein.* angezeigt.

   Hinweis: Wenn Sie bei der letzten Verwendung von Guard angegeben haben, dass Guard sich das Sicherheitspasswort merken soll, wird die E-Mail je nach Einstellung sofort angezeigt.
2. Geben Sie das Guard-Sicherheitspasswort ein.

   Bei Bedarf können Sie festlegen, wie lange sich Guard das Sicherheitspasswort merkt. Dazu aktivieren Sie **Bei Guard angemeldet bleiben**. Wählen Sie in der Liste einen Wert.
3. Klicken Sie auf **OK**. Der Inhalt wird im Klartext angezeigt.

   Wenn die E-Mail Anhänge enthält, werden Funktionen angezeigt, mit denen Sie die Anhänge entschlüsselt oder verschlüsselt weiterverwenden können.

Hinweis: Sie können diese E-Mail nur mit einer verschlüsselten E-Mail beantworten oder weiterleiten.

3.2.2 Verschlüsselte E-Mails senden

Sie haben folgende Möglichkeiten:

- Eine E-Mail verschlüsselt senden. Nur Sie und die Empfänger können den Inhalt der E-Mail lesen.

  Achtung: Wenn Sie einen verschlüsselt gespeicherten E-Mail Entwurf senden, wird dieser Entwurf nach dem Senden aus dem Ordner *Entwürfe* gelöscht.
- Eine E-Mail mit Signatur senden. Die Signatur stellt sicher, dass der Empfänger erkennen kann, ob der E-Mail Inhalt auf dem Transportweg verändert wurde.
- Eine E-Mail verschlüsselt und mit Signatur senden.

So senden Sie eine verschlüsselte E-Mail:

1. Verfassen Sie in der App *E-Mail* wie gewohnt eine E-Mail.

   Auf der Seite *Verfassen* klicken Sie rechts oben auf das Symbol **Verschlüsseln** .

   Alternativ klicken Sie unterhalb des Betreffs auf **Sicherheit**. Aktivieren Sie **Verschlüsseln**.

   Symbole neben den Empfängern zeigen an, ob die Nachricht für diesen Empfänger verschlüsselt werden kann. Wenn Sie auf ein Symbol zeigen, wird eine Erläuterung angezeigt.

2. Um weitere Optionen zu verwenden, klicken Sie auf **Sicherheit**. Aktivieren Sie bei Bedarf die folgenden Optionen.

   Um die E-Mail zusätzlich zu signieren, aktivieren Sie **Signieren**.

   Für den Fall, dass der E-Mail Client eines Empfängers kein PGP unterstützt, die Nachricht aber trotzdem lesbar sein soll, aktivieren Sie **PGP Inline**. Wenn Sie diese Einstellung verwenden, können Sie keine E-Mails im HTML-Format senden.

   Damit der Empfänger die E-Mail verschlüsselt beantworten kann, benötigt er Ihren öffentlichen Schlüssel. Bei Bedarf können Sie Ihren öffentlichen Schlüssel als Anhang senden. Dazu aktivieren Sie **Meinen Schlüssel anhängen**.

3. Klicken Sie auf **Verschlüsselt senden**.

   Wenn Sie an externe Empfänger senden, wird ein Fenster angezeigt, in dem Sie den externen Empfängern Hinweise zum Öffnen der verschlüsselten E-Mail [12] senden können.

   Wenn Sie einem externen Empfänger das erste Mal eine verschlüsselte E-Mail senden, erhält der externe Empfänger Ihren öffentlichen Schlüssel als E-Mail Anhang.

3.2.3 Wie lesen externe Empfänger eine verschlüsselte E-Mail?

Sie können verschlüsselte E-Mails auch an externe Empfänger senden, die keine Benutzer der Groupware sind. Beim Hinzufügen eines externen Empfängers prüft Guard, ob für diesen Empfänger ein öffentlicher Schlüssel verfügbar ist. Je nach Resultat verwendet Guard unterschiedliche Verfahren zum Senden der verschlüsselten E-Mail.

- Wenn ein öffentlicher Schlüssel des Empfängers gefunden wird:
  - Die Nachricht wird mit diesem Schlüssel verschlüsselt gesendet. Der Empfänger kann die Nachricht mit Hilfe seines privaten Schlüssels lesen.
  - Damit Ihnen der Empfänger verschlüsselt antworten kann, wird Ihr öffentlicher Schlüssel als Anhang mitgesendet. Der Anhang heißt public.asc. Der Empfänger kann diesen Schlüssel in seinen E-Mail Client importieren.
- Wenn kein öffentlicher Schlüssel gefunden wird:
  - Wenn der Externe Benutzer bereits ein Gastkonto besitzt, erhält er eine E-Mail mit dem Link zu der Anmeldeseite für sein Gastkonto. Nachdem er sich angemeldet hat, kann er die verschlüsselte E-Mail auf der Gastseite lesen. Bei Bedarf kann er dort die E-Mail verschlüsselt beantworten.
  - Wenn kein Gastkonto vorhanden ist, wird ein Gastkonto angelegt. Der externe Empfänger erhält eine E-Mail, die einen Link zur Gastseite und ein automatisch erzeugtes Passwort enthält. Auf der Gastseite meldet er sich an. Anschließend kann er ein eigenes Passwort anlegen.

    Je nach Konfiguration werden das automatisch erzeugte Passwort und der Link zur Gastseite mit separaten E-Mail gesendet.
  - Je nach Konfiguration der Groupware werden die E-Mails von Gastkonten nach einer bestimmten Anzahl von Tagen vom Server gelöscht. Damit diese E-Mails weiterhin gelesen werden können, enthält die E-Mail mit dem Link zur Gastseite im Anhang die verschlüsselte E-Mail. Der Anhang heißt encrypted.asc. Dieser Anhang kann auf der Gastseite hochgeladen und gelesen werden.

3.3 Dateien verschlüsseln

Sie haben folgende Möglichkeiten:

- Dateien verschlüsseln
- Neue verschlüsselte Datei anlegen
- Verschlüsselte Datei öffnen
- Verschlüsselte Datei herunterladen
- Datei entschlüsseln

3.3.1 Dateien verschlüsseln

Wenn Sie eine Datei verschlüsseln, wird nur die letzte Version der Datei verschlüsselt. Alle vorhergehenden Versionen werden gelöscht.

So verschlüsseln Sie eine Datei:

Achtung: Wenn Sie eine Datei verschlüsseln, werden alle Versionen außer der aktuellen Version der Datei gelöscht. Wenn Sie eine ältere Version weiterhin benötigen, sichern Sie diese Version, bevor Sie die Datei verschlüsseln.

1. In der App *Drive* wählen Sie im Anzeigebereich eine Datei oder mehrere Dateien. Klicken Sie in der Werkzeugleiste auf das Symbol **Aktionen** . Klicken Sie im Menü auf **Verschlüsseln**.

   Alternativ verwenden Sie im *Viewer* das Symbol **Aktionen** . Klicken Sie im Menü auf **Verschlüsseln**.

2. Wenn die Datei mehrere Versionen enthält, wird das Fenster *Dateien verschlüsseln* angezeigt. Bestätigen Sie, dass Sie die Datei verschlüsseln und alle vorherigen Versionen löschen wollen, indem Sie auf **OK** klicken.

   Wenn die Datei nur eine Version enthält, wird die Datei ohne weitere Nachfrage verschlüsselt.

3.3.2 Neue verschlüsselte Datei anlegen

Sie können eine neue verschlüsselte Datei anlegen, indem Sie eine lokal vorhandene Datei verschlüsselt hochladen.

So legen Sie eine neue verschlüsselte Datei an:

1. In der App *Drive* öffnen Sie im Ordnerbaum einen Ordner.

   Hinweis: Öffnen Sie einen Ordner, in dem Sie die Berechtigung zum Anlegen von Objekten haben.

2. Klicken Sie in der Werkzeugleiste auf **Neu**. Klicken Sie auf **Lokale Datei hinzufügen und verschlüsseln**.

3. Im Fenster *Datei hochladen* wählen Sie eine Datei oder mehrere Dateien.

   Klicken Sie auf **Öffnen**. Unten im Anzeigebereich wird der aktuelle Fortschritt angezeigt.

   Um den Vorgang abzubrechen, klicken Sie unten rechts im Anzeigebereich auf **Datei-Details**. Im Fenster *Upload-Fortschritt* klicken Sie neben einem Dateinamen auf **Abbrechen**.

Tipp: Sie können eine neue verschlüsselte Datei auch anlegen, indem Sie eine Datei vom Desktop Ihres Betriebssystems in das Fenster der App *Drive* ziehen und dort in der unteren Hälfte ablegen.

3.3.3 Verschlüsselte Datei öffnen

Sie können eine verschlüsselte Datei öffnen, um sie zu lesen oder zu bearbeiten. Auf dem Server bleibt die Datei weiterhin verschlüsselt.

So öffnen Sie eine verschlüsselte Datei:

1. In der App *Drive* wählen Sie im Anzeigebereich eine verschlüsselte Datei. Klicken Sie in der Werkzeugleiste auf das Symbol **Ansicht** .
2. Wenn sich das Fenster *Guard-Sicherheitspasswort eingeben* öffnet, geben Sie das Guard-Sicherheitspasswort ein.

   Bei Bedarf können Sie festlegen, wie lange sich Guard das Sicherheitspasswort merkt. Dazu aktivieren Sie **Passwort merken**. Wählen Sie in der Liste einen Wert.

   Klicken Sie auf **OK**.

3.3.4 Verschlüsselte Datei herunterladen

Sie können eine verschlüsselte Datei herunterladen, um sie lokal zu lesen oder zu bearbeiten. Auf dem Server bleibt die Datei weiterhin verschlüsselt.

So laden Sie eine verschlüsselte Datei herunter:

1. In der App *Drive* wählen Sie im Anzeigebereich eine verschlüsselte Datei. Klicken Sie in der Werkzeugleiste auf das Symbol **Ansicht** .

   Hinweis: Wenn Sie statt dessen im Popup auf **Download** klicken, ist die heruntergeladene Datei weiterhin verschlüsselt.
2. Wenn sich das Fenster *Guard-Sicherheitspasswort eingeben* öffnet, geben Sie das Guard-Sicherheitspasswort ein.

   Bei Bedarf können Sie festlegen, wie lange sich Guard das Sicherheitspasswort merkt. Dazu aktivieren Sie **Passwort merken**. Wählen Sie in der Liste einen Wert.

   Klicken Sie auf **OK**.
3. Klicken Sie im Viewer auf das Symbol **Aktionen** . Klicken Sie auf **Entschlüsselt herunterladen**.

3.3.5 Datei entschlüsseln

Sie können die Verschlüsselung von einer Datei entfernen, indem Sie die Datei entschlüsseln.

So entschlüsseln Sie eine Datei:

1. In der App *Drive* wählen Sie im Anzeigebereich eine verschlüsselte Datei. Klicken Sie in der Werkzeugleiste auf das Symbol **Aktionen** . Klicken Sie im Menü auf **Verschlüsselung entfernen**.
2. Wenn sich das Fenster *Guard-Sicherheitspasswort eingeben* öffnet, geben Sie das Guard-Sicherheitspasswort ein.

   Bei Bedarf können Sie festlegen, wie lange das Guard-Sicherheitspasswort gelten soll. Dazu aktivieren Sie **Passwort merken**. Wählen Sie in der Liste einen Wert.

   Klicken Sie auf **OK**.

3.4 Von Guard abmelden

Sie können sich vonGuard abmelden, ohne die Groupware zu beenden. Wenn Sie anschließend eine verschlüsselte E-Mail, Datei oder Ordner öffnen wollen, müssen Sie das Guard-Sicherheitspasswort wieder eingeben.
Hinweis: Diese Funktion ist nur verfügbar, wenn Sie **Passwort merken** aktivieren, während Sie eine verschlüsselte E-Mail oder Datei öffnen.

So melden Sie sich von Guard ab:

1. Klicken Sie in der Menüleiste rechts auf das Symbol **Systemmenü** .
2. Klicken Sie im Menü auf **Bei Guard abmelden**.

3.5 Guard Einstellungen

Sie haben die folgenden Möglichkeiten:

- Zum Verwalten Ihres Guard Sicherheitspasswortes verwenden Sie die Guard Sicherheitseinstellungen.
- Zum Anpassen der Voreinstellungen zum Senden sicherer E-Mails verwenden Sie die PGP-Verschlüsselungseinstellungen.
- Bei Bedarf können Sie Ihre PGP Schlüssel verwalten.

3.5.1 Guard Sicherheitseinstellungen

Sie haben die folgenden Möglichkeiten:

- Das Guard-Sicherheitspasswort ändern
- Wenn Sie Ihr Guard-Sicherheitspasswort verloren haben, können Sie sich ein temporäres Guard-Sicherheitspasswort schicken lassen, indem Sie das Guard-Sicherheitspasswort zurücksetzen.
- Die sekundäre E-Mail-Adresse ändern

So ändern Sie das Guard-Sicherheitspasswort:

1. Klicken Sie in der Menüleiste rechts auf das Symbol **Systemmenü** . Klicken Sie im Menü auf **Einstellungen**.
2. Klicken Sie in der Seitenleiste auf **Guard-Sicherheit**.
3. Geben Sie unterhalb von *Passwort* in **Aktuelles Guard-Sicherheitspasswort eingeben** das Passwort ein, das Sie bisher für die Verschlüsselung Ihrer Daten verwendet haben.

   Geben Sie in **Neues Guard-Sicherheitspasswort eingeben** das Passwort ein, das Sie ab sofort die Verschlüsselung Ihrer Daten verwenden möchten.

   Geben Sie in **Neues Guard-Sicherheitspasswort bestätigen** das neue Passwort erneut ein.
4. Klicken Sie auf **Guard-Sicherheitspasswort ändern**.

So setzen Sie das Guard-Sicherheitspasswort zurück:

1. Klicken Sie in der Menüleiste rechts auf das Symbol **Systemmenü** . Klicken Sie im Menü auf **Einstellungen**.
2. Klicken Sie in der Seitenleiste auf **Guard-Sicherheit**.
3. Klicken Sie auf **Guard-Sicherheitspasswort zurücksetzen**. Ein neues Passwort wird an Ihre sekundäre E-Mail-Adresse gesendet.

   Wenn Sie keine sekundäre E-Mail-Adresse angegeben haben, wird das neue Passwort an Ihre primäre E-Mail-Adresse gesendet.
4. Dieses neue Passwort ist jetzt Ihr aktuelles Guard-Sicherheitspasswort. Sie sollten dieses Passwort sofort ändern.

So ändern Sie Ihre sekundäre E-Mail-Adresse zum Zurücksetzen des Passwort für die Verschlüsselung:

1. Klicken Sie in der Menüleiste rechts auf das Symbol **Systemmenü** . Klicken Sie im Menü auf **Einstellungen**.
2. Klicken Sie in der Seitenleiste auf **Guard-Sicherheit**.
3. Geben Sie unterhalb von *Sekundäre E-Mail* in **Aktuelles Guard-Sicherheitspasswort eingeben** das Passwort ein, das Sie für die Verschlüsselung Ihrer Daten verwenden.

   Geben Sie in **Neue sekundäre E-Mail-Adresse eingeben** die E-Mail-Adresse ein, an die ein temporäres Passwort gesendet wird, mit dessen Hilfe Sie Ihr Guard-Sicherheitspasswort bei Bedarf zurücksetzen können.

   Klicken Sie auf **E-Mail ändern**.

3.5.2 PGP-Verschlüsselungseinstellungen

Die PGP-Verschlüsselungseinstellungen legen fest, welche Voreinstellungen beim Verfassen von E-Mails angeboten werden. Wenn Sie eine neue E-Mail verfassen, können Sie diese Voreinstellungen jedesmal anpassen, bevor Sie die E-Mail versenden.

So ändern Sie die PGP-Verschlüsselungseinstellungen:

1. Klicken Sie in der Menüleiste rechts auf das Symbol **Systemmenü** . Klicken Sie im Menü auf **Einstellungen**.
2. Öffnen Sie in der Seitenleiste den Eintrag **Guard-Sicherheit**. Klicken Sie auf **Erweiterte Einstellungen**.
3. Ändern Sie unterhalb von *PGP-Verschlüsselungseinstellungen* eine Einstellung.

Die folgenden Einstellungen sind verfügbar.

Standardmäßig beim Erstellen einer E-Mail verschlüsselt senden

Bestimmt, ob eine neue E-Mail standardmäßig mit PGP verschlüsselt wird.

Standardmäßig Signatur zu ausgehenden E-Mails hinzufügen

Bestimmt, ob eine neue E-Mail standardmäßig mit PGP signiert wird.

Erweiterte PGP-Funktionen aktivieren

Bestimmt, ob PGP-Funktionen wie Schlüsselverwaltung angezeigt werden.

Als PGP-Standard PGP Inline für neue E-Mails verwenden

Um diese Einstellung anzuzeigen, aktivieren Sie das Kontrollfeld **Erweiterte PGP-Funktionen aktivieren**.
Diese Einstellung bestimmt, ob die PGP Verschlüsselung Inline erfolgt. Nutzen Sie diese Einstellung nur dann, wenn wenn der E-Mail Client eines Empfängers kein PGP unterstützt, die Nachricht aber trotzdem lesbar sein soll. Wenn Sie diese Einstellung verwenden, können Sie keine E-Mails im HTML-Format senden.

3.5.3 Schlüssel verwalten

Um verschlüsselte Nachrichten zu senden oder zu empfangen, sind die Funktionen zur Schlüsselverwaltung normalerweise nicht erforderlich. Jedoch können Sie diese Funktionen zum Beispiel bei den folgenden Anforderungen verwenden:

- Sie möchten Ihre Guard PGP Schlüssel in anderen E-Mail Clients verwenden, zum Beispiel in lokalen E-Mail Clients.
- Sie besitzen PGP Schlüssel aus anderen PGP Anwendungen. Sie möchten diese Schlüssel in Guard verwenden.
- Sie besitzen den öffentlichen Schlüssel eines externen Partners. Um verschlüsselte Nachrichten dieses externen Partners zu lesen, ohne auf einen Schlüsselserver zuzugreifen, möchten Sie seinen öffentlichen Schlüssel in Guard importieren.
- Sie möchten einem Empfänger Ihren öffentlichen Schlüssel zur Verfügung stellen, damit der Empfänger Ihre verschlüsselten Nachrichten lesen kann, ohne das er dazu auf einen Schlüsselserver zugreifen muss.

So öffnen Sie die Seite zur Verwaltung Ihrer Schlüssel:

1. Klicken Sie in der Menüleiste rechts auf das Symbol **Systemmenü** . Klicken Sie im Menü auf **Einstellungen**.
2. Öffnen Sie in der Seitenleiste den Eintrag **Guard-Sicherheit**. Klicken Sie auf Klicken Sie auf **Erweiterte Einstellungen**.

   Aktivieren Sie **Erweiterte PGP-Funktionen aktivieren**.

Die Seite enthält diese Bestandteile.

- Elemente zum Anpassen der Guard Standardeinstellungen
- Bereich *Ihre Schlüssel*. Enthält Funktionen zum Verwalten Ihrer privaten und öffentlichen PGP-Schlüssel.

  Ihre vorhandenen Schlüssel werden unterhalb von *Ihre Schlüsselliste* angezeigt. Die Schlüsselliste enthält diese beiden Schlüssel:

  - Einen Hauptschlüssel. Dieser Schlüssel wird unter Anderem zum Signieren Ihrer E-Mails verwendet.
  - Einen Unterschlüssel. Dieser Schlüssel wird zum Verschlüsseln und Entschlüsseln von E-Mails und Dateien verwendet.

  Die Unterscheidung in Hauptschlüssel und Unterschlüssel ist ein Merkmal der PGP Verschlüsselungstechnik. Jeder Hauptschlüssel und jeder Unterschlüssel enthält wiederum einen öffentlichen Schlüssel und einen privaten Schlüssel. Je nach Aktion benutzt Guard automatisch den erforderlichen Schlüssel.
- Bereich *Öffentliche Schlüssel*. Zeigt die öffentlichen Schlüssel, die Sie oder andere Benutzer freigegeben haben. Wenn der öffentliche Schlüssel eines Benutzers in dieser Liste erscheint, können Sie annehmen, dass dieser Benutzer die E-Mails entschlüsseln kann, die Sie dem Benutzer verschlüsselt senden.
- Abgelaufene Schlüssel werden in roter Farbe angezeigt.

Die folgenden Funktionen sind verfügbar:

- Ihren öffentlichen Schlüssel herunterladen
- Ihren öffentlichen Schlüssel per E-Mail senden
- Ihren Schlüsseln neue Schlüssel hinzufügen, indem Sie lokale Schlüssel hochladen oder neue Guard Schlüssel erzeugen
- Einen Schlüssel zum aktuellen Schlüssel machen
- Zu einen Schlüssel Details anzeigen
- Einen Schlüssel löschen
- Ihren privaten Schlüssel herunterladen
- Einem Schlüssel ein weiteres E-Mail Konto hinzufügen
- Den öffentlichen Schlüssel eines externen Partners hochladen

So laden Sie Ihren öffentlichen Schlüssel herunter:

1. Öffnen Sie in den Einstellungen die Seite zur Verwaltung der Schlüssel.
2. Klicken Sie unterhalb von *Ihre Schlüssel* auf **Öffentlichen PGP-Schlüssel herunterladen**.

So senden Sie Ihren öffentlichen Schlüssel per E-Mail:

1. Öffnen Sie in den Einstellungen die Seite zur Verwaltung der Schlüssel.
2. Klicken Sie unterhalb von *Ihre Schlüssel* auf **Ihren öffentlichen PGP-Schlüssel per E-Mail versenden**.

So fügen Sie Ihren Schlüsseln einen neuen Schlüssel hinzu:

1. Öffnen Sie in den Einstellungen die Seite zur Verwaltung der Schlüssel.
2. Klicken Sie unterhalb von *Ihre Schlüssel* neben *Ihre Schlüsselliste* auf das Symbol **Hinzufügen** + . Das Fenster *Schlüssel hinzufügen* öffnet sich.
3. Führen Sie eine der folgenden Aktionen aus:
   - Um einen privaten Schlüssel hinzuzufügen, klicken Sie auf **Privaten Schlüssel hochladen**. Wählen Sie eine Datei, die einen privaten Schlüssel enthält. Das Fenster *Private Schlüssel hochladen* öffnet sich.

     Geben Sie Ihr Guard Sicherheitspasswort ein, um den neuen Schlüssel hochzuladen. Geben Sie ein neues Passwort für den neuen Schlüssel ein.
   - Um einen öffentlichen Schlüssel hinzuzufügen, klicken Sie auf **Nur öffentlichen Schlüssel hochladen**. Wählen Sie eine Datei, die einen öffentlichen Schlüssel enthält.
   - Um ein neues Schlüsselpaar zu erzeugen, klicken Sie auf **Neue Schlüssel erstellen**. Das Fenster *Create Guard Security Keys* öffnet sich.

     Geben Sie ein Passwort für den neuen Schlüssel ein. Bestätigen Sie das Passwort.

     Der neue Schlüssel besteht aus einem Hauptschlüssel und einem zugehörigen Unterschlüssel.

   Der neue Schlüssel wird in Ihrer Schlüsselliste oben eingetragen. Der neue Schlüssel wird zum aktuellen Schlüssel.

So machen Sie einen Schlüssel aktuell:

Diese Funktion können Sie verwenden, wenn Sie Ihre Schlüsselliste mehr als einen Haupt- und Unterschlüssel enthält. Der aktuelle Schlüssel wird künftig zur Verschlüsselung verwendet.

1. Öffnen Sie in den Einstellungen die Seite zur Verwaltung der Schlüssel.
2. Klicken Sie unterhalb von *Ihre Schlüsselliste* neben einem Schlüssel auf das Kontrollfeld unterhalb von **Aktuell**. Wenn Sie einen Hauptschlüssel aktuell machen, wird der zugehörige Unterschlüssel ebenfalls aktuell, und umgekehrt.

So zeigen Sie Details zu einem Schlüssel an:

Sie können Details zu den Schlüsseln abfragen. Die Details zu einem Schlüssel sind insbesondere für Benutzer mit PGP Kenntnissen von Bedeutung.

1. Öffnen Sie in den Einstellungen die Seite zur Verwaltung der Schlüssel.
2. Klicken Sie unterhalb von *Ihre Schlüsselliste* neben einem Schlüssel auf das **Details** 🔍. Das Fenster *Schlüssel-Details* wird geöffnet. Um die Signaturen des Schlüssels anzuzeigen, klicken Sie auf **Signaturen**.

So löschen Sie einen Schlüssel:

1. Öffnen Sie in den Einstellungen die Seite zur Verwaltung der Schlüssel.
2. Klicken Sie unterhalb von *Ihre Schlüssel* neben *Ihre Schlüsselliste* auf das Symbol **Löschen** . Das Fenster *Privaten Schlüssel löschen* öffnet sich.
3. Führen Sie eine der folgenden Aktionen aus:
   - Um einen privaten Schlüssel zu widerrufen, klicken Sie auf **Widerrufen**.

     Geben Sie das Passwort für den privaten Schlüssel ein. Bei Bedarf wählen eine Grund für das Widerrufen des Schlüssels.

     Klicken Sie auf **Widerrufen**.
   - Um einen privaten Schlüssel zu löschen, klicken Sie auf **Löschen**.

     Geben Sie das Passwort für den privaten Schlüssel ein.

     Klicken Sie auf **Löschen**.

   Wenn Sie einen Hauptschlüssel löschen, wird der zugehörige Unterschlüssel ebenfalls gelöscht, und umgekehrt.

So laden Sie Ihren privaten Schlüssel herunter:

Vorsicht: Das Herunterladen eines privaten Schlüssels auf Ihren Arbeitsplatzrechner kann ein Sicherheitsrisiko darstellen. Stellen Sie sicher, dass sich niemand Zugang zu Ihrem privaten Schlüssel verschaffen kann.

1. Öffnen Sie in den Einstellungen die Seite zur Verwaltung der Schlüssel.
2. Klicken Sie unterhalb von *Ihre Schlüssel* in der Liste der privaten Schlüssel neben einem Schlüssel auf das Symbol **Herunterladen** .

So fügen Sie einem Schlüssel ein weiteres E-Mail Konto hinzu:

Wenn Sie einem Schlüssel weitere Benutzer-ID's hinzufügen, können Sie den Schlüssel für mehrere E-Mail Konten verwenden.

1. Öffnen Sie in den Einstellungen die Seite zur Verwaltung der Schlüssel.
2. Klicken Sie unterhalb von *Ihre Schlüssel* neben *Ihre Schlüsselliste* auf das Symbol **Bearbeiten** . Das Fenster *Benutzer-ID hinzufügen* öffnet sich.
3. Geben Sie einen Namen für die Benutzer-ID ein. Geben Sie die E-Mail Adresse ein, für die Sie diesen Schlüssel verwenden wollen.

   Geben Sie Ihr Passwort für diesen Schlüssel ein.

   Klicken Sie auf **OK**.

So laden Sie den öffentlichen Schlüssel eines externen Partners hoch:

1. Öffnen Sie in den Einstellungen die Seite zur Verwaltung der Schlüssel.
2. Klicken Sie unterhalb von *Öffentliche Schlüssel* neben *Liste der öffentlichen PGP-Schlüssel* auf das Symbol **Hinzufügen** . Wählen Sie eine Datei, die einen öffentlichen Schlüssel enthält.

Stichwortverzeichnis