Servizio Acronis Notary

24.03

Manuale dell'amministratore

REVISIONE: 11/04/2024

Sommario

Informazioni sul servizio di autenticazione Acronis Notary **3**
Funzionamento dell’autenticazione 3
Ruoli utente 3
Limitazioni 4
Browser Web supportati 4
Utilizzo del servizio di autenticazione **5**
Attivazione dell'account 5
Accesso all’interfaccia Web del servizio di autenticazione 5
Utilizzo del servizio di autenticazione come utente dell'autenticazione 5
Autenticazione dei file 5
Verifica dell'autenticità dei file 8
Firma di file 9
Modelli di documento 13
Utilizzo del servizio di autenticazione come amministratore dell'autenticazione 17
Gestione del servizio di autenticazione **19**
Gestione delle chiavi API 19
Amministrare gli account utente e le quote 20
Quote 20
Notifiche 21
Report utilizzo 21
Indice **22**

Informazioni sul servizio di autenticazione Acronis Notary

Il servizio di autenticazione Acronis Notary è una soluzione completa basata su blockchain che consente di eseguire le seguenti operazioni:

- Autenticare un file.
- Controllare se un file autenticato (o una sua copia) è autentica e non ha subito modifiche dal momento in cui è stato autenticato.
- Inviare un file a più persone per apporvi la firma elettronica e quindi autenticare il certificato di firma.

Il servizio è disponibile mediante un'interfaccia Web denominata console di autenticazione.

Funzionamento dell'autenticazione

Per autenticare un file, è necessario caricarlo nell'archivio cloud. Dopo aver caricato il file, il servizio di autenticazione elabora un'impronta digitale, nota come codice hash, di tale file. Viene elaborato un codice hash univoco per ogni file.

Nota
L'API del servizio di autenticazione consente di autenticare un file senza caricarlo nell'archivio cloud. È invece possibile usare l'hash pregenerato del file. Per ulteriori informazioni sull'uso delle API, fare riferimento a "Gestione delle chiavi API".

Il servizio di autenticazione invia il codice hash al database Ethereum, basato su blockchain. Il database garantisce che il codice hash non subisca modifiche.

Per verificare l'autenticità del file, il servizio elabora il codice hash del file e quindi lo confronta al codice hash archiviato nel database. La corrispondenza dei codici garantisce che il file sia ancora lo stesso e non sia stato modificato.

Ruoli utente

Nel servizio di autenticazione esistono due ruoli: ruolo di amministratore dell'autenticazione e ruolo di utente dell'autenticazione.

Sia gli amministratori che gli utenti possono accedere a tutte le funzionalità del servizio dalla console di autenticazione.

Tutti gli utenti possono accedere solo ai propri modelli e file autenticati e firmati.

Gli amministratori dispongono di diritti superiori per visualizzare e lavorare con i modelli e i file autenticati e firmati che appartengono agli altri utenti o amministratori del tenant cliente. Amministratori e utenti possono gestire le chiavi API del servizio di autenticazione e utilizzare l'API di autenticazione. Gli amministratori e gli utenti possono accedere solo alle proprie chiavi API.

Inoltre, a un amministratore del servizio di autenticazione può essere assegnato il ruolo di amministratore dell'azienda. Questo ruolo gli garantisce l'accesso al portale di gestione, dove l'amministratore può gestire gli account utente, le quote, le notifiche e i report.

Limitazioni

- Non è possibile autenticare tramite la console di autenticazione i file di dimensioni maggiori di 1 GB. Tali file possono essere autenticati solo tramite l'API del servizio di autenticazione, inviando al servizio l'hash pre-calcolato del file.
- Non è possibile firmare tramite la console di autenticazione i file di dimensioni maggiori di 1 GB. Tali file possono essere firmati solo tramite l'API del servizio di autenticazione, inviando al servizio il collegamento al file.

Browser Web supportati

L'interfaccia Web supporta i seguenti browser:

- Google Chrome 29 o versione successiva
- Mozilla Firefox 23 o versione successiva
- Opera 16 o versione successiva
- Microsoft Edge 25 o versioni successive
- Safari 8 o versioni successive in esecuzione nei sistemi operativi macOS e iOS

In altri browser Web (inclusi browser Safari eseguiti in altri sistemi operativi), l'interfaccia utente potrebbe essere visualizzata in modo non corretto o alcune funzioni potrebbero non essere disponibili.

Utilizzo del servizio di autenticazione

Attivazione dell'account

Dopo aver eseguito l’accesso al servizio, l'utente riceverà un messaggio e-mail contenente le seguenti informazioni:

- **Un collegamento di attivazione dell'account**. Fare clic sul collegamento e impostare la password per l'account. Ricordare il login mostrato nella pagina di attivazione dell'account.
- **Un collegamento alla pagina di accesso della console di autenticazione.** Utilizzare questo collegamento per i futuri accessi alla console. Login e password sono gli stessi del passaggio precedente.

Accesso all’interfaccia Web del servizio di autenticazione

È possibile accedere al servizio di autenticazione se l’account è stato attivato.

Per accedere al servizio di autenticazione

1. Passare alla pagina di accesso al servizio. L'indirizzo della pagina di accesso era incluso nel messaggio e-mail di attivazione.
2. Digitare il login e quindi fare clic su **Continua**.
3. Digitare la password e quindi fare clic su **Accedi**.
4. Se si dispone del ruolo di amministratore dell’azienda, fare clic su **Notary**.
   Gli utenti che non hanno il ruolo di amministratore dell’azienda possono accedere direttamente alla console di autenticazione.

È possibile cambiare la lingua dell'interfaccia web facendo clic sull'icona dell’account nell'angolo in alto a destra.

Se **Notary** non è l'unico servizio che si è sottoscritto, è possibile passare da un servizio all'altro usando l'icona  nell'angolo in alto a destra. Gli amministratori dell’azienda possono usare questa icona anche per passare al portale di gestione.

Utilizzo del servizio di autenticazione come utente dell'autenticazione

Gli utenti del servizio di autenticazione possono accedere solo ai propri modelli e file autenticati e firmati.

Autenticazione dei file

Per autenticare un file

1. Fare clic su **File autenticati**.
2. Se non sono presenti file autenticati, fare clic su **Sfoglia**. In alternativa, fare clic su **Aggiungi file**, quindi su **Sfoglia**.
3. Selezionare i file da autenticare.

   Dopo aver selezionato un file, il software ne avvia il caricamento nell'archivio cloud.
4. Dopo aver caricato tutti i file, fare clic su **Autentica**.

   Il software elabora un codice hash per ogni file. Gli stati dei file cambiano in **In corso**. L'utilizzo della quota di **Autenticazioni** viene aumentata del numero di file aggiunti.
5. Attendere fino a quando ogni stato del file cambia da **In corso** ad **Autenticato**.

   Il processo di autenticazione può richiedere fino a 70 minuti. Per ridurre il costo di ogni autenticazione, il servizio raccoglie gli hash nel corso di un'ora, quindi crea un albero hash basato sugli hash raccolti e invia la root dell'albero hash al registro della blockchain. A questo punto, il servizio attende che la transazione venga confermata nel registro della blockchain e quindi modifica gli stati dei file in **Autenticato**. Quando lo stato del file passa a **Autenticato**, l'utente riceve una notifica tramite e-mail.

   Nota
   Se un file non risulta ancora autenticato 24 ore dopo essere stato caricato, lo stato passa da **In corso** a **Autenticazione in sospeso**, e l'utente riceve una notifica tramite e-mail.

Certificato di autenticazione

Dopo aver completato l'autenticazione, il servizio crea un certificato di autenticazione per ogni file. Tale certificato comprova in modo irrefutabile che il file è stato autenticato a un orario specifico. Il certificato contiene:

- Informazioni sull'autenticazione (nome del file, hash, dimensione, indicatore data e ora dell'autenticazione, richiedente, GUID del richiedente, firmatario, ID della transazione blockchain e ID del certificato).
- Istruzioni su come verificare il file manualmente, senza utilizzare il servizio di autenticazione.

Nota
Tenere presente che i dati personali, come l'e-mail e l'indirizzo IP, saranno conservati nell'audit trail e saranno accessibili a tutti i firmatari.

Operazioni con i file autenticati

Per scaricare un file dall'archivio cloud

1. Fare clic su **File autenticati**.
2. Individuare il file nell'elenco.

   È possibile filtrare i file per stato, ordinarli per nome, stato, date di autenticazione e caricamento, oppure usare la funzione di ricerca.
3. Fare clic su  oppure fare clic sul nome del file, quindi su **Scarica**.

Per visualizzare il certificato di autenticazione di un file

1. Fare clic su **File autenticati**.
2. Individuare il file nell'elenco. I certificati di autenticazione sono disponibili solo per i file con lo stato **Autenticato**.
   È possibile filtrare i file per stato, ordinarli per nome, stato, date di autenticazione e caricamento, oppure usare la funzione di ricerca.
3. Fare clic sul nome file.
4. Fare clic su **Visualizza e scarica certificato di autenticazione** per visualizzare il certificato in una nuova scheda.

> **Nota**
> È possibile copiare i valori di **Hash del file (SHA-256)**, **ID certificato** o **RICEVUTA BLOCKCHAIN** del file di autenticazione facendo clic sull'icona **Copia negli appunti** corrispondente.

Per scaricare il certificato di autenticazione di un file

1. Fare clic su **File autenticati**.
2. Individuare il file nell'elenco. I certificati di autenticazione sono disponibili solo per i file con lo stato **Autenticato**.
   È possibile filtrare i file per stato, ordinarli per nome, stato, date di autenticazione e caricamento, oppure usare la funzione di ricerca.
3. Fare clic sul nome file.
4. Fare clic su **Visualizza e scarica certificato di autenticazione** per visualizzare il certificato in una nuova scheda.
5. Nella nuova scheda, fare clic su **Scarica certificato di autenticazione**.

Per eliminare un file dall'archivio cloud

1. Fare clic su **File autenticati**.
2. Individuare il file nell'elenco.
   È possibile filtrare i file per stato, ordinarli per nome, stato, date di autenticazione e caricamento, oppure usare la funzione di ricerca.
3. Fare clic su  oppure fare clic sul nome del file, quindi su **Elimina**.
   Se il file è stato autenticato, resterà autenticato. È consigliabile salvare il certificato di autenticazione o salvare il collegamento diretto a questo prima di confermare l'eliminazione.

> **Importante**
> Se l'autenticazione è in corso, non è possibile annullarla. Non ci sarà modo tuttavia di visualizzare o scaricare il certificato di autenticazione del file.

4. Fare di nuovo clic su **Elimina** per confermare la decisione.

Verifica dell'autenticità dei file

È possibile verificare l'autenticità caricando il file nell'archivio cloud o usando la ricevuta blockchain del certificato di autenticazione del file.

I file che vengono caricati per la verifica non utilizzano la quota dell'**Archivio Notary**. Dopo aver completato il processo di verifica, i file vengono eliminati dall'archivio cloud.

Per verificare l'autenticità del file caricandolo nell'archivio cloud

1. Accedere al certificato di autenticazione come descritto nella procedura Per visualizzare il certificato di autenticazione di un file.
2. Trovare l'ID del certificato e copiarlo.
3. Nella console di autenticazione, fare clic su **Verifica**.
4. Fare clic su **Sfoglia**, quindi selezionare il file di cui si desidera verificare l'autenticità. È possibile selezionare più file.
   Dopo aver selezionato un file, il software ne avvia il caricamento nell'archivio cloud.
5. Specificare l'ID del certificato del file per confermare di essere autorizzati alla verifica del file.
6. Fare clic su **Verifica**.
7. Il software visualizza i rapporti di verifica dei file selezionati.
   - Se il file è autentico, lo stato viene impostato su **Autenticato**.
   - Se il file non è autentico o non è mai stato autenticato, lo stato viene impostato su **Non autenticato**.
   - Se l'autenticazione del file è ancora in corso, lo stato viene impostato su **In corso**.

Per verificare un file usando una ricevuta blockchain

1. Accedere al certificato di autenticazione come descritto nella procedura Per visualizzare il certificato di autenticazione di un file.
2. Individuare la sezione **Ricevuta blockchain** e copiare i contenuti indicati di seguito, incluse le parentesi:

   ```
   {
    "key": "filename.pdf",
    "eTag": "52bf7a18744b384afba39f3646d8e245...",
    "size": 1267387,
    "sequencer": "B56C3FE5ED984F5337"
   }
   ```

   Queste stringhe includono nome file, hash SHA-256, dimensioni in byte e numero della transazione blockchain.
3. Nella console di autenticazione, fare clic su **Verifica**.
4. Fare clic su **Verifica utilizzando la ricevuta blockchain**.
5. Incollare i contenuti copiati nella sezione **Ricevuta blockchain** nel campo vuoto.

6. Fare clic su **Verifica**.
7. Il software visualizza i rapporti di verifica.
   - Se il file è autentico, lo stato viene impostato su **Autenticato**.
   - Se il file non è autentico o non è mai stato autenticato, lo stato viene impostato su **Non autenticato**.
   - Se l'autenticazione del file è ancora in corso, lo stato viene impostato su **In corso**.

Per verificare un file usando un hash del file

1. Accedere al certificato di autenticazione come descritto nella procedura Per visualizzare il certificato di autenticazione di un file.
2. Trovare l'hash del file e l'ID del certificato e copiarli.
3. Nella console di autenticazione, fare clic su **Verifica**.
4. Fare clic su **Verifica utilizzando l'hash del file**.
5. Specificare l'hash del file.
6. Specificare l'ID del certificato del file per confermare di essere autorizzati alla verifica del file.
7. Fare clic su **Verifica**.
8. Il software visualizza i rapporti di verifica.
   - Se il file è autentico, lo stato viene impostato su **Autenticato**.
   - Se il file non è autentico o non è mai stato autenticato, lo stato viene impostato su **Non autenticato**.
   - Se l'autenticazione del file è ancora in corso, lo stato viene impostato su **In corso**.

Pagina di verifica pubblica

Esiste anche una pagina di verifica pubblica, dove un utente non autorizzato può verificare l'autenticità di un file con una delle tre modalità seguenti:

- caricando il file stesso e l'ID del certificato;
- specificando un hash del file e l'ID del certificato;
- fornendo una ricevuta blockchain e l'ID del certificato.

Firma di file

Il servizio di autenticazione consente di inviare un file a più persone per apporvi la firma elettronica, o per firmarlo elettronicamente come unico firmatario.

Per firmare un file, è necessario caricarlo nel cloud storage o crearlo da un modello.

Per i file che possono essere convertiti in formato di file .pdf, la firma a mano, quella convertita in testo o le iniziali del firmatario possono essere incorporate come immagini nel documento firmato. In questo caso, il contenuto del file firmato viene salvato con le firme elettroniche incorporate nel file .pdf del certificato e il file viene quindi autenticato utilizzando il servizio di autenticazione.

Questa funzionalità è supportata per i seguenti formati di file: .txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx e .pdf.

È possibile utilizzare le eSignature per firmare elettronicamente i tipi di documenti seguenti:

- Contratti di affitto o locazione
- Contratti di vendita
- Contratti di acquisto di beni
- Contratti di erogazione di prestito
- Fogli di autorizzazione
- Documenti finanziari
- Documenti assicurativi
- Esclusioni di responsabilità
- Documenti sanitari
- Documenti di ricerca
- Certificati di autenticità dei prodotti
- Contratti di non divulgazione
- Lettere di proposta
- Contratti di riservatezza
- Contratti con terzisti indipendenti

Per i file che non possono essere convertiti in formato .pdf, dopo aver firmato il file, il servizio di autenticazione genera un certificato di firma che contiene le firme acquisite per il file. Il certificato viene quindi autenticato usando il servizio di autenticazione. I file firmati non vengono autenticati.

Firma di un file come unico firmatario

È possibile caricare un file e apporre la firma elettronica come unico firmatario.

Per caricare un file e apporre la firma elettronica come unico firmatario

1. Fare clic su **File firmati**.
2. [Facoltativo] Per aggiungere un nuovo file da firmare, fare clic su **Sfoglia**, oppure su **Aggiungi file**, quindi su **Sfoglia**.
3. Selezionare il file da firmare.
   Dopo aver selezionato un file, il software ne avvia il caricamento nell'archivio cloud.
4. Nella finestra di dialogo **Aggiungi firmatari**, selezionare **Sono l'unico firmatario**, quindi fare clic su **Avanti**.
5. Nel campo **Aggiungi campi al documento** trascinare i campi da aggiungere al documento.
6. Fare clic su **Visualizza in anteprima e invia**.
7. Visualizzare l'anteprima del documento, quindi fare clic su **Invia**.

Il documento appare nell'elenco dei file firmati con lo stato **In attesa dell'utente**.

8. Nella scheda **File**, fare clic sul documento e quindi su **Firma**.
9. Nella finestra di dialogo **Inserire il proprio nome, le iniziali e la firma elettronica**, selezionare il metodo per firmare il file.
   - **Firma elettronica e iniziali suggerite** – la firma elettronica e le iniziali vengono generate automaticamente. È possibile modificarle manualmente, se necessario.
   - **Firma elettronica e iniziali scritte a mano** – trascinare la firma e le iniziali nei campi corrispondenti; verranno così incluse come immagini nel documento firmato.

   Nota
   Questa opzione è supportata per i seguenti formati di file: .txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx e .pdf.
10. Selezionare la casella di controllo **Confermo di aver letto e accettato** e fare clic su **Avanti**.
11. Nella finestra di dialogo **Firma documento**, fare clic nel campo **Firma elettronica** per completarlo con la firma elettronica personale.
12. Fare clic su **Visualizza in anteprima e firma**.
13. Visualizzare l'anteprima del documento, quindi fare clic su **Firma**.
    Il file firmato viene salvato come formato di file .pdf.
14. Una volta completato il processo, selezionare il file firmato e fare clic sulla scheda **Certificato di firma elettronica** e quindi su **Certificato di firma elettronica** per scaricare un documento in formato PDF contenente:
    - La sezione del certificato di firma elettronica che raccoglie tutte le firme.
    - La sezione **Audit Trail** con la cronologia delle attività: data e ora in cui l'invito è stato spedito ai firmatari, data e ora in cui ciascun firmatario ha firmato il file e così via.
15. Fare clic su **Visualizza e scarica certificato di autenticazione** e quindi su **Visualizza e scarica certificato di autenticazione** per scaricare il certificato di autenticazione del certificato di firma elettronica. Il certificato di autenticazione diventa disponibile entro 70 minuti dal completamento delle procedure di firma.

Invio di un file alla firma per più firmatari

È possibile caricare un file e inviarlo a più firmatari per apporre la firma elettronica.

Per inviare un file alla firma per più firmatari

1. Fare clic su **File firmati**.
2. Se non sono presenti file firmati, fare clic su **Sfoglia**. In alternativa, fare clic su **Aggiungi file**, quindi su **Sfoglia**.
3. Selezionare il file da firmare.
   Dopo aver selezionato un file, il software ne avvia il caricamento nell'archivio cloud.

4. Nella finestra di dialogo **Aggiungi firmatari** fare clic su **Aggiungi firmatari** e quindi digitare l'indirizzo e-mail dei firmatari. Ripetere il passaggio per ogni firmatario che si desidera aggiungere.

   Importante
   Non è possibile aggiungere o rimuovere i firmatari dopo aver inviato gli inviti. Per rimuovere un firmatario, fare clic sull'icona del cestino. Assicurarsi quindi che l'elenco includa tutti coloro la cui firma è richiesta prima di passare alla fase successiva.

5. Fare clic su **Avanti**.
6. Nella finestra di dialogo **Aggiungi campi al documento**, aggiungere i firmatari e i campi personalizzati necessari.
7. Fare clic su **Visualizza in anteprima e invia**.
8. Visualizzare l'anteprima del documento, quindi fare clic su **Invia** per inviare gli inviti ai firmatari. Ciascun firmatario riceve un'e-mail con la richiesta di firma. Si riceve una notifica per ogni firma apposta dai vari firmatari del file e al completamento dell'intero processo.
9. Una volta completato il processo, selezionare il file firmato e quindi fare clic sulla scheda **Certificato di firma elettronica** e quindi su **Certificato di firma elettronica** per scaricare un documento in formato PDF contenente:
   - La sezione del certificato di firma elettronica che raccoglie tutte le firme.
   - La sezione **Audit Trail** con la cronologia delle attività: data e ora in cui l'invito è stato spedito ai firmatari, data e ora in cui ciascun firmatario ha firmato il file e così via.

Dopo aver completato il processo, ogni firmatario riceve una notifica che contiene:

- Un collegamento al file firmato.
- Un collegamento al certificato di firma elettronica.
- Un collegamento al certificato di autenticazione del certificato di firma elettronica. Il certificato di autenticazione diventa disponibile entro 70 minuti dal completamento delle procedure di firma.

Operazioni con file firmati

Per scaricare un file firmato dall'archivio cloud

1. Fare clic su **File firmati**.
2. Individuare nell'elenco il file necessario.
   È possibile filtrare i file per stato, ordinarli per nome, stato, date di autenticazione e caricamento, oppure usare la funzione di ricerca.
3. Fare clic su  oppure fare clic sul nome del file, quindi su **Scarica**.

Per eliminare un file firmato dall'archivio cloud

1. Quando si elimina un file firmato dall'archivio cloud, viene eliminato anche il corrispondente certificato di firma elettronica. Se si ritiene che il certificato di firma elettronica possa essere

necessario in futuro, verificare di averne salvato una copia locale come descritto nel passaggio 6 della procedura "Per firmare un file".

Il certificato di firma resta non autenticato.

2. Fare clic su **File firmati**.
3. Individuare nell'elenco il file necessario.
   È possibile filtrare i file per stato, ordinarli per nome, stato, date di autenticazione e caricamento, oppure usare la funzione di ricerca.
4. Fare clic su  oppure fare clic sul nome del file, quindi su **Elimina**.
5. Confermare la propria decisione.
   È consigliabile scaricare il certificato di autenticazione del certificato di firma elettronica o salvare il collegamento diretto a questo prima di confermare l'eliminazione.

Modelli di documento

È possibile creare modelli di documento e utilizzarli per generare con facilità nuovi file per la firma elettronica.

Il modello di documento costituisce un progetto di base per transazioni ripetibili. Con i modelli di documento è possibile creare il contenuto del documento, inclusa una serie di campi obbligatori o facoltativi, e assegnare successivamente i firmatari corretti. Destinatari e firmatari possono essere modificati ogni volta che si utilizza un modello di documento per creare un nuovo file.

Per creare un modello di documento:

1. caricare un file in formato PDF o in un formato che sia possibile convertire in formato PDF: TXT, DOC, DOCX, XLS, XLSX, PPT, PPTX e PDF.
2. aggiungere almeno un campo Firmatario al modello
3. aggiungere campi per ogni firmatario aggiuntivo, se necessario
4. aggiungere campi personalizzati, se necessario
5. salvare il modello

Nota
È possibile salvare un modello di documento solo se include almeno un campo Firmatario.

Campi del modello di documento

Il processo di creazione di un modello di documento consiste nel caricare un file che contiene le informazioni principali, al quale vengono quindi aggiunti campi predefiniti o personalizzati.

Esistono due tipi di campi del modello di documento: Campi **Firmatario** e campi **Personalizzati**.

I campi Firmatario sono campi rigidamente predefiniti nei quali inserire le informazioni sul firmatario. È possibile aggiungere e rimuovere tali campi da un modello e configurarli in modo che siano obbligatori o facoltativi, ma non è possibile modificarne il nome.

Nome del campo Firmatario	Descrizione
Nome	Nome del firmatario del documento.
Firma	Firma del firmatario del file. Il campo è obbligatorio per impostazione predefinita. Per renderlo facoltativo, selezionare la casella di controllo **Opzionale**.
Iniziali	Iniziali del firmatario del file. Il campo è obbligatorio per impostazione predefinita. Per renderlo facoltativo, selezionare la casella di controllo **Opzionale**.

I campo personalizzati sono campi di testo libero che è possibile aggiungere al modello, in base alle necessità. È possibile definire il nome del campo personalizzato (ad esempio **Data** o **Indirizzo di fatturazione**) al momento della creazione del modello, e compilarne il contenuto quando si crea un nuovo file dal modello.

Nota
Il contenuto dei campi personalizzati viene visualizzato sempre con lo stesso carattere e dimensione.

Creazione di un modello di documento

È possibile creare un modello e utilizzarlo per generare con facilità nuovi file per la firma elettronica.

Per creare un modello di documento

1. Fare clic su **File firmati**>**Modelli**.
2. Fare clic su **Crea modello**.
3. Nella finestra **Caricare i documenti per il modello**, utilizzare una delle seguenti opzioni per caricare il file:
   - trascinare e rilasciare il file;
   - fare clic su **Sfoglia**, individuare il file e selezionarlo.
4. **Importante**
   Il modello deve essere in formato di file PDF, TXT, DOC, DOCX, XLS, XLSX, PPT o PPTX.
5. Nella scheda **Firmatari**, fare clic su almeno uno dei campi predefiniti per il **Firmatario 1**.

   Nota
   Dopo aver fatto clic su un campo, questo verrà visualizzato nel modello. Sarà possibile selezionarlo e trascinarlo per modificarne la posizione nel modello. È anche possibile trascinare i bordi corrispondenti del campo per modificarne la dimensione.

6. [Facoltativo] Per ogni firmatario che si desidera aggiungere:
   a. Fare clic su **Aggiungi firmatario**.
   b. Aggiungere almeno uno dei campi Firmatario al modello.
7. [Facoltativo] Per aggiungere un campo personalizzato, nella scheda **Campi personalizzati**:
   a. Fare clic sull'icona a forma di matita accanto all'etichetta Campo personalizzato.
   b. Nella finestra **Rinomina campo personalizzato**, digitare un nome per il campo personalizzato. La lunghezza massima consentita del nome è di 30 caratteri.
   c. Fare clic sul campo per aggiungerlo al modello di documento e utilizzare il mouse per spostarlo nella posizione appropriata.
8. [Facoltativo] Per ogni campo personalizzato che si desidera aggiungere:
   a. Fare clic su **Aggiungi campo personalizzato**.
   b. Fare clic sull'icona a forma di matita accanto all'etichetta Campo personalizzato.
   c. Nella finestra **Rinomina campo personalizzato**, digitare un nome per il campo personalizzato. La lunghezza massima consentita del nome è di 30 caratteri.
   d. Fare clic sul campo per aggiungerlo al modello di documento e utilizzare il mouse per spostarlo nella posizione appropriata.
9. Fare clic su **Visualizza in anteprima e crea**.
10. Se le informazioni nel modello sono corrette, fare clic su **Crea**.
    Il nuovo modello è ora visibile nella pagina **Modelli**. Per ulteriori informazioni sulle azioni che è possibile eseguire nella pagina **Modelli**, vedere "Gestione di modelli di documento" (pag. 15).

Gestione di modelli di documento

Una volta creato, il modello viene elencato nella pagina **Modelli**. Nella pagina **Modelli** è possibile visualizzare ulteriori informazioni sui modelli esistenti ed eseguire le azioni seguenti:

- Visualizzare l'anteprima di un modello di documento
- Creare un file da un modello di documento
- Rinominare un modello di documento
- Eliminare un modello di documento

La tabella seguente descrive le informazioni disponibili nella pagina **Modelli**.

Nome colonna	Descrizione
Nome modello	Il nome del modello.
Documenti caricato	Il nome del file per il quale è stato creato il modello.
Documenti creati	Il numero di file creati utilizzando questo modello.
Creazione	Data e ora in cui è stato caricato il modello.
ID	Numero ID di sistema del modello; viene generato automaticamente.

Anteprima di un modello di documento

Per visualizzare l'anteprima di un modello di documento

1. In **File firmati** > **Modelli**, individuare il modello di documento di cui visualizzare l'anteprima.
2. Fare clic su  , quindi su **Anteprima**.
3. Dopo aver completato la visualizzazione dell'anteprima, fare clic su **Fine**.

Ridenominazione di un modello di documento

Per rinominare un modello di documento

1. In **File firmati** > **Modelli**, individuare il modello di documento da rinominare.
2. Fare clic su  , quindi su **Rinomina**.
3. Nel campo **Nome modello**, aggiornare il nome del modello.
4. Fare clic su **Rinomina**.

Eliminazione di un modello di documento

Per eliminare un modello di documento

1. In **File firmati** > **Modelli**, individuare il modello di documento da eliminare.
2. Fare clic su  , quindi su **Elimina**.

Creazione di un documento da un modello

È possibile creare con facilità un nuovo documento da un modello di documento esistente, e inviarlo per essere firmato elettronicamente.

Per creare documento da un modello di documento

1. Fare clic su **File firmati**>**Modelli**.
2. Nell'elenco dei modelli di documento, individuare il modello di documento da utilizzare.
3. Fare clic su  , quindi su **Crea documento**.
4. Nella finestra **Crea documento dal modello**, nel campo **Nome documento** digitare il nome del file.
5. Digitare gli indirizzi e-mail dei firmatari del documento.

> **Nota**
> L'indirizzo e-mail immesso verrà utilizzato per inviare un'e-mail a tutti i firmatari del file. Questo messaggio e-mail contiene un collegamento che i firmatari possono utilizzare per visualizzare e apporre la firma elettronica sul file.

6. Se il modello contiene campi personalizzati, fare clic su **Avanti**. Altrimenti, andare al passaggio 8.
7. Inserire le informazioni richieste nei campi personalizzati.

Nota
La lunghezza dei campi personalizzati è limitata a 250 simboli.

8. Fare clic su **Visualizza in anteprima e crea**.
9. Se le informazioni nel file sono corrette, fare clic su **Crea**.

Nota
Il file viene creato, e diventa visibile in **File firmati**->**File**. Il nome del modello utilizzato per creare il documento è visibile nella colonna **Nome modello**.
Un'e-mail che contiene un collegamento per visualizzare e apporre la firma elettronica sul file viene inviato a tutti i firmatari del documento. Ogni firmatario del documento potrà apporre la propria firma seguendo la procedura "Firma di un file creato da un modello" (pag. 17).

Firma di un file creato da un modello

Dopo aver creato un file da un modello, tutti i firmatari del file ricevono un'e-mail con un collegamento da utilizzare per apporre la firma elettronica sul file.

Per apporre la firma elettronica su un file creato da un modello

1. Nella casella di posta, individuare la notifica e-mail inviata dal mittente notaryacronissg@gmail.com, e aprirla.
2. Fare clic su **Rivedere e firmare**.
3. Nella finestra **Inserire il proprio nome, le iniziali e la firma**, immettere le informazioni richieste e la firma elettronica.
4. Selezionare la casella **Confermo di aver letto e accettato**.
5. Fare clic su **Fine**.
6. Nella finestra **Firma documento**, fare clic sui campi pertinenti per immettere i dati del passaggio 3.
7. Fare clic su **Visualizza in anteprima e firma**.
8. Dopo aver visualizzato l'anteprima del file, fare clic su **Firma**.

Il file firmato viene salvato in formato di file PDF. Vengono creati un Certificato di firma e un Certificato di autenticazione del certificato di firma. Il certificato di autenticazione diventa disponibile entro 70 minuti dal completamento delle procedure di firma. È possibile scaricare il file e i certificati.

Utilizzo del servizio di autenticazione come amministratore dell'autenticazione

Quando lavora con modelli, file autenticati e con firma elettronica di sua proprietà, l'amministratore dell'autenticazione può eseguire le stesse funzioni di un utente dell'autenticazione. Per ulteriori

informazioni, consultare "Utilizzo del servizio di autenticazione come utente dell'autenticazione" (pag. 5).

In aggiunta, l'amministratore dell'autenticazione può eseguire diverse funzioni che non sono disponibili all'utente dell'autenticazione:

- Visualizzare i modelli, i file autenticati e con firma elettronica creati da altri utenti o amministratori nel tenant cliente.
- Visualizzare il proprietario di tutti i modelli, dei file autenticati e con firma elettronica nel tenant cliente. Il proprietario è visualizzato nella colonna **Proprietario** della console del servizio di autenticazione, nelle schede **File autenticati**, **File firmati** e **Modelli**.
- Visualizzare il progresso delle procedure di firma di tutti i documenti creati da altri utenti o amministratori del tenant cliente.

  Nota
  L'amministratore non può firmare documenti per conto di altri utenti. L'amministratore può firmare solo documenti ai quali è stato aggiunto come firmatario.

- Rinviare gli inviti ai firmatari di un documento che è stato creato da un altro utente o amministratore del tenant cliente.
- Scaricare i modelli originali, i file autenticati e con firma elettronica creati da altri utenti o amministratori nel tenant cliente.
- Scaricare i file firmati (se il processo di firma del documento mediante firma elettronica è stato completato) creati da altri utenti o amministratori del tenant cliente.
- Scaricare i file di certificato della firma (se il processo di firma del documento mediante firma elettronica è stato completato) dei file con firma elettronica creati da altri utenti o amministratori del tenant cliente.
- Eliminare i modelli e i file autenticati e firmati creati da altri utenti o amministratori del tenant cliente. Ai proprietari dei modelli o dei file eliminati viene inviata una notifica e-mail.
- Creare nuovi documenti dai modelli di documento creati da altri utenti o amministratori del tenant cliente. Ai proprietari dei modelli di documento viene inviata una notifica e-mail.

Gestione del servizio di autenticazione

Questa sezione descrive le funzionalità che sono disponibili solo agli amministratori del servizio di autenticazione.

Gestione delle chiavi API

È possibile integrare il servizio di autenticazione in sistemi di terze parti usando l'interfaccia API del servizio stesso. Per ulteriori informazioni sull'uso dell'API, fare riferimento alla guida dello sviluppatore all'indirizzo https://developer.acronis.com/doc/notary/v2/guide/.

Un amministratore del servizio di autenticazione può creare e gestire le chiavi API per le integrazioni.

Per creare una chiave API

1. Fare clic su **Chiavi API** > **Crea chiave API**.
2. Creare e immettere un nome univoco per la chiave API.
3. Fare clic su **Crea**.
4. Al momento della creazione, per la chiave API è impostato lo stato predefinito **Abilitata**.

> **Importante**
> Copiare e salvare la chiave. Per ragioni di sicurezza, la chiave è visualizzata solo una volta. Non è possibile recuperare la chiave in caso di perdita.

Per disabilitare una chiave API

1. Fare clic su **Chiavi API**.
2. Individuare nell'elenco la chiave necessaria.
   È possibile filtrare le chiavi per stato e ordinarle per nome, stato e data di creazione.
3. Fare clic su  , quindi su **Disabilita**.
4. Confermare la propria decisione.
   Tutte le integrazioni che utilizzano questa chiave verranno arrestate. Sarà possibile riabilitare la chiave in qualsiasi momento.

Per abilitare una chiave API disabilitata

1. Fare clic su **Chiavi API**.
2. Individuare nell'elenco la chiave necessaria.
   È possibile filtrare le chiavi per stato e ordinarle per nome, stato e data di creazione.
3. Fare clic su  , quindi su **Abilita**.

Per eliminare una chiave API

1. Fare clic su **Chiavi API**.
2. Individuare nell'elenco la chiave necessaria.
   È possibile filtrare le chiavi per stato e ordinarle per nome, stato e data di creazione.
3. Fare clic su  , quindi su **Elimina**.
4. Confermare la propria decisione.
   Tutte le integrazioni che utilizzano questa chiave verranno arrestate. Non è possibile recuperare una chiave API eliminata.

Amministrare gli account utente e le quote

Nel portale di gestione sono disponibili funzioni per amministrare gli account utente e le quote di utilizzo del servizio. Per accedere al portale di gestione, fare clic su **Portale di gestione** al momento dell'accesso al servizio di autenticazione, oppure fare clic sull'icona  nell'angolo in alto a destra e quindi fare clic su **Portale di gestione**. L'accesso al portale è consentito solo agli utenti ai quali è stato assegnato il ruolo di amministratore dell'azienda.

Per informazioni su come amministrare gli account utente e le relative quote, fare riferimento al Manuale dell'amministratore del portale di gestione. Per accedere al documento fare clic sull'icona del punto interrogativo nel portale di gestione.

Questa sezione offre ulteriori informazioni sulla gestione del servizio di autenticazione.

Quote

Le quote consentono di limitare la capacità degli utenti di utilizzare il servizio. Per impostare le quote, selezionare l'utente nella scheda **Utenti**, quindi fare clic sull'icona a forma di matita nella sezione **Quote**.

Quando la quota viene superata, viene inviata una notifica all'indirizzo e-mail dell'utente. Se non viene impostata un'eccedenza di quota, la quota viene considerata "flessibile". Ciò significa che non vengono applicati limiti relativi all'utilizzo del servizio.

È possibile specificare eccedenze di quota. Il surplus della quota consente all'utente di superare la quota del valore specificato. Quando si supera l'eccedenza, vengono applicati i limiti relativi all'uso del servizio di autenticazione.

In modo simile, i provider dei servizi gestiti possono anche specificare le quote per le aziende dei propri clienti.

Sono disponibili le quote seguenti:

- **Archivio Notary**
  L'Archivio Notary è l'archivio cloud del servizio di autenticazione nel quale vengono memorizzati i file autenticati, i file firmati e i file di cui è in corso il processo di autenticazione o di firma. Questa quota definisce lo spazio massimo che può essere occupato dai file in questione.

Per diminuire l’utilizzo della quota, è possibile eliminare i file già autenticati o firmati dall’archivio.

- **Autenticazioni**
  Questa quota definisce il numero massimo di file autenticabili tramite il servizio di autenticazione. Un file viene considerato autenticato non appena viene caricato nell’archivio di autenticazione e il relativo stato di autenticazione cambia in In corso.
  Se lo stesso file viene autenticato più volte, ogni autenticazione vale come una nuova.
- **eSignature**
  Questa quota definisce il numero massimo di file che possono essere firmati tramite il servizio di autenticazione. Un file viene considerato firmato non appena viene inviato alla firma.
- **Modelli di documento**
  Questa quota definisce il numero massimo di modelli di documento che il cliente può salvare.

Notifiche

Per modificare le impostazioni di notifica per un utente, selezionare l'utente nella scheda **Utenti**, quindi fare clic sull'icona a forma di matita nella sezione **Impostazioni**. Sono disponibili le seguenti impostazioni di notifica:

- **Notifiche relative al superamento delle quote** (abilitata per impostazione predefinita)
  Notifiche relative al superamento delle quote.
- **Report di utilizzo pianificati**
  I report di utilizzo descritti più avanti che vengono inviati il primo giorno di ogni mese.

Tutte le notifiche vengono inviate all’indirizzo e-mail dell'utente.

Report utilizzo

Il report sull'utilizzo del servizio di autenticazione contiene i seguenti dati relativi all'azienda o a un'unità:

- Dimensione dei file archiviati nell’archivio di autenticazione (ad eccezione dei file in corso di verifica) per unità, per utente.
- Numero di autenticazioni per unità, per utente.
- Numero di file firmati per unità, per utente.
- Dimensione totale dei file archiviati nell’archivio di autenticazione (ad eccezione dei file in corso di verifica).
- Numero totale di autenticazioni.
- Numero totale di file firmati.

Indice

A

Accesso all’interfaccia Web del servizio di autenticazione 5

Amministrare gli account utente e le quote 20

Attivazione dell'account 5

Autenticazione dei file 5

B

Browser Web supportati 4

C

Campi del modello di documento 13

Certificato di autenticazione 6

Creazione di un documento da un modello 16

Creazione di un modello di documento 14

F

Firma di file 9

Firma di un file come unico firmatario 10

Firma di un file creato da un modello 17

Funzionamento dell’autenticazione 3

G

Gestione del servizio di autenticazione 19

Gestione delle chiavi API 19

Gestione di modelli di documento 15

I

Informazioni sul servizio di autenticazione Acronis Notary 3

Invio di un file alla firma per più firmatari 11

L

Limitazioni 4

M

Modelli di documento 13

N

Notifiche 21

O

Operazioni con file firmati 12

Operazioni con i file autenticati 6

P

Pagina di verifica pubblica 9

Q

Quote 20

R

Report utilizzo 21

Ruoli utente 3

U

Utilizzo del servizio di autenticazione 5

Utilizzo del servizio di autenticazione come amministratore dell'autenticazione 17

Utilizzo del servizio di autenticazione come utente dell'autenticazione 5

V

Verifica dell'autenticità dei file 8