

OBSKURA

SICUREZZA INVISIBILE PER I TUOI DATI

MANUALE DI ISTRUZIONI

VERSIONE 0.3.0 · MACOS · WINDOWS · LINUX · OTTOBRE 2026

MANUALE DI ISTRUZIONI

INDICE

01	Benvenuto in Obskura	Cosa fa, database e casseforti	03
02	Installazione e primo avvio	macOS, Windows, Linux · la chiave di accesso · l'interfaccia	04
03	Password e file chiave	Credenziali, Argon2id, scelta del cifrario	05
04	Database di password	Creare, sbloccare, organizzare le voci	07
05	Gestire le voci	Generatore, campi, allegati, cronologia	08
06	Strumenti del database	Ricerca, copia sicura, menu del database	09
07	Casseforti di file	Creare una cassaforte e cifrare file	10
08	Lavorare con i file	Aprire, modificare, esportare	11
09	Server remoti	SFTP, WebDAV, SMB, FTP/FTPS	12
10	Più dispositivi in tempo reale	Sincronizzazione in tempo reale, notifiche	14
11	Chiave di accesso e dispositivi	File di accompagnamento, ID e percorsi di ogni dispositivo	15
12	Backup automatico	Seconda destinazione, copie datate, per dispositivo	17
13	Importare ed esportare	Gestori online, CSV da KeePass e altri	18
14	Lingue	Lingua automatica, file XML, nuove traduzioni	20
15	Blocco e impostazioni	Blocco automatico, appunti, tema, nome del dispositivo	23
16	Scorciatoie e crittografia	Tasti rapidi e dettagli tecnici	24
17	Buone pratiche e problemi	Backup, domande frequenti	25

CONVENZIONI

I nomi di pulsanti e menu sono in **grassetto**. Le combinazioni di tasti sono scritte così: `Ctrl/⌘` + `L`, dove `Ctrl` vale per Windows e Linux e `⌘` per macOS. Nomi di file ed estensioni sono in `carattere fisso`. Le schermate mostrano l'interfaccia nella lingua di questo manuale.

INTRODUZIONE

01 BENVENUTO IN OBSKURA

Obskura custodisce password e file con crittografia di livello militare. Niente account e nessun servizio di terzi: i tuoi dati restano dove decidi tu, sul computer o sul tuo server.

Ogni database e ogni cassaforte è un normale file o una normale cartella. Puoi tenerli sul disco del computer, su una chiavetta USB, dentro una cartella sincronizzata come Dropbox, OneDrive o iCloud Drive, oppure direttamente su un tuo server SFTP, WebDAV, SMB o FTP, e averne quanti ne vuoi: uno personale, uno di lavoro, uno condiviso con la famiglia. Più computer possono usarli insieme e vedono le modifiche degli altri in tempo reale, anche se ci arrivano da percorsi diversi.

DATABASE DI PASSWORD

Un singolo file `.obk`, sul modello di KeePass. Contiene voci con nome utente, password, indirizzo, note, campi personalizzati, allegati e cronologia delle modifiche, ordinate in gruppi.

CASSAFORTE DI FILE

Una cartella, sul modello di Cryptomator. Dentro ci trascini documenti, foto e archivi: ogni file viene cifrato singolarmente, nomi e struttura delle cartelle compresi.

COME FUNZIONA LA PROTEZIONE

Quando crei un database o una cassaforte scegli una **password principale**, un **file chiave** o entrambi. Da queste credenziali Obskura ricava la chiave di cifratura con Argon2id, un algoritmo pensato apposta per rendere lentissimi i tentativi di indovinare la password. I dati vengono poi cifrati con AES-256, lo standard approvato per le informazioni classificate **TOP SECRET**.

Le credenziali non vengono mai salvate da nessuna parte. Senza di esse il contenuto è illeggibile a chiunque, sviluppatori compresi.

IMPORTANTE

Non esiste alcun modo per recuperare una password dimenticata o un file chiave perso. Scegli una password che ricordi, e conserva una copia del file chiave in un luogo sicuro e separato.

IN SINTESI

AES-256-GCM · XChaCha20-Poly1305 · Serpent · Twofish · Camellia · Cascate di cifrari · Argon2id fino a 2 GiB · HKDF-SHA256 · AES-SIV per i nomi dei file · Memoria azzerata alla chiusura · Nessun account · SFTP · WebDAV · SMB · FTPS · Tempo reale · Backup automatico · Percorsi per dispositivo · 8 lingue · macOS · Windows · Linux

PER INIZIARE

02 INSTALLAZIONE E PRIMO AVVIO

macOS

Apri il file `.dmg` e trascina Obskura in **Applicazioni**. Al primo avvio, se macOS blocca l'app, vai in **Impostazioni di Sistema → Privacy e sicurezza** e scegli **Apri comunque**.

Windows

Esegui il programma di installazione `.exe`, che usa automaticamente la lingua di Windows, oppure avvia la versione portatile senza installare nulla. Se compare l'avviso di SmartScreen, fai clic su **Ulteriori informazioni → Esegui comunque**.

Linux

Usa il pacchetto `.deb` (Debian, Ubuntu), `.rpm` (Fedora, openSUSE) oppure l'`.AppImage`, che non richiede installazione: rendilo eseguibile e avvialo.

PRIMO AVVIO: LINGUA E CHIAVE DI ACCESSO

Obskura si apre nella lingua del sistema (italiano, inglese, tedesco, spagnolo, russo, cinese, giapponese o arabo; per le altre lingue usa l'inglese). Al primo avvio ti chiede di creare la **chiave di accesso Obskura** oppure, se usi già Obskura su un altro computer, di inserire quella che hai generato lì. Il capitolo 11 spiega a cosa serve.

LA SCHERMATA INIZIALE

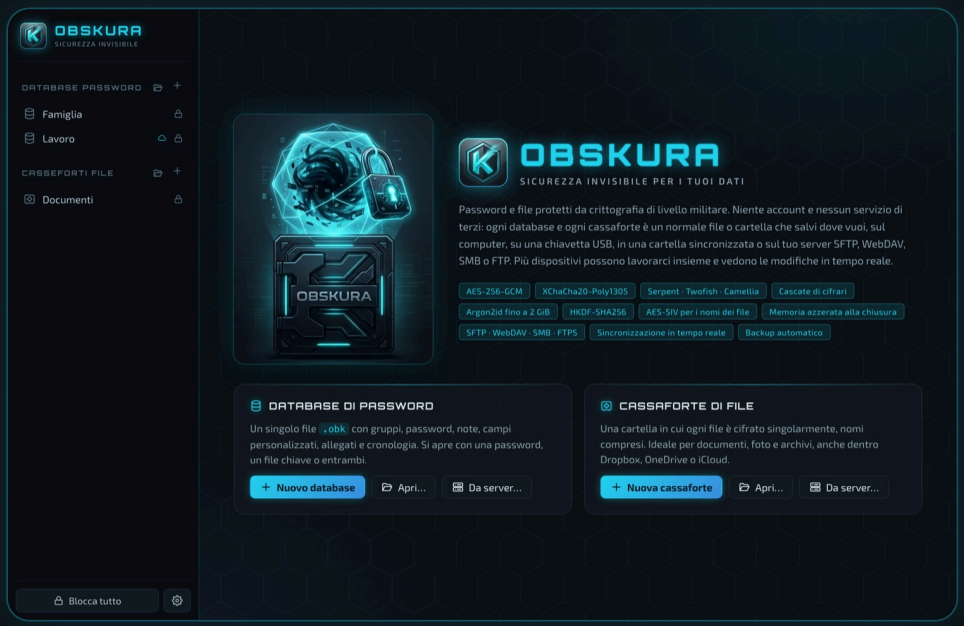


FIG. 1 La schermata di benvenuto, con la barra laterale.

Nella **barra laterale** ci sono le sezioni **Database password** e **Casseforti file**. Accanto a ciascun titolo trovi due pulsanti: la cartella per **aprire** un elemento esistente e il **+** per crearne uno nuovo.

- Ogni elemento aperto di recente resta in elenco, solo con il suo nome: i percorsi non compaiono mai. Il lucchetto indica lo stato: **chiuso** se bloccato, **aperto** se sbloccato.
- Passando sopra un elemento compare una **×** per toglierlo dai recenti (il file non viene eliminato) oppure un lucchetto per bloccarlo subito.
- In fondo: **Blocca tutto** e l'ingranaggio delle **Impostazioni**.

PROTEGGERE I DATI

03 PASSWORD E FILE CHIAVE

Database e casseforti si aprono con una **password principale**, un **file chiave** o con entrambi insieme. La combinazione delle due è la protezione più forte: servono qualcosa che *sai* e qualcosa che *possiedi*.

PASSWORD PRINCIPALE

Una frase lunga è più sicura di una parola complessa: quattro o cinque parole a caso sono facili da ricordare e difficilissime da indovinare. L'indicatore sotto il campo ne stima la robustezza in bit.

Il pulsante con il dado apre il **generatore** se preferisci una password casuale.

FILE CHIAVE

Come in KeePass, **qualsiasi file** può fare da chiave. Puoi scegliere **Usa un file esistente** oppure **Genera nuovo**: Obskura crea un file di chiave casuale nella posizione che indichi.

Tienilo per esempio su una chiavetta USB, separato dal database. Obskura ricorda dove si trova su ogni dispositivo e lo cerca da sola a ogni apertura (capitolo 11).

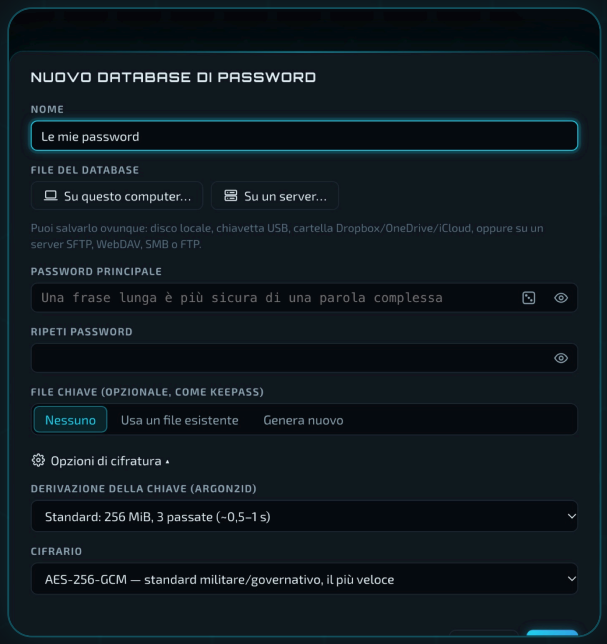


FIG. 2 Creazione di un database con le opzioni di cifratura aperte.

OPZIONI DI CIFRATURA

Con **Opzioni di cifratura** scegli quanto deve essere costosa la derivazione della chiave e quale cifrario usare. Le impostazioni predefinite, Standard e AES-256-GCM, sono già sicure per qualsiasi uso; tutte le alternative sono descritte nella pagina seguente.

IL FILE CHIAVE NON VA MAI MODIFICATO

Se usi un file qualunque (una foto, un documento) come chiave, anche una minima modifica lo rende inutilizzabile. I file generati da Obskura sono in un formato testuale riconosciuto, che resta valido anche se cambiano gli a capo. In ogni caso conservane una copia di sicurezza.

PROTEGGERE I DATI

03 SCEGLIERE IL CIFRARIO

DERIVAZIONE DELLA CHIAVE (ARGON2ID)

Argon2id trasforma le tue credenziali nella chiave di cifratura: più memoria e passate usa, più è costoso per un attaccante provare milioni di password.

LIVELLO	PARAMETRI	TEMPO DI APERTURA
Standard	256 MiB di memoria, 3 passate	circa 0,5–1 secondi
Alta	1 GiB, 4 passate	circa 2–4 secondi
Estrema	2 GiB, 6 passate	circa 5–12 secondi

LIVELLO ESTREMO

Ogni apertura richiede **2 GiB di memoria libera**. Su un computer con poca RAM il database o la cassaforte potrebbero non aprirsi: sceglilo solo se userai i tuoi file su computer adeguati.

CIFRARI

Tutti i cifrari usano chiavi da 256 bit e sono **autenticati**: qualsiasi alterazione dei dati viene rilevata.

CIFRARIO	CARATTERISTICHE
AES-256-GCM	**Predefinito.** Standard USA approvato per informazioni TOP SECRET, il più veloce grazie all'accelerazione hardware.
XChaCha20-Poly1305	Cifrario a flusso, veloce su qualsiasi processore anche senza istruzioni AES.
Serpent-256-GCM	Finalista del concorso AES, con il margine di sicurezza più ampio (32 round). Più lento.
Twofish-256-GCM	Finalista del concorso AES, progettato da Bruce Schneier e colleghi.
Camellia-256-GCM	Standard internazionale ISO/IEC, raccomandato in Europa (NESSIE) e Giappone (CRYPTREC).
Cascata AES · Twofish · Serpent	**La scelta più forte.** Tre cifrature in sequenza con chiavi indipendenti: i dati restano protetti anche se due dei tre algoritmi venissero un giorno violati.
Cascata AES · XChaCha20	Unisce un cifrario a blocchi e uno a flusso, di famiglie completamente diverse.

CASSEFORTI

Nelle casseforti il cifrario scelto protegge sia le chiavi sia il contenuto di ogni file. Se lo cambi con **Cambia password / file chiave**, i file già presenti restano cifrati con il precedente e quelli aggiunti da quel momento usano il nuovo. Il cifrario attivo è indicato in basso a destra nella cassaforte.

PASSWORD MANAGER

04 DATABASE DI PASSWORD

CREARE UN DATABASE

1. Fai clic su **Nuovo database** nella schermata iniziale, oppure sul **+** accanto a **Database password**.
2. Scrivi un **nome** e scegli dove salvare il file `.obk`: **Su questo computer…** o **Su un server…**.
3. Imposta password e/o file chiave (capitolo 03).
4. Premi **Crea**. Il database si apre già sbloccato.

APRIRE E SBLOCCARE

1. Seleziona il database nella barra laterale, oppure usa l'icona cartella per aprire un file `.obk` esistente.
2. Inserisci la password. Il file chiave e la copia di backup vengono cercati automaticamente; se il file chiave non si trova, sceglilo con **Scegli…**.
3. Premi **Sblocca** o `Invio`.

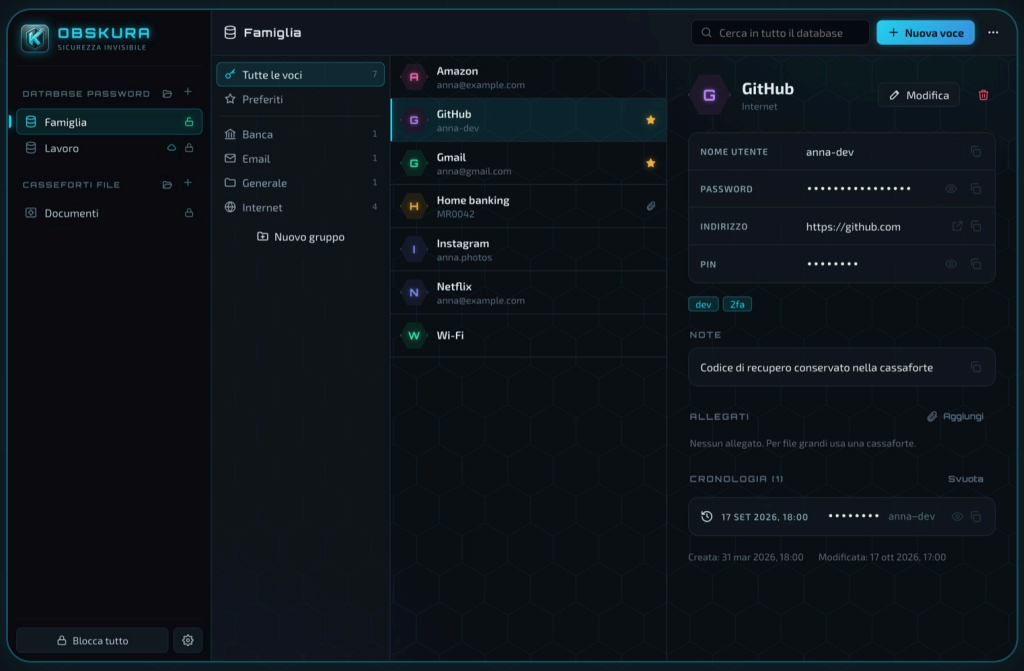


FIG. 3 Un database sbloccato: gruppi, elenco delle voci e dettaglio della voce selezionata.

LE TRE COLONNE

- **Gruppi**: **Tutte le voci**, **Preferiti** e le tue cartelle. Passando sopra un gruppo compaiono i comandi per creare un sottogruppo, modificarlo o eliminarlo; **Nuovo gruppo** è in fondo all'elenco.
- **Voci**: titolo e nome utente di ogni voce. La stella indica i preferiti, la graffetta gli allegati. Con un **doppio clic** copi direttamente la password.
- **Dettaglio**: tutti i campi della voce, con i pulsanti per mostrare, copiare o aprire l'indirizzo nel browser.

DATABASE DI PASSWORD

05 GESTIRE LE VOCI

Per aggiungere una voce premi **Nuova voce** (o `Ctrl/⌘` + `N`); per cambiarla selezionala e premi **Modifica**. Salva con il pulsante in fondo o con `Ctrl/⌘` + `S`. Ogni modifica viene scritta subito sul file del database.



FIG. 4 L'editor di una voce con il generatore aperto.

CAMPI DI UNA VOCE

Titolo e gruppo	Nome della voce e cartella in cui si trova.
Nome utente	Account, email o codice cliente.
Password	Con indicatore di robustezza e generatore.
Indirizzo	Si apre nel browser dal dettaglio.
Note	Testo libero, cifrato come tutto il resto.
Etichette	Parole chiave separate da virgola.
Scadenza	Data oltre la quale cambiare la password.

La **stella** in alto aggiunge la voce ai **Preferiti**.

GENERATORE DI PASSWORD

Fai clic sul dado nel campo password. Scegli la **lunghezza** (da 8 a 64 caratteri) e le famiglie di caratteri (`a–z`, `A–Z`, `0–9`, `!@#$`); con **Escludi ambigui** eviti caratteri che si confondono come l, 1, O e 0. Poi **Rigenera**, **Copia** oppure **Usa questa password**. Le password sono generate con il generatore casuale crittografico del sistema.

CAMPI PERSONALIZZATI

Aggiungi informazioni extra come PIN, codici di recupero o domande di sicurezza. Spunta **Protetto** per mostrarle nascoste, come una password.

ALLEGATI E CRONOLOGIA

Allega file fino a **64 MB** ciascuno (per file più grandi usa una cassaforte). Ogni modifica conserva la versione precedente: la **Cronologia** tiene le ultime **20** e permette di copiare una vecchia password.

DATABASE DI PASSWORD

06 STRUMENTI DEL DATABASE

CERCARE

Il campo **Cerca in tutto il database** in alto (o `Ctrl/⌘` + `F`) filtra le voci di tutti i gruppi mentre scrivi. `Esc` svuota la ricerca.

COPIARE IN MODO SICURO

I pulsanti di copia accanto a nome utente, password e campi protetti mettono il valore negli appunti, che Obskura **svuota automaticamente** dopo 20 secondi (valore modificabile nelle impostazioni). Gli appunti vengono cancellati solo se contengono ancora il valore copiato: se nel frattempo hai copiato altro, non lo tocca.

IL MENU DEL DATABASE

Il pulsante ⋯ in alto a destra contiene:

VOCE	A COSA SERVE
Proprietà del database	Cambiare nome e descrizione del database.
Cambia password / file chiave	Impostare nuove credenziali. Il database viene ricifrato con chiavi nuove.
Salva una copia di backup…	Scrivere una copia cifrata del database in un'altra posizione.
Backup automatico…	Configurare la seconda destinazione delle copie (capitolo 12).
Dispositivi e percorsi…	Vedere quali dispositivi usano il database e i loro percorsi (capitolo 11).
Importa / Esporta	Da un gestore online o da CSV, e verso CSV (capitolo 13).
Blocca database	Chiudere il database e cancellarne i dati dalla memoria.

SALVATAGGIO E SINCRONIZZAZIONE

Ogni modifica viene salvata subito, in modo **atomico**: il nuovo file viene scritto a parte e sostituisce il vecchio solo quando è completo, così un'interruzione di corrente non può corromperlo. Se nel frattempo un altro computer ha modificato il database, Obskura **unisce** le due versioni prima di salvare: non si perde nulla (capitolo 10). L'unico caso che richiede una scelta è quando su un altro dispositivo sono state cambiate **password o file chiave**: Obskura propone di bloccare il database per riaprirlo con le nuove credenziali.

> **CONSIGLIO**
>
> Per usare lo stesso database su più computer mettilo su un tuo server (capitolo 09) o in una cartella sincronizzata: puoi tenerlo aperto ovunque contemporaneamente.

FILE CIFRATI

07 CASSEFORTI DI FILE

Una cassaforte è una cartella che contiene i tuoi file in forma cifrata. Vista dall'esterno è solo un insieme di file con nomi illeggibili: non si capisce né cosa contengono né come sono organizzati.

CREARE UNA CASSAFORTE

1. Fai clic su **Nuova cassaforte**, o sul **+** accanto a **Casseforti file**.
2. Scegli un nome e la cartella in cui crearla, anche dentro Dropbox, OneDrive o iCloud Drive, o su un server.
3. Imposta password e/o file chiave e premi **Crea**.

AGGIUNGERE FILE

- **Trascina** file e cartelle dal Finder / Esplora risorse nella finestra: vengono cifrati nella cartella che stai guardando.
- Oppure usa **Aggiungi file** o **Aggiungi cartella**.
- Gli originali non vengono toccati: dopo averli cifrati puoi eliminarli tu.

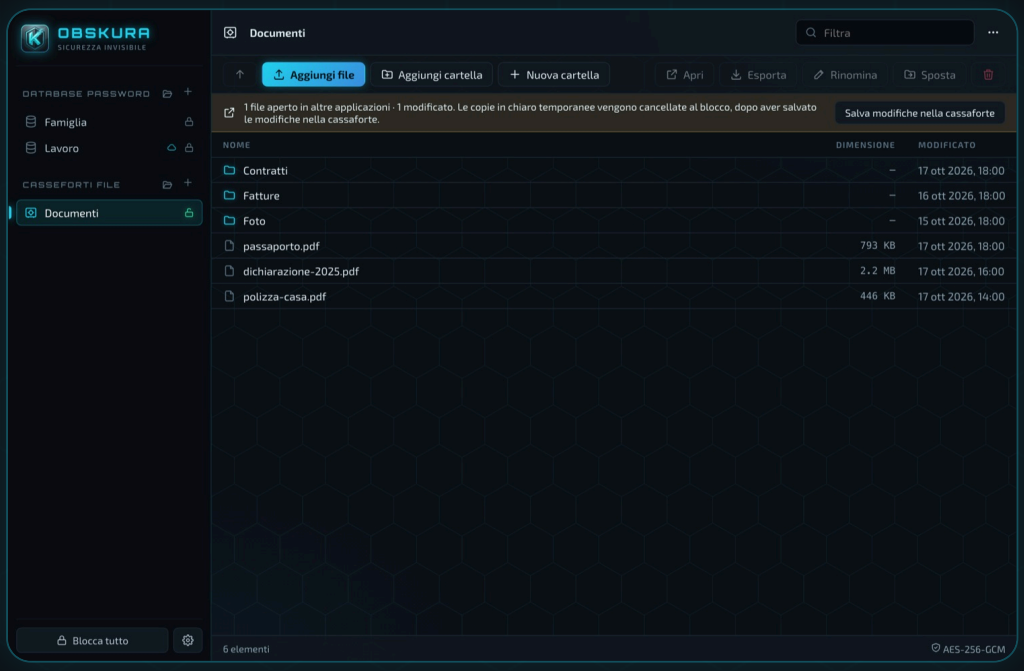


FIG. 5 Una cassaforte sbloccata.

LA BARRA DEI COMANDI

↑ torna alla cartella superiore · **Nuova cartella** crea una sottocartella · **Apri**, **Esporta**, **Rinomina**, **Sposta** ed **Elimina** agiscono sugli elementi selezionati. Selezioni più elementi con `Ctrl/⌘` + clic o `Maiusc` + clic. In basso, la barra di stato mostra il numero di elementi e l'avanzamento delle operazioni.

CASSEFORTI DI FILE

08 LAVORARE CON I FILE

APRIRE E MODIFICARE UN FILE

Fai doppio clic su un file (o selezionalo e premi **Apri**). Obskura lo decifra in una cartella temporanea protetta e lo apre con l'applicazione predefinita del sistema.

1. Modifica e salva il file normalmente nell'altra applicazione.
2. In Obskura compare una banda che indica i file aperti e quelli modificati.
3. Premi **Salva modifiche nella cassaforte** per ricifrare la nuova versione.

> **COPIE TEMPORANEE IN CHIARO**
>
> Finché un file è aperto, la sua copia decifrata esiste sul disco. Quando blocchi la cassaforte Obskura salva prima le modifiche rimaste e poi **cancella le copie temporanee**. Chiudi il file nell'altra applicazione prima di bloccare.

ESPORTARE

Esporta decifra gli elementi selezionati, cartelle comprese, in una cartella a tua scelta. I file esportati sono **in chiaro**: usa questa funzione solo quando ti servono fuori dalla cassaforte.

ORGANIZZARE

Rinomina con **Rinomina** o `F2`; sposta con **Sposta** scegliendo la cartella di destinazione. **Elimina** (o `Canc`) chiede sempre conferma. Il campo **Filtra** mostra solo gli elementi il cui nome contiene il testo inserito.

SINCRONIZZAZIONE CON IL CLOUD

Ogni file della cassaforte è cifrato separatamente: se cambi un documento, il servizio di sincronizzazione carica solo quel file. Per questo le casseforti funzionano bene dentro Dropbox, OneDrive, Google Drive o iCloud Drive.

COM'È FATTA UNA CASSAFORTE SUL DISCO

ELEMENTO	CONTENUTO
`vault.obkv`	Le chiavi della cassaforte, cifrate con le tue credenziali.
`vault.obkv.bak`	Copia identica di sicurezza, nel caso il primo file si danneggi.
`vault.obkx`	Il file di accompagnamento, cifrato con la chiave di accesso: file chiave, backup e percorsi di ogni dispositivo (capitolo 11).
`d/`	Tutti i file e le cartelle cifrati, affiancati: la struttura reale non è visibile.

Per aprire una cassaforte esistente usa l'icona cartella accanto a **Casseforti file** e scegli la sua cartella principale. Non modificare né spostare a mano i file al suo interno.

DOVE SALVARE

09 SERVER REMOTI

Database e casseforti non devono stare per forza sul computer: Obskura li apre e li salva direttamente su un tuo server, senza programmi di sincronizzazione in mezzo. I dati viaggiano e restano sul server **già cifrati**: l'amministratore del server, o chi lo violasse, vede solo file illeggibili.

PROTOCOLLO	DOVE SI USA	NOTE
SFTP	NAS (Synology, QNAP, TrueNAS), server Linux, VPS	Consigliato. Password o chiave SSH.
WebDAV	Nextcloud, ownCloud, Synology, QNAP, Box, Koofr	Su HTTPS. Per Nextcloud il percorso è `/remote.php/dav/files/<utente>`.
SMB	Cartelle condivise di Windows, NAS, Samba	SMB 2 e 3; indica il nome della condivisione.
FTPS	Hosting e server FTP con TLS	FTP cifrato con `AUTH TLS`.
FTP	Server FTP tradizionali	Le credenziali del server viaggiano in chiaro: meglio FTPS o SFTP.

CONFIGURARE UNA CONNESSIONE

1. Apri **Impostazioni → Connessioni ai server** e premi **Nuova connessione**.
2. Scegli il protocollo e inserisci indirizzo, porta (se diversa da quella standard), utente e password.
3. Premi **Prova connessione**, poi **Salva**.

La password del server finisce nel **portachiavi del sistema** (Portachiavi di macOS, Gestione credenziali di Windows, Secret Service su Linux), mai nel file delle impostazioni. Viene anche copiata, cifrata, nel file di accompagnamento: gli altri tuoi computer ricreano la connessione da soli.



FIG. 6 Una nuova connessione SFTP.

CHIAVE DEL SERVER (SFTP)

Al primo collegamento Obskura mostra l'**impronta** della chiave del server e ti chiede di accettarla, come fa `ssh`. Se in seguito l'impronta cambia, il collegamento viene rifiutato finché non la confermi di nuovo: potrebbe essere qualcuno che si spaccia per il tuo server. Se non è cambiato nulla sul server, non accettare.

APRIRE E SALVARE SU UN SERVER

- **Aprire:** l'icona cartella accanto a **Database password** o **Casseforti file** offre **Da questo computer…** e **Da un server…**. Lo stesso nella schermata iniziale con **Da server…**.
- **Creare:** nella finestra **Nuovo database** o **Nuova cassaforte** scegli **Su un server…** al posto di **Su questo computer…**.
- Gli elementi su un server compaiono tra i recenti con l'icona della **nuvola**; una volta aperti mostrano l'etichetta `SERVER` nella barra in alto.



FIG. 7 Il navigatore del server: scegli la connessione e la cartella.

Nel navigatore scegli la connessione in alto a sinistra e muoviti tra le cartelle. Per un database fai clic sul file `.obk`; per una cassaforte entra nella sua cartella (quella con `vault.obkv`) e premi **Apri questa cassaforte**. Con l'icona cartella+ crei una nuova cartella sul server.

PRESTAZIONI

I database sono piccoli e si aprono in un attimo anche da remoto. Le casseforti trasferiscono un file alla volta, quando lo apri o lo esporti: con file molto grandi conta la velocità della connessione.

COLLABORAZIONE

10 PIÙ DISPOSITIVI IN TEMPO REALE

Lo stesso database o la stessa cassaforte possono essere aperti contemporaneamente su più computer: le modifiche fatte su uno compaiono sugli altri entro pochi secondi.

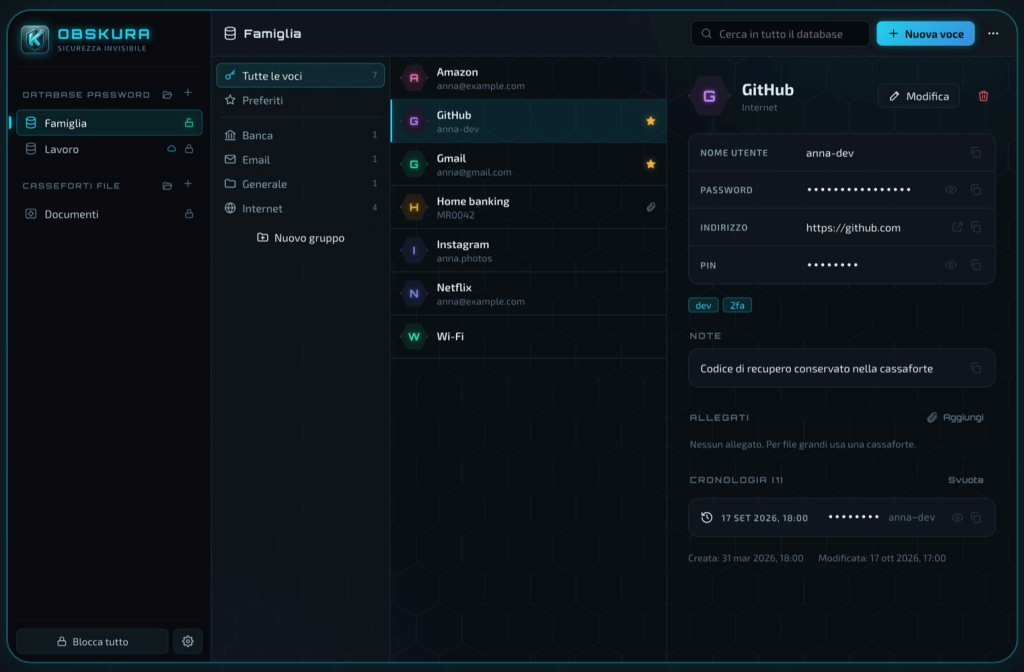


FIG. 8 Una notifica: un altro dispositivo ha aggiunto e modificato delle voci.

COME FUNZIONA

- Obskura controlla il file ogni **2 secondi** su disco locale o in una cartella sincronizzata, ogni **5 secondi** su un server. Il controllo legge solo i primi 88 byte del file.
- Quando trova una versione nuova la **unisce** alla tua, voce per voce, mostra una notifica con le voci aggiunte, modificate o eliminate e aggiorna subito l'elenco.
- Se due persone modificano la **stessa voce**, vince la modifica più recente; l'altra non si perde: finisce nella **Cronologia** della voce.
- Un'eliminazione arriva a tutti, a meno che nel frattempo qualcuno abbia modificato quella voce: in quel caso la modifica ha la precedenza e la voce resta.
- Nelle casseforti, quando qualcuno aggiunge, rinomina o elimina file nella cartella che stai guardando, l'elenco si aggiorna da solo.

OROLOGI DEI COMPUTER

Per decidere quale modifica è più recente Obskura usa l'ora dei computer: tienili sincronizzati (impostazione automatica dell'ora, attiva di solito su tutti i sistemi).

RITROVARE TUTTO, OVUNQUE

11 CHIAVE DI ACCESSO E DISPOSITIVI

Ogni database e ogni cassaforte ha accanto un piccolo file cifrato che ricorda dove sono file chiave, backup e server, e come ci arriva ciascuno dei tuoi dispositivi. Lo protegge la chiave di accesso Obskura.

LA CHIAVE DI ACCESSO OBSKURA

È un codice di 55 caratteri generato al primo avvio (o inserito, se lo hai creato su un altro computer). Resta nel portachiavi del sistema; da **Impostazioni → Chiave di accesso Obskura** puoi:

- **Mostra**: rivederlo e copiarlo, per inserirlo su un altro computer.
- **Cambia chiave…**: generarne uno nuovo. Obskura ricifra subito i file di accompagnamento raggiungibili; gli altri si aggiornano alla prima apertura (le chiavi precedenti restano valide per leggerli).
- **Inserisci chiave…**: usare la chiave attuale se è stata cambiata su un altro computer.

I FILE DI ACCOMPAGNAMENTO

Sono cifrati con AES-256-GCM e illeggibili senza la chiave di accesso:

FILE	CONTIENE
`.obk.obkx`	Accanto a ogni database: posizione del file chiave, configurazione del backup, connessioni ai server e i record dei dispositivi.
`vault.obkx`	Dentro ogni cassaforte: le stesse informazioni.
`recenti.obkx`	Nella cartella dei dati dell'app: l'elenco dei recenti. Sul disco non restano percorsi in chiaro.

APRIRE DA UN ALTRO COMPUTER

Inserita la chiave di accesso sul nuovo computer, basta selezionare il database: Obskura legge il file di accompagnamento, ricrea le connessioni ai server mancanti, trova il file chiave (nella posizione nota per quel dispositivo, accanto al database, nei percorsi degli altri dispositivi o nella copia di backup) e propone la copia di backup se l'originale non è raggiungibile.

IMPORTANTE

La chiave di accesso non sostituisce la password dei database: senza password (e file chiave) i dati restano illeggibili. Conservala comunque in un luogo sicuro: senza di essa devi scegliere a mano file chiave e backup.

DISPOSITIVI E PERCORSI

Ogni computer che usa Obskura ha un **identificativo univoco**, generato al primo avvio, e un **nome** (quello del computer, modificabile in **Impostazioni → Nome di questo dispositivo**). Ogni volta che apre un database o una cassaforte, registra nel file di accompagnamento cifrato il proprio record:

DATO	ESEMPIO
Identificativo e nome	`3f2a9c1e-…` · «MacBook di casa»
Sistema e versione	macOS · Obskura 0.3.0 · ultimo accesso
Percorso del database	`/Users/anna/Dropbox/conti.obk` sul Mac, `D:\Dropbox\conti.obk` sul PC
Percorso del file chiave	`/Volumes/USB/chiave.obkey` oppure `E:\chiave.obkey`
Backup proprio	una cartella di quel dispositivo, oppure la configurazione comune (capitolo 12)

LA FINESTRA «DISPOSITIVI E PERCORSI»

Dal menu ⋯ di un database o di una cassaforte scegli **Dispositivi e percorsi…**:

- vedi tutti i dispositivi registrati, con sistema, versione, ultimo accesso, uso del file chiave e destinazione del backup;
- l'icona a forma di occhio mostra i percorsi di ciascuno; la matita rinomina questo dispositivo;
- il cestino **dimentica** un dispositivo che non usi più: i suoi percorsi e il suo backup vengono tolti dal file (se lo riapre, si registra di nuovo).

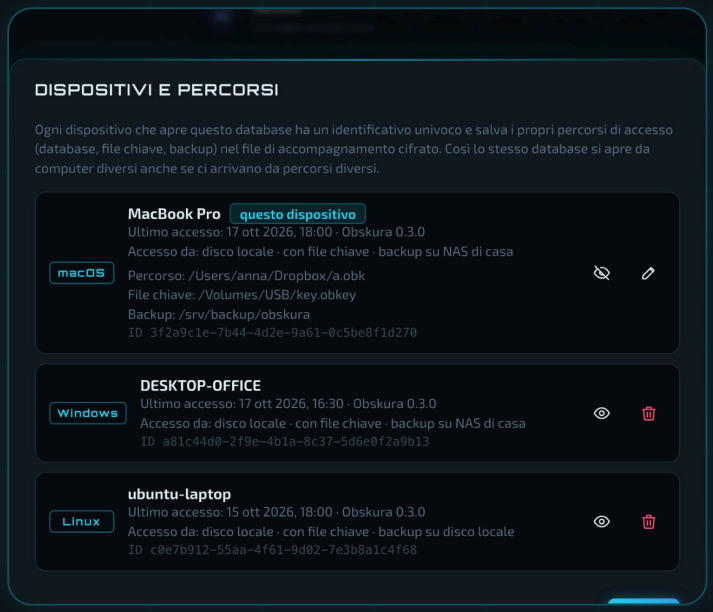


FIG. 9 I dispositivi che usano un database.

PERCHÉ SERVE

Lo stesso database in Dropbox ha percorsi diversi su Mac, Windows e Linux, e la chiavetta con il file chiave cambia lettera o nome. Grazie ai record per dispositivo ognuno ritrova i propri percorsi, senza sovrascrivere quelli degli altri.

SICUREZZA DEI DATI

12 BACKUP AUTOMATICO

Ogni database e ogni cassaforte può avere una **seconda destinazione**, su questo computer (per esempio un disco esterno) o su qualsiasi server configurato. A ogni modifica Obskura vi copia la nuova versione in background, senza rallentarti.

1. Dal menu ··· del database o della cassaforte scegli **Backup automatico…**
2. Attiva **Backup automatico attivo** e scegli la cartella: **Su questo computer…** o **Su un server…**.
3. Se la destinazione è un server, puoi spuntare **Usa questa configurazione su tutti i dispositivi**.
4. Per i database scegli quante **copie datate** conservare.
5. Premi **Salva**. Con **Esegui ora** puoi forzare una copia completa.

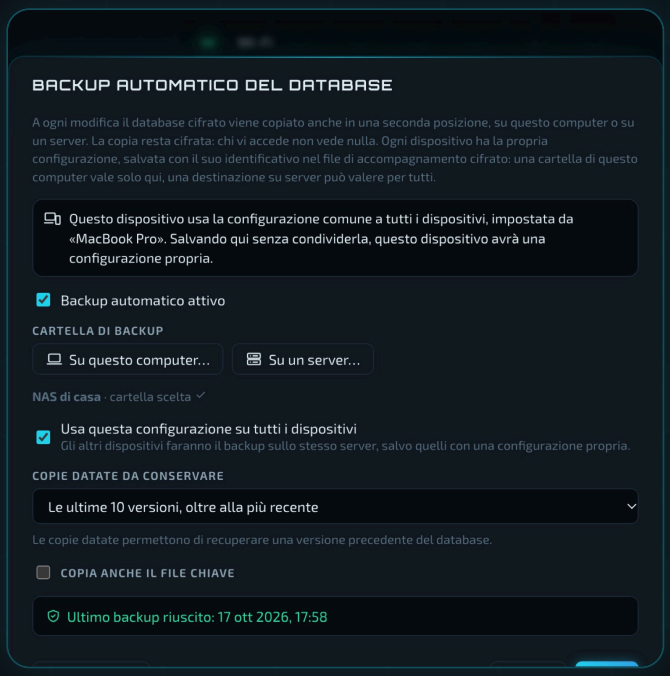


FIG. 10 Backup su un NAS, comune a tutti i dispositivi.

COSA	COME VIENE COPIATO
Database	Il file `.obk` nella cartella di backup, più le copie datate `nome.AAAAMMGG-hhmmss.obk`; le più vecchie oltre il limite vengono eliminate.
Cassaforte	Una replica della cartella cifrata: a ogni modifica vengono ricopiati solo i file toccati. La copia si apre come una normale cassaforte.
File chiave	Facoltativo: copiato una volta, quando salvi l'impostazione, nella cartella che indichi.

UN BACKUP PER OGNI DISPOSITIVO

- Ogni dispositivo ha la **propria configurazione**, salvata con il suo identificativo nel file di accompagnamento: una cartella locale (per esempio un disco esterno del Mac) vale solo su quel dispositivo.
- Una destinazione su server può diventare **comune**: gli altri dispositivi la usano, salvo quelli che hanno una configurazione propria. La finestra indica chi l'ha impostata.
- Le copie restano **cifrate**: la destinazione di backup non deve essere fidata.
- Se un backup non riesce compare un avviso; Obskura riprova alla modifica successiva.

FILE CHIAVE E BACKUP

Non mettere il file chiave nella stessa cartella del backup: chi accedesse a quella cartella avrebbe sia il database sia metà delle credenziali.

DA E VERSO ALTRI PROGRAMMI

13 IMPORTARE ED ESPORTARE

IMPORTARE DA UN GESTORE ONLINE

Obskura accede direttamente al tuo vecchio servizio, scarica la cassaforte cifrata e la decifra sul tuo computer, senza passare da un file esportato in chiaro. Le credenziali servono solo per quell'accesso e non vengono salvate.

1. Apri il database di destinazione e scegli ••• → **Importa da un gestore online…**
2. Scegli il servizio e accedi; se hai la verifica in due passaggi Obskura chiede il codice.
3. Controlla l'anteprima: numero di voci, cartelle, esempi.
4. Decidi se ricreare le cartelle come gruppi e se saltare le voci già presenti, poi premi **Importa**.

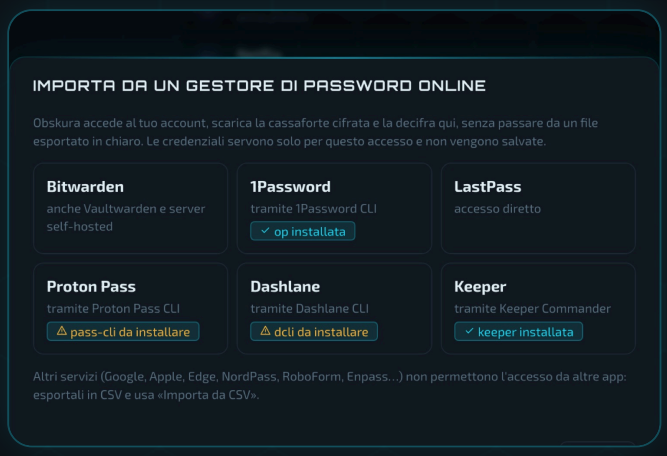


FIG. 11 La scelta del servizio da cui importare.

SERVIZIO	ACCESSO
Bitwarden / Vaultwarden	Diretto, anche bitwarden.eu e server self-hosted; in alternativa con la chiave API personale.
LastPass	Diretto, con verifica in due passaggi (codice o conferma sul telefono).
1Password	Tramite 1Password CLI (`op`), autorizzata dall'app 1Password o con email, password e Secret Key.
Proton Pass	Tramite Proton Pass CLI (`pass-cli`), con accesso dal browser.
Dashlane	Tramite Dashlane CLI (`dcli`), dopo un primo `dcli sync` nel terminale.
Keeper	Tramite Keeper Commander (`keeper`).

Cartelle, campi personalizzati, codici TOTP, carte e note vengono conservati. Gli altri servizi (Google, Apple, Edge, NordPass…) non permettono l'accesso da altre app: esportali in CSV.

IMPORTARE DA CSV (KEEPASS E ALTRI)

1. Nel programma di origine esporta in CSV: KeePass 2 **File → Esporta → KeePass CSV (1.x)**, KeePassXC **Database → Esporta → File CSV**, Bitwarden, 1Password, Chrome, Edge e Firefox dalle rispettive impostazioni.
2. In Obskura apri il database e scegli ⋯ → **Importa da CSV (KeePass, …)…**
3. Scegli il file: Obskura riconosce il formato e le colonne e mostra un'anteprima.
4. Decidi se ricreare i gruppi del file e se saltare le voci già presenti, poi premi **Importa**.

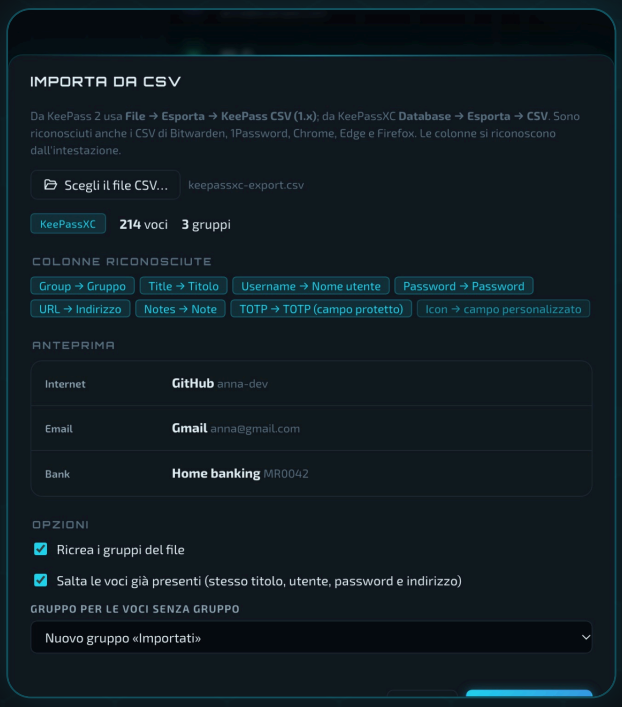


FIG. 12 Anteprima di un'esportazione KeePassXC.

Gruppi, etichette, codici TOTP (salvati come campo protetto), date di creazione e scadenze vengono conservati; le colonne non riconosciute diventano campi personalizzati. Reimportare lo stesso file non crea doppioni.

ESPORTARE IN CSV

⋯ → **Esporta in CSV…** crea un file con le colonne di KeePassXC, più etichette, scadenza, preferiti e campi personalizzati: si reimporta in Obskura, in KeePassXC e nella maggior parte dei password manager.

> **IL CSV NON È CIFRATO**
>
> Il file contiene tutte le password in chiaro. Usalo solo per spostare i dati, poi cancellalo. Dopo l'importazione elimina anche il CSV esportato dal vecchio programma. Per i backup usa il backup automatico, che resta cifrato.

PERSONALIZZARE

14 LINGUE

Obskura parla otto lingue e se ne possono aggiungere altre: tutti i testi dell'app stanno in file XML, uno per lingua.

SCEGLIERE LA LINGUA

All'avvio Obskura usa la lingua del sistema; se non è tra quelle incluse usa l'inglese. In **Impostazioni → Lingua** puoi lasciare **Automatica** o sceglierne una: il cambio è immediato, anche per i messaggi d'errore. L'arabo si legge da destra a sinistra e l'interfaccia si capovolge di conseguenza.

Italiano	it
English	en
Deutsch	de
Español	es
Русский	ru
中文（简体）	zh
日本語	ja
العربية	ar

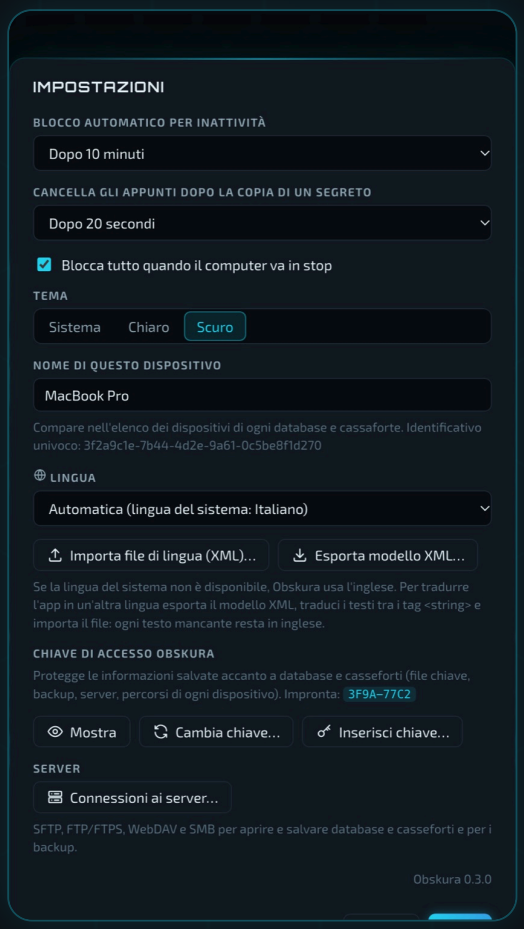


FIG. 13 La sezione Lingua nelle impostazioni.

AGGIUNGERE UNA LINGUA

1. In **Impostazioni → Lingua** premi **Esporta modello XML…**: ottieni il file completo della lingua attuale (o scarica dal sito lo zip con gli XML di tutte le lingue).
2. Cambia nell'intestazione `code` (codice della lingua, per esempio `fr` o `pt-BR`), `name` e, per le lingue da destra a sinistra, `dir="rtl"`.
3. Traduci il testo di ogni elemento `<string>` con un qualsiasi editor di testo, salvando in UTF-8.
4. Premi **Importa file di lingua (XML)…**: la lingua compare subito nell'elenco ed è usata in automatico sui sistemi in quella lingua.

IL FORMATO DEL FILE

Un file di lingua è un XML con un elemento `<language>` e un `<string>` per ogni testo:

```
<?xml version="1.0" encoding="UTF-8"?>
<language code="fr" name="Français" english-name="French" dir="ltr">
  <string key="common.cancel">Annuler</string>
  <string key="db.syncFailed">Échec de la synchronisation : {message}</string>
  <string key="vault.itemsN.one">{count} élément</string>
  <string key="vault.itemsN.other">{count} éléments</string>
</language>
```

- l'attributo `key` non va tradotto né cambiato;
- i segnaposto tra graffe, come `{count}` o `{name}`, vanno lasciati come sono: l'app li sostituisce con numeri e nomi;
- i tag `<b>` e `<code>` nel testo vanno conservati;
- le chiavi che finiscono con `.one`, `.two`, `.few`, `.many` e `.other` sono le forme plurali: usa quelle della tua lingua, `.other` è obbligatoria;
- un testo mancante viene mostrato in inglese, quindi una traduzione parziale funziona già.

CORREGGERE UNA LINGUA INCLUSA

Un file XML con lo stesso `code` di una lingua inclusa (per esempio `it`) non la sostituisce: ne corregge solo le voci che contiene. Nelle impostazioni compare con l'indicazione **correzioni** e si toglie con la ×, tornando ai testi originali.

> **CONSIGLIO**
>
> I file importati restano nella cartella dei dati dell'app e valgono solo su quel computer: importali anche sugli altri.

TRADURRE CON IL MODELLO XML VUOTO

Per una nuova lingua puoi partire dal modello vuoto `obskura-translation-template.xml`, che si scarica dal sito (`obskura.bytenooks.com`, sezione Download). Contiene una riga per ogni testo dell'app: il testo va scritto tra `<string …>` e `</string>`, mentre l'attributo `en` riporta il testo inglese di riferimento e può restare dov'è (l'app lo ignora).

```
<language code="fr" name="Français" english-name="French" dir="ltr">
  <string key="common.lock" en="Lock">Verrouiller</string>
  <string key="common.settings" en="Settings">Paramètres</string>
  <string key="common.cancel" en="Cancel">Annuler</string>
</language>
```

1. Scarica il modello e salvalo con il codice della tua lingua, per esempio `fr.xml`.
2. Nella prima riga `<language>` compila `code`, `name`, `english-name` e, se serve, `dir="rtl"`.
3. Scrivi le traduzioni con un editor di testo che salvi in UTF-8, rispettando le regole qui sopra.
4. **Elimina le righe che non traduci**: un testo lasciato vuoto comparirebbe vuoto nell'app, mentre una riga assente viene mostrata in inglese.
5. Importa il file in **Impostazioni → Lingua** e controlla i testi nell'app.

CONDIVIDI LA TUA TRADUZIONE

Inviala allo sviluppatore dalla pagina Contatti del sito: scegli l'argomento «Traduzione» e allega il file XML (fino a 3 MB; un file di lingua completo pesa circa 100–150 KB). Le traduzioni ricevute potranno essere incluse nelle prossime versioni.

SICUREZZA

15 BLOCCO E IMPOSTAZIONI

Quando blocchi un database o una cassaforte, Obskura chiude la sessione e **azzera in memoria** chiavi e dati decifrati. Per riaprirli servono di nuovo le credenziali.

MODI PER BLOCCARE

- **Blocca tutto** in fondo alla barra laterale, oppure `Ctrl/⌘` + `L`.
- Il lucchetto accanto a un elemento sbloccato della barra laterale, o la voce **Blocca** nel menu ⋯.
- **Automaticamente**, dopo un periodo di inattività o quando il computer va in stop.

IMPOSTAZIONI

IMPOSTAZIONE	EFFETTO	PREDEFINITO
Blocco automatico per inattività	Blocca tutto dopo 1–60 minuti senza usare mouse o tastiera, oppure mai.	10 minuti
Cancella gli appunti	Svuota gli appunti 10–120 secondi dopo la copia di un segreto, oppure mai.	20 secondi
Blocco in stop	Blocca tutto quando il computer va in sospensione.	Attivo
Tema	Sistema, Chiaro o Scuro.	Scuro
Nome di questo dispositivo	Compare nell'elenco dei dispositivi di ogni database e cassaforte; sotto c'è l'identificativo univoco.	Nome del computer
Lingua	Automatica o una delle lingue disponibili; importazione ed esportazione dei file XML (capitolo 14).	Automatica
Chiave di accesso Obskura	Mostrare, cambiare o inserire la chiave (capitolo 11).	—
Server	Le connessioni SFTP, FTP/FTPS, WebDAV e SMB (capitolo 09).	—

Le impostazioni non contengono segreti: le password dei server sono nel portachiavi del sistema e l'elenco dei recenti è cifrato con la chiave di accesso.

RIFERIMENTO

16 SCORCIATOIE E CRITTOGRAFIA

SCORCIATOIE DA TASTIERA

TASTI	DOVE	AZIONE
`Ctrl/⌘` + `L`	Ovunque	Blocca tutto
`Esc`	Finestre di dialogo	Chiude la finestra
`Ctrl/⌘` + `F`	Database	Cerca
`Ctrl/⌘` + `N`	Database	Nuova voce
`Ctrl/⌘` + `S`	Editor di una voce	Salva la voce
Doppio clic	Elenco voci	Copia la password
`Ctrl/⌘` + `A`	Cassaforte	Seleziona tutto
`Enter`	Cassaforte	Apre il file o la cartella
`F2`	Cassaforte	Rinomina
`Del` · `⌘` + `⌫`	Cassaforte	Elimina gli elementi selezionati
`⌫`	Cassaforte	Torna alla cartella superiore

DETTAGLI CRITTOGRAFICI

COMPONENTE	ALGORITMO
Derivazione della chiave	Argon2id: 256 MiB / 3 passate, 1 GiB / 4 passate o 2 GiB / 6 passate, sale casuale da 256 bit.
Chiave composita	SHA-256 di password (normalizzata NFC) e file chiave, come KeePass KDBX4.
Cifratura	AES-256, XChaCha20, Serpent, Twofish, Camellia o cascate, sempre autenticati (GCM o Poly1305); nelle cascate ogni strato ha una chiave propria derivata via HKDF.
Sottochiavi	HKDF-SHA256 con un seme nuovo a ogni salvataggio.
Integrità	Intestazione autenticata: ogni alterazione impedisce l'apertura.
Nomi nelle casseforti	AES-SIV, legati alla cartella che li contiene.
Contenuto dei file	Blocchi da 64 KiB, chiave casuale per file, protezione da riordino e troncamento.
File di accompagnamento	AES-256-GCM con una chiave derivata via HKDF dalla chiave di accesso Obskura (256 bit casuali).
Memoria	Chiavi e dati in chiaro restano nel processo nativo e vengono azzerati alla chiusura.

SUPPORTO

17 BUONE PRATICHE E PROBLEMI

BUONE PRATICHE

- **Attiva il backup automatico** o copia regolarmente i file `.obk` e le cartelle delle casseforti su un disco esterno. Sono già cifrati, quindi il backup è sicuro ovunque lo conservi.
- **Conserva il file chiave separatamente** dal database e tienine almeno una copia di riserva.
- **Conserva la chiave di accesso Obskura** su carta o in un luogo diverso dal computer.
- **Usa una password diversa per ogni servizio**, generata con il generatore: dovrai ricordarne solo una.
- **Blocca quando ti allontani**: `Ctrl/⌘` + `L` è il gesto più rapido.
- **Dimentica i dispositivi** che non usi più, dalla finestra **Dispositivi e percorsi**.

DOMANDE FREQUENTI

HO DIMENTICATO LA PASSWORD PRINCIPALE. POSSO RECUPERARLA?

No. È proprio ciò che rende Obskura sicuro: nessuno, nemmeno gli sviluppatori, può aprire un database o una cassaforte senza le credenziali giuste.

«PASSWORD O FILE CHIAVE ERRATI», MA SONO SICURO CHE SIANO GIUSTI.

Controlla di aver scelto lo stesso file chiave usato alla creazione e che non sia stato modificato. Se hai usato password *e* file chiave, servono entrambi. Verifica anche il tasto Bloc Maiusc.

L'APERTURA RICHIEDE QUALCHE SECONDO. È NORMALE?

Sì: è il tempo di Argon2id, voluto per rallentare chi prova a indovinare la password. Con il livello Alta servono alcuni secondi e 1 GiB di memoria libera, con Estrema fino a 12 secondi e 2 GiB.

SU UN ALTRO COMPUTER IL FILE CHIAVE NON VIENE TROVATO.

Collega il supporto che lo contiene: Obskura lo cerca nel percorso che quel computer ha usato l'ultima volta, accanto al database, nei percorsi degli altri dispositivi e nella copia di backup. Se non lo trova, sceglilo con **Scegli…**: la volta successiva il percorso sarà ricordato per quel dispositivo.

COMPARE «PROTETTE CON UNA CHIAVE DI ACCESSO DIVERSA».

La chiave di accesso è stata cambiata su un altro computer. Fai clic su **Inserisci la chiave attuale** e usa quella nuova; puoi comunque sbloccare con la password e scegliere a mano il file chiave.

È COMPARSO «CREDENZIALI CAMBIATE ALTROVE».

Su un altro dispositivo qualcuno ha cambiato password o file chiave del database. Scegli **Blocca** e riaprilo con le nuove credenziali; **Sovrascrivi** annullerebbe il cambio fatto altrove.

NON RIESCO A COLLEGARMI AL SERVER.

Controlla indirizzo, porta e credenziali con **Prova connessione**. Per WebDAV verifica il percorso base (per Nextcloud `/remote.php/dav/files/<utente>`); per SMB il nome della condivisione. Con un certificato autofirmato attiva **Accetta certificati autofirmati** solo in una rete fidata.

LE MODIFICHE A UN FILE DELLA CASSAFORTE NON RISULTANO SALVATE.

Assicurati di aver salvato il file nell'altra applicazione, poi premi **Salva modifiche nella cassaforte**. Se blocchi la cassaforte con il file ancora aperto, Obskura prova comunque a salvarlo prima di cancellare la copia temporanea.

L'APP SI APRE IN UNA LINGUA CHE NON È LA MIA.

Obskura segue la lingua del sistema; se la tua non è inclusa usa l'inglese. Scegli la lingua in **Impostazioni → Lingua** o importa un file XML (capitolo 14).

MACOS O WINDOWS DICONO CHE L'APP NON È VERIFICATA.

L'app non è firmata con un certificato commerciale. Segui le istruzioni del capitolo 02 per aprirla la prima volta.



OBSKURA

SICUREZZA INVISIBILE PER I TUOI DATI

Password manager e casseforti di file cifrate · sul tuo computer o sul tuo server

macOS · Windows · Linux · Versione **0.3.0**

https://obskura.bytenooks.com