Ssh_Tunnel

User manual · Manuel d'utilisation · Manuale d'uso · Manual de utilizare · ユーザー マニュアル

Language · Langue · Lingua · Limba · 言語.....**Page · Page · Pagina · Pagina · ページ**

EN English.....2

FR Français.....31

IT Italiano.....60

RO Română.....89

JA 日本語.....118

DevService.net — Raffaele Romano

Ssh_Tunnel

SSH client for controlled remote access

User and Administration Manual

Software version 27.2.2036.6127 · DB rev. 2

© Raffaele Romano
October 2026

Contents

1. Introduction....5
1.1 Who this manual is for....5
1.2 Documented version....5

2. Basic concepts....6

3. Installation and requirements....7
3.1 Required files....7
3.2 Requirements....7
3.3 Embedded programs....7
3.4 External parameter file (optional)....7
3.5 Optional components in the folder....8

4. Startup and login....9
4.1 The login screen....9
4.2 Entering the password....10
4.3 Login screen menu....10
4.4 Importing a certificate....10

5. Two-step verification (PC authorization)....12
5.1 When it is required....12
5.2 Requesting the codes....12
5.3 Authorization levels....12
5.4 «Varie» menu of the two-step verification....13
5.5 Revoking the authorization....13

6. The main window....14
6.1 Overview....14
6.2 Options....14
6.3 Main window menu....15

7. Connection and remote sessions....16
7.1 Connecting to the SSH server....16
7.2 Opening a session on a remote PC....16
7.3 Connection types....17
7.4 RDP/VNC/Term button....18
7.5 Disconnecting and exiting....18

8. Managing port forwardings....19
8.1 Enabling editing....19
8.2 Fields of a forwarding....19
8.3 Operations on the list....19

9. Managing SSH servers....21

10. «Apri come Putty» mode....22

11. Certificate management....23
11.1 Aggiorna modifiche....23
11.2 Cambio Password....23
11.3 Cambio Password Intermedia....23
11.4 Export Certificato....23
11.5 Elimina Certificato....23

12. Albatros redirection (DbKey)....24

13. Log and database maintenance.....25
13.1 Message panel and log.....25
13.2 Mostra Log.....25
13.3 Invia Log via Mail.....25
13.4 Maintenance.....25
13.5 Database structure.....25
14. Security.....26
15. Messages and troubleshooting.....27
Appendix A – Quick summary for the user.....28
Appendix B – Certificate structure.....29
Appendix C – Technical notes for the developer.....30

1. Introduction

Ssh_Tunnel is an SSH client for Windows, developed in VB.NET, that provides controlled access to PCs and servers on a company network (via RDP, VNC, SSH terminal or IP cameras) through an encrypted tunnel to a company SSH server.

It was created as an alternative to tools such as TeamViewer, AnyDesk and the like: these guarantee encrypted traffic, but anyone who has the credentials can access the systems, tying network security to third parties. Ssh_Tunnel instead:

- contains no password in plain text: all connection parameters are enclosed in an **encrypted certificate**, which can be opened only with the login password given to the user;
- assigns each recipient (support center, technician, consultant) a **unique certificate**, so that the SSH server recognizes who is connecting and records the date, time and duration;
- can tie its use to a specific PC through a **two-step verification** (code sent by e-mail), with permanent, daily or single-session authorization;
- notifies every access to a remote PC by e-mail, indicating from which computer the connection was made;
- shows the user only the connections provided for by their certificate, presented as a list of computers to double-click.

1.1 Who this manual is for

The manual is divided into three parts:

- **Everyday use** (chapters 3–7): installation, login, two-step verification, connection and opening of remote sessions. This is the part to give to whoever receives the program.
- **Administration** (chapters 8–13): management of port forwardings, servers, certificates, Albatros redirection, logs and the database.
- **Technical reference** (chapters 14–15 and appendices): architecture, security, certificate structure, messages and troubleshooting.

1.2 Documented version

Item	Value
Program	Ssh_Tunnel
Software version	27.2.2036.6127 (build date 11/10/2026)
Database revision	2
Certificate version	2 (Algoritmo = 1)
Platform	.NET Framework 4.8, Windows, 32-bit and 64-bit builds
Main libraries	Renci SSH.NET 2025, System.Data.SQLite, AlbatrosCommon
Interface languages	Italian, English, French, Japanese, Romanian (chosen automatically based on the Windows language)

The version shown by the program has the form `Sw ver.: 27.2.2036.6127 - 11/10/2026`: the date is derived from the revision number (days elapsed since 01/01/2010) and therefore corresponds to the build date.

2. Basic concepts

Before using the program, it is useful to know some terms that recur in all the screens.

Term	Meaning
Profile	Name that identifies a certificate (e.g. «Sede -> Cliente»). Several profiles can coexist in the same database; at startup you choose which one to use.
Certificate	Encrypted block containing everything needed for the connection: SSH server and ports, SSH credentials, private key, list of port forwardings, RDP/VNC files, e-mail addresses, permissions. It is distributed as a `.Ssh_T` file and imported into the database.
Login password	Password requested at startup. It decrypts the certificate: without it the program knows neither the servers nor the credentials.
Intermediate password (remote access)	Second password requested when opening a session on a remote PC. It prevents a program left open and unattended from being used by others.
Connection-specific password	Intermediate password defined for a single entry in the list; if present, it takes precedence over the general one.
Two-step verification	Additional check: the first time the program is used on a PC, a code is requested by e-mail. The authorization is tied to the PC's hardware.
Persistent / OneDay / OneTime code	The three two-step verification codes: permanent authorization, valid until midnight, valid for the current session only (see chapter 5).
Port forwarding (tunnel)	Mapping «local address and port → remote host and port» established through the SSH connection. Each reachable computer corresponds to a forwarding.
DbKey	Key used by the Albatros applications to choose the working database; Ssh_Tunnel can change it automatically on connection and disconnection (chapter 12).

3. Installation and requirements

3.1 Required files

Ssh_Tunnel requires neither installation nor administrator rights. Just copy into the same folder:

File	Description
`Ssh_Tunnel_<Nome>.exe`	Program executable (the name can be customized per recipient; it may end with 32 or 64).
`Ssh_Tunnel_<Nome>.db`	Encrypted SQLite database containing certificates, parameters and log.

The database name is derived from the executable name, removing any `32` or `64` suffix and adding `.db`. Example: `Ssh_Tunnel_Esempio64.exe` looks for `Ssh_Tunnel_Esempio.db`. In this way the 32-bit and 64-bit versions share the same database.

> **Note**
>
> If the database does not exist, it is created empty at first startup; in that case you must import a certificate (section 4.4) before you can log in.
>
> If the message «Riscontrata anomalia tra la versione attesa e quella trovata nel Database di servizio» (Mismatch found between the expected version and the one found in the service database) appears, move the program to a folder without write restrictions (for example, not under `C:\Program Files`).

3.2 Requirements

- Windows with .NET Framework 4.8.
- Outbound Internet access to the company SSH server (the default port is 200, unless otherwise specified in the certificate).
- For two-step verification and notifications: ability to send e-mail (the program uses the internal SMTP parameters of the Albatros library).

3.3 Embedded programs

The executable contains the auxiliary programs, which are extracted only when needed to the temporary folder `%TEMP%\Albatros\Ssh_Tunnel` and deleted at startup and on exit:

Component	Use
`vncviewer.exe` / `vncviewer32.exe`	VNC viewer (64-bit or 32-bit version depending on the process).
`rdp.exe`	RDP+ client (remote desktop with automatic password passing).
`gencrypt.exe`	Password encryption for RDP+.
`AlbatrosRDP.exe`	Proprietary RDP client with secure password passing.
`Ssh_Console.exe`	SSH terminal console.
`IPCamera.exe`	IP camera viewer.

3.4 External parameter file (optional)

Through the external parameter mechanism of the AlbatrosCommon library (text file with lines `Var_<nome>=<valore>`, see the example `Data\Ssh_Tunnel_Merge.txt` in the source code) you can set:

Parameter	Effect	Default
`PathDbSSH_Tunnel`	Database folder	Executable folder
`FileNameDbSSH_Tunnel`	Database file name	Derived from the exe name
`DoNotUseLogSSH_Tunnel`	If `True`, disables logging to the database and saving of the last profile/server used	`False`

3.5 Optional components in the folder

If these files are present in the program folder, Ssh_Tunnel recognizes them:

- `Ssh_Updater.exe`: started automatically when the login screen opens (program update).
- `Database4.exe` or `Database5Pro.exe`, `DbMigration.exe`, `Convert.exe`: appear in the **FishCodeLib** menu (DB management, migration, conversion).

4. Startup and login

4.1 The login screen

When you start the executable, the **Password** screen appears. The title shows the current time.

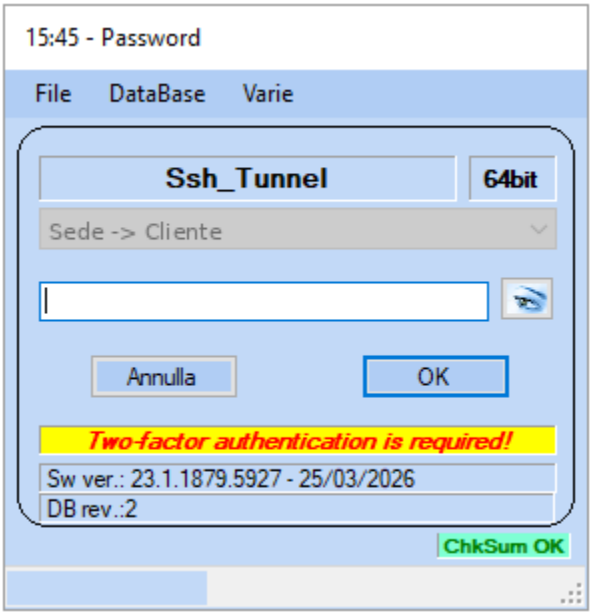

Figure 1 – Login screen with two-step verification request

Element	Function
Program name and «64bit/32bit»	Indicates the version running.
Profile list	Profiles in the database. If there is only one, it is locked; if there are several, the last one used is proposed.
Password field and «eye» button	Entry of the login password; the eye shows/hides the characters.
Annulla / OK	Closes the program / confirms the password. (Annulla = Cancel)
Status line	PC authorization status (see the following table).
Sw ver. / DB rev.	Version of the program, of the certificate and of the database.
ChkSum OK	Integrity check of the executable: if it is missing or reports an error, do not continue.

The status line can show:

Message	Meaning
«Two-factor authentication is required!» (yellow/red)	The PC is not authorized: after the password, two-step verification will be requested.
«One Day Code is active!» (yellow)	The PC is authorized until midnight today.
«Persistent Code is active!» (green)	The PC is permanently authorized.

4.2 Entering the password

1. Select the profile (if there is more than one).
2. Type the login password and press **OK**.
3. If the password is correct, the certificate is decrypted; if verification is required, the two-step verification screen opens (chapter 5), otherwise the main window.

> **Caution**
>
> After **3 wrong passwords** the program closes.
>
> If Ssh_Tunnel is already running, you are asked whether to open a new instance; if you answer No, the instance already open is brought to the foreground.

4.3 Login screen menu

Menu	Item	Function
File	Esci	Closes the program.
DataBase	Gestione Log › Abilita Log	Visible only if the log is disabled by a parameter: re-enables it for the session.
	Gestione Log › Mostra Log	View the log (chapter 13).
	Gestione Log › Invia Log via Mail	Send the log as an attachment (chapter 13).
	Utility › Compatta Database	Runs VACUUM on the SQLite database.
	Utility › Open Ssh_Tunnel DB path	Opens the database folder in File Explorer (the full path is in the item's tooltip).
	Utility › Importa Certificato Ssh Tunnel	Import of a `.Ssh_T` file (section 4.4).
	FishCodeLib	External tools, if present (section 3.5).
Varie	Abilita Accesso con Doppio Passaggio	Revokes the authorization stored for the profile on this PC (section 5.5).
	Apri come Putty	Starts the program in free SSH client mode (chapter 10).
	Scarica AlbatrosRDP	Saves `AlbatrosRDP.exe` to the user's Downloads folder and opens the folder.

4.4 Importing a certificate

A new profile is added by importing the `.Ssh_T` certificate file received from the administrator.

1. From the login screen, choose **DataBase › Utility › Importa Certificato Ssh Tunnel** (Import Ssh Tunnel certificate).
2. Drag the `.Ssh_T` file onto the indicated area, or double-click the area to select the file.
3. Enter the certificate password.
4. The program shows the name and owner and asks for confirmation; if a profile with the same name already exists, it asks whether to replace it.
5. When finished, the new profile appears in the list on the login screen.

Note

If the password is wrong, the program replies «Pwd errata» (Wrong password) and nothing is imported. The certificate is saved in the database still encrypted: the password is not stored.

5. Two-step verification (PC authorization)

5.1 When it is required

Two-step verification is triggered only if the certificate contains at least one e-mail address for the codes and the PC in use is not already authorized for that profile. The authorization is tied to the computer's hardware identifier (CPU ID or, if not available, the serial number of the motherboard or disk), so copying the program to another PC requires a new authorization.

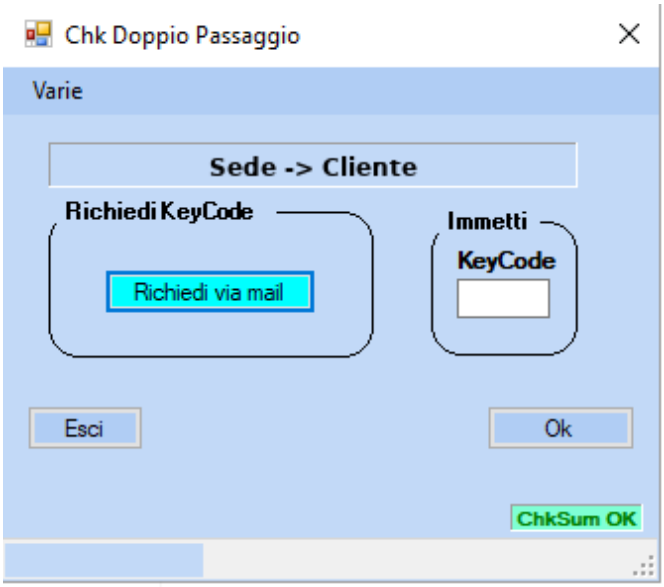

Figure 2 – «Chk Doppio Passaggio» screen

5.2 Requesting the codes

1. Press **Richiedi via mail** (Request by e-mail). The program generates three random 5-digit codes and sends them to the addresses specified in the certificate.
2. Wait for the e-mail; the text «Codici inviati» (Codes sent) appears.
3. Enter one of the codes received in the **KeyCode** field and press **Ok**.

The codes are generated when the screen opens and remain valid only while it is open: if you close the program, you must request new ones. Each e-mail also contains the identification data of the requesting PC (local and public IP, PC name, serial numbers of disk, CPU and motherboard).

Recipients of the codes, based on the addresses configured in the certificate:

Address in the certificate	Codes received
Main e-mail (`Mail`)	Persistent, OneDay and OneTime
OneDay e-mail (`MailOneDay`)	OneDay and OneTime
OneTime e-mail (`MailTemp`)	OneTime only

If two addresses are the same, the e-mail is not duplicated. In this way the permanent code can be reserved for the administrator, while the customer receives only the temporary codes.

5.3 Authorization levels

Code	Effect	Expiry
Persistent	The PC remains authorized for the profile; the code is no longer requested on subsequent startups.	None (until revoked)

Code	Effect	Expiry
OneDay	The PC is authorized for the whole day.	Midnight of the current day
OneTime	Authorizes only the current session; a new code is needed when the program is reopened.	Program closing, and in any case midnight

> **Caution**
>
> With the OneDay and OneTime codes, the main window shows «Ssh Tunnel: disattivazione alle 00.00» (Ssh Tunnel: deactivation at 00:00): at midnight the warning «Ssh Tunnel arrestato per scadenza password...» (Ssh Tunnel stopped because the password has expired...) appears and the program closes, also closing any open cameras.
>
> After **3 wrong codes** the screen closes. If no code is entered within **5 minutes**, the program closes automatically (with a 10-second countdown).

5.4 «Varie» menu of the two-step verification

Item	Function
Mostra Chk Mail Persistente	Makes the «Invia solo alla Mail Principale» (Send only to the main e-mail) option visible: if enabled, the codes are sent only to the address that receives the Persistent code.
Aggiorna Timer	Restarts the 5-minute wait.
Invia Codice via SMS al Supporto	Sends the three codes by SMS to the support number preset in the program (useful if e-mail does not work).

5.5 Revoking the authorization

To remove the Persistent or OneDay authorization from a PC: on the login screen, select the profile and choose **Varie › Abilita Accesso con Doppio Passaggio**, then confirm. The code will be requested again at the next login. The item is active only when the PC is already authorized.

> **Note**
>
> The authorization is saved, encrypted, in the Windows registry of the current user: `HKEY_CURRENT_USER\Software\Albatros.net`, value `Ssh_Tunnel_<Profilo>`. It is therefore valid for the Windows user who obtained it.

6. The main window

6.1 Overview

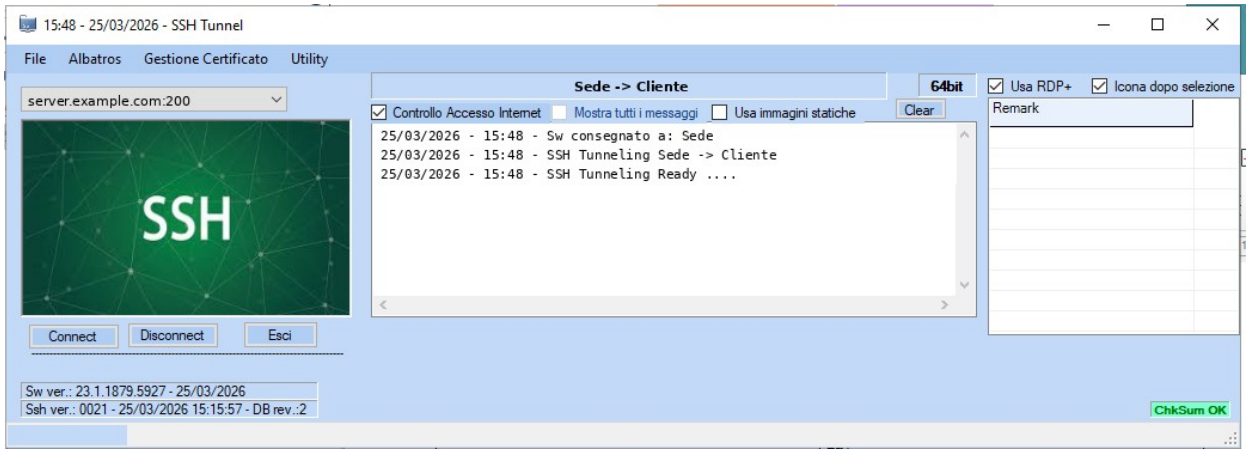

Figure 3 – Main window before connecting

Area	Content
Top left	List of available SSH servers (visible if there is more than one or if the certificate allows editing it).
Status image	SSH logo when idle; animation of successful or interrupted connection during use.
Buttons	**Connetti** (Connect), **Disconnetti** (Disconnect), **Esci** (Exit) and, if there are several profiles in the database, **Riavvia** (Restart: returns to the login screen to change profile).
Central panel	Message panel with date and time. Error lines are in red; those containing «###» have a yellow background.
List on the right	Reachable computers (Remark column), filled in after connecting.
Status bar	Software and certificate version, DB revision, «ChkSum OK».

6.2 Options

Option	Effect
Chk Internet	Before connecting, checks that the Internet is reachable; if it is not, waits until the connection is available again. Enabled by default.
Mostra tutti i messaggi	Also shows the port forwarding details (local and remote IPs and ports) in the message panel. Not available for «locked» certificates.
Usa immagini statiche	Replaces the status animations with static images.
Icona dopo selezione	Display option for the computer list.
RDP+ / AlbatrosRDP / MS RDP / Old RDP+	Chooses the client used for remote desktop connections (section 7.3). Default: MS RDP.
Clear	Clears the message panel and shows the certificate information again.

6.3 Main window menu

Menu	Item	Function
File	Esci	Disconnects, cleans up temporary files and closes the program.
Albatros	Parametri	Albatros redirection / DbKey (chapter 12).
	FishCodeLib	External tools (if present and if the certificate is not locked).
Gestione Certificato	Aggiorna modifiche	Saves modified servers and forwardings in the certificate (section 11.1).
	Cambio Password / Port FF	Changes the login password.
	Cambio Pwd Intermedia / Port FF	Changes the intermediate password.
	Export Certificato	Exports the certificate to a `.Ssh_T` file.
	Elimina Certificato	Removes the profile from the database.
	Apri percorso DB Ssh_Tunnel	Opens the database folder.
Utility	Ping No-IP	Resolves the selected server's name via DNS and shows its IP.
	Ping IP	Pings the server, if specified as an IP address.
	Scarica AlbatrosRDP	Saves `AlbatrosRDP.exe` to the Downloads folder.

In «Apri come Putty» mode the Albatros and Gestione Certificato menus are not available.

7. Connection and remote sessions

7.1 Connecting to the SSH server

1. Check that the message panel shows **SSH Tunneling Ready ....**
2. If the server list is visible, choose the server: under normal conditions the first one is sufficient; the others are alternative access points to use if the main server does not respond (some work only from inside the company network).
3. Press **Connetti**.

The message panel shows the sequence of operations:

```
Disconnected
Testing Internet connection status
Connecting...
Server: <nome server>
port: 200
Connecting to <nome server>:200
CONNECTED
S.O. <sistema operativo del server>
```

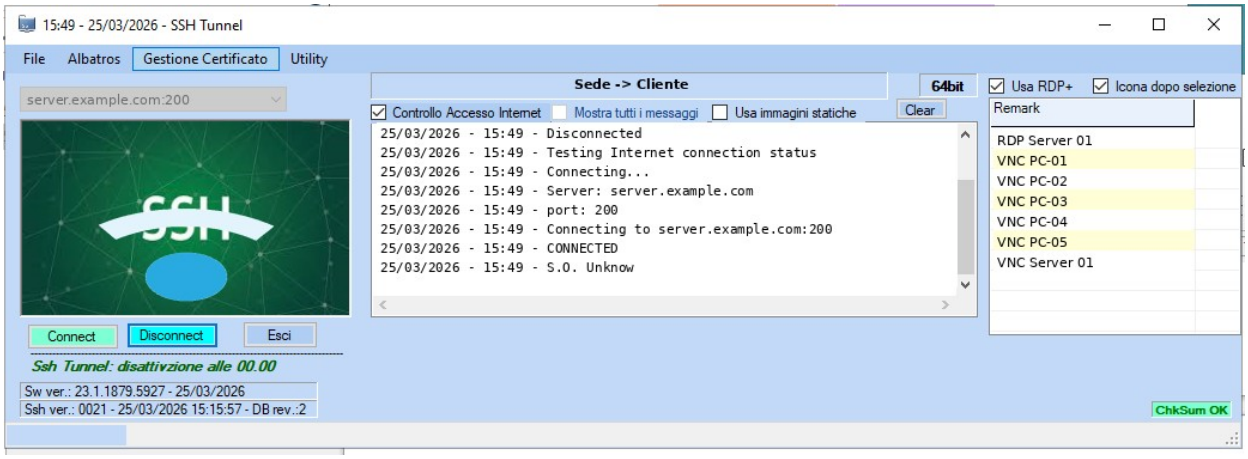

Figure 4 – Connection established: the list of reachable computers on the right

Operating details:

- The server can be specified as `host:porta`; without a port, the one in the certificate is used and, if none, **200**. Text after an apostrophe (`'`) is treated as a comment.
- Authentication uses the SSH credentials contained in the certificate and, if present, the private key.
- After connecting, the program detects the server's operating system (`ver` command for Windows, `lsb_release -d` for Linux).
- The chosen server is remembered for the profile and proposed again at the next startup.
- If the connection drops, the program reports it («Connection Lost») and tries to reconnect automatically until you press **Disconnetti**.
- If the certificate provides only one server, the window is minimized at startup and, if the certificate enables the RDP button, the connection starts automatically.

7.2 Opening a session on a remote PC

1. Once connected, **double-click** the desired computer in the list on the right.
2. If an intermediate password is required, a window with the connection name appears: enter it and press **OK**.
3. The remote session opens and the Ssh_Tunnel window is minimized.

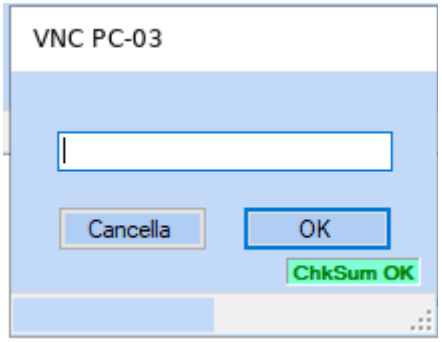

Figure 5 – Intermediate password request for a connection

Caution

After **3 wrong intermediate passwords** the program disconnects and closes («Superato il limite di tentativi ammessi», Maximum number of attempts exceeded).

Note

If the certificate provides an access notification e-mail, each time an RDP or VNC session is opened an e-mail is sent with the subject «SSh_Tunnel di <proprietario> su <connessione>» and the data of the PC from which the connection was made.

7.3 Connection types

The session type depends on the configuration of the entry in the certificate:

Type	Program used	Notes
Remote desktop (RDP)	Client chosen with the RDP options	Default type for entries with an RDP file.
VNC	`vncviewer.exe` (shared session)	The remote PC's password, if present in the certificate, is passed automatically. With a PC that is logged off, Windows credentials may be needed.
Terminal	`Ssh_Console.exe`	SSH console to the specified host.
Camera	`IPCamera.exe`	The windows are tiled automatically on the screen; recordings go to `C:\SDT_Cam_Recorder\`. Reopening the same camera closes the previous window.

Remote desktop clients:

Option	Behavior
MS RDP	Uses Windows `mstsc.exe` with a temporary .rdp file. The remote PC's password is not passed.
RDP+	Uses the embedded RDP+ client in full screen, with redirected drives and printers; the remote PC's password is encrypted with gencrypt and passed automatically.
Old RDP+	Like RDP+, but passes the password as it is (for passwords already encrypted in the certificate).
AlbatrosRDP	Uses the proprietary AlbatrosRDP client: the parameters are passed encrypted and the password through a private channel (named pipe), without appearing on the command line.

7.4 RDP/VNC/Term button

If the certificate provides for it, the **RDP/VNC/Term** button appears while the connection is active; it directly opens the «static» connection defined in the certificate without going through the list. With the certificate's AutoRDP option, this connection opens by itself immediately after connecting.

7.5 Disconnecting and exiting

- **Disconnetti**: closes all forwardings, cameras and the SSH connection; stops the reconnection attempts.
- **Esci** (or closing the window): disconnects, deletes the temporary files and closes the program.
- **Riavvia**: like Esci, but returns to the login screen to choose another profile.

8. Managing port forwardings

This part is available only if the certificate allows the forwardings to be modified (`AllowsNewForwards` permission) or in «Apri come Putty» mode. In that case the main window is taller and shows the editing section below the buttons.

8.1 Enabling editing

1. Select **Accedi a Port Forwarding** (Access port forwarding): the intermediate password is requested.
2. With the correct password, the editing section becomes editable and the forwarding list allows multiple selection and export to Excel.

8.2 Fields of a forwarding

Field	Meaning
Host Locale / Porta	Address and port on which the program listens on the local PC (e.g. 127.0.0.2:3390). The `*` button next to the host enters 127.0.0.2.
Host Remoto / Porta	Destination host and port, as seen from the SSH server (e.g. 192.168.1.10:3389).
Nota (Remark)	Name that appears in the computer list. Required.
Pwd	Password of the remote PC, passed to VNC or RDP+. The eye button shows it; **RDP Crypt** encrypts it with gencrypt for RDP+.
RDP	Content of the connection file. The three `*` buttons generate a template: complete .rdp file, VNC line, terminal line.

Templates generated by the buttons:

- RDP: standard .rdp file with `full address` and `server port` set to the local host and port, full screen, clipboard, printers and drives redirected.
- VNC: `vnc_config /connect <host>:<porta> /autoacceptnodsm /shared /autoscaling`.
- Terminal: `term_config server=<host> port=<porta> login= password= ppkkeyfilename= ppkkey= ppkkeypwd=` (to be completed).

In the content you can use the placeholders `##host##` and `##port##`, which are replaced when the connection is opened with the local host and port of the forwarding. An entry appears in the computer list only if it is checked and has the RDP field filled in; entries without an RDP file only create the tunnel.

8.3 Operations on the list

Command	Effect
Click a row	Loads the entry into the fields for editing.
`<==`	Inserts the entry into the list or updates the selected one (requests the intermediate password again). All fields except RDP and Pwd are required.
Pulisci	Clears the fields.
Tutti i Tag / Inverti Tag	Checks all entries / inverts the check marks. Only checked entries are activated.
Predefinito	Restores the list as it was at the last save of the certificate.

If the specified local port is already used by another entry, the program offers to automatically search for the first free port.

Caution

Changes take effect at the **next connection** (the warning «Modifiche attive alla prossima connessione», Changes active at the next connection, appears).

To make them permanent, you must save them in the certificate with **Gestione Certificato › Aggiorna modifiche**; otherwise they are lost when the program closes.

9. Managing SSH servers

If the certificate allows the servers to be modified (`AllowServerIpEditing` permission), the server list becomes editable and a panel of commands appears:

Command	Effect
Aggiungi	Adds the typed text to the list (format `host:porta`).
Elimina	Removes the typed/selected entry (at least one must remain).
+ / -	Move the selected entry within the list.
R	Replaces the text of the last selected entry with the typed text.

These changes must also be saved with **Gestione Certificato › Aggiorna modifiche**. While connected, the server list is locked.

10. «Apri come Putty» mode

From the login screen, **Varie › Apri come Putty** (Open as Putty) opens the main window without a certificate, as a generic SSH client. The following fields appear:

Field	Use
Hostname / Porta	SSH server (default port 22).
Nome utente / Password	SSH credentials.
KeyFile / Pwd KeyFile	Private key (`.ppk`, `.OpenSsh`, `.pri`) and its passphrase; the `....` button opens the file selection.
Timeout (sec.)	Connection timeout and keep-alive interval (default 3).

Forwardings are defined as described in chapter 8 and apply only to the session: in this mode there is no certificate in which to save them.

11. Certificate management

All items of the **Gestione Certificato** (Certificate management) menu first ask for confirmation if a connection is active (it will be closed) and then for the current password. When finished, the program closes with the message «Aggiornamento Effettuato: Rientrare nel programma» (Update completed: restart the program).

11.1 Aggiorna modifiche

(Save changes.) Rebuilds the certificate with the current list of servers and forwardings (including check marks and passwords) and saves it in the database with the same password. At each save, the certificate version number (`Ssh ver.`) increases.

11.2 Cambio Password

(Change password.) After the current password, enter the new password twice; it must meet these requirements:

- at least 8 characters;
- at least 1 lowercase and 2 uppercase letters;
- at least 1 number;
- at least 2 special characters.

The certificate is re-encrypted with the new password. If the password is the same as the previous one, the certificate is updated anyway.

11.3 Cambio Password Intermedia

(Change intermediate password.) Sets the password requested when opening remote sessions. There are no complexity requirements.

11.4 Export Certificato

(Export certificate.) Exports the certificate to `C:\Ssh_Tunnel_Certificates\<Profilo>.Ssh_T`, encrypted with the password specified during the export, ready to be delivered and imported on another PC (section 4.4).

The export requires an **authorization password**, which can be obtained in two ways:

- by pressing the send-code button: a random code is sent to the access notification e-mail (or, if none, to the main e-mail);
- with the administrative password reserved for the developer, valid only on PCs with Persistent authorization.

After authorization, you choose the password with which to encrypt the exported file.

11.5 Elimina Certificato

(Delete certificate.) After the current password, the profile is deleted from the database. If other profiles remain in the database, the program returns to the login screen; otherwise it closes.

12. Albatros redirection (DbKey)

The **Albatros › Parametri** item opens the **Reindirizza Albatros** (Redirect Albatros) screen, designed for integration with the Albatros applications: when the tunnel to a site is opened, the applications can be automatically directed to that site's database.

The upper part lists the configurations in the Albatros environment (key, local DB and note, remote DB and note, ping IP), as a reference for choosing the key. The lower part contains the profile settings:

Field	Meaning
Abilitato	Enables the function for the profile.
Alla Connessione	DbKey to set when the SSH connection succeeds.
Alla Disconn.	DbKey to set on disconnection.
Percorso file txt DbKey	Folder in which to write the `_DbKey.txt` file (Predefinito button: `C:\ProgramData\Albatros\Common\`).
Nota Connessione / Nota Disconnessione	Text written to the message panel and the log when the key is applied.

Pressing **Registra** (Save) saves the settings in the Albatros environment with keys such as `[<Profilo>]_DbKeyEnabled`, `[<Profilo>]_DbKeyAtConnection` etc., and applies them immediately according to the connection state. On connection or disconnection, the program writes `DbKey=<valore>` to the `_DbKey.txt` file and notes it in the message panel.

13. Log and database maintenance

13.1 Message panel and log

Every line shown in the message panel is also recorded in the Log table of the database, together with the process (session) identifier and, on the first write, the PC's hardware information. The log can be disabled with the `DoNotUseLogSSH_Tunnel` parameter.

13.2 Mostra Log

From the login screen, **DataBase › Gestione Log › Mostra Log** (Show log): specify the date range (from date / to date) and press **Ricerca** (Search). Session, date, time, PC information and message are shown.

13.3 Invia Log via Mail

DataBase › Gestione Log › Invia Log via Mail (Send log by e-mail): specify the date range and destination address and press **Invia** (Send). The log for the period is exported to Excel, compressed into a zip file and sent; the temporary files are then deleted.

13.4 Maintenance

- **Compatta Database** (Compact database): recovers the free space in the file (VACUUM). It is also run automatically each time the certificate is saved.
- **Open Ssh_Tunnel DB path**: opens the database folder, useful for backups.

13.5 Database structure

The database is a password-protected SQLite file, at revision 2. At startup, the program creates any missing tables and automatically upgrades revision 1 databases.

Table	Content
Parameters	Key/value pairs: `DbVersion`, `login` (last profile used), `[<Profilo>]_IP` (last server used).
Certificati	Proprietario, Profilo, Version, VersionDate, Certificato (encrypted text).
Licenza	KeyLicenza, Assegnatario, DataAssegnazione, CertificatoLicenza (prepared, currently not used).
Log	IdSession, DataLog, PcInfo, KeyInfo, Info.

14. Security

- **Encrypted certificate**: every sensitive value is encrypted with Triple DES using a key derived from the login password; the certificate as a whole is in turn encrypted. The password is never saved.
- **No visible credentials**: SSH credentials, private key and remote PC passwords stay inside the program and are passed directly to the clients.
- **Hardware binding**: two-step verification authorizations are valid only for the PC and the Windows user on which they were obtained.
- **Attempt limit**: 3 attempts for the login password, for the two-step verification codes and for the intermediate password.
- **Expiry at midnight** for OneDay and OneTime authorizations.
- **Traceability**: e-mail with the PC data at every code request and every RDP/VNC access, local session log, access logging on the SSH server.
- **Cleanup**: auxiliary programs and temporary .rdp files are deleted at startup and on exit.
- **Integrity**: the «ChkSum OK» indicator shows that the executable has not been tampered with.

> **Note**
>
> The intermediate password is not a true cryptographic protection: it serves to prevent use of the program when it is left open and unattended.

15. Messages and troubleshooting

Message / symptom	Cause and remedy
«Password errata: impossibile continuare»	(Wrong password: cannot continue.) Wrong login password or wrong profile. After 3 errors the program closes.
«Certificato inesistente»	(Certificate not found.) The selected profile is not in the database: import the certificate.
«Two-factor authentication is required!»	PC not authorized: follow chapter 5.
«Invio mail ... per doppia verifica fallito!!!»	(Sending two-step verification e-mail ... failed.) E-mail sending problem (network, firewall, SMTP). Try again or use «Invia Codice via SMS al Supporto».
«Codice errato: Tentativi n di 3»	(Wrong code: attempt n of 3.) Code typed incorrectly or from a previous request.
«Chiusura automatica per mancato input codice»	(Automatic closing because no code was entered.) The 5 minutes elapsed without the code being entered.
«Internet Connection Not Available» / «Waiting ...»	No Internet connection; the program waits. Clear «Chk Internet» to skip the check.
«Errore login!!!»	(Login error.) Unable to prepare the connection (invalid credentials or certificate key). Contact the administrator.
Connection not established	Server unreachable: try an alternative server from the list; use Utility › Ping No-IP to check name resolution.
«### Error Forward Host: ...»	The local port of the forwarding is in use by another program or the local host is not valid.
«Connection Lost»	Connection dropped: the program reconnects by itself.
«Password errata» / «Superato il limite di tentativi ammessi»	(Wrong password / Maximum number of attempts exceeded.) Wrong intermediate password; at the third error the program closes.
«Ssh Tunnel arrestato per scadenza password...»	Midnight reached with OneDay/OneTime authorization: restart and request a new code.
«Riscontrata anomalia tra la versione attesa e quella trovata nel Database di servizio»	The database cannot be updated: move the program to a folder with write permissions.
«Operazione annullata per password difforme»	(Operation canceled: password does not match.) Wrong current password in the Gestione Certificato functions.
«Porta già utilizzata: Cerco la prima occorrenza libera?»	(Port already in use: search for the first free one?) Local port already assigned to another forwarding.
«Dati Insufficienti!»	(Insufficient data.) Required fields are missing when entering a forwarding.

Appendix A – Quick summary for the user

1. Copy the `.exe` and `.db` files into the same folder.
2. Start the executable and enter the login password.
3. If requested, press «Richiedi via mail» and enter the OneDay or OneTime code received.
4. Wait for «SSH Tunneling Ready ....» and press **Connetti**.
5. Double-click the desired computer in the list on the right.
6. Enter the intermediate password, if requested.
7. Work on the remote PC; when finished, press **Disconnetti** or **Esci**.

Appendix B – Certificate structure

The certificate (version 2) is a text made of `Chiave = "valore"` lines, encrypted as a whole with the password. Sensitive values are in turn individually encrypted. List of recognized keys:

Key	Content
`Algoritmo`	Version of the encryption algorithm (1).
`Nominativo`	Profile name (plain text).
`SshUserDllVersion`	Sequence number and date of the last save.
`Bloccato`	Certificate with reduced functions (no details in the message panel, no external tools).
`ShowRdpButton`	Shows the RDP/VNC/Term button for the static connection.
`AutoRDP`	Opens the static connection immediately after connecting.
`AllowsNewForwards`	Allows the port forwardings to be modified.
`AllowServerIpEditing`	Allows the server list to be modified.
`Proprietario`	Recipient of the software («Sw consegnato a»).
`Login`, `Password`	SSH credentials.
`Certificate`, `CertificatePassword`, `FileCertificato`	SSH private key (text or embedded resource) and its passphrase.
`PwdRemoteAccess`	Intermediate password.
`Server`, `ServerPort`	List of servers separated by `&` and default port.
`RdpCommandLine`, `RdpFileStatico`	Command line and file of the static connection.
`Mail`, `MailOneDay`, `MailTemp`	Recipients of the two-step verification codes.
`MailInfoAccess`	Recipient of the access notifications.
`Cellulare`	Mobile phone number (prepared).
`RedirectPortsCount`	Number of forwardings.
`RedirectPorts(i, …)`	For each forwarding: LocalHost, LocalPort, RemoteHost, RemotePort, Remark, RdpFile, Enabled (Y/N), PasswordRdpFF, PwdActivateRdpConnection.

Appendix C – Technical notes for the developer

While writing the manual, some points to be checked emerged in the code. This appendix is for internal use: it must be removed before the manual is given to the program's recipients.

File / routine	Remark
ModSetting.Log	Checks that the database exists in `Application.StartupPath` with the exe name, ignoring `PathDbSSH_Tunnel` and `FileNameDbSSH_Tunnel`: if the DB is elsewhere or has another name, the log is not written.
ModSetting.RemoveParam	The query uses `lower('?')`: the parameter between quotes is not substituted, so the deletion has no effect.
ModSetting.DecodCertificate	The comparison `ToLower.Contains("Algoritmo =")` contains an uppercase letter and is never true: the `Algoritmo` value is not read (currently without consequences, it is always 1).
FrmStart_Load	`ContaErrori` is local to the loop and is reset at each iteration; moreover, if the two-step verification fails or the screen is closed, `Exit Sub` does not terminate the application: check that no process remains running without a window.
frmMainProgram, server `+` / `-` buttons	The tooltips are swapped: `-` (tooltip «Sposta Giù», Move down) moves up, `+` (tooltip «Sposta Su», Move up) moves down.
frmMainProgram, template buttons `*`	The tooltip says `###Host### / ###Port###`, but the placeholders replaced by the code are `##host##` / `##port##`.
EseguiExportCertificato	The «supercode» enables saving the password to a `.Ssh_T.Key` file, but `CostruisciRemPwdInfo` and `abilitaSalvataggioPwd` are not used: the function is not implemented.
ChkIconaAfterSelection	The «Icona dopo selezione» option is not referenced in the code.
GetParam / SetParam	The key is concatenated into the SQL query instead of being passed as a parameter.
Source code in general	Credentials and keys are present in plain text in the source code (SMS service, SFTP access for updates, DB password, hash of the administrative password). Anyone with access to the executable can extract them with a .NET decompiler: consider obfuscation or moving them to the server side.

Ssh_Tunnel

Client SSH pour des accès à distance contrôlés

Manuel d'utilisation et d'administration

Version du logiciel 27.2.2036.6127 · rév. BD 2

© Raffaele Romano
Octobre 2026

Sommaire

1. Introduction....34
1.1 À qui s'adresse ce manuel....34
1.2 Version documentée....34

2. Concepts fondamentaux....35

3. Installation et configuration requise....36
3.1 Fichiers nécessaires....36
3.2 Configuration requise....36
3.3 Programmes intégrés....36
3.4 Fichier de paramètres externe (facultatif)....37
3.5 Composants facultatifs dans le dossier....37

4. Démarrage et connexion....38
4.1 La fenêtre de connexion....38
4.2 Saisie du mot de passe....39
4.3 Menus de la fenêtre de connexion....39
4.4 Importation d'un certificat....39

5. Double vérification (autorisation du PC)....41
5.1 Quand est-elle demandée....41
5.2 Demande des codes....41
5.3 Niveaux d'autorisation....42
5.4 Menu « Varie » de la double vérification....42
5.5 Révocation de l'autorisation....42

6. La fenêtre principale....43
6.1 Vue d'ensemble....43
6.2 Options....43
6.3 Menus de la fenêtre principale....44

7. Connexion et sessions à distance....45
7.1 Connexion au serveur SSH....45
7.2 Ouverture d'une session sur un PC distant....45
7.3 Types de connexion....46
7.4 Bouton RDP/VNC/Term....47
7.5 Déconnexion et sortie....47

8. Gestion des redirections de port....48
8.1 Activer la modification....48
8.2 Champs d'une redirection....48
8.3 Opérations sur la liste....48

9. Gestion des serveurs SSH....50

10. Mode « Apri come Putty »....51

11. Gestion du certificat....52
11.1 Aggiorna modifiche....52
11.2 Cambio Password....52
11.3 Cambio Password Intermedia....52
11.4 Export Certificato....52
11.5 Elimina Certificato....52

12. Redirection Albatros (DbKey)....53

13. Journal et maintenance de la base de données.....54
13.1 Registre et journal.....54
13.2 Mostra Log.....54
13.3 Invia Log via Mail.....54
13.4 Maintenance.....54
13.5 Structure de la base de données.....54
14. Sécurité.....55
15. Messages et dépannage.....56
Annexe A – Récapitulatif rapide pour l'utilisateur.....57
Annexe B – Structure du certificat.....58
Annexe C – Notes techniques pour le développeur.....59

1. Introduction

Ssh_Tunnel est un client SSH pour Windows, développé en VB.NET, qui permet d'atteindre de manière contrôlée les PC et serveurs d'un réseau d'entreprise (via RDP, VNC, terminal SSH ou caméras IP) à travers un tunnel chiffré vers un serveur SSH de l'entreprise.

Il est né comme alternative à des outils tels que TeamViewer, AnyDesk et similaires : ceux-ci garantissent un trafic chiffré, mais quiconque possède les identifiants peut accéder aux systèmes, ce qui fait dépendre la sécurité du réseau de tiers. Ssh_Tunnel, au contraire :

- ne contient aucun mot de passe en clair : tous les paramètres de connexion sont enfermés dans un **certificat chiffré**, qui ne peut être ouvert qu'avec le mot de passe d'accès remis à l'utilisateur ;
- attribue à chaque destinataire (centre d'assistance, technicien, consultant) un **certificat unique**, de sorte que le serveur SSH reconnaisse qui se connecte et en enregistre la date, l'heure et la durée ;
- peut lier l'utilisation à un PC précis grâce à une **double vérification** (code envoyé par e-mail), avec une autorisation permanente, journalière ou pour la seule session ;
- notifie par e-mail chaque accès à un PC distant, en indiquant depuis quel ordinateur la connexion a eu lieu ;
- présente à l'utilisateur uniquement les connexions prévues par son certificat, sous la forme d'une liste d'ordinateurs sur lesquels double-cliquer.

1.1 À qui s'adresse ce manuel

Le manuel est divisé en trois parties :

- **Utilisation quotidienne** (chapitres 3–7) : installation, connexion, double vérification, connexion et ouverture des sessions à distance. C'est la partie à remettre à la personne qui reçoit le programme.
- **Administration** (chapitres 8–13) : gestion des redirections de port, des serveurs, des certificats, de la redirection Albatros, des journaux et de la base de données.
- **Référence technique** (chapitres 14–15 et annexes) : architecture, sécurité, structure du certificat, messages et dépannage.

1.2 Version documentée

Élément	Valeur
Programme	Ssh_Tunnel
Version du logiciel	27.2.2036.6127 (date de build 11/10/2026)
Révision de la base de données	2
Version du certificat	2 (Algorithme = 1)
Plateforme	.NET Framework 4.8, Windows, compilations 32 et 64 bits
Bibliothèques principales	Renci SSH.NET 2025, System.Data.SQLite, AlbatrosCommon
Langues de l'interface	Italien, anglais, français, japonais, roumain (choix automatique selon la langue de Windows)

La version affichée par le programme a la forme `Sw ver.: 27.2.2036.6127 - 11/10/2026` : la date est déduite du numéro de révision (jours écoulés depuis le 01/01/2010) et correspond donc à la date de compilation.

2. Concepts fondamentaux

Avant d'utiliser le programme, il est utile de connaître quelques termes qui reviennent dans toutes les fenêtres.

Terme	Signification
Profil	Nom qui identifie un certificat (ex. « Sede -> Cliente »). Plusieurs profils peuvent coexister dans la même base de données ; au démarrage, vous choisissez celui à utiliser.
Certificat	Bloc chiffré qui contient tout ce qui est nécessaire à la connexion : serveur SSH et ports, identifiants SSH, clé privée, liste des redirections de port, fichiers RDP/VNC, adresses e-mail, autorisations. Il est distribué sous forme de fichier `.Ssh_T` et importé dans la base de données.
Mot de passe d'accès	Mot de passe demandé au démarrage. Il déchiffre le certificat : sans lui, le programme ne connaît ni les serveurs ni les identifiants.
Mot de passe intermédiaire (accès à distance)	Second mot de passe demandé au moment d'ouvrir une session sur un PC distant. Il sert à éviter qu'un programme laissé ouvert et sans surveillance soit utilisé par d'autres personnes.
Mot de passe spécifique de connexion	Mot de passe intermédiaire défini pour une seule entrée de la liste ; s'il est présent, il prévaut sur le mot de passe général.
Double vérification	Vérification supplémentaire : à la première utilisation sur un PC, un code est demandé par e-mail. L'autorisation est liée au matériel du PC.
Code Persistent / OneDay / OneTime	Les trois codes de la double vérification : autorisation permanente, valable jusqu'à minuit, valable pour la seule session (voir chapitre 5).
Redirection de port (tunnel)	Association « adresse et port locaux → hôte et port distants » établie à travers la connexion SSH. Chaque ordinateur accessible correspond à une redirection.
DbKey	Clé utilisée par les applications Albatros pour choisir la base de données de travail ; Ssh_Tunnel peut la modifier automatiquement à la connexion et à la déconnexion (chapitre 12).

3. Installation et configuration requise

3.1 Fichiers nécessaires

Ssh_Tunnel ne nécessite ni installation ni droits d'administrateur. Il suffit de copier dans le même dossier :

Fichier	Description
`Ssh_Tunnel_<Nome>.exe`	Exécutable du programme (le nom peut être personnalisé pour chaque destinataire ; il peut se terminer par 32 ou 64).
`Ssh_Tunnel_<Nome>.db`	Base de données SQLite chiffrée qui contient les certificats, les paramètres et le journal.

Le nom de la base de données est déduit du nom de l'exécutable, en retirant l'éventuel suffixe `32` ou `64` et en ajoutant `.db`. Exemple : `Ssh_Tunnel_Esempio64.exe` recherche `Ssh_Tunnel_Esempio.db`. Ainsi, la version 32 bits et la version 64 bits partagent la même base de données.

> **Remarque**
>
> Si la base de données n'existe pas, elle est créée vide au premier démarrage ; dans ce cas, il faut importer un certificat (section 4.4) avant de pouvoir se connecter.
>
> Si le message « Riscontrata anomalia tra la versione attesa e quella trovata nel Database di servizio » apparaît, déplacez le programme dans un dossier sans restrictions d'écriture (par exemple pas sous `C:\Program Files`).

3.2 Configuration requise

- Windows avec .NET Framework 4.8.
- Accès Internet sortant vers le serveur SSH de l'entreprise (le port par défaut est le 200, sauf indication contraire dans le certificat).
- Pour la double vérification et les notifications : possibilité d'envoyer des e-mails (le programme utilise les paramètres SMTP internes de la bibliothèque Albatros).

3.3 Programmes intégrés

L'exécutable contient les programmes auxiliaires, qui sont extraits uniquement en cas de besoin dans le dossier temporaire `%TEMP%\Albatros\Ssh_Tunnel` et supprimés au démarrage et à la sortie :

Composant	Utilisation
`vncviewer.exe` / `vncviewer32.exe`	Visionneuse VNC (version 64 ou 32 bits selon le processus).
`rdp.exe`	Client RDP+ (bureau à distance avec transmission automatique du mot de passe).
`gencrypt.exe`	Chiffrement des mots de passe pour RDP+.
`AlbatrosRDP.exe`	Client RDP propriétaire avec transmission sécurisée du mot de passe.
`Ssh_Console.exe`	Console de terminal SSH.
`IPCamera.exe`	Visionneuse de caméras IP.

3.4 Fichier de paramètres externe (facultatif)

Grâce au mécanisme des paramètres externes de la bibliothèque AlbatrosCommon (fichier texte avec des lignes `Var_<nome>=<valore>`, voir l'exemple `Data\Ssh_Tunnel_Merge.txt` dans les sources), il est possible de définir :

Paramètre	Effet	Par défaut
`PathDbSSH_Tunnel`	Dossier de la base de données	Dossier de l'exécutable
`FileNameDbSSH_Tunnel`	Nom du fichier de base de données	Dérivé du nom de l'exe
`DoNotUseLogSSH_Tunnel`	Si `True`, désactive le journal dans la base de données et l'enregistrement du dernier profil/serveur utilisé	`False`

3.5 Composants facultatifs dans le dossier

Si les fichiers suivants sont présents dans le dossier du programme, Ssh_Tunnel les reconnaît :

- `Ssh_Updater.exe` : est lancé automatiquement à l'ouverture de la fenêtre de connexion (mise à jour du programme).
- `Database4.exe` ou `Database5Pro.exe`, `DbMigration.exe`, `Convert.exe` : apparaissent dans le menu **FishCodeLib** (gestion de BD, migration, conversion).

4. Démarrage et connexion

4.1 La fenêtre de connexion

Au lancement de l'exécutable, la fenêtre **Password** apparaît. Le titre indique l'heure actuelle.

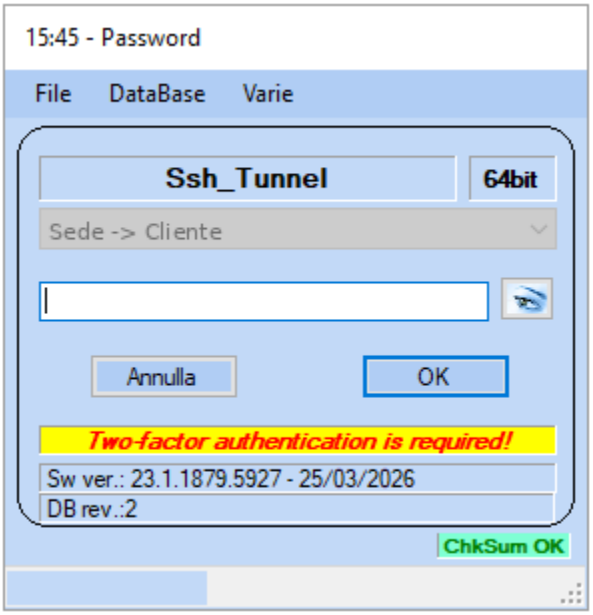

Figure 1 – Fenêtre de connexion avec demande de double vérification

Élément	Fonction
Nom du programme et « 64bit/32bit »	Indique la version en cours d'exécution.
Liste des profils	Profils présents dans la base de données. S'il n'y en a qu'un, il est verrouillé ; s'il y en a plusieurs, le dernier utilisé est proposé.
Champ du mot de passe et bouton « œil »	Saisie du mot de passe d'accès ; l'œil affiche/masque les caractères.
Annulla / OK	Ferme le programme / confirme le mot de passe.
Ligne d'état	État de l'autorisation du PC (voir le tableau suivant).
Sw ver. / DB rev.	Version du programme, du certificat et de la base de données.
ChkSum OK	Contrôle d'intégrité de l'exécutable : s'il est absent ou signale une erreur, ne continuez pas.

La ligne d'état peut afficher :

Message	Signification
« Two-factor authentication is required! » (jaune/rouge)	Le PC n'est pas autorisé : après le mot de passe, la double vérification sera demandée.
« One Day Code is active! » (jaune)	Le PC est autorisé jusqu'à minuit aujourd'hui.
« Persistent Code is active! » (vert)	Le PC est autorisé de façon permanente.

4.2 Saisie du mot de passe

1. Sélectionnez le profil (s'il y en a plusieurs).
2. Saisissez le mot de passe d'accès et appuyez sur **OK**.
3. Si le mot de passe est correct, le certificat est déchiffré ; si la vérification est prévue, la fenêtre de double vérification s'ouvre (chapitre 5), sinon la fenêtre principale.

> **Attention**
>
> Après **3 mots de passe erronés**, le programme se ferme.
>
> Si Ssh_Tunnel est déjà en cours d'exécution, il vous est demandé si vous voulez ouvrir une nouvelle instance ; si vous répondez No, l'instance déjà ouverte est mise au premier plan.

4.3 Menus de la fenêtre de connexion

Menu	Commande	Fonction
File	Esci	Ferme le programme.
DataBase	Gestione Log › Abilita Log	Visible uniquement si le journal est désactivé par paramètre : le réactive pour la session.
	Gestione Log › Mostra Log	Consultation du journal (chapitre 13).
	Gestione Log › Invia Log via Mail	Envoi du journal en pièce jointe (chapitre 13).
	Utility › Compatta Database	Exécute le VACUUM de la base de données SQLite.
	Utility › Open Ssh_Tunnel DB path	Ouvre dans l'Explorateur de fichiers le dossier de la base de données (le chemin complet figure dans l'info-bulle de la commande).
	Utility › Importa Certificato Ssh Tunnel	Importation d'un fichier `.Ssh_T` (section 4.4).
	FishCodeLib	Outils externes, s'ils sont présents (section 3.5).
Varie	Abilita Accesso con Doppio Passaggio	Révoque l'autorisation mémorisée pour le profil sur ce PC (section 5.5).
	Apri come Putty	Lance le programme en mode client SSH libre (chapitre 10).
	Scarica AlbatrosRDP	Enregistre `AlbatrosRDP.exe` dans le dossier Téléchargements de l'utilisateur et ouvre ce dossier.

4.4 Importation d'un certificat

Un nouveau profil s'ajoute en important le fichier de certificat `.Ssh_T` reçu de l'administrateur.

1. Dans la fenêtre de connexion, choisissez **DataBase › Utility › Importa Certificato Ssh Tunnel**.
2. Faites glisser le fichier `.Ssh_T` dans la zone indiquée, ou double-cliquez dessus pour le choisir.
3. Saisissez le mot de passe du certificat.
4. Le programme affiche le nom et le propriétaire et demande confirmation ; s'il existe déjà un profil portant le même nom, il demande s'il faut le remplacer.
5. À la fin, le nouveau profil apparaît dans la liste de la fenêtre de connexion.

Remarque

Si le mot de passe est erroné, le programme répond « Pwd errata » et rien n'est importé. Le certificat est enregistré dans la base de données toujours chiffré : le mot de passe n'est pas mémorisé.

5. Double vérification (autorisation du PC)

5.1 Quand est-elle demandée

La double vérification n'intervient que si le certificat contient au moins une adresse e-mail pour les codes et si le PC utilisé n'est pas déjà autorisé pour ce profil. L'autorisation est liée à l'identifiant matériel de l'ordinateur (ID du processeur ou, à défaut, numéro de série de la carte mère ou du disque) : copier le programme sur un autre PC nécessite donc une nouvelle autorisation.

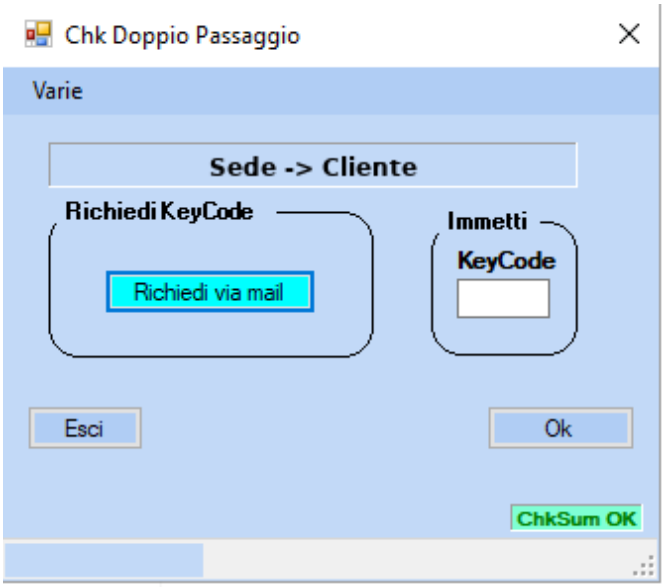

Figure 2 – Fenêtre « Chk Doppio Passaggio »

5.2 Demande des codes

1. Appuyez sur **Richiedi via mail**. Le programme génère trois codes aléatoires à 5 chiffres et les envoie aux adresses prévues par le certificat.
2. Attendez l'e-mail ; le texte « Codici inviati » apparaît.
3. Saisissez l'un des codes reçus dans le champ **KeyCode** et appuyez sur **Ok**.

Les codes sont générés à l'ouverture de la fenêtre et ne restent valables que tant qu'elle est ouverte : si vous fermez le programme, vous devez en demander de nouveaux. Chaque e-mail contient aussi les données d'identification du PC demandeur (IP locale et publique, nom du PC, numéros de série du disque, du processeur et de la carte mère).

Destinataires des codes, selon les adresses configurées dans le certificat :

Adresse dans le certificat	Codes reçus
E-mail principal (`Mail`)	Persistent, OneDay et OneTime
E-mail OneDay (`MailOneDay`)	OneDay et OneTime
E-mail OneTime (`MailTemp`)	OneTime uniquement

Si deux adresses coïncident, l'e-mail n'est pas envoyé en double. Ainsi, le code permanent peut être réservé à l'administrateur, tandis que le client ne reçoit que les codes temporaires.

5.3 Niveaux d'autorisation

Code	Effet	Expiration
Persistent	Le PC reste autorisé pour le profil ; aux ouvertures suivantes, le code n'est plus demandé.	Aucune (jusqu'à révocation)
OneDay	Le PC est autorisé pour toute la journée.	Minuit du jour en cours
OneTime	Autorise uniquement la session en cours ; à la réouverture, un nouveau code est nécessaire.	Fermeture du programme, et dans tous les cas minuit

> **Attention**
>
> Avec les codes OneDay et OneTime, la fenêtre principale affiche « Ssh Tunnel: disattivazione alle 00.00 » : à minuit, l'avertissement « Ssh Tunnel arrestato per scadenza password... » apparaît et le programme se ferme, en fermant aussi les caméras ouvertes.
>
> Après **3 codes erronés**, la fenêtre se ferme. Si aucun code n'est saisi dans les **5 minutes**, le programme se ferme automatiquement (avec un compte à rebours de 10 secondes).

5.4 Menu « Varie » de la double vérification

Commande	Fonction
Mostra Chk Mail Persistente	Rend visible l'option « Invia solo alla Mail Principale » : si elle est activée, les codes ne sont envoyés qu'à l'adresse qui reçoit le code Persistent.
Aggiorna Timer	Relance les 5 minutes d'attente.
Invia Codice via SMS al Supporto	Envoie les trois codes par SMS au numéro du support prédéfini dans le programme (utile si l'e-mail ne fonctionne pas).

5.5 Révocation de l'autorisation

Pour retirer à un PC l'autorisation Persistent ou OneDay : dans la fenêtre de connexion, sélectionnez le profil et choisissez **Varie › Abilita Accesso con Doppio Passaggio**, puis confirmez. Lors de la connexion suivante, le code sera de nouveau demandé. La commande n'est active que lorsque le PC est déjà autorisé.

> **Remarque**
>
> L'autorisation est enregistrée, chiffrée, dans le Registre Windows de l'utilisateur actuel : `HKEY_CURRENT_USER\Software\Albatros.net`, valeur `Ssh_Tunnel_<Profilo>`. Elle n'est donc valable que pour l'utilisateur Windows qui l'a obtenue.

6. La fenêtre principale

6.1 Vue d'ensemble

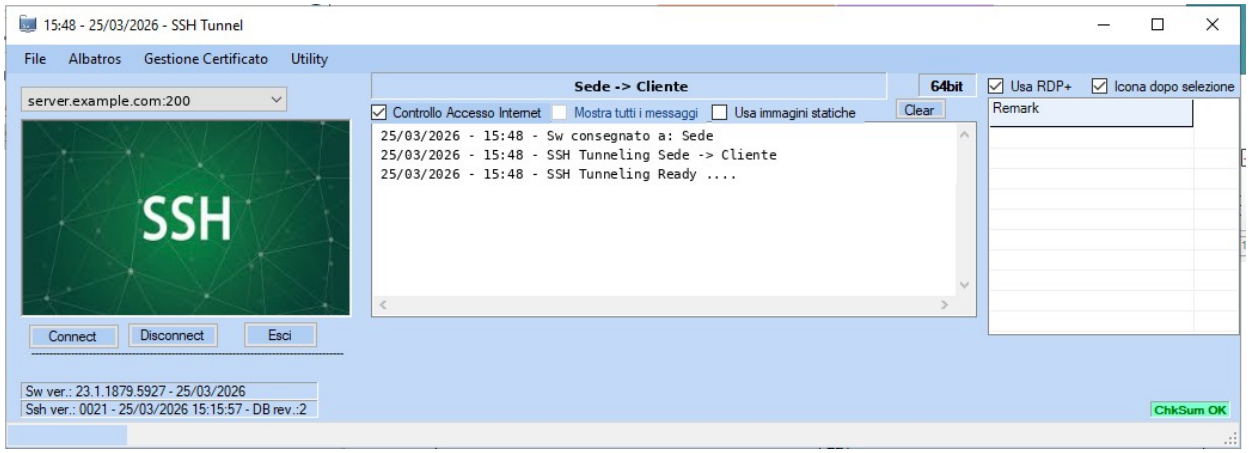

Figure 3 – Fenêtre principale avant la connexion

Zone	Contenu
En haut à gauche	Liste des serveurs SSH disponibles (visible s'il y en a plusieurs ou si le certificat en autorise la modification).
Image d'état	Logo SSH au repos ; animation de connexion réussie ou interrompue pendant l'utilisation.
Boutons	**Connetti**, **Disconnetti**, **Esci** et, si la base de données contient plusieurs profils, **Riavvia** (revient à la fenêtre de connexion pour changer de profil).
Panneau central	Registre des messages avec la date et l'heure. Les lignes d'erreur sont en rouge ; celles qui contiennent « ### » ont un fond jaune.
Liste à droite	Ordinateurs accessibles (colonne Remark), remplie après la connexion.
Barre d'état	Version du logiciel et du certificat, révision de la BD, « ChkSum OK ».

6.2 Options

Option	Effet
Chk Internet	Avant de se connecter, vérifie qu'Internet est accessible ; en cas d'absence, attend que la connexion redevienne disponible. Activée par défaut.
Mostra tutti i messaggi	Affiche aussi dans le registre les détails des redirections de port (IP et ports locaux et distants). Non disponible pour les certificats « bloqués ».
Usa immagini statiche	Remplace les animations d'état par des images fixes.
Icona dopo selezione	Option d'affichage de la liste des ordinateurs.
RDP+ / AlbatrosRDP / MS RDP / Old RDP+	Choisit le client utilisé pour les connexions Bureau à distance (section 7.3). Par défaut : MS RDP.
Clear	Vide le registre et réaffiche les informations du certificat.

6.3 Menus de la fenêtre principale

Menu	Commande	Fonction
File	Esci	Déconnecte, nettoie les fichiers temporaires et ferme le programme.
Albatros	Parametri	Redirection Albatros / DbKey (chapitre 12).
	FishCodeLib	Outils externes (s'ils sont présents et si le certificat n'est pas bloqué).
Gestione Certificato	Aggiorna modifiche	Enregistre dans le certificat les serveurs et redirections modifiés (section 11.1).
	Cambio Password / Port FF	Change le mot de passe d'accès.
	Cambio Pwd Intermedia / Port FF	Change le mot de passe intermédiaire.
	Export Certificato	Exporte le certificat dans un fichier `.Ssh_T`.
	Elimina Certificato	Supprime le profil de la base de données.
	Apri percorso DB Ssh_Tunnel	Ouvre le dossier de la base de données.
Utility	Ping No-IP	Résout via DNS le nom du serveur sélectionné et en affiche l'IP.
	Ping IP	Exécute un ping vers le serveur, s'il est indiqué sous forme d'adresse IP.
	Scarica AlbatrosRDP	Enregistre `AlbatrosRDP.exe` dans le dossier Téléchargements.

En mode « Apri come Putty », les menus Albatros et Gestione Certificato ne sont pas disponibles.

7. Connexion et sessions à distance

7.1 Connexion au serveur SSH

1. Vérifiez dans le registre la présence du texte **SSH Tunneling Ready ....**
2. Si la liste des serveurs est visible, choisissez le serveur : dans des conditions normales, le premier suffit ; les autres sont des accès alternatifs à utiliser si le serveur principal ne répond pas (certains ne fonctionnent que depuis l'intérieur du réseau de l'entreprise).
3. Appuyez sur **Connetti**.

Le registre affiche la séquence des opérations :

```
Disconnected
Testing Internet connection status
Connecting...
Server: <nome server>
port: 200
Connecting to <nome server>:200
CONNECTED
S.O. <sistema operativo del server>
```

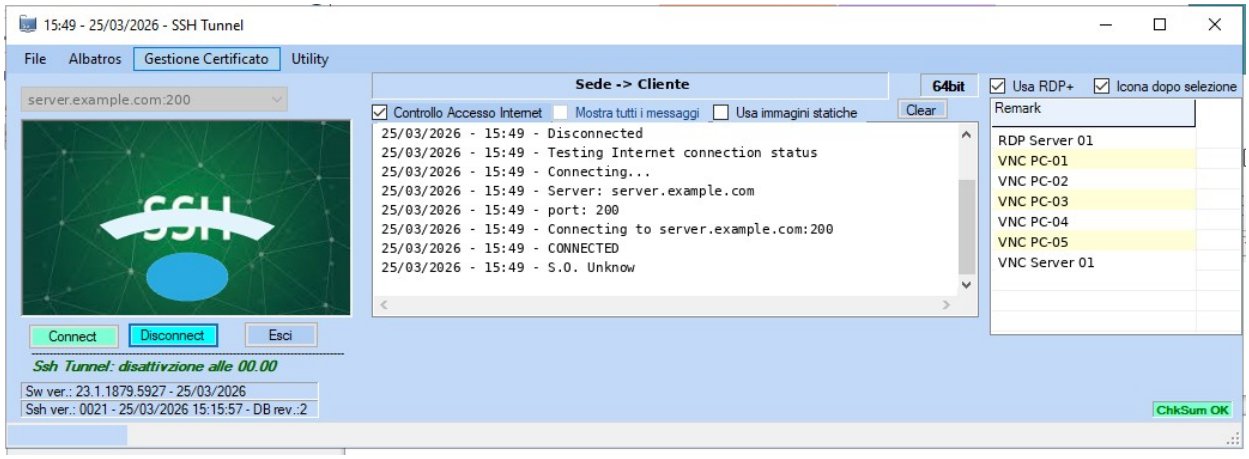

Figure 4 – Connexion établie : à droite, la liste des ordinateurs accessibles

Détails de fonctionnement :

- Le serveur peut être indiqué sous la forme `host:porta` ; sans port, celui du certificat est utilisé et, à défaut, le **200**. Le texte qui suit une apostrophe (`'`) est considéré comme un commentaire.
- L'authentification utilise les identifiants SSH contenus dans le certificat et, si elle est présente, la clé privée.
- Après la connexion, le programme détecte le système d'exploitation du serveur (commande `ver` pour Windows, `lsb_release -d` pour Linux).
- Le serveur choisi est mémorisé pour le profil et reproposé au démarrage suivant.
- Si la connexion tombe, le programme le signale (« Connection Lost ») et tente de se reconnecter automatiquement jusqu'à ce que vous appuyiez sur **Disconnetti**.
- Si le certificat ne prévoit qu'un seul serveur, la fenêtre est réduite au démarrage et, si le certificat active le bouton RDP, la connexion démarre automatiquement.

7.2 Ouverture d'une session sur un PC distant

1. Une fois la connexion établie, **double-cliquez** sur l'ordinateur souhaité dans la liste de droite.
2. Si le mot de passe intermédiaire est prévu, une fenêtre portant le nom de la connexion apparaît : saisissez-le et appuyez sur **OK**.
3. La session à distance s'ouvre et la fenêtre de Ssh_Tunnel est réduite.

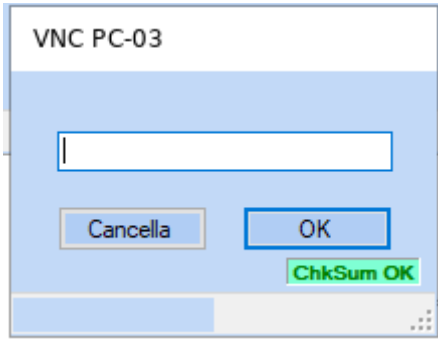

Figure 5 – Demande du mot de passe intermédiaire pour une connexion

> **Attention**
> Après **3 mots de passe intermédiaires erronés**, le programme se déconnecte et se ferme (« Superato il limite di tentativi ammessi »).

> **Remarque**
> Si le certificat prévoit un e-mail de notification des accès, à l'ouverture de chaque session RDP ou VNC un e-mail est envoyé avec l'objet « SSh_Tunnel di <proprietario> su <connessione> » et les données du PC depuis lequel la connexion a été établie.

7.3 Types de connexion

Le type de session dépend de la configuration de l'entrée dans le certificat :

Type	Programme utilisé	Remarques
Bureau à distance (RDP)	Client choisi avec les options RDP	Type par défaut pour les entrées avec fichier RDP.
VNC	`vncviewer.exe` (session partagée)	Le mot de passe du PC distant, s'il figure dans le certificat, est transmis automatiquement. Avec un PC à l'état déconnecté (logoff), les identifiants Windows peuvent être nécessaires.
Terminal	`Ssh_Console.exe`	Console SSH vers l'hôte indiqué.
Caméra	`IPCamera.exe`	Les fenêtres se disposent automatiquement côte à côte à l'écran ; les enregistrements vont dans `C:\SDT_Cam_Recorder\`. Si vous rouvrez la même caméra, la fenêtre précédente est fermée.

Clients pour le Bureau à distance :

Option	Comportement
MS RDP	Utilise `mstsc.exe` de Windows avec un fichier .rdp temporaire. Le mot de passe du PC distant n'est pas transmis.
RDP+	Utilise le client RDP+ intégré en plein écran, avec lecteurs et imprimantes redirigés ; le mot de passe du PC distant est chiffré avec gencrypt et transmis automatiquement.
Old RDP+	Comme RDP+, mais transmet le mot de passe tel quel (pour les mots de passe déjà chiffrés dans le certificat).

Option	Comportement
AlbatrosRDP	Utilise le client propriétaire AlbatrosRDP : les paramètres sont transmis chiffrés et le mot de passe via un canal réservé (named pipe), sans apparaître dans la ligne de commande.

7.4 Bouton RDP/VNC/Term

Si le certificat le prévoit, lorsque la connexion est active, le bouton **RDP/VNC/Term** apparaît ; il ouvre directement la connexion « statique » définie dans le certificat sans passer par la liste. Avec l'option AutoRDP du certificat, cette connexion s'ouvre d'elle-même juste après la connexion.

7.5 Déconnexion et sortie

- **Disconnetti** : ferme toutes les redirections, les caméras et la connexion SSH ; interrompt les tentatives de reconnexion.
- **Esci** (ou fermeture de la fenêtre) : déconnecte, supprime les fichiers temporaires et ferme le programme.
- **Riavvia** : comme Esci, mais revient à la fenêtre de connexion pour choisir un autre profil.

8. Gestion des redirections de port

Cette partie n'est disponible que si le certificat autorise la modification des redirections (autorisation `AllowsNewForwards`) ou en mode « Apri come Putty ». Dans ce cas, la fenêtre principale est plus haute et affiche la section de modification sous les boutons.

8.1 Activer la modification

1. Cochez **Accedi a Port Forwarding** : le mot de passe intermédiaire est demandé.
2. Avec le mot de passe correct, la section de modification devient modifiable et la liste des redirections permet la sélection multiple et l'exportation vers Excel.

8.2 Champs d'une redirection

Champ	Signification
Host Locale / Porta	Adresse et port sur lesquels le programme écoute sur le PC local (ex. 127.0.0.2:3390). Le bouton * à côté de l'hôte insère 127.0.0.2.
Host Remoto / Porta	Hôte et port de destination, vus depuis le serveur SSH (ex. 192.168.1.10:3389).
Nota (Remark)	Nom qui apparaît dans la liste des ordinateurs. Obligatoire.
Pwd	Mot de passe du PC distant, transmis à VNC ou RDP+. Le bouton œil l'affiche ; **RDP Crypt** le chiffre avec gencrypt pour RDP+.
RDP	Contenu du fichier de connexion. Les trois boutons * génèrent un modèle : fichier .rdp complet, ligne VNC, ligne terminal.

Modèles générés par les boutons :

- RDP : fichier .rdp standard avec `full address` et `server port` égaux à l'hôte et au port locaux, plein écran, presse-papiers, imprimantes et lecteurs redirigés.
- VNC : `vnc_config /connect <host>:<porta> /autoacceptnodsm /shared /autoscaling`.
- Terminal : `term_config server=<host> port=<porta> login= password= ppkkeyfilename= ppkkey= ppkkeypwd=` (à compléter).

Dans le contenu, vous pouvez utiliser les espaces réservés `##host##` et `##port##`, remplacés au moment de l'ouverture par l'hôte et le port locaux de la redirection. Une entrée n'apparaît dans la liste des ordinateurs que si elle est cochée et que son champ RDP est renseigné ; les entrées sans fichier RDP créent uniquement le tunnel.

8.3 Opérations sur la liste

Commande	Effet
Clic sur une ligne	Charge l'entrée dans les champs pour la modifier.
`<==`	Insère l'entrée dans la liste ou met à jour celle qui est sélectionnée (redemande le mot de passe intermédiaire). Tous les champs sauf RDP et Pwd sont obligatoires.
Pulisci	Vide les champs.
Tutti i Tag / Inverti Tag	Coche toutes les entrées / inverse les coches. Seules les entrées cochées sont activées.
Predefinito	Rétablit la liste telle qu'elle était lors du dernier enregistrement du certificat.

Si le port local indiqué est déjà utilisé par une autre entrée, le programme propose de rechercher automatiquement le premier port libre.

> **Attention**
>
> Les modifications deviennent actives à la **connexion suivante** (l'avertissement « Modifiche attive alla prossima connessione » apparaît).
>
> Pour les rendre permanentes, il faut les enregistrer dans le certificat avec **Gestione Certificato › Aggiorna modifiche** ; sinon, elles sont perdues à la fermeture.

9. Gestion des serveurs SSH

Si le certificat autorise la modification des serveurs (autorisation `AllowServerIpEditing`), la liste des serveurs devient modifiable et un cadre de commandes apparaît :

Commande	Effet
Aggiungi	Ajoute à la liste le texte saisi (format `host:porta`).
Elimina	Supprime l'entrée saisie/sélectionnée (il doit en rester au moins une).
+ / -	Déplacent l'entrée sélectionnée dans la liste.
R	Remplace le texte de la dernière entrée sélectionnée par le texte saisi.

Ces modifications doivent elles aussi être enregistrées avec **Gestione Certificato › Aggiorna modifiche**. Pendant la connexion, la liste des serveurs est verrouillée.

10. Mode « Apri come Putty »

Depuis la fenêtre de connexion, **Varie › Apri come Putty** ouvre la fenêtre principale sans certificat, comme client SSH générique. Les champs suivants apparaissent :

Champ	Utilisation
Hostname / Porta	Serveur SSH (port par défaut 22).
Nome utente / Password	Identifiants SSH.
KeyFile / Pwd KeyFile	Clé privée (`.ppk`, `.OpenSsh`, `.pri`) et sa phrase secrète ; le bouton `....` ouvre la sélection de fichier.
Timeout (sec.)	Délai d'expiration de connexion et intervalle de keep-alive (3 par défaut).

Les redirections se définissent comme décrit au chapitre 8 et ne valent que pour la session : dans ce mode, il n'existe pas de certificat dans lequel les enregistrer.

11. Gestion du certificat

Toutes les commandes du menu **Gestione Certificato** demandent d'abord confirmation si une connexion est active (elle sera fermée), puis le mot de passe actuel. À la fin, le programme se ferme avec le message « Aggiornamento Effettuato: Rientrare nel programma ».

11.1 Aggiorna modifiche

Reconstruit le certificat avec la liste actuelle des serveurs et des redirections (y compris les coches et les mots de passe) et l'enregistre dans la base de données avec le même mot de passe. À chaque enregistrement, le numéro de version du certificat (`Ssh ver.`) augmente.

11.2 Cambio Password

Après le mot de passe actuel, saisissez deux fois le nouveau mot de passe, qui doit respecter les exigences suivantes :

- au moins 8 caractères ;
- au moins 1 lettre minuscule et 2 majuscules ;
- au moins 1 chiffre ;
- au moins 2 caractères spéciaux.

Le certificat est rechiffré avec le nouveau mot de passe. Si le mot de passe est identique au précédent, le certificat est tout de même mis à jour.

11.3 Cambio Password Intermedia

Définit le mot de passe demandé à l'ouverture des sessions à distance. Aucune exigence de complexité n'est prévue.

11.4 Export Certificato

Exporte le certificat dans `C:\Ssh_Tunnel_Certificates\<Profilo>.Ssh_T`, chiffré avec le mot de passe indiqué lors de l'exportation, prêt à être remis et importé sur un autre PC (section 4.4).

L'exportation nécessite un **mot de passe d'autorisation**, que l'on peut obtenir de deux façons :

- en appuyant sur le bouton d'envoi de code : un code aléatoire est envoyé à l'adresse e-mail de notification des accès (ou, à défaut, à l'adresse e-mail principale) ;
- avec le mot de passe administratif réservé au développeur, valable uniquement sur un PC disposant de l'autorisation Persistent.

Après l'autorisation, choisissez le mot de passe avec lequel chiffrer le fichier exporté.

11.5 Elimina Certificato

Après le mot de passe actuel, le profil est supprimé de la base de données. S'il reste d'autres profils dans la base de données, le programme revient à la fenêtre de connexion ; sinon, il se ferme.

12. Redirection Albatros (DbKey)

La commande **Albatros › Parametri** ouvre la fenêtre **Reindirizza Albatros**, conçue pour l'intégration avec les applications Albatros : lorsque le tunnel vers un site est ouvert, les applications peuvent être dirigées automatiquement vers la base de données de ce site.

La partie supérieure énumère les configurations présentes dans l'environnement Albatros (clé, BD locale et note, BD distante et note, IP de ping), comme référence pour choisir la clé. La partie inférieure contient les paramètres du profil :

Champ	Signification
Abilitato	Active la fonction pour le profil.
Alla Connessione	DbKey à définir lorsque la connexion SSH réussit.
Alla Disconn.	DbKey à définir à la déconnexion.
Percorso file txt DbKey	Dossier dans lequel écrire le fichier `_DbKey.txt` (bouton Predefinito : `C:\ProgramData\Albatros\Common\`).
Nota Connessione / Nota Disconnessione	Texte reporté dans le registre et dans le journal lorsque la clé est appliquée.

En appuyant sur **Registra**, les paramètres sont enregistrés dans l'environnement Albatros avec des clés du type `[<Profilo>]_DbKeyEnabled`, `[<Profilo>]_DbKeyAtConnection`, etc., et appliqués immédiatement selon l'état de la connexion. À la connexion ou à la déconnexion, le programme écrit `DbKey=<valore>` dans le fichier `_DbKey.txt` et le note dans le registre.

13. Journal et maintenance de la base de données

13.1 Registre et journal

Chaque ligne affichée dans le panneau des messages est aussi enregistrée dans la table Log de la base de données, avec l'identifiant de processus (session) et, lors de la première écriture, les informations matérielles du PC. Le journal peut être désactivé avec le paramètre `DoNotUseLogSSH_Tunnel`.

13.2 Mostra Log

Dans la fenêtre de connexion, **DataBase › Gestione Log › Mostra Log** : indiquez l'intervalle de dates (date de début / date de fin) et appuyez sur **Ricerca**. La session, la date, l'heure, les informations du PC et le message sont affichés.

13.3 Invia Log via Mail

DataBase › Gestione Log › Invia Log via Mail : indiquez l'intervalle de dates et l'adresse de destination, puis appuyez sur **Invia**. Le journal de la période est exporté vers Excel, compressé en zip et envoyé ; les fichiers temporaires sont ensuite supprimés.

13.4 Maintenance

- **Compatta Database** : récupère l'espace libre dans le fichier (VACUUM). Cette opération est aussi exécutée automatiquement à chaque enregistrement du certificat.
- **Open Ssh_Tunnel DB path** : ouvre le dossier de la base de données, utile pour les copies de sauvegarde.

13.5 Structure de la base de données

La base de données est un fichier SQLite protégé par mot de passe, en révision 2. Au démarrage, le programme crée les tables manquantes et met automatiquement à jour les bases de données de la révision 1.

Table	Contenu
Parameters	Paires clé/valeur : `DbVersion`, `login` (dernier profil utilisé), `[<Profilo>]_IP` (dernier serveur utilisé).
Certificati	Proprietario, Profilo, Version, VersionDate, Certificato (texte chiffré).
Licenza	KeyLicenza, Assegnatario, DataAssegnazione, CertificatoLicenza (prévue, actuellement non utilisée).
Log	IdSession, DataLog, PcInfo, KeyInfo, Info.

14. Sécurité

- **Certificat chiffré** : chaque valeur sensible est chiffrée en Triple DES avec une clé dérivée du mot de passe d'accès ; le certificat dans son ensemble est à son tour chiffré. Le mot de passe n'est jamais enregistré.
- **Aucun identifiant visible** : les identifiants SSH, la clé privée et les mots de passe des PC distants restent à l'intérieur du programme et sont transmis directement aux clients.
- **Lien avec le matériel** : les autorisations de la double vérification ne valent que pour le PC et l'utilisateur Windows sur lesquels elles ont été obtenues.
- **Limite de tentatives** : 3 tentatives pour le mot de passe d'accès, pour les codes de la double vérification et pour le mot de passe intermédiaire.
- **Expiration à minuit** pour les autorisations OneDay et OneTime.
- **Traçabilité** : e-mail avec les données du PC à chaque demande de codes et à chaque accès RDP/VNC, journal local des sessions, enregistrement des accès sur le serveur SSH.
- **Nettoyage** : les programmes auxiliaires et les fichiers .rdp temporaires sont supprimés au démarrage et à la sortie.
- **Intégrité** : l'indicateur « ChkSum OK » signale que l'exécutable n'a pas été altéré.

> **Remarque**
>
> Le mot de passe intermédiaire n'est pas une véritable protection cryptographique : il sert à empêcher l'utilisation du programme laissé ouvert et sans surveillance.

15. Messages et dépannage

Message / symptôme	Cause et solution
«Password errata: impossibile continuare»	Mot de passe d'accès erroné ou mauvais profil. Après 3 erreurs, le programme se ferme.
«Certificato inesistente»	Le profil sélectionné n'est pas dans la base de données : importez le certificat.
«Two-factor authentication is required!»	PC non autorisé : suivez le chapitre 5.
«Invio mail ... per doppia verifica fallito!!!»	Problème d'envoi d'e-mail (réseau, pare-feu, SMTP). Réessayez ou utilisez « Invia Codice via SMS al Supporto ».
«Codice errato: Tentativi n di 3»	Code saisi de manière erronée ou provenant d'une demande précédente.
«Chiusura automatica per mancato input codice»	Les 5 minutes se sont écoulées sans que le code soit saisi.
«Internet Connection Not Available» / «Waiting ...»	La connexion Internet est absente ; le programme attend. Décochez « Chk Internet » pour ignorer le contrôle.
«Errore login!!!»	Impossible de préparer la connexion (identifiants ou clé du certificat non valides). Contactez l'administrateur.
La connexion ne s'établit pas	Serveur inaccessible : essayez un serveur alternatif de la liste ; utilisez Utility › Ping No-IP pour vérifier la résolution du nom.
«### Error Forward Host: ...»	Le port local de la redirection est occupé par un autre programme ou l'hôte local n'est pas valide.
«Connection Lost»	Connexion tombée : le programme se reconnecte tout seul.
«Password errata» / «Superato il limite di tentativi ammessi»	Mot de passe intermédiaire erroné ; à la troisième erreur, le programme se ferme.
«Ssh Tunnel arrestato per scadenza password...»	Minuit est atteint avec une autorisation OneDay/OneTime : redémarrez et demandez un nouveau code.
«Riscontrata anomalia tra la versione attesa e quella trovata nel Database di servizio»	La base de données ne peut pas être mise à jour : déplacez le programme dans un dossier avec des autorisations d'écriture.
«Operazione annullata per password difforme»	Mot de passe actuel erroné dans les fonctions de Gestione Certificato.
«Porta già utilizzata: Cerco la prima occorrenza libera?»	Port local déjà attribué à une autre redirection.
«Dati Insufficienti!»	Des champs obligatoires manquent lors de l'insertion d'une redirection.

Annexe A – Récapitulatif rapide pour l'utilisateur

1. Copiez le `.exe` et le `.db` dans le même dossier.
2. Lancez l'exécutable et saisissez le mot de passe d'accès.
3. Si cela est demandé, appuyez sur « Richiedi via mail » et saisissez le code OneDay ou OneTime reçu.
4. Attendez « SSH Tunneling Ready .... » et appuyez sur **Connetti**.
5. Double-cliquez sur l'ordinateur souhaité dans la liste de droite.
6. Saisissez le mot de passe intermédiaire, s'il est demandé.
7. Travaillez sur le PC distant ; à la fin, appuyez sur **Disconnetti** ou **Esci**.

Annexe B – Structure du certificat

Le certificat (version 2) est un texte composé de lignes `Chiave = "valore"`, chiffré dans son ensemble avec le mot de passe. Les valeurs sensibles sont à leur tour chiffrées individuellement. Liste des clés reconnues :

Clé	Contenu
`Algoritmo`	Version de l'algorithme de chiffrement (1).
`Nominativo`	Nom du profil (en clair).
`SshUserDllVersion`	Numéro progressif et date du dernier enregistrement.
`Bloccato`	Certificat aux fonctions réduites (pas de détails dans le registre, pas d'outils externes).
`ShowRdpButton`	Affiche le bouton RDP/VNC/Term pour la connexion statique.
`AutoRDP`	Ouvre la connexion statique juste après la connexion.
`AllowsNewForwards`	Autorise la modification des redirections de port.
`AllowServerIpEditing`	Autorise la modification de la liste des serveurs.
`Proprietario`	Destinataire du logiciel (« Sw consegnato a »).
`Login`, `Password`	Identifiants SSH.
`Certificate`, `CertificatePassword`, `FileCertificato`	Clé privée SSH (texte ou ressource incorporée) et sa phrase secrète.
`PwdRemoteAccess`	Mot de passe intermédiaire.
`Server`, `ServerPort`	Liste des serveurs séparés par `&` et port par défaut.
`RdpCommandLine`, `RdpFileStatico`	Ligne de commande et fichier de la connexion statique.
`Mail`, `MailOneDay`, `MailTemp`	Destinataires des codes de la double vérification.
`MailInfoAccess`	Destinataire des notifications d'accès.
`Cellulare`	Numéro de téléphone portable (prévu).
`RedirectPortsCount`	Nombre de redirections.
`RedirectPorts(i, …)`	Pour chaque redirection : LocalHost, LocalPort, RemoteHost, RemotePort, Remark, RdpFile, Enabled (Y/N), PasswordRdpFF, PwdActivateRdpConnection.

Annexe C – Notes techniques pour le développeur

Lors de la rédaction du manuel, quelques points à vérifier sont apparus dans le code. Cette annexe est à usage interne : elle doit être retirée avant de remettre le manuel aux destinataires du programme.

Fichier / routine	Observation
ModSetting.Log	Vérifie l'existence de la base de données dans `Application.StartupPath` avec le nom de l'exe, en ignorant `PathDbSSH_Tunnel` et `FileNameDbSSH_Tunnel` : si la BD se trouve ailleurs ou porte un autre nom, le journal n'est pas écrit.
ModSetting.RemoveParam	La requête utilise `lower('?')` : le paramètre entre apostrophes n'est pas substitué, la suppression reste donc sans effet.
ModSetting.DecodCertificate	La comparaison `ToLower.Contains("Algoritmo =")` contient une majuscule et n'est jamais vraie : la valeur `Algoritmo` n'est pas lue (aujourd'hui sans conséquence, elle vaut toujours 1).
FrmStart_Load	`ContaErrori` est locale à la boucle et se remet à zéro à chaque itération ; de plus, si la double vérification échoue ou si la fenêtre est fermée, `Exit Sub` ne termine pas l'application : vérifiez qu'il ne reste pas de processus actif sans fenêtre.
frmMainProgram, boutons + / - des serveurs	Les info-bulles sont inversées : - (info-bulle « Sposta Giù ») déplace vers le haut, + (info-bulle « Sposta Su ») déplace vers le bas.
frmMainProgram, boutons de modèle *	L'info-bulle indique `###Host### / ###Port###`, mais les espaces réservés substitués par le code sont `##host##` / `##port##`.
EseguiExportCertificato	Le « supercode » active l'enregistrement du mot de passe dans un fichier `.Ssh_T.Key`, mais `CostruisciRemPwdInfo` et `abilitaSalvataggioPwd` ne sont pas utilisés : la fonction n'est pas implémentée.
ChkIconaAfterSelection	L'option « Icona dopo selezione » n'est pas référencée dans le code.
GetParam / SetParam	La clé est concaténée dans la requête SQL au lieu d'être transmise comme paramètre.
Sources en général	Les sources contiennent en clair des identifiants et des clés (service SMS, accès SFTP pour les mises à jour, mot de passe de la BD, empreinte du mot de passe administratif). Quiconque a accès à l'exécutable peut les extraire avec un décompilateur .NET : envisagez l'obfuscation ou le déplacement côté serveur.

Ssh_Tunnel

Client SSH per accessi remoti controllati

Manuale d'uso e di amministrazione

Versione software 27.2.2036.6127 · DB rev. 2

© Raffaele Romano
Ottobre 2026

Indice

1. Introduzione....63
1.1 A chi è rivolto questo manuale....63
1.2 Versione documentata....63

2. Concetti fondamentali....64

3. Installazione e requisiti....65
3.1 File necessari....65
3.2 Requisiti....65
3.3 Programmi incorporati....65
3.4 File di parametri esterno (opzionale)....65
3.5 Componenti facoltativi nella cartella....66

4. Avvio e accesso....67
4.1 La maschera di accesso....67
4.2 Inserimento della password....68
4.3 Menu della maschera di accesso....68
4.4 Importazione di un certificato....68

5. Doppio passaggio (autorizzazione del PC)....70
5.1 Quando viene richiesto....70
5.2 Richiesta dei codici....70
5.3 Livelli di autorizzazione....70
5.4 Menu «Varie» del doppio passaggio....71
5.5 Revoca dell'autorizzazione....71

6. La finestra principale....72
6.1 Panoramica....72
6.2 Opzioni....72
6.3 Menu della finestra principale....73

7. Connessione e sessioni remote....74
7.1 Connessione al server SSH....74
7.2 Apertura di una sessione su un PC remoto....74
7.3 Tipi di connessione....75
7.4 Pulsante RDP/VNC/Term....76
7.5 Disconnessione e uscita....76

8. Gestione dei port forwarding....77
8.1 Abilitare la modifica....77
8.2 Campi di un forwarding....77
8.3 Operazioni sull'elenco....77

9. Gestione dei server SSH....79

10. Modalità «Apri come Putty»....80

11. Gestione del certificato....81
11.1 Aggiorna modifiche....81
11.2 Cambio Password....81
11.3 Cambio Password Intermedia....81
11.4 Export Certificato....81
11.5 Elimina Certificato....81

12. Reindirizzamento Albatros (DbKey)....82

13. Log e manutenzione del database....83
13.1 Registro e log.... 83
13.2 Mostra Log.... 83
13.3 Invia Log via Mail.... 83
13.4 Manutenzione.... 83
13.5 Struttura del database.... 83
14. Sicurezza....84
15. Messaggi e risoluzione dei problemi....85
Appendice A – Riepilogo rapido per l'utente....86
Appendice B – Struttura del certificato....87
Appendice C – Note tecniche per lo sviluppatore....88

1. Introduzione

Ssh_Tunnel è un client SSH per Windows, sviluppato in VB.NET, che consente di raggiungere in modo controllato PC e server di una rete aziendale (via RDP, VNC, terminale SSH o telecamere IP) attraverso un tunnel cifrato verso un server SSH dell'azienda.

Nasce come alternativa a strumenti come TeamViewer, AnyDesk e simili: questi garantiscono un traffico cifrato, ma chiunque possieda le credenziali può accedere ai sistemi, legando la sicurezza della rete a soggetti terzi. Ssh_Tunnel invece:

- non contiene in chiaro alcuna password: tutti i parametri di collegamento sono racchiusi in un **certificato cifrato**, apribile solo con la password di accesso consegnata all'utente;
- assegna a ogni destinatario (centro di assistenza, tecnico, consulente) un **certificato univoco**, così che il server SSH riconosca chi si collega e ne registri data, ora e durata;
- può legare l'utilizzo a uno specifico PC tramite un **doppio passaggio** (codice inviato via mail), con autorizzazione permanente, giornaliera o per la sola sessione;
- notifica via mail ogni accesso a un PC remoto, indicando da quale computer è avvenuto il collegamento;
- espone all'utente solo le connessioni previste dal suo certificato, presentate come un elenco di computer su cui fare doppio clic.

1.1 A chi è rivolto questo manuale

Il manuale è diviso in tre parti:

- **Uso quotidiano** (capitoli 3–7): installazione, accesso, doppio passaggio, connessione e apertura delle sessioni remote. È la parte da consegnare a chi riceve il programma.
- **Amministrazione** (capitoli 8–13): gestione dei port forwarding, dei server, dei certificati, del reindirizzamento Albatros, dei log e del database.
- **Riferimento tecnico** (capitoli 14–15 e appendici): architettura, sicurezza, struttura del certificato, messaggi e risoluzione dei problemi.

1.2 Versione documentata

Voce	Valore
Programma	Ssh_Tunnel
Versione software	27.2.2036.6127 (data di build 11/10/2026)
Revisione database	2
Versione certificato	2 (Algoritmo = 1)
Piattaforma	.NET Framework 4.8, Windows, compilazioni a 32 e 64 bit
Librerie principali	Renci SSH.NET 2025, System.Data.SQLite, AlbatrosCommon
Lingue dell'interfaccia	Italiano, Inglese, Francese, Giapponese, Rumeno (scelta automatica in base alla lingua di Windows)

La versione mostrata dal programma ha la forma `Sw ver.: 27.2.2036.6127 - 11/10/2026`: la data è ricavata dal numero di revisione (giorni trascorsi dal 01/01/2010) e corrisponde quindi alla data di compilazione.

2. Concetti fondamentali

Prima di usare il programma è utile conoscere alcuni termini che ricorrono in tutte le maschere.

Termine	Significato
Profilo	Nome che identifica un certificato (es. «Sede -> Cliente»). Nello stesso database possono convivere più profili; all'avvio si sceglie quale usare.
Certificato	Blocco cifrato che contiene tutto ciò che serve al collegamento: server SSH e porte, credenziali SSH, chiave privata, elenco dei port forwarding, file RDP/VNC, indirizzi mail, permessi. Viene distribuito come file `.Ssh_T` e importato nel database.
Password di accesso	Password richiesta all'avvio. Decifra il certificato: senza di essa il programma non conosce né i server né le credenziali.
Password intermedia (accesso remoto)	Seconda password chiesta al momento di aprire una sessione su un PC remoto. Serve a evitare che un programma lasciato aperto e incustodito venga usato da altri.
Password specifica di connessione	Password intermedia definita per una singola voce dell'elenco; se presente prevale su quella generale.
Doppio passaggio	Verifica aggiuntiva: al primo utilizzo su un PC si chiede un codice via mail. L'autorizzazione è legata all'hardware del PC.
Codice Persistent / OneDay / OneTime	I tre codici del doppio passaggio: autorizzazione permanente, valida fino a mezzanotte, valida per la sola sessione (vedi capitolo 5).
Port forwarding (tunnel)	Associazione «indirizzo e porta locali → host e porta remoti» instaurata attraverso la connessione SSH. Ogni computer raggiungibile corrisponde a un forwarding.
DbKey	Chiave usata dagli applicativi Albatros per scegliere il database di lavoro; Ssh_Tunnel può cambiarla automaticamente alla connessione e alla disconnessione (capitolo 12).

3. Installazione e requisiti

3.1 File necessari

Ssh_Tunnel non richiede installazione né diritti di amministratore. È sufficiente copiare nella stessa cartella:

File	Descrizione
`Ssh_Tunnel_<Nome>.exe`	Eseguibile del programma (il nome può essere personalizzato per destinatario; può terminare con 32 o 64).
`Ssh_Tunnel_<Nome>.db`	Database SQLite cifrato che contiene certificati, parametri e log.

Il nome del database viene ricavato dal nome dell'eseguibile, togliendo l'eventuale suffisso `32` o `64` e aggiungendo `.db`. Esempio: `Ssh_Tunnel_Esempio64.exe` cerca `Ssh_Tunnel_Esempio.db`. In questo modo la versione a 32 e quella a 64 bit condividono lo stesso database.

> **Nota**
>
> Se il database non esiste viene creato vuoto al primo avvio; in tal caso occorre importare un certificato (paragrafo 4.4) prima di poter accedere.
>
> Se compare il messaggio «Riscontrata anomalia tra la versione attesa e quella trovata nel Database di servizio», spostare il programma in una cartella senza limitazioni di scrittura (ad esempio non sotto `C:\Program Files`).

3.2 Requisiti

- Windows con .NET Framework 4.8.
- Accesso a Internet in uscita verso il server SSH aziendale (la porta predefinita è la 200, salvo diversa indicazione nel certificato).
- Per il doppio passaggio e le notifiche: possibilità di inviare mail (il programma usa i parametri SMTP interni della libreria Albatros).

3.3 Programmi incorporati

L'eseguibile contiene al proprio interno i programmi ausiliari, che vengono estratti solo quando servono nella cartella temporanea `%TEMP%\Albatros\Ssh_Tunnel` e cancellati all'avvio e all'uscita:

Componente	Uso
`vncviewer.exe` / `vncviewer32.exe`	Visualizzatore VNC (versione a 64 o 32 bit in base al processo).
`rdp.exe`	Client RDP+ (desktop remoto con passaggio automatico della password).
`gencrypt.exe`	Cifratura delle password per RDP+.
`AlbatrosRDP.exe`	Client RDP proprietario con passaggio sicuro della password.
`Ssh_Console.exe`	Console terminale SSH.
`IPCamera.exe`	Visualizzatore di telecamere IP.

3.4 File di parametri esterno (opzionale)

Tramite il meccanismo dei parametri esterni della libreria AlbatrosCommon (file di testo con righe `Var_<nome>=<valore>`, vedi l'esempio `Data\Ssh_Tunnel_Merge.txt` nei sorgenti) si possono impostare:

Parametro	Effetto	Predefinito
`PathDbSSH_Tunnel`	Cartella del database	Cartella dell'eseguibile
`FileNameDbSSH_Tunnel`	Nome del file database	Derivato dal nome dell'exe
`DoNotUseLogSSH_Tunnel`	Se `True` disattiva il log su database e il salvataggio dell'ultimo profilo/server usato	`False`

3.5 Componenti facoltativi nella cartella

Se nella cartella del programma sono presenti questi file, Ssh_Tunnel li riconosce:

- `Ssh_Updater.exe`: viene avviato automaticamente all'apertura della maschera di accesso (aggiornamento del programma).
- `Database4.exe` o `Database5Pro.exe`, `DbMigration.exe`, `Convert.exe`: compaiono nel menu **FishCodeLib** (gestione DB, migrazione, conversione).

4. Avvio e accesso

4.1 La maschera di accesso

Avviando l'eseguibile compare la maschera **Password**. Nel titolo è riportata l'ora corrente.

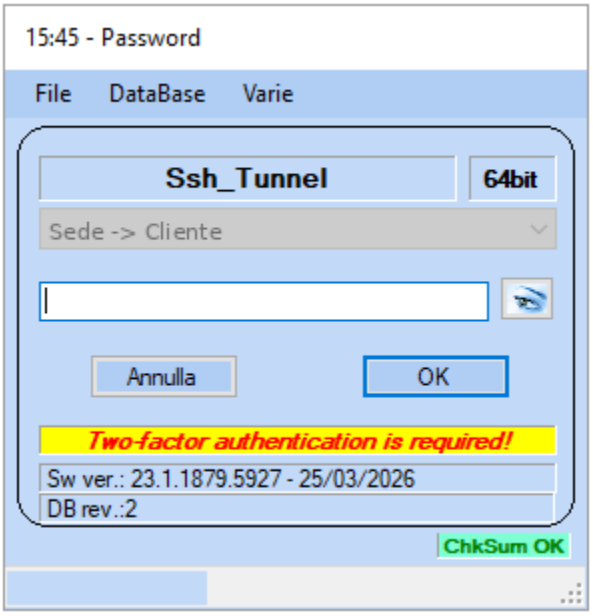

Figura 1 – Maschera di accesso con richiesta di doppio passaggio

Elemento	Funzione
Nome programma e «64bit/32bit»	Indica la versione in esecuzione.
Elenco profili	Profili presenti nel database. Se ce n'è uno solo è bloccato; se sono più d'uno viene proposto l'ultimo usato.
Campo password e pulsante «occhio»	Inserimento della password di accesso; l'occhio mostra/nasconde i caratteri.
Annulla / OK	Chiude il programma / conferma la password.
Riga di stato	Stato dell'autorizzazione del PC (vedi tabella seguente).
Sw ver. / DB rev.	Versione del programma, del certificato e del database.
ChkSum OK	Controllo di integrità dell'eseguibile: se manca o segnala un errore, non proseguire.

La riga di stato può mostrare:

Messaggio	Significato
«Two-factor authentication is required!» (giallo/rosso)	Il PC non è autorizzato: dopo la password sarà chiesto il doppio passaggio.
«One Day Code is active!» (giallo)	Il PC è autorizzato fino a mezzanotte di oggi.
«Persistent Code is active!» (verde)	Il PC è autorizzato in modo permanente.

4.2 Inserimento della password

1. Selezionare il profilo (se ce n'è più di uno).
2. Digitare la password di accesso e premere **OK**.
3. Se la password è corretta il certificato viene decifrato; se è prevista la verifica, si apre la maschera del doppio passaggio (capitolo 5), altrimenti la finestra principale.

> **Attenzione**
>
> Dopo **3 password errate** il programma si chiude.
>
> Se Ssh_Tunnel è già in esecuzione viene chiesto se aprire una nuova istanza; rispondendo No, viene portata in primo piano quella già aperta.

4.3 Menu della maschera di accesso

Menu	Voce	Funzione
File	Esci	Chiude il programma.
DataBase	Gestione Log › Abilita Log	Visibile solo se il log è disattivato da parametro: lo riattiva per la sessione.
	Gestione Log › Mostra Log	Consultazione del log (capitolo 13).
	Gestione Log › Invia Log via Mail	Invio del log in allegato (capitolo 13).
	Utility › Compatta Database	Esegue il VACUUM del database SQLite.
	Utility › Open Ssh_Tunnel DB path	Apre in Esplora risorse la cartella del database (il percorso completo è nel suggerimento della voce).
	Utility › Importa Certificato Ssh Tunnel	Importazione di un file `.Ssh_T` (paragrafo 4.4).
	FishCodeLib	Strumenti esterni, se presenti (paragrafo 3.5).
Varie	Abilita Accesso con Doppio Passaggio	Revoca l'autorizzazione memorizzata per il profilo su questo PC (paragrafo 5.5).
	Apri come Putty	Avvia il programma in modalità client SSH libero (capitolo 10).
	Scarica AlbatrosRDP	Salva `AlbatrosRDP.exe` nella cartella Download dell'utente e la apre.

4.4 Importazione di un certificato

Un nuovo profilo si aggiunge importando il file certificato `.Ssh_T` ricevuto dall'amministratore.

1. Dalla maschera di accesso scegliere **DataBase › Utility › Importa Certificato Ssh Tunnel**.
2. Trascinare il file `.Ssh_T` nell'area indicata, oppure farvi doppio clic per sceglierlo.
3. Inserire la password del certificato.
4. Il programma mostra nominativo e proprietario e chiede conferma; se esiste già un profilo con lo stesso nome chiede se sostituirlo.
5. Al termine il nuovo profilo compare nell'elenco della maschera di accesso.

> **Nota**
>
> Se la password è errata il programma risponde «Pwd errata» e nulla viene importato. Il certificato viene salvato nel database ancora cifrato: la password non viene memorizzata.

5. Doppio passaggio (autorizzazione del PC)

5.1 Quando viene richiesto

Il doppio passaggio scatta solo se il certificato contiene almeno un indirizzo mail per i codici e il PC in uso non è già autorizzato per quel profilo. L'autorizzazione è legata all'identificativo hardware del computer (ID della CPU o, in mancanza, numero di serie della scheda madre o del disco), per cui copiare il programma su un altro PC richiede una nuova autorizzazione.

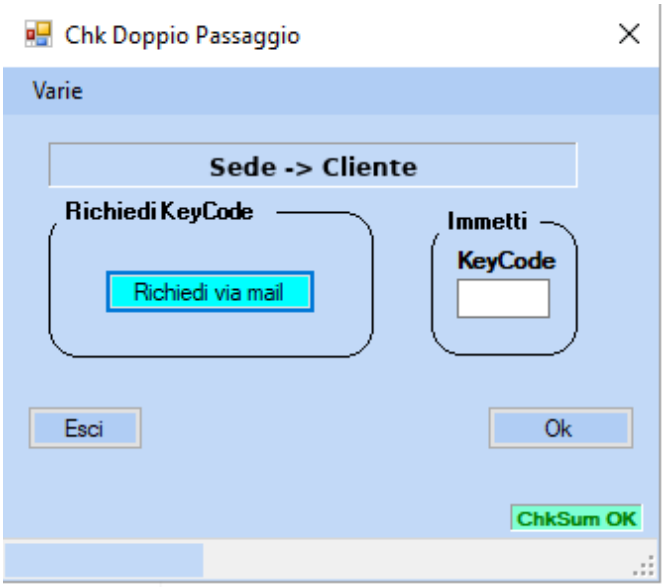

Figura 2 – Maschera «Chk Doppio Passaggio»

5.2 Richiesta dei codici

1. Premere **Richiedi via mail**. Il programma genera tre codici casuali di 5 cifre e li invia agli indirizzi previsti dal certificato.
2. Attendere la mail; compare la scritta «Codici inviati».
3. Inserire uno dei codici ricevuti nel campo **KeyCode** e premere **Ok**.

I codici vengono generati all'apertura della maschera e restano validi solo finché essa è aperta: chiudendo il programma occorre richiederne di nuovi. Ogni mail contiene anche i dati identificativi del PC richiedente (IP locale e pubblico, nome PC, numeri di serie di disco, CPU e scheda madre).

Destinatari dei codici, in base agli indirizzi configurati nel certificato:

Indirizzo nel certificato	Codici ricevuti
Mail principale (`Mail`)	Persistent, OneDay e OneTime
Mail OneDay (`MailOneDay`)	OneDay e OneTime
Mail OneTime (`MailTemp`)	Solo OneTime

Se due indirizzi coincidono la mail non viene duplicata. In questo modo il codice permanente può essere riservato all'amministratore, mentre al cliente arrivano solo i codici temporanei.

5.3 Livelli di autorizzazione

Codice	Effetto	Scadenza
Persistent	Il PC resta autorizzato per il profilo; alle aperture successive non si chiede più il codice.	Nessuna (fino a revoca)

Codice	Effetto	Scadenza
OneDay	Il PC è autorizzato per tutta la giornata.	Mezzanotte del giorno corrente
OneTime	Autorizza solo la sessione in corso; alla riapertura serve un nuovo codice.	Chiusura del programma, e comunque mezzanotte

> **Attenzione**
>
> Con i codici OneDay e OneTime la finestra principale mostra «Ssh Tunnel: disattivazione alle 00.00»: allo scattare della mezzanotte compare l'avviso «Ssh Tunnel arrestato per scadenza password...» e il programma si chiude, chiudendo anche le telecamere aperte.
>
> Dopo **3 codici errati** la maschera si chiude. Se nessun codice viene inserito entro **5 minuti** il programma si chiude automaticamente (con un conto alla rovescia di 10 secondi).

5.4 Menu «Varie» del doppio passaggio

Voce	Funzione
Mostra Chk Mail Persistente	Rende visibile l'opzione «Invia solo alla Mail Principale»: se attivata, i codici vengono spediti soltanto all'indirizzo che riceve il codice Persistent.
Aggiorna Timer	Fa ripartire i 5 minuti di attesa.
Invia Codice via SMS al Supporto	Invia i tre codici via SMS al numero del supporto preimpostato nel programma (utile se la mail non funziona).

5.5 Revoca dell'autorizzazione

Per togliere a un PC l'autorizzazione Persistent o OneDay: nella maschera di accesso selezionare il profilo e scegliere **Varie › Abilita Accesso con Doppio Passaggio**, quindi confermare. Al successivo accesso verrà richiesto di nuovo il codice. La voce è attiva solo quando il PC risulta già autorizzato.

> **Nota**
>
> L'autorizzazione è salvata, cifrata, nel registro di Windows dell'utente corrente: `HKEY_CURRENT_USER\Software\Albatros.net`, valore `Ssh_Tunnel_<Profilo>`. È quindi valida per l'utente Windows che l'ha ottenuta.

6. La finestra principale

6.1 Panoramica

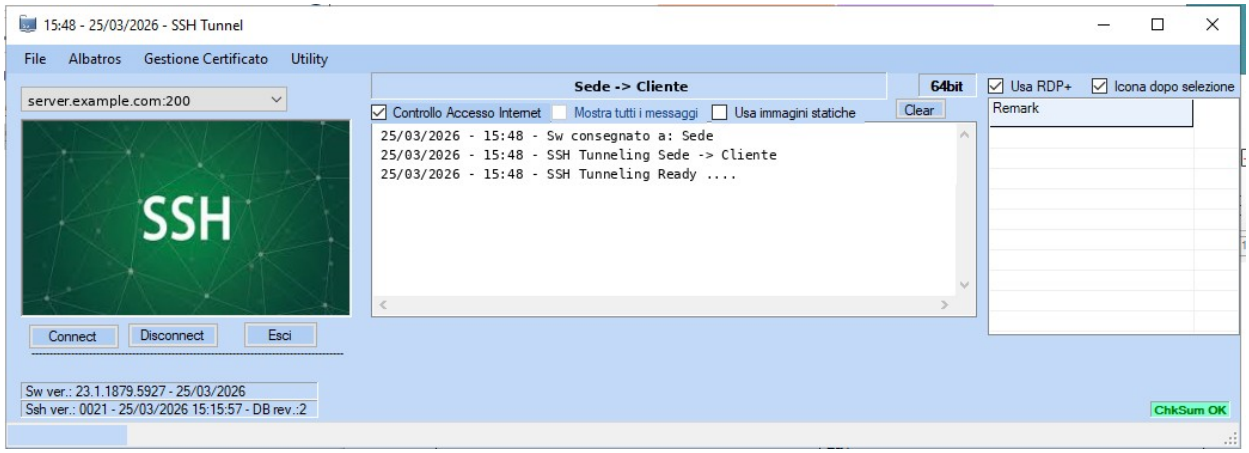

Figura 3 – Finestra principale prima della connessione

Area	Contenuto
In alto a sinistra	Elenco dei server SSH disponibili (visibile se ce n'è più d'uno o se il certificato ne consente la modifica).
Immagine di stato	Logo SSH a riposo; animazione di connessione riuscita o interrotta durante l'uso.
Pulsanti	**Connetti**, **Disconnetti**, **Esci** e, se nel database ci sono più profili, **Riavvia** (torna alla maschera di accesso per cambiare profilo).
Pannello centrale	Registro dei messaggi con data e ora. Le righe di errore sono in rosso; quelle che contengono «###» hanno sfondo giallo.
Elenco a destra	Computer raggiungibili (colonna Remark), popolato dopo la connessione.
Barra di stato	Versione del software e del certificato, revisione DB, «ChkSum OK».

6.2 Opzioni

Opzione	Effetto
Chk Internet	Prima di connettersi verifica che Internet sia raggiungibile; in assenza attende finché la connessione torna disponibile. Attiva per impostazione predefinita.
Mostra tutti i messaggi	Mostra nel registro anche i dettagli dei port forwarding (IP e porte locali e remote). Non disponibile per i certificati «bloccati».
Usa immagini statiche	Sostituisce le animazioni di stato con immagini fisse.
Icona dopo selezione	Opzione di visualizzazione dell'elenco computer.
RDP+ / AlbatrosRDP / MS RDP / Old RDP+	Sceglie il client usato per le connessioni desktop remoto (paragrafo 7.3). Predefinito: MS RDP.
Clear	Svuota il registro e ripropone le informazioni del certificato.

6.3 Menu della finestra principale

Menu	Voce	Funzione
File	Esci	Disconnette, pulisce i file temporanei e chiude il programma.
Albatros	Parametri	Reindirizzamento Albatros / DbKey (capitolo 12).
	FishCodeLib	Strumenti esterni (se presenti e se il certificato non è bloccato).
Gestione Certificato	Aggiorna modifiche	Salva nel certificato server e forwarding modificati (paragrafo 11.1).
	Cambio Password / Port FF	Cambia la password di accesso.
	Cambio Pwd Intermedia / Port FF	Cambia la password intermedia.
	Export Certificato	Esporta il certificato in un file `.Ssh_T`.
	Elimina Certificato	Rimuove il profilo dal database.
	Apri percorso DB Ssh_Tunnel	Apre la cartella del database.
Utility	Ping No-IP	Risolve via DNS il nome del server selezionato e ne mostra l'IP.
	Ping IP	Esegue un ping verso il server, se indicato come indirizzo IP.
	Scarica AlbatrosRDP	Salva `AlbatrosRDP.exe` nella cartella Download.

Nella modalità «Apri come Putty» i menu Albatros e Gestione Certificato non sono disponibili.

7. Connessione e sessioni remote

7.1 Connessione al server SSH

1. Verificare nel registro la scritta **SSH Tunneling Ready ....**
2. Se l'elenco server è visibile, scegliere il server: in condizioni normali è sufficiente il primo; gli altri sono accessi alternativi da usare se il server principale non risponde (alcuni funzionano solo dall'interno della rete aziendale).
3. Premere **Connetti**.

Il registro mostra la sequenza delle operazioni:

```
Disconnected
Testing Internet connection status
Connecting...
Server: <nome server>
port: 200
Connecting to <nome server>:200
CONNECTED
S.O. <sistema operativo del server>
```

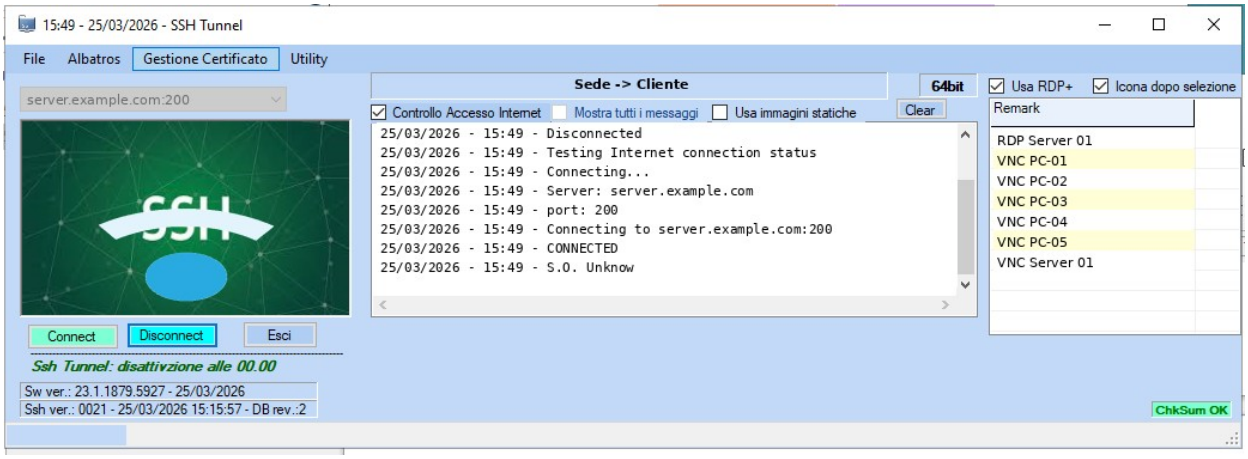

Figura 4 – Connessione stabilita: a destra l'elenco dei computer raggiungibili

Dettagli di funzionamento:

- Il server può essere indicato come `host:porta`; senza porta si usa quella del certificato e, in mancanza, la **200**. Il testo dopo un apostrofo (`'`) è considerato un commento.
- L'autenticazione usa le credenziali SSH contenute nel certificato e, se presente, la chiave privata.
- Dopo la connessione il programma rileva il sistema operativo del server (comando `ver` per Windows, `lsb_release -d` per Linux).
- Il server scelto viene ricordato per il profilo e riproposto all'avvio successivo.
- Se la connessione cade, il programma lo segnala («Connection Lost») e tenta di riconnettersi automaticamente finché non si preme **Disconnetti**.
- Se il certificato prevede un solo server, all'avvio la finestra viene ridotta a icona e, se il certificato abilita il pulsante RDP, la connessione parte automaticamente.

7.2 Apertura di una sessione su un PC remoto

1. A connessione avvenuta, fare **doppio clic** sul computer desiderato nell'elenco di destra.
2. Se è prevista la password intermedia compare una finestra con il nome della connessione: inserirla e premere **OK**.
3. Si apre la sessione remota e la finestra di Ssh_Tunnel viene ridotta a icona.

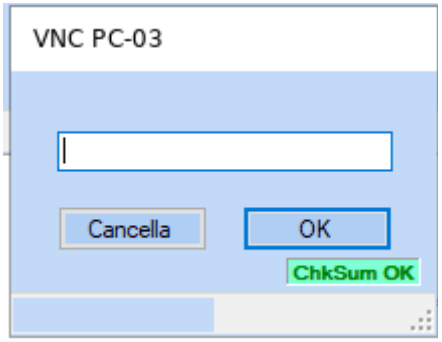

Figura 5 – Richiesta della password intermedia per una connessione

Attenzione

Dopo **3 password intermedie errate** il programma si disconnette e si chiude («Superato il limite di tentativi ammessi»).

Nota

Se il certificato prevede una mail di notifica accessi, all'apertura di ogni sessione RDP o VNC viene inviata una mail con oggetto «SSh_Tunnel di <proprietario> su <connessione>» e i dati del PC da cui è partito il collegamento.

7.3 Tipi di connessione

Il tipo di sessione dipende dalla configurazione della voce nel certificato:

Tipo	Programma usato	Note
Desktop remoto (RDP)	Client scelto con le opzioni RDP	Tipo predefinito per le voci con file RDP.
VNC	`vncviewer.exe` (sessione condivisa)	La password del PC remoto, se presente nel certificato, viene passata automaticamente. Con PC in stato di logoff possono servire le credenziali Windows.
Terminale	`Ssh_Console.exe`	Console SSH verso l'host indicato.
Telecamera	`IPCamera.exe`	Le finestre si affiancano automaticamente sullo schermo; le registrazioni vanno in `C:\SDT_Cam_Recorder\`. Riaprendo la stessa telecamera la finestra precedente viene chiusa.

Client per il desktop remoto:

Opzione	Comportamento
MS RDP	Usa `mstsc.exe` di Windows con un file .rdp temporaneo. La password del PC remoto non viene passata.
RDP+	Usa il client RDP+ incorporato a schermo intero, con unità e stampanti reindirizzate; la password del PC remoto viene cifrata con gencrypt e passata in automatico.
Old RDP+	Come RDP+, ma passa la password così com'è (per password già cifrate nel certificato).

Opzione	Comportamento
AlbatrosRDP	Usa il client proprietario AlbatrosRDP: i parametri vengono passati cifrati e la password tramite un canale riservato (named pipe), senza comparire nella riga di comando.

7.4 Pulsante RDP/VNC/Term

Se il certificato lo prevede, a connessione attiva compare il pulsante **RDP/VNC/Term**, che apre direttamente la connessione «statica» definita nel certificato senza passare dall'elenco. Con l'opzione AutoRDP del certificato questa connessione si apre da sola subito dopo la connessione.

7.5 Disconnessione e uscita

- **Disconnetti**: chiude tutti i forwarding, le telecamere e la connessione SSH; interrompe i tentativi di riconnessione.
- **Esci** (o chiusura della finestra): disconnette, cancella i file temporanei e chiude il programma.
- **Riavvia**: come Esci, ma torna alla maschera di accesso per scegliere un altro profilo.

8. Gestione dei port forwarding

Questa parte è disponibile solo se il certificato consente di modificare i forwarding (permesso `AllowsNewForwards`) oppure in modalità «Apri come Putty». In tal caso la finestra principale è più alta e mostra la sezione di editing sotto i pulsanti.

8.1 Abilitare la modifica

1. Spuntare **Accedi a Port Forwarding**: viene chiesta la password intermedia.
2. Con la password corretta la sezione di editing diventa modificabile e l'elenco dei forwarding consente selezione multipla ed esportazione in Excel.

8.2 Campi di un forwarding

Campo	Significato
Host Locale / Porta	Indirizzo e porta su cui il programma ascolta sul PC locale (es. 127.0.0.2:3390). Il pulsante * accanto all'host inserisce 127.0.0.2.
Host Remoto / Porta	Host e porta di destinazione, visti dal server SSH (es. 192.168.1.10:3389).
Nota (Remark)	Nome che compare nell'elenco dei computer. Obbligatorio.
Pwd	Password del PC remoto, passata a VNC o RDP+. Il pulsante occhio la mostra; **RDP Crypt** la cifra con gencrypt per RDP+.
RDP	Contenuto del file di connessione. I tre pulsanti * generano un modello: file .rdp completo, riga VNC, riga terminale.

Modelli generati dai pulsanti:

- RDP: file .rdp standard con `full address` e `server port` pari a host e porta locali, schermo intero, appunti, stampanti e unità reindirizzati.
- VNC: `vnc_config /connect <host>:<porta> /autoacceptnodsm /shared /autoscaling`.
- Terminale: `term_config server=<host> port=<porta> login= password= ppkkeyfilename= ppkkey= ppkkeypwd=` (da completare).

Nel contenuto si possono usare i segnaposto `##host##` e `##port##`, sostituiti al momento dell'apertura con host e porta locali del forwarding. Una voce compare nell'elenco dei computer solo se è spuntata e ha il campo RDP valorizzato; le voci senza file RDP creano solo il tunnel.

8.3 Operazioni sull'elenco

Comando	Effetto
Clic su una riga	Carica la voce nei campi per modificarla.
`<==`	Inserisce la voce nell'elenco o aggiorna quella selezionata (richiede di nuovo la password intermedia). Tutti i campi tranne RDP e Pwd sono obbligatori.
Pulisci	Svuota i campi.
Tutti i Tag / Inverti Tag	Spunta tutte le voci / inverte le spunte. Solo le voci spuntate vengono attivate.
Predefinito	Ripristina l'elenco com'era nell'ultimo salvataggio del certificato.

Se la porta locale indicata è già usata da un'altra voce, il programma propone di cercare automaticamente la prima porta libera.

Attenzione

Le modifiche diventano attive alla **connessione successiva** (compare l'avviso «Modifiche attive alla prossima connessione»).

Per renderle permanenti occorre salvarle nel certificato con **Gestione Certificato › Aggiorna modifiche**; altrimenti vanno perse alla chiusura.

9. Gestione dei server SSH

Se il certificato consente la modifica dei server (permesso `AllowServerIpEditing`), l'elenco dei server diventa editabile e compare un riquadro di comandi:

Comando	Effetto
Aggiungi	Aggiunge all'elenco il testo digitato (formato `host:porta`).
Elimina	Rimuove la voce digitata/selezionata (deve restarne almeno una).
+ / -	Spostano la voce selezionata nell'elenco.
R	Sostituisce il testo dell'ultima voce selezionata con quello digitato.

Anche queste modifiche vanno salvate con **Gestione Certificato › Aggiorna modifiche**. Durante la connessione l'elenco server è bloccato.

10. Modalità «Apri come Putty»

Dalla maschera di accesso, **Varie › Apri come Putty** apre la finestra principale senza certificato, come client SSH generico. Compaiono i campi:

Campo	Uso
Hostname / Porta	Server SSH (porta predefinita 22).
Nome utente / Password	Credenziali SSH.
KeyFile / Pwd KeyFile	Chiave privata (`.ppk`, `.OpenSsh`, `.pri`) e relativa passphrase; il pulsante `....` apre la selezione file.
Timeout (sec.)	Timeout di connessione e intervallo di keep-alive (predefinito 3).

I forwarding si definiscono come descritto nel capitolo 8 e valgono solo per la sessione: in questa modalità non esiste un certificato in cui salvarli.

11. Gestione del certificato

Tutte le voci del menu **Gestione Certificato** chiedono prima conferma se è attiva una connessione (verrà chiusa) e poi la password attuale. Al termine il programma si chiude con il messaggio «Aggiornamento Effettuato: Rientrare nel programma».

11.1 Aggiorna modifiche

Ricostruisce il certificato con l'elenco attuale di server e forwarding (comprese spunte e password) e lo salva nel database con la stessa password. A ogni salvataggio il numero di versione del certificato (`Ssh ver.`) aumenta.

11.2 Cambio Password

Dopo la password attuale si inserisce due volte la nuova password, che deve rispettare questi requisiti:

- almeno 8 caratteri;
- almeno 1 lettera minuscola e 2 maiuscole;
- almeno 1 numero;
- almeno 2 caratteri speciali.

Il certificato viene ricifrato con la nuova password. Se la password coincide con la precedente il certificato viene comunque aggiornato.

11.3 Cambio Password Intermedia

Imposta la password richiesta all'apertura delle sessioni remote. Non sono previsti requisiti di complessità.

11.4 Export Certificato

Esporta il certificato in `C:\Ssh_Tunnel_Certificates\<Profilo>.Ssh_T`, cifrato con la password indicata in fase di export, pronto per essere consegnato e importato su un altro PC (paragrafo 4.4).

L'export richiede una **password autorizzativa**, ottenibile in due modi:

- premendo il pulsante di invio codice: un codice casuale viene spedito alla mail di notifica accessi (o, in mancanza, alla mail principale);
- con la password amministrativa riservata allo sviluppatore, valida solo su PC con autorizzazione Persistent.

Dopo l'autorizzazione si sceglie la password con cui cifrare il file esportato.

11.5 Elimina Certificato

Dopo la password attuale il profilo viene cancellato dal database. Se nel database restano altri profili il programma torna alla maschera di accesso, altrimenti si chiude.

12. Reindirizzamento Albatros (DbKey)

La voce **Albatros › Parametri** apre la maschera **Reindirizza Albatros**, pensata per l'integrazione con gli applicativi Albatros: quando si apre il tunnel verso una sede, gli applicativi possono essere indirizzati automaticamente al database di quella sede.

La parte superiore elenca le configurazioni presenti nell'ambiente Albatros (chiave, DB locale e nota, DB remoto e nota, IP di ping), come riferimento per scegliere la chiave. La parte inferiore contiene le impostazioni del profilo:

Campo	Significato
Abilitato	Attiva la funzione per il profilo.
Alla Connessione	DbKey da impostare quando la connessione SSH riesce.
Alla Disconn.	DbKey da impostare alla disconnessione.
Percorso file txt DbKey	Cartella in cui scrivere il file `_DbKey.txt` (pulsante Predefinito: `C:\ProgramData\Albatros\Common\`).
Nota Connessione / Nota Disconnessione	Testo riportato nel registro e nel log quando la chiave viene applicata.

Premendo **Registra** le impostazioni vengono salvate nell'ambiente Albatros con chiavi del tipo `[<Profilo>]_DbKeyEnabled`, `[<Profilo>]_DbKeyAtConnection` ecc., e applicate subito in base allo stato della connessione. Alla connessione o disconnessione il programma scrive `DbKey=<valore>` nel file `_DbKey.txt` e lo annota nel registro.

13. Log e manutenzione del database

13.1 Registro e log

Ogni riga mostrata nel pannello messaggi viene anche registrata nella tabella Log del database, insieme all'identificativo di processo (sessione) e, alla prima scrittura, alle informazioni hardware del PC. Il log è disattivabile con il parametro `DoNotUseLogSSH_Tunnel`.

13.2 Mostra Log

Dalla maschera di accesso, **DataBase › Gestione Log › Mostra Log**: indicare l'intervallo di date (da data / a data) e premere **Ricerca**. Vengono mostrati sessione, data, ora, informazioni PC e messaggio.

13.3 Invia Log via Mail

DataBase › Gestione Log › Invia Log via Mail: indicare intervallo di date e indirizzo di destinazione e premere **Invia**. Il log del periodo viene esportato in Excel, compresso in zip e spedito; i file temporanei vengono poi cancellati.

13.4 Manutenzione

- **Compatta Database**: recupera lo spazio libero nel file (VACUUM). Viene eseguita automaticamente anche a ogni salvataggio del certificato.
- **Open Ssh_Tunnel DB path**: apre la cartella del database, utile per copie di sicurezza.

13.5 Struttura del database

Il database è un file SQLite protetto da password, alla revisione 2. All'avvio il programma crea le tabelle mancanti e aggiorna automaticamente i database della revisione 1.

Tabella	Contenuto
Parameters	Coppie chiave/valore: `DbVersion`, `login` (ultimo profilo usato), `[<Profilo>]_IP` (ultimo server usato).
Certificati	Proprietario, Profilo, Version, VersionDate, Certificato (testo cifrato).
Licenza	KeyLicenza, Assegnatario, DataAssegnazione, CertificatoLicenza (predisposta, attualmente non usata).
Log	IdSession, DataLog, PcInfo, KeyInfo, Info.

14. Sicurezza

- **Certificato cifrato**: ogni valore sensibile è cifrato con Triple DES usando una chiave derivata dalla password di accesso; il certificato nel suo insieme è a sua volta cifrato. La password non viene mai salvata.
- **Nessuna credenziale visibile**: credenziali SSH, chiave privata e password dei PC remoti restano all'interno del programma e vengono passate direttamente ai client.
- **Legame con l'hardware**: le autorizzazioni del doppio passaggio valgono solo per il PC e l'utente Windows su cui sono state ottenute.
- **Limite di tentativi**: 3 tentativi per la password di accesso, per i codici del doppio passaggio e per la password intermedia.
- **Scadenza a mezzanotte** per le autorizzazioni OneDay e OneTime.
- **Tracciabilità**: mail con i dati del PC a ogni richiesta di codici e a ogni accesso RDP/VNC, log locale delle sessioni, registrazione degli accessi sul server SSH.
- **Pulizia**: i programmi ausiliari e i file .rdp temporanei vengono cancellati all'avvio e all'uscita.
- **Integrità**: l'indicatore «ChkSum OK» segnala che l'eseguibile non è stato alterato.

> **Nota**
>
> La password intermedia non è una vera protezione crittografica: serve a impedire l'uso del programma lasciato aperto e incustodito.

15. Messaggi e risoluzione dei problemi

Messaggio / sintomo	Causa e rimedio
«Password errata: impossibile continuare»	Password di accesso errata o profilo sbagliato. Dopo 3 errori il programma si chiude.
«Certificato inesistente»	Il profilo selezionato non è nel database: importare il certificato.
«Two-factor authentication is required!»	PC non autorizzato: seguire il capitolo 5.
«Invio mail ... per doppia verifica fallito!!!»	Problema di invio mail (rete, firewall, SMTP). Riprovare o usare «Invia Codice via SMS al Supporto».
«Codice errato: Tentativi n di 3»	Codice digitato in modo errato o di una richiesta precedente.
«Chiusura automatica per mancato input codice»	Superati i 5 minuti senza inserire il codice.
«Internet Connection Not Available» / «Waiting ...»	Manca la connessione a Internet; il programma attende. Togliere «Chk Internet» per saltare il controllo.
«Errore login!!!»	Impossibile preparare la connessione (credenziali o chiave del certificato non valide). Contattare l'amministratore.
Connessione che non si stabilisce	Server non raggiungibile: provare un server alternativo dell'elenco; usare Utility › Ping No-IP per verificare la risoluzione del nome.
«### Error Forward Host: ...»	La porta locale del forwarding è occupata da un altro programma o l'host locale non è valido.
«Connection Lost»	Connessione caduta: il programma si riconnette da solo.
«Password errata» / «Superato il limite di tentativi ammessi»	Password intermedia errata; al terzo errore il programma si chiude.
«Ssh Tunnel arrestato per scadenza password...»	Raggiunta la mezzanotte con autorizzazione OneDay/OneTime: riavviare e richiedere un nuovo codice.
«Riscontrata anomalia tra la versione attesa e quella trovata nel Database di servizio»	Il database non può essere aggiornato: spostare il programma in una cartella con permessi di scrittura.
«Operazione annullata per password difforme»	Password attuale errata nelle funzioni di Gestione Certificato.
«Porta già utilizzata: Cerco la prima occorrenza libera?»	Porta locale già assegnata a un altro forwarding.
«Dati Insufficienti!»	Mancano campi obbligatori nell'inserimento di un forwarding.

Appendice A – Riepilogo rapido per l'utente

1. Copiare `.exe` e `.db` nella stessa cartella.
2. Avviare l'eseguibile e inserire la password di accesso.
3. Se richiesto, premere «Richiedi via mail» e inserire il codice OneDay o OneTime ricevuto.
4. Attendere «SSH Tunneling Ready ....» e premere **Connetti**.
5. Fare doppio clic sul computer desiderato nell'elenco di destra.
6. Inserire la password intermedia, se richiesta.
7. Lavorare sul PC remoto; al termine premere **Disconnetti** o **Esci**.

Appendice B – Struttura del certificato

Il certificato (versione 2) è un testo di righe `Chiave = "valore"`, cifrato nel suo insieme con la password. I valori sensibili sono a loro volta cifrati singolarmente. Elenco delle chiavi riconosciute:

Chiave	Contenuto
`Algoritmo`	Versione dell'algoritmo di cifratura (1).
`Nominativo`	Nome del profilo (in chiaro).
`SshUserDllVersion`	Numero progressivo e data dell'ultimo salvataggio.
`Bloccato`	Certificato con funzioni ridotte (niente dettagli nel registro, niente strumenti esterni).
`ShowRdpButton`	Mostra il pulsante RDP/VNC/Term per la connessione statica.
`AutoRDP`	Apre la connessione statica subito dopo la connessione.
`AllowsNewForwards`	Consente la modifica dei port forwarding.
`AllowServerIpEditing`	Consente la modifica dell'elenco server.
`Proprietario`	Destinatario del software («Sw consegnato a»).
`Login`, `Password`	Credenziali SSH.
`Certificate`, `CertificatePassword`, `FileCertificato`	Chiave privata SSH (testo o risorsa incorporata) e relativa passphrase.
`PwdRemoteAccess`	Password intermedia.
`Server`, `ServerPort`	Elenco server separati da `&` e porta predefinita.
`RdpCommandLine`, `RdpFileStatico`	Riga di comando e file della connessione statica.
`Mail`, `MailOneDay`, `MailTemp`	Destinatari dei codici del doppio passaggio.
`MailInfoAccess`	Destinatario delle notifiche di accesso.
`Cellulare`	Numero di cellulare (predisposto).
`RedirectPortsCount`	Numero dei forwarding.
`RedirectPorts(i, …)`	Per ogni forwarding: LocalHost, LocalPort, RemoteHost, RemotePort, Remark, RdpFile, Enabled (Y/N), PasswordRdpFF, PwdActivateRdpConnection.

Appendice C – Note tecniche per lo sviluppatore

Durante la stesura del manuale sono emersi nel codice alcuni punti da verificare. Questa appendice è a uso interno: va tolta prima di consegnare il manuale ai destinatari del programma.

File / routine	Osservazione
ModSetting.Log	Verifica l'esistenza del database in `Application.StartupPath` con il nome dell'exe, ignorando `PathDbSSH_Tunnel` e `FileNameDbSSH_Tunnel`: se il DB è altrove o ha un altro nome, il log non viene scritto.
ModSetting.RemoveParam	La query usa `lower('?')`: il parametro tra apici non viene sostituito, quindi la cancellazione non ha effetto.
ModSetting.DecodCertificate	Il confronto `ToLower.Contains("Algoritmo =")` contiene una maiuscola e non è mai vero: il valore `Algoritmo` non viene letto (oggi senza conseguenze, vale sempre 1).
FrmStart_Load	`ContaErrori` è locale al ciclo e si azzera a ogni giro; inoltre se il doppio passaggio fallisce o la maschera viene chiusa, `Exit Sub` non termina l'applicazione: verificare che non resti un processo attivo senza finestra.
frmMainProgram, pulsanti + / - server	I tooltip sono invertiti: - (tooltip «Sposta Giù») sposta in su, + (tooltip «Sposta Su») sposta in giù.
frmMainProgram, pulsanti modello *	Il tooltip indica `###Host### / ###Port###`, ma i segnaposto sostituiti dal codice sono `##host##` / `##port##`.
EseguiExportCertificato	La «supercode» abilita il salvataggio della password su file `.Ssh_T.Key`, ma `CostruisciRemPwdInfo` e `abilitaSalvataggioPwd` non vengono usati: la funzione non è implementata.
ChkIconaAfterSelection	L'opzione «Icona dopo selezione» non è referenziata nel codice.
GetParam / SetParam	La chiave è concatenata nella query SQL anziché passata come parametro.
Sorgenti in generale	Nei sorgenti sono presenti in chiaro credenziali e chiavi (servizio SMS, accesso SFTP per gli aggiornamenti, password del DB, impronta della password amministrativa). Chi ha accesso all'eseguibile può estrarle con un decompilatore .NET: valutare offuscamento o spostamento lato server.

Ssh_Tunnel

Client SSH pentru acces la distanță controlat

Manual de utilizare și de administrare

Versiunea software 27.2.2036.6127 · DB rev. 2

© Raffaele Romano
Octombrie 2026

Cuprins

1. Introducere....92
1.1 Cui se adresează acest manual....92
1.2 Versiunea documentată....92

2. Concepte fundamentale....93

3. Instalare și cerințe....94
3.1 Fișiere necesare....94
3.2 Cerințe....94
3.3 Programe încorporate....94
3.4 Fișier de parametri extern (opțional)....94
3.5 Componente opționale în folder....95

4. Pornire și autentificare....96
4.1 Fereastra de autentificare....96
4.2 Introducerea parolei....97
4.3 Meniul ferestrei de autentificare....97
4.4 Importarea unui certificat....97

5. Verificarea în doi pași (autorizarea PC-ului)....99
5.1 Când este solicitată....99
5.2 Solicitarea codurilor....99
5.3 Niveluri de autorizare....99
5.4 Meniul „Varie” al verificării în doi pași....100
5.5 Revocarea autorizării....100

6. Fereastra principală....101
6.1 Prezentare generală....101
6.2 Opțiuni....101
6.3 Meniul ferestrei principale....102

7. Conectare și sesiuni la distanță....103
7.1 Conectarea la serverul SSH....103
7.2 Deschiderea unei sesiuni pe un PC la distanță....103
7.3 Tipuri de conexiune....104
7.4 Butonul RDP/VNC/Term....105
7.5 Deconectare și ieșire....105

8. Gestionarea redirecționărilor de porturi....106
8.1 Activarea modificării....106
8.2 Câmpurile unei redirecționări....106
8.3 Operațiuni asupra listei....106

9. Gestionarea serverelor SSH....108

10. Modul „Apri come Putty”....109

11. Gestionarea certificatului....110
11.1 Aggiorna modifiche....110
11.2 Cambio Password....110
11.3 Cambio Password Intermedia....110
11.4 Export Certificato....110
11.5 Elimina Certificato....110

12. Redirecționarea Albatros (DbKey)....111

13. Jurnale și întreținerea bazei de date....112
13.1 Registru și jurnal.... 112
13.2 Mostra Log.... 112
13.3 Invia Log via Mail.... 112
13.4 Întreținere.... 112
13.5 Structura bazei de date.... 112
14. Securitate....113
15. Mesaje și depanare....114
Anexa A – Rezumat rapid pentru utilizator....115
Anexa B – Structura certificatului....116
Anexa C – Note tehnice pentru dezvoltator....117

1. Introducere

Ssh_Tunnel este un client SSH pentru Windows, dezvoltat în VB.NET, care permite accesarea controlată a PC-urilor și serverelor dintr-o rețea de companie (prin RDP, VNC, terminal SSH sau camere IP) printr-un tunel criptat către un server SSH al companiei.

A apărut ca alternativă la instrumente precum TeamViewer, AnyDesk și altele similare: acestea garantează un trafic criptat, dar oricine deține acreditările poate accesa sistemele, legând securitatea rețelei de terți. Ssh_Tunnel, în schimb:

- nu conține nicio parolă în clar: toți parametrii de conectare sunt încapsulați într-un **certificat criptat**, care poate fi deschis numai cu parola de acces furnizată utilizatorului;
- atribuie fiecărui destinatar (centru de asistență, tehnician, consultant) un **certificat unic**, astfel încât serverul SSH să recunoască cine se conectează și să înregistreze data, ora și durata;
- poate lega utilizarea de un anumit PC printr-o **verificare în doi pași** (cod trimis prin e-mail), cu autorizare permanentă, zilnică sau numai pentru sesiunea curentă;
- notifică prin e-mail fiecare acces la un PC la distanță, indicând de pe ce computer s-a realizat conexiunea;
- prezintă utilizatorului numai conexiunile prevăzute în certificatul său, sub forma unei liste de computere pe care se face dublu clic.

1.1 Cui se adresează acest manual

Manualul este împărțit în trei părți:

- **Utilizare zilnică** (capitolele 3–7): instalare, autentificare, verificare în doi pași, conectare și deschiderea sesiunilor la distanță. Este partea care se predă celui care primește programul.
- **Administrare** (capitolele 8–13): gestionarea redirecționărilor de porturi, a serverelor, a certificatelor, a redirecționării Albatros, a jurnalelor și a bazei de date.
- **Referință tehnică** (capitolele 14–15 și anexele): arhitectură, securitate, structura certificatului, mesaje și depanare.

1.2 Versiunea documentată

Element	Valoare
Program	Ssh_Tunnel
Versiune software	27.2.2036.6127 (data build-ului 11/10/2026)
Revizia bazei de date	2
Versiunea certificatului	2 (Algoritm = 1)
Platformă	.NET Framework 4.8, Windows, compilări pe 32 și 64 de biți
Biblioteci principale	Renci SSH.NET 2025, System.Data.SQLite, AlbatrosCommon
Limbile interfeței	Italiană, engleză, franceză, japoneză, română (alegere automată în funcție de limba Windows)

Versiunea afișată de program are forma `Sw ver.: 27.2.2036.6127 - 11/10/2026`: data este derivată din numărul reviziei (zile scurse de la 01/01/2010) și corespunde, așadar, datei compilării.

2. Concepte fundamentale

Înainte de a utiliza programul, este util să cunoașteți câțiva termeni care apar în toate ferestrele.

Termen	Semnificație
Profil	Nume care identifică un certificat (de ex. „Sede -> Cliente”). În aceeași bază de date pot coexista mai multe profiluri; la pornire se alege cel care va fi folosit.
Certificat	Bloc criptat care conține tot ce este necesar pentru conectare: serverul SSH și porturile, acreditările SSH, cheia privată, lista redirecționărilor de porturi, fișierele RDP/VNC, adresele de e-mail, permisiunile. Este distribuit ca fișier `.Ssh_T` și importat în baza de date.
Parolă de acces	Parola solicitată la pornire. Decriptează certificatul: fără ea, programul nu cunoaște nici serverele, nici acreditările.
Parolă intermediară (acces la distanță)	A doua parolă, solicitată în momentul deschiderii unei sesiuni pe un PC la distanță. Are rolul de a împiedica folosirea de către alții a unui program lăsat deschis și nesupravegheat.
Parolă specifică de conexiune	Parolă intermediară definită pentru un singur element din listă; dacă există, are prioritate față de cea generală.
Verificare în doi pași	Verificare suplimentară: la prima utilizare pe un PC se solicită un cod prin e-mail. Autorizarea este legată de hardware-ul PC-ului.
Cod Persistent / OneDay / OneTime	Cele trei coduri ale verificării în doi pași: autorizare permanentă, valabilă până la miezul nopții, valabilă numai pentru sesiunea curentă (vezi capitolul 5).
Redirecționare de port (tunel)	Asocierea „adresă și port locale → gazdă și port la distanță” stabilită prin conexiunea SSH. Fiecărui computer accesibil îi corespunde o redirecționare.
DbKey	Cheie folosită de aplicațiile Albatros pentru a alege baza de date de lucru; Ssh_Tunnel o poate schimba automat la conectare și la deconectare (capitolul 12).

3. Instalare și cerințe

3.1 Fișiere necesare

Ssh_Tunnel nu necesită instalare și nici drepturi de administrator. Este suficient să copiați în același folder:

Fișier	Descriere
`Ssh_Tunnel_<Nome>.exe`	Executabilul programului (numele poate fi personalizat pentru fiecare destinatar; se poate termina cu 32 sau 64).
`Ssh_Tunnel_<Nome>.db`	Bază de date SQLite criptată care conține certificate, parametri și jurnale.

Numele bazei de date este derivat din numele executabilului, eliminând eventualul sufix `32` sau `64` și adăugând `.db`. Exemplu: `Ssh_Tunnel_Esempio64.exe` caută `Ssh_Tunnel_Esempio.db`. Astfel, versiunea pe 32 și cea pe 64 de biți partajează aceeași bază de date.

> **Notă**
>
> Dacă baza de date nu există, este creată goală la prima pornire; în acest caz trebuie importat un certificat (secțiunea 4.4) înainte de a vă putea autentifica.
>
> Dacă apare mesajul „Riscontrata anomalia tra la versione attesa e quella trovata nel Database di servizio”, mutați programul într-un folder fără restricții de scriere (de exemplu, nu sub `C:\Program Files`).

3.2 Cerințe

- Windows cu .NET Framework 4.8.
- Acces la Internet de ieșire către serverul SSH al companiei (portul implicit este 200, dacă certificatul nu indică altfel).
- Pentru verificarea în doi pași și notificări: posibilitatea de a trimite e-mailuri (programul folosește parametrii SMTP interni ai bibliotecii Albatros).

3.3 Programe încorporate

Executabilul conține programele auxiliare, care sunt extrase numai atunci când este nevoie în folderul temporar `%TEMP%\Albatros\Ssh_Tunnel` și șterse la pornire și la ieșire:

Componentă	Utilizare
`vncviewer.exe` / `vncviewer32.exe`	Vizualizator VNC (versiune pe 64 sau 32 de biți în funcție de proces).
`rdp.exe`	Client RDP+ (desktop la distanță cu transmiterea automată a parolei).
`gencrypt.exe`	Criptarea parolelor pentru RDP+.
`AlbatrosRDP.exe`	Client RDP proprietar cu transmiterea securizată a parolei.
`Ssh_Console.exe`	Consolă terminal SSH.
`IPCamera.exe`	Vizualizator pentru camere IP.

3.4 Fișier de parametri extern (opțional)

Prin mecanismul parametrilor externi al bibliotecii AlbatrosCommon (fișier text cu rânduri `Var_<nome>=<valore>`, vezi exemplul `Data\Ssh_Tunnel_Merge.txt` din surse) se pot seta:

Parametru	Efect	Implicit
`PathDbSSH_Tunnel`	Folderul bazei de date	Folderul executabilului
`FileNameDbSSH_Tunnel`	Numele fișierului bazei de date	Derivat din numele exe-ului
`DoNotUseLogSSH_Tunnel`	Dacă este `True`, dezactivează jurnalul în baza de date și salvarea ultimului profil/server utilizat	`False`

3.5 Componente opționale în folder

Dacă aceste fișiere se află în folderul programului, Ssh_Tunnel le recunoaște:

- `Ssh_Updater.exe`: este pornit automat la deschiderea ferestrei de autentificare (actualizarea programului).
- `Database4.exe` sau `Database5Pro.exe`, `DbMigration.exe`, `Convert.exe`: apar în meniul **FishCodeLib** (gestionarea bazei de date, migrare, conversie).

4. Pornire și autentificare

4.1 Fereastra de autentificare

La pornirea executabilului apare fereastra **Password**. În titlu este afișată ora curentă.

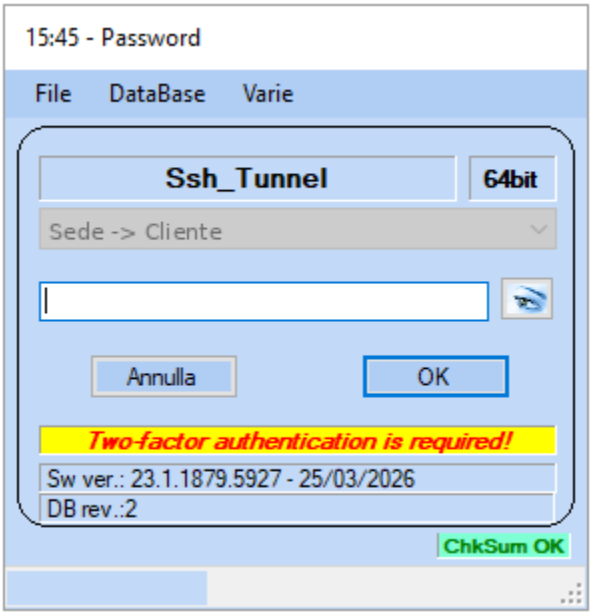

Figura 1 – Fereastra de autentificare cu solicitarea verificării în doi pași

Element	Funcție
Numele programului și „64bit/32bit”	Indică versiunea în execuție.
Lista profilurilor	Profilurile din baza de date. Dacă există unul singur, este blocat; dacă sunt mai multe, se propune ultimul utilizat.
Câmpul parolă și butonul „ochi”	Introducerea parolei de acces; ochiul afișează/ascunde caracterele.
Annulla / OK	Închide programul / confirmă parola.
Rândul de stare	Starea autorizării PC-ului (vezi tabelul următor).
Sw ver. / DB rev.	Versiunea programului, a certificatului și a bazei de date.
ChkSum OK	Verificarea integrității executabilului: dacă lipsește sau semnalează o eroare, nu continuați.

Rândul de stare poate afișa:

Mesaj	Semnificație
„Two-factor authentication is required!” (galben/roșu)	PC-ul nu este autorizat: după parolă se va solicita verificarea în doi pași.
„One Day Code is active!” (galben)	PC-ul este autorizat până la miezul nopții de azi.
„Persistent Code is active!” (verde)	PC-ul este autorizat permanent.

4.2 Introducerea parolei

1. Selectați profilul (dacă există mai multe).
2. Tastați parola de acces și apăsați **OK**.
3. Dacă parola este corectă, certificatul este decriptat; dacă este prevăzută verificarea, se deschide fereastra verificării în doi pași (capitolul 5), altfel fereastra principală.

> **Atenție**
>
> După **3 parole greșite**, programul se închide.
>
> Dacă Ssh_Tunnel rulează deja, se întreabă dacă se deschide o nouă instanță; răspunzând No (Nu), este adusă în prim-plan instanța deja deschisă.

4.3 Meniul ferestrei de autentificare

Meniu	Element	Funcție
File	Esci	Închide programul.
DataBase	Gestione Log › Abilita Log	Vizibil numai dacă jurnalul este dezactivat prin parametru: îl reactivează pentru sesiunea curentă.
	Gestione Log › Mostra Log	Consultarea jurnalului (capitolul 13).
	Gestione Log › Invia Log via Mail	Trimiterea jurnalului ca atașament (capitolul 13).
	Utility › Compatta Database	Execută VACUUM pe baza de date SQLite.
	Utility › Open Ssh_Tunnel DB path	Deschide în Explorer folderul bazei de date (calea completă se află în sfatul ecran al elementului).
	Utility › Importa Certificato Ssh Tunnel	Importarea unui fișier `.Ssh_T` (secțiunea 4.4).
	FishCodeLib	Instrumente externe, dacă există (secțiunea 3.5).
Varie	Abilita Accesso con Doppio Passaggio	Revocă autorizarea memorată pentru profil pe acest PC (secțiunea 5.5).
	Apri come Putty	Pornește programul în modul client SSH liber (capitolul 10).
	Scarica AlbatrosRDP	Salvează `AlbatrosRDP.exe` în folderul Descărcări al utilizatorului și îl deschide.

4.4 Importarea unui certificat

Un profil nou se adaugă importând fișierul certificat `.Ssh_T` primit de la administrator.

1. Din fereastra de autentificare alegeți **DataBase › Utility › Importa Certificato Ssh Tunnel**.
2. Glisați fișierul `.Ssh_T` în zona indicată sau faceți dublu clic pe ea pentru a-l alege.
3. Introduceți parola certificatului.
4. Programul afișează numele și proprietarul și cere confirmare; dacă există deja un profil cu același nume, întreabă dacă trebuie înlocuit.
5. La final, noul profil apare în lista din fereastra de autentificare.

> **Notă**
>
> Dacă parola este greșită, programul răspunde „Pwd errata” și nu se importă nimic. Certificatul este salvat în baza de date tot criptat: parola nu este memorată.

5. Verificarea în doi pași (autorizarea PC-ului)

5.1 Când este solicitată

Verificarea în doi pași se declanșează numai dacă certificatul conține cel puțin o adresă de e-mail pentru coduri și PC-ul utilizat nu este deja autorizat pentru acel profil. Autorizarea este legată de identificatorul hardware al computerului (ID-ul procesorului sau, în lipsa acestuia, numărul de serie al plăcii de bază sau al discului), astfel încât copierea programului pe alt PC necesită o nouă autorizare.

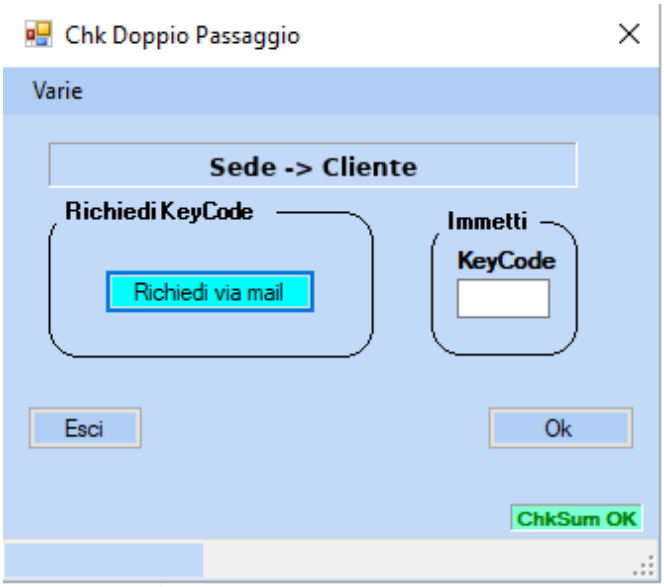

Figura 2 – Fereastra „Chk Doppio Passaggio”

5.2 Solicitarea codurilor

1. Apăsați **Richiedi via mail** (Solicitare prin e-mail). Programul generează trei coduri aleatorii de 5 cifre și le trimite la adresele prevăzute în certificat.
2. Așteptați e-mailul; apare textul „Codici inviati”.
3. Introduceți unul dintre codurile primite în câmpul **KeyCode** și apăsați **Ok**.

Codurile sunt generate la deschiderea ferestrei și rămân valabile numai cât timp aceasta este deschisă: dacă închideți programul, trebuie să solicitați altele noi. Fiecare e-mail conține și datele de identificare ale PC-ului solicitant (IP local și public, numele PC-ului, numerele de serie ale discului, procesorului și plăcii de bază).

Destinatarii codurilor, în funcție de adresele configurate în certificat:

Adresa din certificat	Coduri primite
E-mail principal (`Mail`)	Persistent, OneDay și OneTime
E-mail OneDay (`MailOneDay`)	OneDay și OneTime
E-mail OneTime (`MailTemp`)	Numai OneTime

Dacă două adrese coincid, e-mailul nu este dublat. Astfel, codul permanent poate fi rezervat administratorului, în timp ce clientul primește numai codurile temporare.

5.3 Niveluri de autorizare

Cod	Efect	Expirare
Persistent	PC-ul rămâne autorizat pentru profil; la deschiderile ulterioare codul nu mai este solicitat.	Niciuna (până la revocare)

Cod	Efect	Expirare
OneDay	PC-ul este autorizat pentru întreaga zi.	Miezul nopții zilei curente
OneTime	Autorizează numai sesiunea curentă; la redeschidere este necesar un cod nou.	Închiderea programului și, în orice caz, miezul nopții

Atenție

Cu codurile OneDay și OneTime, fereastra principală afișează „Ssh Tunnel: disattivazione alle 00.00”: la miezul nopții apare avertismentul „Ssh Tunnel arrestato per scadenza password...” și programul se închide, închizând și camerele deschise.

După **3 coduri greșite**, fereastra se închide. Dacă niciun cod nu este introdus în **5 minute**, programul se închide automat (cu o numărătoare inversă de 10 secunde).

5.4 Meniul „Varie” al verificării în doi pași

Element	Funcție
Mostra Chk Mail Persistente	Face vizibilă opțiunea „Invia solo alla Mail Principale”: dacă este activată, codurile sunt trimise numai la adresa care primește codul Persistent.
Aggiorna Timer	Repornește cele 5 minute de așteptare.
Invia Codice via SMS al Supporto	Trimite cele trei coduri prin SMS la numărul de asistență presetat în program (util dacă e-mailul nu funcționează).

5.5 Revocarea autorizării

Pentru a retrage unui PC autorizarea Persistent sau OneDay: în fereastra de autentificare selectați profilul și alegeți **Varie › Abilita Accesso con Doppio Passaggio**, apoi confirmați. La următoarea autentificare, codul va fi solicitat din nou. Elementul este activ numai când PC-ul este deja autorizat.

Notă

Autorizarea este salvată, criptată, în registry-ul Windows al utilizatorului curent: `HKEY_CURRENT_USER\Software\Albatros.net`, valoarea `Ssh_Tunnel_<Profilo>`. Prin urmare, este valabilă pentru utilizatorul Windows care a obținut-o.

6. Fereastra principală

6.1 Prezentare generală

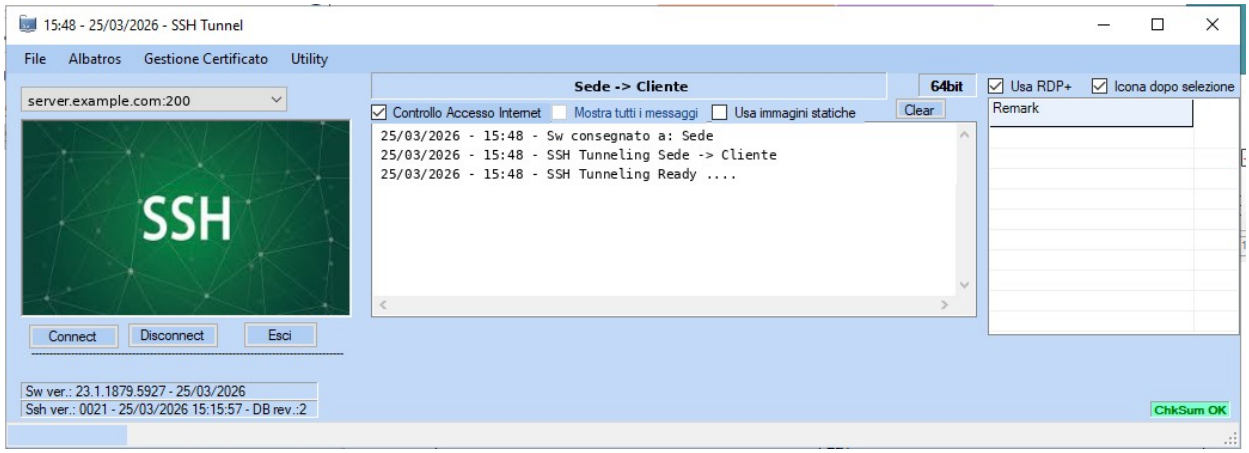

Figura 3 – Fereastra principală înainte de conectare

Zonă	Conținut
Stânga sus	Lista serverelor SSH disponibile (vizibilă dacă există mai multe sau dacă certificatul permite modificarea lor).
Imagine de stare	Sigla SSH în repaus; animație de conectare reușită sau întreruptă în timpul utilizării.
Butoane	**Connetti**, **Disconnetti**, **Esci** și, dacă în baza de date există mai multe profiluri, **Riavvia** (revine la fereastra de autentificare pentru a schimba profilul).
Panoul central	Registrul mesajelor cu data și ora. Rândurile de eroare sunt în roșu; cele care conțin „###” au fundal galben.
Lista din dreapta	Computere accesibile (coloana Remark), completată după conectare.
Bara de stare	Versiunea software-ului și a certificatului, revizia DB, „ChkSum OK”.

6.2 Opțiuni

Opțiune	Efect
Chk Internet	Înainte de conectare verifică dacă Internetul este accesibil; în lipsa lui, așteaptă până când conexiunea redevine disponibilă. Activă implicit.
Mostra tutti i messaggi	Afișează în registru și detaliile redirecționărilor de porturi (IP-urile și porturile locale și la distanță). Nu este disponibilă pentru certificatele „blocate”.
Usa immagini statiche	Înlocuiește animațiile de stare cu imagini fixe.
Icona dopo selezione	Opțiune de afișare a listei de computere.
RDP+ / AlbatrosRDP / MS RDP / Old RDP+	Alege clientul folosit pentru conexiunile desktop la distanță (secțiunea 7.3). Implicit: MS RDP.
Clear	Golește registrul și reafișează informațiile certificatului.

6.3 Meniul ferestrei principale

Meniu	Element	Funcție
File	Esci	Deconectează, curăță fișierele temporare și închide programul.
Albatros	Parametri	Redirecționarea Albatros / DbKey (capitolul 12).
	FishCodeLib	Instrumente externe (dacă există și dacă certificatul nu este blocat).
Gestione Certificato	Aggiorna modifiche	Salvează în certificat serverele și redirecționările modificate (secțiunea 11.1).
	Cambio Password / Port FF	Schimbă parola de acces.
	Cambio Pwd Intermedia / Port FF	Schimbă parola intermediară.
	Export Certificato	Exportă certificatul într-un fișier `.Ssh_T`.
	Elimina Certificato	Elimină profilul din baza de date.
	Apri percorso DB Ssh_Tunnel	Deschide folderul bazei de date.
Utility	Ping No-IP	Rezolvă prin DNS numele serverului selectat și afișează IP-ul acestuia.
	Ping IP	Execută un ping către server, dacă este indicat ca adresă IP.
	Scarica AlbatrosRDP	Salvează `AlbatrosRDP.exe` în folderul Descărcări.

În modul „Apri come Putty”, meniurile Albatros și Gestione Certificato nu sunt disponibile.

7. Conectare și sesiuni la distanță

7.1 Conectarea la serverul SSH

1. Verificați în registru textul **SSH Tunneling Ready ....**
2. Dacă lista serverelor este vizibilă, alegeți serverul: în condiții normale este suficient primul; celelalte sunt accese alternative de folosit dacă serverul principal nu răspunde (unele funcționează numai din interiorul rețelei companiei).
3. Apăsați **Connetti** (Conectare).

Registrul afișează succesiunea operațiunilor:

```
Disconnected
Testing Internet connection status
Connecting...
Server: <nome server>
port: 200
Connecting to <nome server>:200
CONNECTED
S.O. <sistema operativo del server>
```

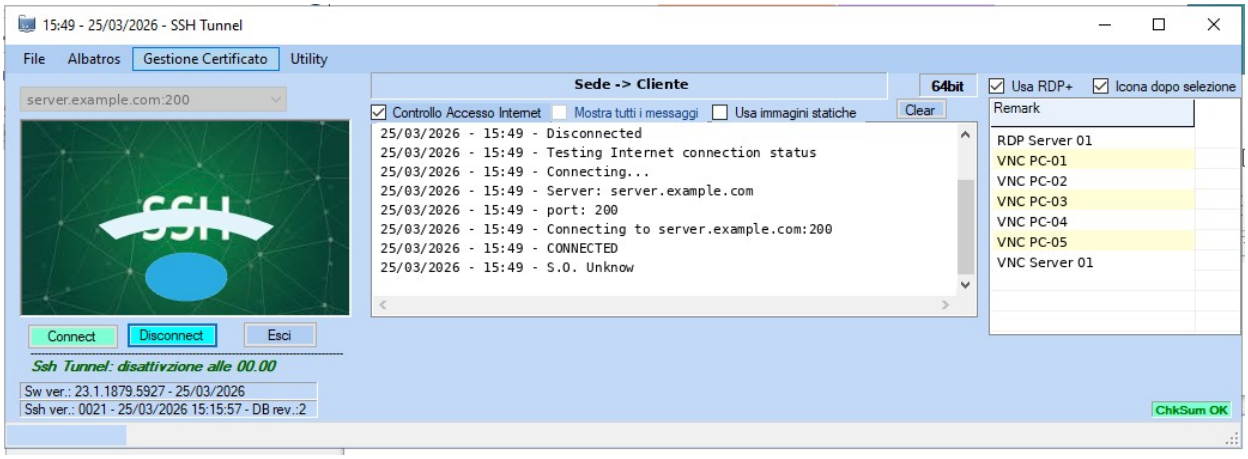

Figura 4 – Conexiune stabilită: în dreapta, lista computerelor accesibile

Detalii de funcționare:

- Serverul poate fi indicat ca `host:porta`; fără port se folosește cel din certificat și, în lipsa acestuia, **200**. Textul de după un apostrof (`'`) este considerat comentariu.
- Autentificarea folosește acreditările SSH conținute în certificat și, dacă există, cheia privată.
- După conectare, programul detectează sistemul de operare al serverului (comanda `ver` pentru Windows, `lsb_release -d` pentru Linux).
- Serverul ales este memorat pentru profil și propus din nou la următoarea pornire.
- Dacă conexiunea cade, programul o semnalează („Connection Lost”) și încearcă să se reconecteze automat până când apăsați **Disconnetti**.
- Dacă certificatul prevede un singur server, la pornire fereastra este minimizată și, dacă certificatul activează butonul RDP, conexiunea pornește automat.

7.2 Deschiderea unei sesiuni pe un PC la distanță

1. După conectare, faceți **dublu clic** pe computerul dorit din lista din dreapta.
2. Dacă este prevăzută parola intermediară, apare o fereastră cu numele conexiunii: introduceți-o și apăsați **OK**.
3. Se deschide sesiunea la distanță, iar fereastra Ssh_Tunnel este minimizată.

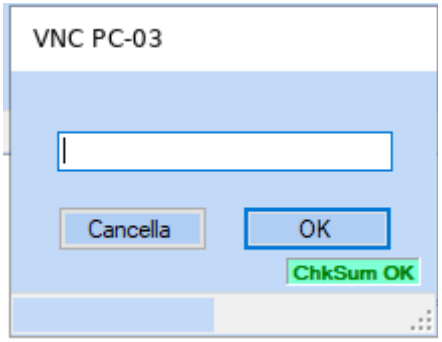

Figura 5 – Solicitarea parolei intermediare pentru o conexiune

Atenție

După **3 parole intermediare greșite**, programul se deconectează și se închide („Superato il limite di tentativi ammessi”).

Notă

Dacă certificatul prevede un e-mail de notificare a accesărilor, la deschiderea fiecărei sesiuni RDP sau VNC se trimite un e-mail cu subiectul „SSh_Tunnel di <proprietario> su <connessione>” și datele PC-ului de pe care a pornit conexiunea.

7.3 Tipuri de conexiune

Tipul sesiunii depinde de configurarea elementului în certificat:

Tip	Program utilizat	Note
Desktop la distanță (RDP)	Clientul ales cu opțiunile RDP	Tip implicit pentru elementele cu fișier RDP.
VNC	`vncviewer.exe` (sesiune partajată)	Parola PC-ului la distanță, dacă există în certificat, este transmisă automat. Cu PC-ul în starea deconectat (logoff) pot fi necesare acreditările Windows.
Terminal	`Ssh_Console.exe`	Consolă SSH către gazda indicată.
Cameră	`IPCamera.exe`	Ferestrele se aranjează automat una lângă alta pe ecran; înregistrările merg în `C:\SDT_Cam_Recorder\`. La redeschiderea aceleiași camere, fereastra anterioară este închisă.

Clienți pentru desktopul la distanță:

Opțiune	Comportament
MS RDP	Folosește `mstsc.exe` din Windows cu un fișier .rdp temporar. Parola PC-ului la distanță nu este transmisă.
RDP+	Folosește clientul RDP+ încorporat pe ecran complet, cu unitățile și imprimantele redirecționate; parola PC-ului la distanță este criptată cu gencrypt și transmisă automat.
Old RDP+	Ca RDP+, dar transmite parola ca atare (pentru parolele deja criptate în certificat).
AlbatrosRDP	Folosește clientul proprietar AlbatrosRDP: parametrii sunt transmiși criptați, iar parola printr-un canal rezervat (named pipe), fără a apărea în linia de comandă.

7.4 Butonul RDP/VNC/Term

Dacă certificatul prevede acest lucru, cu conexiunea activă apare butonul **RDP/VNC/Term**, care deschide direct conexiunea „statică” definită în certificat, fără a trece prin listă. Cu opțiunea AutoRDP a certificatului, această conexiune se deschide singură imediat după conectare.

7.5 Deconectare și ieșire

- **Disconnetti** (Deconectare): închide toate redirecționările, camerele și conexiunea SSH; întrerupe încercările de reconectare.
- **Esci** (Ieșire) (sau închiderea ferestrei): deconectează, șterge fișierele temporare și închide programul.
- **Riavvia** (Repornire): ca Esci, dar revine la fereastra de autentificare pentru a alege alt profil.

8. Gestionarea redirecționărilor de porturi

Această parte este disponibilă numai dacă certificatul permite modificarea redirecționărilor (permisiunea `AllowsNewForwards`) sau în modul „Apri come Putty”. În acest caz, fereastra principală este mai înaltă și afișează secțiunea de editare sub butoane.

8.1 Activarea modificării

1. Bifați **Accedi a Port Forwarding**: se solicită parola intermediară.
2. Cu parola corectă, secțiunea de editare devine modificabilă, iar lista redirecționărilor permite selecția multiplă și exportul în Excel.

8.2 Câmpurile unei redirecționări

Câmp	Semnificație
Host Locale / Porta	Adresa și portul pe care programul ascultă pe PC-ul local (de ex. 127.0.0.2:3390). Butonul * de lângă gazdă introduce 127.0.0.2.
Host Remoto / Porta	Gazda și portul de destinație, văzute de serverul SSH (de ex. 192.168.1.10:3389).
Nota (Remark)	Numele care apare în lista computerelor. Obligatoriu.
Pwd	Parola PC-ului la distanță, transmisă către VNC sau RDP+. Butonul ochi o afișează; **RDP Crypt** o criptează cu gencrypt pentru RDP+.
RDP	Conținutul fișierului de conexiune. Cele trei butoane * generează un model: fișier .rdp complet, rând VNC, rând terminal.

Modele generate de butoane:

- RDP: fișier .rdp standard cu `full address` și `server port` egale cu gazda și portul local, ecran complet, clipboard, imprimante și unități redirecționate.
- VNC: `vnc_config /connect <host>:<porta> /autoacceptnodsm /shared /autoscaling`.
- Terminal: `term_config server=<host> port=<porta> login= password= ppkkeyfilename= ppkkey= ppkkeypwd=` (de completat).

În conținut se pot folosi substituenții `##host##` și `##port##`, înlocuiți la deschidere cu gazda și portul local ale redirecționării. Un element apare în lista computerelor numai dacă este bifat și are câmpul RDP completat; elementele fără fișier RDP creează doar tunelul.

8.3 Operațiuni asupra listei

Comandă	Efect
Clic pe un rând	Încarcă elementul în câmpuri pentru a-l modifica.
<==	Inserează elementul în listă sau îl actualizează pe cel selectat (solicită din nou parola intermediară). Toate câmpurile, cu excepția RDP și Pwd, sunt obligatorii.
Pulisci	Golește câmpurile.
Tutti i Tag / Inverti Tag	Bifează toate elementele / inversează bifele. Sunt activate numai elementele bifate.
Predefinito	Restabilește lista așa cum era la ultima salvare a certificatului.

Dacă portul local indicat este deja folosit de un alt element, programul propune căutarea automată a primului port liber.

> **Atenție**
>
> Modificările devin active la **următoarea conectare** (apare avertismentul „Modifiche attive alla prossima connessione”).
>
> Pentru a le face permanente, trebuie salvate în certificat cu **Gestione Certificato › Aggiorna modifiche**; altfel se pierd la închidere.

9. Gestionarea serverelor SSH

Dacă certificatul permite modificarea serverelor (permisiunea `AllowServerIpEditing`), lista serverelor devine editabilă și apare un panou de comenzi:

Comandă	Efect
Aggiungi	Adaugă în listă textul tastat (format `host:porta`).
Elimina	Elimină elementul tastat/selectat (trebuie să rămână cel puțin unul).
+ / -	Mută elementul selectat în listă.
R	Înlocuiește textul ultimului element selectat cu cel tastat.

Și aceste modificări trebuie salvate cu **Gestione Certificato › Aggiorna modifiche**. În timpul conexiunii, lista serverelor este blocată.

10. Modul „Apri come Putty”

Din fereastra de autentificare, **Varie › Apri come Putty** deschide fereastra principală fără certificat, ca un client SSH generic. Apar câmpurile:

Câmp	Utilizare
Hostname / Porta	Server SSH (port implicit 22).
Nome utente / Password	Acreditări SSH.
KeyFile / Pwd KeyFile	Cheia privată (`.ppk`, `.OpenSsh`, `.pri`) și fraza de acces aferentă; butonul `....` deschide selecția fișierului.
Timeout (sec.)	Timeout de conectare și interval keep-alive (implicit 3).

Redirecționările se definesc așa cum este descris în capitolul 8 și sunt valabile numai pentru sesiunea curentă: în acest mod nu există un certificat în care să fie salvate.

11. Gestionarea certificatului

Toate elementele meniului **Gestione Certificato** cer mai întâi confirmare dacă este activă o conexiune (va fi închisă) și apoi parola actuală. La final, programul se închide cu mesajul „Aggiornamento Effettuato: Rientrare nel programma”.

11.1 Aggiorna modifiche

Reconstruiește certificatul cu lista actuală de servere și redirecționări (inclusiv bifele și parolele) și îl salvează în baza de date cu aceeași parolă. La fiecare salvare, numărul versiunii certificatului (`Ssh ver.`) crește.

11.2 Cambio Password

După parola actuală, introduceți de două ori noua parolă, care trebuie să îndeplinească următoarele cerințe:

- cel puțin 8 caractere;
- cel puțin 1 literă mică și 2 majuscule;
- cel puțin 1 cifră;
- cel puțin 2 caractere speciale.

Certificatul este recriptat cu noua parolă. Dacă parola coincide cu cea anterioară, certificatul este oricum actualizat.

11.3 Cambio Password Intermedia

Setează parola solicitată la deschiderea sesiunilor la distanță. Nu sunt prevăzute cerințe de complexitate.

11.4 Export Certificato

Exportă certificatul în `C:\Ssh_Tunnel_Certificates\<Profilo>.Ssh_T`, criptat cu parola indicată la export, gata pentru a fi predat și importat pe alt PC (secțiunea 4.4).

Exportul necesită o **parolă de autorizare**, care poate fi obținută în două moduri:

- apăsând butonul de trimitere a codului: un cod aleatoriu este trimis la adresa de e-mail pentru notificarea accesărilor (sau, în lipsa acesteia, la adresa principală);
- cu parola administrativă rezervată dezvoltatorului, valabilă numai pe PC-uri cu autorizare Persistent.

După autorizare, alegeți parola cu care se criptează fișierul exportat.

11.5 Elimina Certificato

După parola actuală, profilul este șters din baza de date. Dacă în baza de date rămân alte profiluri, programul revine la fereastra de autentificare; altfel se închide.

12. Redirecționarea Albatros (DbKey)

Elementul **Albatros › Parametri** deschide fereastra **Reindirizza Albatros**, gândită pentru integrarea cu aplicațiile Albatros: când se deschide tunelul către un sediu, aplicațiile pot fi direcționate automat către baza de date a acelui sediu.

Partea superioară enumeră configurațiile existente în mediul Albatros (cheie, DB local și notă, DB la distanță și notă, IP de ping), ca referință pentru alegerea cheii. Partea inferioară conține setările profilului:

Câmp	Semnificație
Abilitato	Activează funcția pentru profil.
Alla Connessione	DbKey de setat când conexiunea SSH reușește.
Alla Disconn.	DbKey de setat la deconectare.
Percorso file txt DbKey	Folderul în care se scrie fișierul `_DbKey.txt` (butonul Predefinito: `C:\ProgramData\Albatros\Common\`).
Nota Connessione / Nota Disconnessione	Text afișat în registru și în jurnal când cheia este aplicată.

La apăsarea butonului **Registra**, setările sunt salvate în mediul Albatros cu chei de tipul `[<Profilo>]_DbKeyEnabled`, `[<Profilo>]_DbKeyAtConnection` etc. și aplicate imediat în funcție de starea conexiunii. La conectare sau deconectare, programul scrie `DbKey=<valore>` în fișierul `_DbKey.txt` și notează acest lucru în registru.

13. Jurnale și întreținerea bazei de date

13.1 Registru și jurnal

Fiecare rând afișat în panoul de mesaje este înregistrat și în tabelul Log al bazei de date, împreună cu identificatorul procesului (sesiunea) și, la prima scriere, cu informațiile hardware ale PC-ului. Jurnalul poate fi dezactivat cu parametrul `DoNotUseLogSSH_Tunnel`.

13.2 Mostra Log

Din fereastra de autentificare, **DataBase › Gestione Log › Mostra Log**: indicați intervalul de date (de la data / până la data) și apăsați **Ricerca** (Căutare). Se afișează sesiunea, data, ora, informațiile PC-ului și mesajul.

13.3 Invia Log via Mail

DataBase › Gestione Log › Invia Log via Mail: indicați intervalul de date și adresa de destinație și apăsați **Invia** (Trimitere). Jurnalul perioadei este exportat în Excel, comprimat în zip și trimis; fișierele temporare sunt apoi șterse.

13.4 Întreținere

- **Compatta Database**: recuperează spațiul liber din fișier (VACUUM). Se execută automat și la fiecare salvare a certificatului.
- **Open Ssh_Tunnel DB path**: deschide folderul bazei de date, util pentru copii de siguranță.

13.5 Structura bazei de date

Baza de date este un fișier SQLite protejat prin parolă, la revizia 2. La pornire, programul creează tabelele lipsă și actualizează automat bazele de date de la revizia 1.

Tabel	Conținut
Parameters	Perechi cheie/valoare: `DbVersion`, `login` (ultimul profil utilizat), `[<Profilo>]_IP` (ultimul server utilizat).
Certificati	Proprietario, Profilo, Version, VersionDate, Certificato (text criptat).
Licenza	KeyLicenza, Assegnatario, DataAssegnazione, CertificatoLicenza (pregătit, momentan neutilizat).
Log	IdSession, DataLog, PcInfo, KeyInfo, Info.

14. Securitate

- **Certificat criptat**: fiecare valoare sensibilă este criptată cu Triple DES folosind o cheie derivată din parola de acces; certificatul în ansamblu este, la rândul său, criptat. Parola nu este salvată niciodată.
- **Nicio acreditare vizibilă**: acreditările SSH, cheia privată și parolele PC-urilor la distanță rămân în interiorul programului și sunt transmise direct clienților.
- **Legarea de hardware**: autorizările verificării în doi pași sunt valabile numai pentru PC-ul și utilizatorul Windows pe care au fost obținute.
- **Limită de încercări**: 3 încercări pentru parola de acces, pentru codurile verificării în doi pași și pentru parola intermediară.
- **Expirare la miezul nopții** pentru autorizările OneDay și OneTime.
- **Trasabilitate**: e-mail cu datele PC-ului la fiecare solicitare de coduri și la fiecare acces RDP/VNC, jurnal local al sesiunilor, înregistrarea accesărilor pe serverul SSH.
- **Curățare**: programele auxiliare și fișierele .rdp temporare sunt șterse la pornire și la ieșire.
- **Integritate**: indicatorul „ChkSum OK” semnalează că executabilul nu a fost modificat.

> **Notă**
>
> Parola intermediară nu este o adevărată protecție criptografică: are rolul de a împiedica folosirea programului lăsat deschis și nesupravegheat.

15. Mesaje și depanare

Mesaj / simptom	Cauză și remediere
„Password errata: impossibile continuare” (Parolă greșită: imposibil de continuat)	Parolă de acces greșită sau profil greșit. După 3 erori, programul se închide.
„Certificato inesistente” (Certificat inexistent)	Profilul selectat nu se află în baza de date: importați certificatul.
„Two-factor authentication is required!”	PC neautorizat: urmați capitolul 5.
„Invio mail ... per doppia verifica fallito!!!” (Trimiterea e-mailului ... pentru verificarea în doi pași a eșuat!!!)	Problemă la trimiterea e-mailului (rețea, firewall, SMTP). Reîncercați sau folosiți „Invia Codice via SMS al Supporto”.
„Codice errato: Tentativi n di 3” (Cod greșit: încercarea n din 3)	Cod tastat greșit sau provenit dintr-o solicitare anterioară.
„Chiusura automatica per mancato input codice” (Închidere automată din cauza neintroducerii codului)	Au trecut cele 5 minute fără introducerea codului.
„Internet Connection Not Available” / „Waiting ...”	Lipsește conexiunea la Internet; programul așteaptă. Debifați „Chk Internet” pentru a omite verificarea.
„Errore login!!!” (Eroare de autentificare!!!)	Conexiunea nu poate fi pregătită (acreditări sau cheie ale certificatului nevalide). Contactați administratorul.
Conexiunea nu se stabilește	Serverul nu poate fi accesat: încercați un server alternativ din listă; folosiți Utility › Ping No-IP pentru a verifica rezolvarea numelui.
„### Error Forward Host: ...”	Portul local al redirecționării este ocupat de alt program sau gazda locală nu este validă.
„Connection Lost”	Conexiune căzută: programul se reconectează singur.
„Password errata” / „Superato il limite di tentativi ammessi” (Parolă greșită / S-a depășit limita de încercări permise)	Parolă intermediară greșită; la a treia eroare programul se închide.
„Ssh Tunnel arrestato per scadenza password...” (Ssh Tunnel oprit din cauza expirării parolei...)	S-a ajuns la miezul nopții cu autorizare OneDay/OneTime: reporniți și solicitați un cod nou.
„Riscontrata anomalia tra la versione attesa e quella trovata nel Database di servizio” (Anomalie între versiunea așteptată și cea găsită în baza de date de serviciu)	Baza de date nu poate fi actualizată: mutați programul într-un folder cu permisiuni de scriere.
„Operazione annullata per password difforme” (Operațiune anulată din cauza parolei neconforme)	Parolă actuală greșită în funcțiile Gestione Certificato.
„Porta già utilizzata: Cerco la prima occorrenza libera?” (Port deja utilizat: caut primul port liber?)	Port local deja atribuit unei alte redirecționări.
„Dati Insufficienti!” (Date insuficiente!)	Lipsesc câmpuri obligatorii la introducerea unei redirecționări.

Anexa A – Rezumat rapid pentru utilizator

1. Copiați `.exe` și `.db` în același folder.
2. Porniți executabilul și introduceți parola de acces.
3. Dacă se solicită, apăsați „Richiedi via mail” și introduceți codul OneDay sau OneTime primit.
4. Așteptați „SSH Tunneling Ready ....” și apăsați **Connetti**.
5. Faceți dublu clic pe computerul dorit din lista din dreapta.
6. Introduceți parola intermediară, dacă se solicită.
7. Lucrați pe PC-ul la distanță; la final apăsați **Disconnetti** sau **Esci**.

Anexa B – Structura certificatului

Certificatul (versiunea 2) este un text cu rânduri `Chiave = "valore"`, criptat în ansamblu cu parola. Valorile sensibile sunt, la rândul lor, criptate individual. Lista cheilor recunoscute:

Cheie	Conținut
`Algoritmo`	Versiunea algoritmului de criptare (1).
`Nominativo`	Numele profilului (în clar).
`SshUserDllVersion`	Numărul progresiv și data ultimei salvări.
`Bloccato`	Certificat cu funcții reduse (fără detalii în registru, fără instrumente externe).
`ShowRdpButton`	Afișează butonul RDP/VNC/Term pentru conexiunea statică.
`AutoRDP`	Deschide conexiunea statică imediat după conectare.
`AllowsNewForwards`	Permite modificarea redirecționărilor de porturi.
`AllowServerIpEditing`	Permite modificarea listei de servere.
`Proprietario`	Destinatarul software-ului („Sw consegnato a”).
`Login`, `Password`	Acreditări SSH.
`Certificate`, `CertificatePassword`, `FileCertificato`	Cheia privată SSH (text sau resursă încorporată) și fraza de acces aferentă.
`PwdRemoteAccess`	Parolă intermediară.
`Server`, `ServerPort`	Lista serverelor separate prin `&` și portul implicit.
`RdpCommandLine`, `RdpFileStatico`	Linia de comandă și fișierul conexiunii statice.
`Mail`, `MailOneDay`, `MailTemp`	Destinatarii codurilor verificării în doi pași.
`MailInfoAccess`	Destinatarul notificărilor de acces.
`Cellulare`	Număr de telefon mobil (pregătit).
`RedirectPortsCount`	Numărul redirecționărilor.
`RedirectPorts(i, …)`	Pentru fiecare redirecționare: LocalHost, LocalPort, RemoteHost, RemotePort, Remark, RdpFile, Enabled (Y/N), PasswordRdpFF, PwdActivateRdpConnection.

Anexa C – Note tehnice pentru dezvoltator

În timpul redactării manualului au ieșit la iveală în cod câteva puncte de verificat. Această anexă este de uz intern: trebuie eliminată înainte de a preda manualul destinatarilor programului.

Fișier / rutină	Observație
ModSetting.Log	Verifică existența bazei de date în `Application.StartupPath` cu numele exe-ului, ignorând `PathDbSSH_Tunnel` și `FileNameDbSSH_Tunnel`: dacă DB-ul se află în altă parte sau are alt nume, jurnalul nu este scris.
ModSetting.RemoveParam	Interogarea folosește `lower('?')`: parametrul dintre apostrofuri nu este înlocuit, deci ștergerea nu are efect.
ModSetting.DecodCertificate	Comparația `ToLower.Contains("Algoritmo =")` conține o majusculă și nu este niciodată adevărată: valoarea `Algoritmo` nu este citită (în prezent fără consecințe, este întotdeauna 1).
FrmStart_Load	`ContaErrori` este locală buclei și se resetează la fiecare iterație; în plus, dacă verificarea în doi pași eșuează sau fereastra este închisă, `Exit Sub` nu închide aplicația: verificați să nu rămână un proces activ fără fereastră.
frmMainProgram, butoanele `+` / `-` pentru servere	Sfaturile ecran sunt inversate: `-` (sfat „Sposta Giù”) mută în sus, `+` (sfat „Sposta Su”) mută în jos.
frmMainProgram, butoanele de model `*`	Sfatul ecran indică `###Host### / ###Port###`, dar substituenții înlocuiți de cod sunt `##host##` / `##port##`.
EseguiExportCertificato	„Supercode”-ul activează salvarea parolei în fișierul `.Ssh_T.Key`, dar `CostruisciRemPwdInfo` și `abilitaSalvataggioPwd` nu sunt folosite: funcția nu este implementată.
ChkIconaAfterSelection	Opțiunea „Icona dopo selezione” nu este referită în cod.
GetParam / SetParam	Cheia este concatenată în interogarea SQL în loc să fie transmisă ca parametru.
Surse în general	În surse sunt prezente în clar acreditări și chei (serviciul SMS, accesul SFTP pentru actualizări, parola DB-ului, amprenta parolei administrative). Oricine are acces la executabil le poate extrage cu un decompilator .NET: evaluați ofuscarea sau mutarea lor pe server.

Ssh_Tunnel

管理されたリモート アクセスのための SSH クライアント

操作および管理マニュアル

ソフトウェア バージョン 27.2.2036.6127 · DB rev. 2

© Raffaele Romano

2026 年 10 月

目次

1. はじめに.....121

1.1 本マニュアルの対象読者.....121

1.2 対象バージョン.....121

2. 基本概念.....123

3. インストールと要件.....124

3.1 必要なファイル.....124

3.2 要件.....124

3.3 組み込みプログラム.....124

3.4 外部パラメーター ファイル (省略可能).....125

3.5 フォルダー内のオプション コンポーネント.....125

4. 起動とログイン.....126

4.1 ログイン画面.....126

4.2 パスワードの入力.....127

4.3 ログイン画面のメニュー.....127

4.4 証明書のインポート.....128

5. 二段階認証 (PC の承認).....129

5.1 要求されるタイミング.....129

5.2 コードの要求.....129

5.3 承認のレベル.....130

5.4 二段階認証の「Varie」メニュー.....130

5.5 承認の取り消し.....130

6. メイン ウィンドウ.....131

6.1 概要.....131

6.2 オプション.....131

6.3 メイン ウィンドウのメニュー.....132

7. 接続とリモート セッション.....133

7.1 SSH サーバーへの接続.....133

7.2 リモート PC でのセッションの開始.....133

7.3 接続の種類 134
7.4 RDP/VNC/Term ボタン 135
7.5 切断と終了 135

8. ポート フォワーディングの管理 136
8.1 編集の有効化 136
8.2 フォワーディングのフィールド 136
8.3 一覧に対する操作 136

9. SSH サーバーの管理 138

10. 「Apri come Putty」モード 139

11. 証明書の管理 140
11.1 Aggiorna modifiche 140
11.2 Cambio Password 140
11.3 Cambio Password Intermedia 140
11.4 Export Certificato 140
11.5 Elimina Certificato 140

12. Albatros のリダイレクト (DbKey) 141

13. ログとデータベースのメンテナンス 142
13.1 記録とログ 142
13.2 Mostra Log 142
13.3 Invia Log via Mail 142
13.4 メンテナンス 142
13.5 データベースの構造 142

14. セキュリティ 143

15. メッセージとトラブルシューティング 144

付録 A – ユーザー向けクイック サマリー 146

付録 B – 証明書の構造 147

付録 C – 開発者向け技術メモ 148

1. はじめに

Ssh_Tunnel は VB.NET で開発された Windows 用の SSH クライアントで、社内の SSH サーバーへの暗号化トンネルを通じて、企業ネットワーク内の PC やサーバーに管理された方法でアクセス (RDP、VNC、SSH ターミナル、IP カメラ経由) できるようにします。

TeamViewer、AnyDesk などのツールの代替として開発されました。これらのツールは通信を暗号化しますが、資格情報を持っていれば誰でもシステムにアクセスでき、ネットワークのセキュリティが第三者に依存することになります。これに対して Ssh_Tunnel は次のような特徴があります:

- パスワードを平文で一切含みません。すべての接続パラメーターは**暗号化された証明書**に格納され、ユーザーに渡されたログイン パスワードでのみ開くことができます。
- 各受領者 (サポート センター、技術者、コンサルタント) に**固有の証明書**を割り当てるため、SSH サーバーは接続者を識別し、その日付、時刻、時間を記録できます。
- **二段階認証** (メールで送信されるコード) により、使用を特定の PC に限定できます。承認は永続、1 日限り、またはそのセッションのみのいずれかです。
- リモート PC へのすべてのアクセスをメールで通知し、どのコンピューターから接続したかを示します。
- ユーザーには証明書で定められた接続のみが、ダブルクリックで開けるコンピューターの一覧として表示されます。

1.1 本マニュアルの対象読者

本マニュアルは 3 部で構成されています:

- **日常の使用** (第 3 〜 7 章): インストール、ログイン、二段階認証、接続、リモート セッションの開始。プログラムを受け取るユーザーに渡す部分です。
- **管理** (第 8 〜 13 章): ポート フォワーディング、サーバー、証明書、Albatros のリダイレクト、ログ、データベースの管理。
- **技術リファレンス** (第 14 〜 15 章と付録): アーキテクチャ、セキュリティ、証明書の構造、メッセージ、トラブルシューティング。

1.2 対象バージョン

項目	値
プログラム	Ssh_Tunnel
ソフトウェア バージョン	27.2.2036.6127 (ビルド日 2026/10/11)
データベース リビジョン	2
証明書のバージョン	2 (Algoritmo = 1)
プラットフォーム	.NET Framework 4.8、Windows、32 ビットおよび 64 ビット ビルド
主なライブラリ	Renci SSH.NET 2025、System.Data.SQLite、AlbatrosCommon
インターフェイスの言語	イタリア語、英語、フランス語、日本語、ルーマニア語 (Windows の言語に応じて自動選択)

プログラムに表示されるバージョンは `Sw ver.: 27.2.2036.6127 - 11/10/2026` の形式です。日付はリビジョン番号 (2010/01/01 からの経過日数) から求められるため、コンパイル日に相当します。

2. 基本概念

プログラムを使用する前に、すべての画面で使われるいくつかの用語を理解しておくと便利です。

用語	意味
プロファイル	証明書を識別する名前 (例:「Sede -> Cliente」)。同じデータベースに複数のプロファイルを共存させることができ、起動時に使用するものを選択します。
証明書	接続に必要なすべてを含む暗号化されたブロック: SSH サーバーとポート、SSH の資格情報、秘密キー、ポート フォワーディングの一覧、RDP/VNC ファイル、メール アドレス、権限。`.Ssh_T` ファイルとして配布され、データベースにインポートされます。
ログイン パスワード	起動時に要求されるパスワード。証明書を復号します。これがないと、プログラムはサーバーも資格情報もわかりません。
中間パスワード (リモート アクセス)	リモート PC でセッションを開くときに要求される 2 つ目のパスワード。開いたまま放置されたプログラムを他人に使用されるのを防ぎます。
接続固有のパスワード	一覧の個々の項目に定義された中間パスワード。設定されている場合は全体のパスワードより優先されます。
二段階認証	追加の確認: ある PC で初めて使用するときに、メールでコードを要求します。承認は PC のハードウェアに結び付けられます。
Persistent / OneDay / OneTime コード	二段階認証の 3 種類のコード: 永続的な承認、午前 0 時まで有効な承認、そのセッションのみ有効な承認 (第 5 章を参照)。
ポート フォワーディング (トンネル)	SSH 接続を通じて確立される「ローカル アドレスとポート → リモート ホストとポート」の対応付け。到達可能な各コンピューターが 1 つのフォワーディングに対応します。
DbKey	Albatros アプリケーションが作業用データベースを選択するために使用するキー。Ssh_Tunnel は接続時と切断時にこれを自動的に変更できます (第 12 章)。

3. インストールと要件

3.1 必要なファイル

Ssh_Tunnel にはインストールも管理者権限も必要ありません。次のファイルを同じフォルダーにコピーするだけです:

ファイル	説明
`Ssh_Tunnel_<Nome>.exe`	プログラムの実行可能ファイル (名前は受領者ごとにカスタマイズでき、末尾を 32 または 64 にすることもできます)。
`Ssh_Tunnel_<Nome>.db`	証明書、パラメーター、ログを含む暗号化された SQLite データベース。

データベース名は、実行可能ファイルの名前から末尾の `32` または `64` を取り除き、`.db` を付けたものになります。例: `Ssh_Tunnel_Esempio64.exe` は `Ssh_Tunnel_Esempio.db` を探します。これにより、32 ビット版と 64 ビット版が同じデータベースを共有します。

> **注**
>
> データベースが存在しない場合は、初回起動時に空のデータベースが作成されます。その場合、ログインする前に証明書をインポートする必要があります (4.4 節)。
>
> 「Riscontrata anomalia tra la versione attesa e quella trovata nel Database di servizio」(想定されたバージョンとサービス データベース内のバージョンの間に不整合が見つかりました) というメッセージが表示された場合は、書き込み制限のないフォルダー (たとえば `C:\Program Files` の下以外) にプログラムを移動してください。

3.2 要件

- .NET Framework 4.8 がインストールされた Windows。
- 社内の SSH サーバーへの送信方向のインターネット アクセス (証明書で別の指定がない限り、既定のポートは 200)。
- 二段階認証と通知のために、メールを送信できること (プログラムは Albatros ライブラリ内部の SMTP パラメーターを使用します)。

3.3 組み込みプログラム

実行可能ファイルには補助プログラムが内蔵されており、必要なときにのみ一時フォルダー `%TEMP%\Albatros\Ssh_Tunnel` に展開され、起動時と終了時に削除されます:

コンポーネント	用途
`vncviewer.exe` / `vncviewer32.exe`	VNC ビューアー (プロセスに応じて 64 ビット版または 32 ビット版)。
`rdp.exe`	RDP+ クライアント (パスワードを自動的に渡すリモート デスクトップ)。
`gencrypt.exe`	RDP+ 用のパスワード暗号化。
`AlbatrosRDP.exe`	パスワードを安全に受け渡す独自の RDP クライアント。
`Ssh_Console.exe`	SSH ターミナル コンソール。
`IPCamera.exe`	IP カメラ ビューアー。

3.4 外部パラメーター ファイル (省略可能)

AlbatrosCommon ライブラリの外部パラメーターのしくみ (`Var_<nome>=<valore>` 形式の行を含むテキスト ファイル。ソース内の例 `Data\Ssh_Tunnel_Merge.txt` を参照) を使用して、次の項目を設定できます:

パラメーター	効果	既定値
`PathDbSSH_Tunnel`	データベースのフォルダー	実行可能ファイルのフォルダー
`FileNameDbSSH_Tunnel`	データベース ファイルの名前	exe の名前から派生
`DoNotUseLogSSH_Tunnel`	`True` の場合、データベースへのログ記録と、最後に使用したプロファイル/サーバーの保存を無効にします	`False`

3.5 フォルダー内のオプション コンポーネント

プログラムのフォルダーに次のファイルがある場合、Ssh_Tunnel はそれらを認識します:

- `Ssh_Updater.exe`: ログイン画面を開くときに自動的に起動されます (プログラムの更新)。
- `Database4.exe` または `Database5Pro.exe`、`DbMigration.exe`、`Convert.exe`: **FishCodeLib** メニューに表示されます (DB 管理、移行、変換)。

4. 起動とログイン

4.1 ログイン画面

実行可能ファイルを起動すると **Password** 画面が表示されます。タイトルには現在の時刻が表示されます。

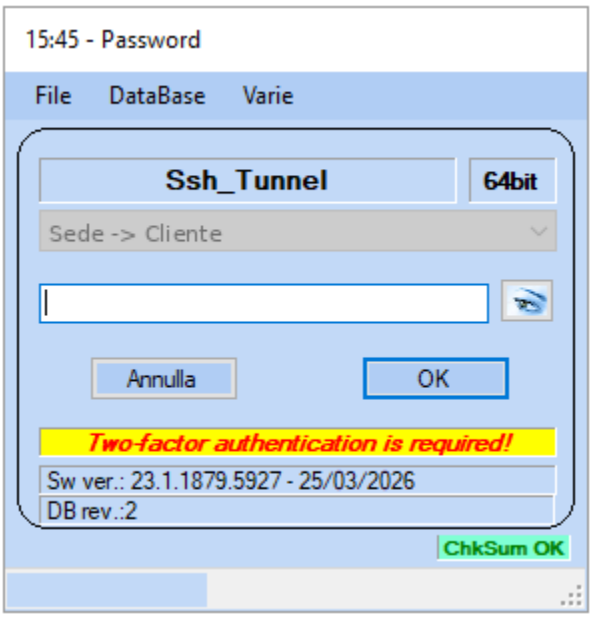

図 1 – 二段階認証を要求しているログイン画面

要素	機能
プログラム名と「64bit/32bit」	実行中のバージョンを示します。
プロファイルの一覧	データベース内のプロファイル。1 つしかない場合はロックされ、複数ある場合は最後に使用したものが提示されます。
パスワード フィールドと「目」のボタン	ログイン パスワードを入力します。目のボタンで文字の表示/非表示を切り替えます。
Annulla / OK	プログラムを終了します / パスワードを確定します。
ステータス行	PC の承認状態 (次の表を参照)。
Sw ver. / DB rev.	プログラム、証明書、データベースのバージョン。
ChkSum OK	実行可能ファイルの整合性チェック。表示されない場合やエラーが示された場合は、先に進まないでください。

ステータス行には次のように表示されることがあります:

メッセージ	意味
「Two-factor authentication is required!」(黄/赤)	PC が承認されていません。パスワードの後に二段階認証が要求されます。
「One Day Code is active!」(黄)	PC は今日の午前 0 時 (深夜) まで承認されています。
「Persistent Code is active!」(緑)	PC は永続的に承認されています。

4.2 パスワードの入力

1. プロファイルを選択します (複数ある場合)。
2. ログイン パスワードを入力して **OK** をクリックします。
3. パスワードが正しければ証明書が復号されます。確認が必要な場合は二段階認証の画面 (第 5 章) が開き、そうでない場合はメイン ウィンドウが開きます。

> **注意**
>
> **パスワードを 3 回間違える**と、プログラムは終了します。
>
> Ssh_Tunnel が既に実行中の場合は、新しいインスタンスを開くかどうかを確認されます。「いいえ」と答えると、既に開いているインスタンスが前面に表示されます。

4.3 ログイン画面のメニュー

メニュー	項目	機能
File	Esci	プログラムを終了します。
DataBase	Gestione Log › Abilita Log	パラメーターでログが無効化されている場合にのみ表示され、セッション中のログを再度有効にします。
	Gestione Log › Mostra Log	ログを表示します (第 13 章)。
	Gestione Log › Invia Log via Mail	ログを添付ファイルとして送信します (第 13 章)。
	Utility › Compatta Database	SQLite データベースの VACUUM を実行します。

メニュー	項目	機能
	Utility › Open Ssh_Tunnel DB path	データベースのフォルダーをエクスプローラーで開きます (完全なパスは項目のヒントに表示されます)。
	Utility › Importa Certificato Ssh Tunnel	`.Ssh_T` ファイルをインポートします (4.4 節)。
	FishCodeLib	外部ツール (存在する場合。3.5 節)。
Varie	Abilita Accesso con Doppio Passaggio	この PC でプロファイルについて記憶されている承認を取り消します (5.5 節)。
	Apri come Putty	プログラムを汎用 SSH クライアント モードで起動します (第 10 章)。
	Scarica AlbatrosRDP	`AlbatrosRDP.exe` をユーザーのダウンロード フォルダーに保存し、そのフォルダーを開きます。

4.4 証明書のインポート

新しいプロファイルは、管理者から受け取った証明書ファイル `.Ssh_T` をインポートして追加します。

1. ログイン画面で **DataBase › Utility › Importa Certificato Ssh Tunnel** を選択します。
2. `.Ssh_T` ファイルを指定された領域にドラッグするか、その領域をダブルクリックしてファイルを選択します。
3. 証明書のパスワードを入力します。
4. プログラムは名義と所有者を表示して確認を求めます。同じ名前のプロファイルが既にある場合は、置き換えるかどうかを確認します。
5. 完了すると、新しいプロファイルがログイン画面の一覧に表示されます。

> **注**
>
> パスワードが間違っている場合、プログラムは「Pwd errata」(パスワードが間違っています) と応答し、何もインポートされません。証明書は暗号化されたままデータベースに保存され、パスワードは記憶されません。

5. 二段階認証 (PC の承認)

5.1 要求されるタイミング

二段階認証は、証明書にコード送信用のメール アドレスが少なくとも 1 つ含まれていて、使用中の PC がそのプロファイルに対してまだ承認されていない場合にのみ実行されます。承認はコンピューターのハードウェア識別子 (CPU の ID、ない場合はマザーボードまたはディスクのシリアル番号) に結び付けられているため、プログラムを別の PC にコピーすると新たな承認が必要になります。

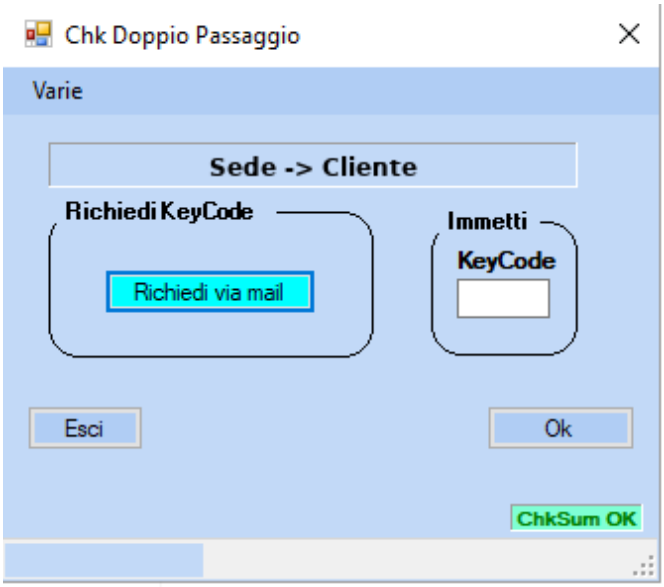

図 2 – 「Chk Doppio Passaggio」画面

5.2 コードの要求

1. **Richiedi via mail** (メールで要求) をクリックします。プログラムは 5 桁のランダムなコードを 3 つ生成し、証明書に定められたアドレスに送信します。
2. メールを待ちます。「Codici inviati」(コードを送信しました) と表示されます。
3. 受け取ったコードのいずれかを **KeyCode** フィールドに入力し、**Ok** をクリックします。

コードは画面を開いたときに生成され、画面が開いている間だけ有効です。プログラムを閉じた場合は、新しいコードを要求する必要があります。各メールには、要求元 PC の識別データ (ローカルおよびパブリック IP、PC 名、ディスク・CPU・マザーボードのシリアル番号) も含まれます。

証明書に設定されたアドレスに応じたコードの受信者:

証明書内のアドレス	受信するコード
メイン メール (`Mail`)	Persistent、OneDay、OneTime

証明書内のアドレス	受信するコード
OneDay メール (`MailOneDay`)	OneDay と OneTime
OneTime メール (`MailTemp`)	OneTime のみ

2 つのアドレスが同じ場合、メールは重複して送信されません。これにより、永続コードを管理者専用にし、顧客には一時的なコードだけを届けることができます。

5.3 承認のレベル

コード	効果	有効期限
Persistent	PC はそのプロファイルについて承認されたままとなり、以降の起動ではコードは要求されません。	なし (取り消すまで)
OneDay	PC はその日いっぱい承認されます。	当日の午前 0 時 (深夜)
OneTime	現在のセッションのみを承認します。再度開くときは新しいコードが必要です。	プログラムの終了時。いずれにしても午前 0 時 (深夜) まで

> **注意**
>
> OneDay および OneTime コードでは、メイン ウィンドウに「Ssh Tunnel: disattivazione alle 00.00」(Ssh Tunnel: 00.00 に無効化) と表示されます。午前 0 時になると「Ssh Tunnel arrestato per scadenza password...」(パスワードの期限切れにより Ssh Tunnel を停止しました...) という警告が表示され、プログラムが終了し、開いているカメラも閉じられます。
>
> **コードを 3 回間違える**と画面が閉じます。**5 分**以内にコードが入力されない場合、プログラムは自動的に終了します (10 秒のカウントダウン付き)。

5.4 二段階認証の「Varie」メニュー

項目	機能
Mostra Chk Mail Persistente	「Invia solo alla Mail Principale」(メイン メールにのみ送信) オプションを表示します。有効にすると、コードは Persistent コードを受け取るアドレスにのみ送信されます。

項目	機能
Aggiorna Timer	5 分間の待機時間をリセットします。
Invia Codice via SMS al Supporto	プログラムにあらかじめ設定されたサポートの番号に、3 つのコードを SMS で送信します (メールが機能しない場合に便利です)。

5.5 承認の取り消し

PC の Persistent または OneDay の承認を取り消すには、ログイン画面でプロファイルを選択し、**Varie › Abilita Accesso con Doppio Passaggio** を選択して確認します。次回のログイン時に再びコードが要求されます。この項目は、PC が既に承認されている場合にのみ有効です。

> **注**
>
> 承認は、現在のユーザーの Windows レジストリに暗号化されて保存されます: `HKEY_CURRENT_USER\Software\Albatros.net`、値 `Ssh_Tunnel_<Profilo>`。したがって、承認はそれを取得した Windows ユーザーに対して有効です。

6. メイン ウィンドウ

6.1 概要

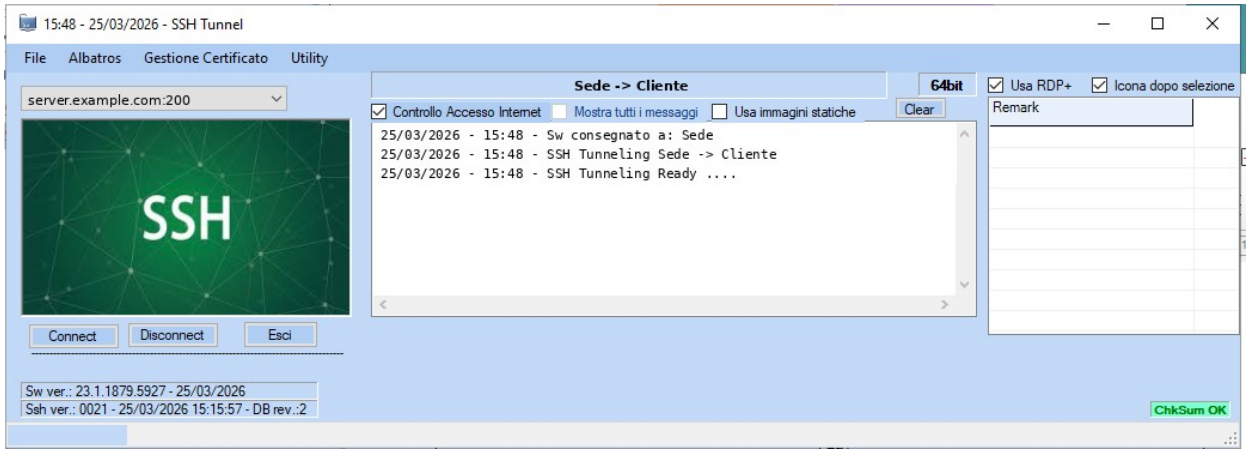

図 3 – 接続前のメイン ウィンドウ

領域	内容
左上	利用可能な SSH サーバーの一覧 (複数ある場合、または証明書で変更が許可されている場合に表示)。
状態の画像	待機中は SSH のロゴ。使用中は接続成功または中断のアニメーション。
ボタン	**Connetti**、**Disconnetti**、**Esci**、およびデータベースに複数のプロファイルがある場合は **Riavvia** (プロファイルを変更するためにログイン画面に戻ります)。
中央のパネル	日付と時刻付きのメッセージの記録。エラー行は赤で表示され、「###」を含む行は背景が黄色になります。
右側の一覧	到達可能なコンピューター (Remark 列)。接続後に表示されます。
ステータス バー	ソフトウェアと証明書のバージョン、DB リビジョン、「ChkSum OK」。

6.2 オプション

オプション	効果
Chk Internet	接続前にインターネットに到達できるかどうかを確認し、到達できない場合は接続が回復するまで待機します。既定で有効です。
Mostra tutti i messaggi	ポート フォワーディングの詳細 (ローカルおよびリモートの IP とポート) も記録に表示します。「ロックされた」証明書では使用できません。
Usa immagini statiche	状態のアニメーションを静止画像に置き換えます。
Icona dopo selezione	コンピューター一覧の表示オプション。
RDP+ / AlbatrosRDP / MS RDP / Old RDP+	リモート デスクトップ接続に使用するクライアントを選択します (7.3 節)。既定値: MS RDP。
Clear	記録を消去し、証明書の情報を再表示します。

6.3 メイン ウィンドウのメニュー

メニュー	項目	機能
File	Esci	切断し、一時ファイルを削除してプログラムを終了します。
Albatros	Parametri	Albatros のリダイレクト / DbKey (第 12 章)。
	FishCodeLib	外部ツール (存在し、証明書がロックされていない場合)。
Gestione Certificato	Aggiorna modifiche	変更したサーバーとフォワーディングを証明書に保存します (11.1 節)。
	Cambio Password / Port FF	ログイン パスワードを変更します。
	Cambio Pwd Intermedia / Port FF	中間パスワードを変更します。
	Export Certificato	証明書を `.Ssh_T` ファイルにエクスポートします。
	Elimina Certificato	データベースからプロファイルを削除します。

メニュー	項目	機能
	Apri percorso DB Ssh_Tunnel	データベースのフォルダーを開きます。
Utility	Ping No-IP	選択したサーバーの名前を DNS で解決し、その IP を表示します。
	Ping IP	サーバーが IP アドレスで指定されている場合、そのサーバーに ping を実行します。
	Scarica AlbatrosRDP	`AlbatrosRDP.exe` をダウンロード フォルダーに保存します。

「Apri come Putty」モードでは、Albatros メニューと Gestione Certificato メニューは使用できません。

7. 接続とリモート セッション

7.1 SSH サーバーへの接続

1. 記録に次の表示があることを確認します: **SSH Tunneling Ready ....**
2. サーバーの一覧が表示されている場合は、サーバーを選択します。通常は最初のサーバーで十分です。その他は、メイン サーバーが応答しない場合に使用する代替アクセスです (一部は社内ネットワーク内からのみ機能します)。
3. **Connetti** をクリックします。

記録に一連の処理が表示されます:

```
Disconnected
Testing Internet connection status
Connecting...
Server: <nome server>
port: 200
Connecting to <nome server>:200
CONNECTED
S.O. <sistema operativo del server>
```

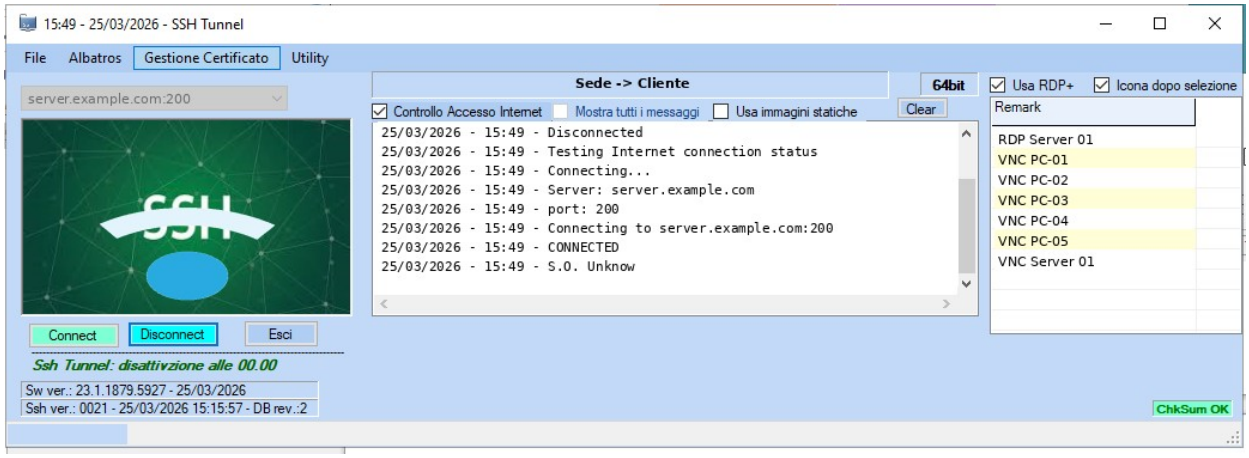

図 4 – 接続確立: 右側に到達可能なコンピューターの一覧

動作の詳細:

- サーバーは `host:porta` の形式で指定できます。ポートがない場合は証明書のポートが使用され、それもない場合は **200** が使用されます。アポストロフィ (') より後のテキストはコメントと見なされます。
- 認証には、証明書に含まれる SSH の資格情報と、存在する場合は秘密キーが使用されます。
- 接続後、プログラムはサーバーのオペレーティング システムを検出します (Windows では `ver` コマンド、Linux では `lsb_release -d`)。
- 選択したサーバーはプロファイルごとに記憶され、次回の起動時に提示されます。

- 接続が切断されると、プログラムはそれを通知し (「Connection Lost」)、**Disconnetti** がクリックされるまで自動的に再接続を試みます。
- 証明書でサーバーが 1 つだけ定められている場合、起動時にウィンドウは最小化され、証明書で RDP ボタンが有効になっていれば、接続が自動的に開始されます。

7.2 リモート PC でのセッションの開始

1. 接続が完了したら、右側の一覧で目的のコンピューターを**ダブルクリック**します。
2. 中間パスワードが設定されている場合は、接続名が表示されたウィンドウが開きます。パスワードを入力して **OK** をクリックします。
3. リモート セッションが開き、Ssh_Tunnel のウィンドウは最小化されます。

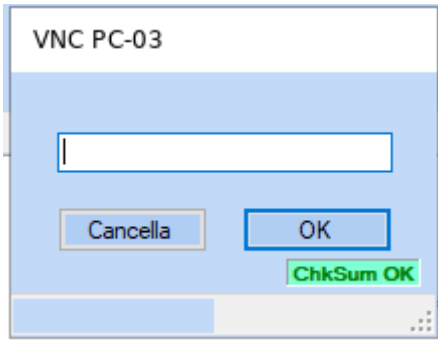

図 5 – 接続に対する中間パスワードの要求

> **注意**
>
> **中間パスワードを 3 回間違える**と、プログラムは切断して終了します (「Superato il limite di tentativi ammessi」(許可された試行回数を超えました))。

> **注**
>
> 証明書でアクセス通知メールが設定されている場合、RDP または VNC セッションを開くたびに、件名「SSh_Tunnel di <proprietario> su <connessione>」で、接続元 PC のデータを含むメールが送信されます。

7.3 接続の種類

セッションの種類は、証明書内の項目の構成によって決まります:

種類	使用するプログラム	備考
リモート デスクトップ (RDP)	RDP オプションで選択したクライアント	RDP ファイルを持つ項目の既定の種類。
VNC	`vncviewer.exe` (共有セッション)	リモート PC のパスワードが証明書にある場合は、自動的に渡されます。PC がログオフ状態の場合は、Windows の資格情報が必要になることがあります。
ターミナル	`Ssh_Console.exe`	指定したホストへの SSH コンソール。
カメラ	`IPCamera.exe`	ウィンドウは画面上に自動的に並べて表示されます。録画は `C:\SDT_Cam_Recorder\` に保存されます。同じカメラを再度開くと、以前のウィンドウは閉じられます。

リモート デスクトップ用のクライアント:

オプション	動作
MS RDP	Windows の `mstsc.exe` を一時的な .rdp ファイルとともに使用します。リモート PC のパスワードは渡されません。
RDP+	内蔵の RDP+ クライアントを全画面で使用し、ドライブとプリンターをリダイレクトします。リモート PC のパスワードは gencrypt で暗号化され、自動的に渡されます。
Old RDP+	RDP+ と同じですが、パスワードをそのまま渡します (証明書内で既に暗号化されているパスワード用)。
AlbatrosRDP	独自のクライアント AlbatrosRDP を使用します。パラメーターは暗号化して渡され、パスワードは専用のチャネル (名前付きパイプ) を通じて渡されるため、コマンド ラインに表示されることはありません。

7.4 RDP/VNC/Term ボタン

証明書で設定されている場合、接続中に **RDP/VNC/Term** ボタンが表示されます。このボタンは、一覧を経由せずに、証明書で定義された「固定」接続を直接開きます。証明書の AutoRDP オプションを使用すると、この接続は接続直後に自動的に開きます。

7.5 切断と終了

- **Disconnetti**: すべてのフォワーディング、カメラ、SSH 接続を閉じ、再接続の試行を停止します。
- **Esci** (またはウィンドウを閉じる): 切断し、一時ファイルを削除してプログラムを終了します。
- **Riavvia**: Esci と同じですが、別のプロファイルを選択するためにログイン画面に戻ります。

8. ポート フォワーディングの管理

この部分は、証明書でフォワーディングの変更が許可されている場合 (`AllowsNewForwards` 権限)、または「Apri come Putty」モードでのみ使用できます。その場合、メイン ウィンドウは縦に大きくなり、ボタンの下に編集セクションが表示されます。

8.1 編集の有効化

1. **Accedi a Port Forwarding** をオンにします。中間パスワードが要求されます。
2. 正しいパスワードを入力すると編集セクションが編集可能になり、フォワーディングの一覧で複数選択と Excel へのエクスポートができるようになります。

8.2 フォワーディングのフィールド

フィールド	意味
Host Locale / Porta	プログラムがローカル PC で待ち受けるアドレスとポート (例: 127.0.0.2:3390)。ホストの横の * ボタンで 127.0.0.2 が入力されます。
Host Remoto / Porta	SSH サーバーから見た宛先のホストとポート (例: 192.168.1.10:3389)。
Nota (Remark)	コンピューターの一覧に表示される名前。必須です。
Pwd	VNC または RDP+ に渡されるリモート PC のパスワード。目のボタンで表示し、**RDP Crypt** で RDP+ 用に gencrypt で暗号化します。
RDP	接続ファイルの内容。3 つの * ボタンでテンプレートを生成します: 完全な .rdp ファイル、VNC の行、ターミナルの行。

ボタンで生成されるテンプレート:

- RDP: `full address` と `server port` をローカルのホストとポートに設定し、全画面、クリップボード、プリンター、ドライブをリダイレクトする標準の .rdp ファイル。
- VNC: `vnc_config /connect <host>:<porta> /autoacceptnodsm /shared /autoscaling`。
- ターミナル: `term_config server=<host> port=<porta> login= password= ppkkeyfilename= ppkkey= ppkkeypwd=` (要補完)。

内容にはプレースホルダー `##host##` と `##port##` を使用でき、開くときにフォワーディングのローカルのホストとポートに置き換えられます。項目がコンピューターの一覧に表示されるのは、チェック

がオンで RDP フィールドに値がある場合のみです。RDP ファイルのない項目はトンネルだけを作成します。

8.3 一覧に対する操作

操作	効果
行をクリック	項目をフィールドに読み込んで編集できるようにします。
<==	項目を一覧に追加するか、選択した項目を更新します (再度中間パスワードが必要です)。RDP と Pwd 以外のすべてのフィールドが必須です。
Pulisci	フィールドを空にします。
Tutti i Tag / Inverti Tag	すべての項目をオンにします / チェックを反転します。チェックがオンの項目だけが有効になります。
Predefinito	一覧を証明書の最後の保存時の状態に戻します。

指定したローカル ポートが既に他の項目で使用されている場合、プログラムは最初の空きポートを自動的に検索することを提案します。

> **注意**
>
> 変更は**次回の接続時**に有効になります (「Modifiche attive alla prossima connessione」(変更は次回の接続時に有効になります) という警告が表示されます)。
>
> 変更を永続化するには、**Gestione Certificato › Aggiorna modifiche** で証明書に保存する必要があります。保存しないと、終了時に失われます。

9. SSH サーバーの管理

証明書でサーバーの変更が許可されている場合 (`AllowServerIpEditing` 権限)、サーバーの一覧が編集可能になり、コマンドのパネルが表示されます:

操作	効果
Aggiungi	入力したテキストを一覧に追加します (`host:porta` 形式)。
Elimina	入力/選択した項目を削除します (少なくとも 1 つは残す必要があります)。
+ / -	選択した項目を一覧内で移動します。
R	最後に選択した項目のテキストを、入力したテキストで置き換えます。

これらの変更も **Gestione Certificato › Aggiorna modifiche** で保存する必要があります。接続中はサーバーの一覧はロックされます。

10. 「Apri come Putty」モード

ログイン画面で **Varie › Apri come Putty** を選択すると、証明書なしで汎用 SSH クライアントとしてメイン ウィンドウが開きます。次のフィールドが表示されます:

フィールド	用途
Hostname / Porta	SSH サーバー (既定のポートは 22)。
Nome utente / Password	SSH の資格情報。
KeyFile / Pwd KeyFile	秘密キー (`.ppk`、`.OpenSsh`、`.pri`) とそのパスフレーズ。`....` ボタンでファイルの選択を開きます。
Timeout (sec.)	接続タイムアウトとキープアライブの間隔 (既定値 3)。

フォワーディングは第 8 章の説明に従って定義し、そのセッションでのみ有効です。このモードでは、保存先となる証明書が存在しません。

11. 証明書の管理

Gestione Certificato メニューのすべての項目では、接続中の場合はまず確認を求め (接続は閉じられます)、次に現在のパスワードを要求します。完了すると、プログラムは「Aggiornamento Effettuato: Rientrare nel programma」(更新が完了しました: プログラムに再度ログインしてください) というメッセージを表示して終了します。

11.1 Aggiorna modifiche

現在のサーバーとフォワーディングの一覧 (チェックとパスワードを含む) で証明書を再構築し、同じパスワードでデータベースに保存します。保存するたびに証明書のバージョン番号 (`Ssh ver.`) が増えます。

11.2 Cambio Password

現在のパスワードの後に新しいパスワードを 2 回入力します。新しいパスワードは次の要件を満たす必要があります:

- 8 文字以上
- 小文字 1 文字以上、大文字 2 文字以上
- 数字 1 文字以上
- 特殊文字 2 文字以上

証明書は新しいパスワードで再暗号化されます。パスワードが以前のものと同じ場合でも、証明書は更新されます。

11.3 Cambio Password Intermedia

リモート セッションを開くときに要求されるパスワードを設定します。複雑さの要件はありません。

11.4 Export Certificato

証明書を `C:\Ssh_Tunnel_Certificates\<Profilo>.Ssh_T` にエクスポートします。証明書はエクスポート時に指定したパスワードで暗号化され、別の PC に渡してインポートできる状態になります (4.4 節)。

エクスポートには**承認パスワード**が必要で、次の 2 つの方法で取得できます:

- コード送信ボタンをクリックする: ランダムなコードがアクセス通知メール (ない場合はメイン メール) に送信されます。
- 開発者専用の管理パスワードを使用する: Persistent 承認を持つ PC でのみ有効です。

承認後、エクスポートするファイルを暗号化するパスワードを選択します。

11.5 Elimina Certificato

現在のパスワードを入力すると、プロファイルがデータベースから削除されます。データベースに他のプロファイルが残っている場合はログイン画面に戻り、残っていない場合はプログラムが終了します。

12. Albatros のリダイレクト (DbKey)

Albatros › Parametri 項目は **Reindirizza Albatros** 画面を開きます。これは Albatros アプリケーションとの統合を目的としたもので、拠点へのトンネルを開いたときに、アプリケーションをその拠点のデータベースに自動的に向けることができます。

上部には、キーを選択する際の参考として、Albatros 環境にある構成 (キー、ローカル DB とメモ、リモート DB とメモ、ping 用 IP) が一覧表示されます。下部にはプロファイルの設定があります:

フィールド	意味
Abilitato	プロファイルでこの機能を有効にします。
Alla Connessione	SSH 接続が成功したときに設定する DbKey。
Alla Disconn.	切断時に設定する DbKey。
Percorso file txt DbKey	`_DbKey.txt` ファイルを書き込むフォルダー (Predefinito ボタン: `C:\ProgramData\Albatros\Common\`)。
Nota Connessione / Nota Disconnessione	キーが適用されたときに記録とログに出力されるテキスト。

Registra をクリックすると、設定は `[<Profilo>]_DbKeyEnabled`、`[<Profilo>]_DbKeyAtConnection` などのキーで Albatros 環境に保存され、接続の状態に応じてすぐに適用されます。接続時または切断時に、プログラムは `DbKey=<valore>` を `_DbKey.txt` ファイルに書き込み、記録に残します。

13. ログとデータベースのメンテナンス

13.1 記録とログ

メッセージ パネルに表示される各行は、プロセス (セッション) の識別子、および最初の書き込み時には PC のハードウェア情報とともに、データベースの Log テーブルにも記録されます。ログはパラメーター `DoNotUseLogSSH_Tunnel` で無効にできます。

13.2 Mostra Log

ログイン画面で **DataBase › Gestione Log › Mostra Log** を選択し、日付の範囲 (開始日 / 終了日) を指定して **Ricerca** をクリックします。セッション、日付、時刻、PC 情報、メッセージが表示されます。

13.3 Invia Log via Mail

DataBase › Gestione Log › Invia Log via Mail: 日付の範囲と送信先アドレスを指定して **Invia** をクリックします。その期間のログが Excel にエクスポートされ、zip に圧縮されて送信されます。その後、一時ファイルは削除されます。

13.4 メンテナンス

- **Compatta Database**: ファイル内の空き領域を回収します (VACUUM)。証明書を保存するたびにも自動的に実行されます。
- **Open Ssh_Tunnel DB path**: データベースのフォルダーを開きます。バックアップの作成に便利です。

13.5 データベースの構造

データベースはパスワードで保護された SQLite ファイルで、リビジョン 2 です。起動時に、プログラムは不足しているテーブルを作成し、リビジョン 1 のデータベースを自動的に更新します。

テーブル	内容
Parameters	キーと値のペア: `DbVersion`、`login` (最後に使用したプロファイル)、`[<Profilo>]_IP` (最後に使用したサーバー)。
Certificati	Proprietario、Profilo、Version、VersionDate、Certificato (暗号化テキスト)。
Licenza	KeyLicenza、Assegnatario、DataAssegnazione、CertificatoLicenza (用意されていますが、現在は未使用)。
Log	IdSession、DataLog、PcInfo、KeyInfo、Info。

14. セキュリティ

- **暗号化された証明書**: 機密性のある各値は、ログイン パスワードから導出したキーを使用して Triple DES で暗号化され、証明書全体もさらに暗号化されます。パスワードが保存されることはありません。
- **資格情報は表示されない**: SSH の資格情報、秘密キー、リモート PC のパスワードはプログラム内部に留まり、クライアントに直接渡されます。
- **ハードウェアとの結び付け**: 二段階認証の承認は、それを取得した PC と Windows ユーザーに対してのみ有効です。
- **試行回数の制限**: ログイン パスワード、二段階認証のコード、中間パスワードについて、それぞれ 3 回まで。
- **午前 0 時の有効期限**: OneDay および OneTime の承認に適用されます。
- **追跡可能性**: コードの要求ごと、および RDP/VNC アクセスごとに PC のデータを含むメール、セッションのローカル ログ、SSH サーバーでのアクセスの記録。
- **クリーンアップ**: 補助プログラムと一時的な .rdp ファイルは、起動時と終了時に削除されます。
- **整合性**: 「ChkSum OK」インジケーターは、実行可能ファイルが改ざんされていないことを示します。

> **注**
>
> 中間パスワードは本当の意味での暗号学的な保護ではありません。開いたまま放置されたプログラムの使用を防ぐためのものです。

15. メッセージとトラブルシューティング

メッセージ / 症状	原因と対処
「Password errata: impossibile continuare」	ログイン パスワードが間違っているか、プロファイルが違います。3 回間違えるとプログラムは終了します。
「Certificato inesistente」	選択したプロファイルがデータベースにありません。証明書をインポートしてください。
「Two-factor authentication is required!」	PC が承認されていません。第 5 章に従ってください。
「Invio mail ... per doppia verifica fallito!!!」	メール送信の問題です (ネットワーク、ファイアウォール、SMTP)。再試行するか、「Invia Codice via SMS al Supporto」を使用してください。
「Codice errato: Tentativi n di 3」	コードの入力を間違えたか、以前の要求のコードを入力しています。
「Chiusura automatica per mancato input codice」	コードを入力しないまま 5 分が経過しました。
「Internet Connection Not Available」/「Waiting ...」	インターネット接続がないため、プログラムが待機しています。チェックを省略するには「Chk Internet」をオフにします。
「Errore login!!!」	接続を準備できません (証明書の資格情報またはキーが無効です)。管理者に連絡してください。
接続が確立されない	サーバーに到達できません。一覧の代替サーバーを試してください。名前解決を確認するには Utility › Ping No-IP を使用します。
「### Error Forward Host: ...」	フォワーディングのローカル ポートが他のプログラムに使用されているか、ローカル ホストが無効です。
「Connection Lost」	接続が切断されました。プログラムは自動的に再接続します。
「Password errata」/「Superato il limite di tentativi ammessi」	中間パスワードが間違っています。3 回目の誤りでプログラムは終了します。

メッセージ / 症状	原因と対処
「Ssh Tunnel arrestato per scadenza password...」	OneDay/OneTime 承認で午前 0 時になりました。再起動して新しいコードを要求してください。
「Riscontrata anomalia tra la versione attesa e quella trovata nel Database di servizio」	データベースを更新できません。書き込み権限のあるフォルダーにプログラムを移動してください。
「Operazione annullata per password difforme」	Gestione Certificato の機能で、現在のパスワードが間違っています。
「Porta già utilizzata: Cerco la prima occorrenza libera?」	ローカル ポートが既に別のフォワーディングに割り当てられています。
「Dati Insufficienti!」	フォワーディングの入力で必須フィールドが不足しています。

付録 A – ユーザー向けクイック サマリー

1. `.exe` と `.db` を同じフォルダーにコピーします。
2. 実行可能ファイルを起動し、ログイン パスワードを入力します。
3. 要求された場合は「Richiedi via mail」をクリックし、受け取った OneDay または OneTime コードを入力します。
4. 「SSH Tunneling Ready ....」が表示されるまで待ち、**Connetti** をクリックします。
5. 右側の一覧で目的のコンピューターをダブルクリックします。
6. 要求された場合は中間パスワードを入力します。
7. リモート PC で作業し、終了したら **Disconnetti** または **Esci** をクリックします。

付録 B – 証明書の構造

証明書 (バージョン 2) は `Chiave = "valore"` 形式の行からなるテキストで、全体がパスワードで暗号化されています。機密性のある値は、さらに個別に暗号化されています。認識されるキーの一覧:

キー	内容
`Algoritmo`	暗号化アルゴリズムのバージョン (1)。
`Nominativo`	プロファイル名 (平文)。
`SshUserDllVersion`	最後の保存の通し番号と日付。
`Bloccato`	機能が制限された証明書 (記録に詳細を表示しない、外部ツールなし)。
`ShowRdpButton`	固定接続用の RDP/VNC/Term ボタンを表示します。
`AutoRDP`	接続直後に固定接続を開きます。
`AllowsNewForwards`	ポート フォワーディングの変更を許可します。
`AllowServerIpEditing`	サーバー一覧の変更を許可します。
`Proprietario`	ソフトウェアの受領者 (「Sw consegnato a」)。
`Login`、`Password`	SSH の資格情報。
`Certificate`、`CertificatePassword`、`FileCertificato`	SSH 秘密キー (テキストまたは埋め込みリソース) とそのパスフレーズ。
`PwdRemoteAccess`	中間パスワード。
`Server`、`ServerPort`	& で区切ったサーバーの一覧と既定のポート。
`RdpCommandLine`、`RdpFileStatico`	固定接続のコマンド ラインとファイル。
`Mail`、`MailOneDay`、`MailTemp`	二段階認証のコードの受信者。
`MailInfoAccess`	アクセス通知の受信者。
`Cellulare`	携帯電話番号 (用意済み)。
`RedirectPortsCount`	フォワーディングの数。

キー	内容
RedirectPorts(i, …)	各フォワーディングについて: LocalHost、 LocalPort、 RemoteHost、 RemotePort、 Remark、 RdpFile、 Enabled (Y/N)、 PasswordRdpFF、 PwdActivateRdpConnection。

付録 C – 開発者向け技術メモ

マニュアルの作成中に、コード内で確認が必要ないくつかの点が見つかりました。この付録は内部用であり、プログラムの受領者にマニュアルを渡す前に削除してください。

ファイル / ルーチン	所見
ModSetting.Log	`PathDbSSH_Tunnel` と `FileNameDbSSH_Tunnel` を無視して、`Application.StartupPath` に exe の名前でデータベースが存在するかどうかを確認しています。DB が別の場所にあるか別の名前の場合、ログは書き込まれません。
ModSetting.RemoveParam	クエリで `lower('?')` を使用しています。引用符で囲まれたパラメーターは置換されないため、削除が機能しません。
ModSetting.DecodCertificate	比較 `ToLower.Contains("Algoritmo =")` には大文字が含まれているため、決して真になりません。`Algoritmo` の値は読み取られません (現在は常に 1 なので影響はありません)。
FrmStart_Load	`ContaErrori` はループ内のローカル変数で、毎回 0 にリセットされます。また、二段階認証に失敗するか画面が閉じられた場合、`Exit Sub` ではアプリケーションが終了しません。ウィンドウのないプロセスが残っていないか確認してください。
frmMainProgram、サーバーの `+` / `-` ボタン	ツールヒントが逆になっています: `-` (ツールヒント「Sposta Giù」) は上に移動し、`+` (ツールヒント「Sposta Su」) は下に移動します。
frmMainProgram、テンプレートの `*`	ツールヒントには `###Host###` / `###Port###` と表示されますが、コードで置換されるプレースホルダーは `##host##` / `##port##` です。
EseguiExportCertificato	「supercode」により `.Ssh_T.Key` ファイルへのパスワードの保存が有効になりますが、`CostruisciRemPwdInfo` と `abilitaSalvataggioPwd` は使用されていません。この機能は実装されていません。
ChkIconaAfterSelection	「Icona dopo selezione」オプションはコード内で参照されていません。

ファイル / ルーチン	所見
GetParam / SetParam	キーがパラメーターとして渡されず、SQL クエリに連結されています。
ソース全般	ソースに資格情報とキーが平文で含まれています (SMS サービス、更新用の SFTP アクセス、DB のパスワード、管理パスワードのハッシュ)。実行可能ファイルにアクセスできる人は、.NET の逆コンパイラーでこれらを抽出できます。難読化またはサーバー側への移動を検討してください。