AlbatrosRDP

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.....28

IT Italiano.....54

RO Română.....80

JA 日本語.....106

DevService.net — Raffaele Romano

AlbatrosRDP

Remote Desktop Client

User and Integration Manual

Version 2.0.162.6127 — October 2026

© Raffaele Romano 2026

Contents

1. Introduction **5**
1.1 Main features 5
1.2 Documented version 5
2. Requirements and installation **6**
2.1 Requirements 6
2.2 Files to distribute 6
2.3 Files and folders used by the program 6
3. Quick start **7**
4. The connection window **8**
4.1 Fields and buttons 8
4.2 Checks before connecting 8
4.3 How the history works 8
5. The remote session **10**
5.1 Opening the session 10
5.2 Full-screen behavior 10
6. The custom status bar **11**
6.1 Text and colors 11
6.2 Buttons 11
6.3 Using the mouse 11
6.4 Hidden bar and automatic display 11
7. The quick menu **12**
7.1 How to open it 12
7.2 Menu items 12
8. The native Microsoft connection bar **13**
8.1 Enabling it 13
8.2 Differences in behavior 13
9. Window mode **14**
10. Interruptions, reconnection and errors **15**
10.1 Server no longer reachable during the session 15
10.2 Automatic reconnection 15
10.3 Watchdog (application not responding) 15
10.4 Unexpected errors 15
10.5 Closing 15
11. Starting from the command line **16**
11.1 Connection parameters 16
11.2 Plain-text parameters 16
11.3 Encrypted parameters 16
11.4 Parameters in a file 17
11.5 Missing or wrong decryption password 17
11.6 Password via named pipe 17
11.7 Binding to a single computer 17
12. Integration from other programs **19**
12.1 The RdpConnectionParams class 19
12.2 The RdpCommandLineManager class 19
12.3 The SecretPipeTransfer class 20
12.4 Encryption format 20
12.5 Customizations in code 20
13. RDP settings applied **22**
14. Security and privacy **23**
15. Diagnostic log **24**
16. Troubleshooting **25**
Appendix A. Program messages **26**
Appendix B. Quick reference **27**

B.1 Keys and mouse..... 27
B.2 Command line..... 27
B.3 Timing values..... 27

1. Introduction

AlbatrosRDP is a Remote Desktop (RDP) client for Windows, developed in VB.NET on .NET Framework 4.8. It uses the Microsoft ActiveX control (`mstscax.dll`), that is, the same engine as Remote Desktop Connection (`mstsc.exe`), and adds a set of features designed for everyday use and for connections through SSH tunnels.

1.1 Main features

- Connection window with a **history** of recent connections (the password is never saved) and a free-text **note** for each connection.
- **Full-screen** session with a **floating status bar**: color-coded by state, draggable, auto-hiding.
- Alternatively, Microsoft's **native connection bar**.
- **Quick menu** opened with **Ctrl+F11**, or by right-clicking the status bar or the title bar.
- **Reachability check** of the server before connecting and, every 2 seconds, during the session.
- **Automatic reconnection** when the session drops.
- **Watchdog**: if the application hangs (for example because of a network drop during authentication), it offers to force it to close.
- **Direct start from the command line**, with plain-text, encrypted (AES-256) or file-based parameters. The decryption password can also be passed through a named pipe, so that it never appears on the command line.
- Optional binding of encrypted parameters to a **single computer** (hardware ID).
- **Diagnostic log** that never contains passwords, keys or parameters.

1.2 Documented version

Item	Value
Program	AlbatrosRDP
Version	2.0.162.6127 (October 2026 revision)
Platform	.NET Framework 4.8, Windows Forms, VB.NET
RDP engine	Microsoft RDP ActiveX control (MSTSCLib), versions 6 to 14
Author	© Raffaele Romano 2026

2. Requirements and installation

2.1 Requirements

- Windows with the Microsoft Remote Desktop client installed (`mstscax.dll`, included as standard in desktop and server editions of Windows).
- .NET Framework 4.8.
- Network access to the RDP server on the specified TCP port (default **3389**), directly or through a tunnel.

When the session starts, the program looks for the most recent RDP control registered on the system (from `MsRdpClient14` down to `MsRdpClient6`). Each version is actually created and tested: if it does not work, it is discarded and the previous one is tried. The version in use is shown in the **Dati connessione...** (Connection details) menu item and in the log.

2.2 Files to distribute

The program needs no installation: just copy it to a folder (for example `C:\Albatros\CompiledPrograms\`). The project produces two versions:

Build folder	Content to copy
`bin\Release\AlbatrosRDP_Secure\`	Version protected with .NET Reactor. The libraries `Interop.MSTSCLib.dll`, `AxInterop.MSTSCLib.dll` and `Newtonsoft.Json.dll` are embedded: `AlbatrosRDP.exe` alone is enough. This is the recommended version for distribution.
`bin\Release\`	Unprotected version: copy `AlbatrosRDP.exe`, `AlbatrosRDP.exe.config` and the three DLLs listed above.

2.3 Files and folders used by the program

Path	Use
`C:\ProgramData\Albatros\Common\CronologRDP.txt`	Connection history (JSON), shared by all users of the computer.
`%LOCALAPPDATA%\Albatros\AlbatrosRDP\AlbatrosRDP.log`	Diagnostic log of the current user; the previous copy is `AlbatrosRDP.1.log`.
`CronologRDP.txt.corrupt-<data>.bak`	Backup copy of the history, created only if the file turns out to be unreadable.

> **Multiple users on the same computer.** With the default ProgramData permissions, the history file created by one user cannot be modified by the others: for them the history is not updated. If needed, an administrator can grant Modify permission to the Users group with: `icacls "C:\ProgramData\Albatros\Common" /grant *S-1-5-32-545:(OI)(CI)M`

3. Quick start

1. Start `AlbatrosRDP.exe` without parameters: the connection window opens.
2. Fill in **Computer** (server name or address), **Porta** (Port), **Nome utente** (User name), optionally **Dominio** (Domain) and **Note** (Notes), then the **Password**. For a server you have already used, just select it from the **Cronologia** (History) and type the password.
3. Press **Connetti** (Connect), or Enter.
4. The program checks that the server is reachable and opens the session in full screen. If Windows asks for credentials (NLA), enter them in the system window.
5. The status bar appears at the top center: green when the session is active.
6. To open the menu, press **Ctrl+F11** (or right-click the status bar).
7. To finish, choose **Disconnetti & Exit** (Disconnect & Exit) from the menu, or the red **X** on the bar, and confirm.

4. The connection window

It opens when the program starts without valid command-line parameters. It resembles the Windows Remote Desktop Connection.

> **Label language.** The window is translated into English, Italian, French and Romanian, but in the current version the language is forced to **English**. The table also shows the English label that appears on screen.

4.1 Fields and buttons

Field	On-screen label	Description
Cronologia	History	List of recent connections, in the format `server:porta {utente}`; you can only select from it, not type. The first entry, -- Nuova connessione -- (New connection), clears the fields. When the window opens, the most recent connection is selected.
✖ (next to the history)	—	Removes the selected entry from the history, after confirmation.
Computer	Computer	Host name, IPv4 or IPv6 address. It also accepts `host:porta` and `[IPv6]:porta`: a port written here takes precedence over the Port field. An IPv6 address without square brackets is taken as having no port.
Porta	Port	Digits only, from 1 to 65535. If empty, 3389 is used.
Nome utente	User name	User of the remote session.
Dominio	Domain	User's domain (optional).
Note	Notes	Free text shown in the status bar, in the window title and at the top of the menu. It is saved in the history.
Password	Password	Password of the remote user. It is never saved. If left empty, Windows will ask for it when connecting.
Mostra password	Show password	Shows the typed password in plain text.
Barra di stato personalizzata	Customized Status Bar	Selected (default): AlbatrosRDP status bar. Cleared: Microsoft native bar (chapter 8). The choice is remembered for each history entry.
Connetti	Connect	Starts the connection (Enter key).
Annulla	Cancel	Closes the program without connecting (Esc key).

If you choose an entry from the history, the cursor goes straight to the password; otherwise to the Computer field. Copyright and version are shown at the bottom left.

4.2 Checks before connecting

- Empty Computer field: "Specificare l'indirizzo del computer." (Specify the computer address.)
- Invalid port in the Computer field (e.g. `server:99999`): "Porta non valida nel campo Computer: indicare un numero compreso tra 1 e 65535 (es. server:3389)." (Invalid port in the Computer field: enter a number between 1 and 65535, e.g. server:3389.)
- Invalid port in the Port field: "Porta non valida: indicare un numero compreso tra 1 e 65535." (Invalid port: enter a number between 1 and 65535.)

4.3 How the history works

- An entry is identified by **Server + Port + User name + Domain**, case-insensitively.

- The note and the bar choice follow the entry but do not identify it: the last value used always applies.
- A connection that is already present is moved to the end of the list, that is, it becomes the most recent.
- At most **20** entries are kept: beyond this number the oldest are deleted.
- Saving takes place when Connect is pressed. It is atomic and protected by an inter-process lock: two instances open at the same time do not delete each other's entries.
- The password is never written to the file.

5. The remote session

5.1 Opening the session

1. The window switches to **full screen** on the current monitor, including the taskbar area. The window title is the note, or "AlbatrosRDP".
2. The remote desktop is requested at the monitor's resolution. Only one monitor is used.
3. Reachability check: a test TCP connection to the server and port, with a 2.5-second timeout (DNS resolution included; IPv4 and IPv6 addresses tried in parallel). The bar shows "Verifica raggiungibilità server:porta..." (Checking reachability of server:port...).
4. If the server does not respond, this appears: "Impossibile raggiungere il server ... (tunnel SSH non attivo oppure rete non disponibile). Riprovare?" (Unable to reach the server ... (SSH tunnel not active or network unavailable). Retry?). **Yes** repeats the check, **No** closes the program.
5. If the server responds, the RDP connection starts ("Connessione in corso...", Connecting...). If the server requires credentials, Windows shows its own window: during this phase AlbatrosRDP suspends keyboard handling and does not stay in the foreground, so as not to cover it.
6. Once the connection is established, the bar turns green and shows `--> server:porta`.

If the session never reaches the connected state (credentials canceled or wrong, no network), the program does not retry forever: it shows "La connessione RDP non è stata stabilita (Credenziali mancanti/annullate oppure errore di rete). L'applicazione verrà chiusa." (The RDP connection was not established (credentials missing/canceled or network error). The application will be closed.) and exits.

5.2 Full-screen behavior

- The window stays on top of the others **only** when it is in the foreground: with Alt+Tab or by clicking another application you switch to other programs as usual.
- The status bar is visible only when AlbatrosRDP is the active application.
- The remote content adapts to the window (smart sizing): in reduced window mode the remote desktop is scaled down proportionally, without scroll bars.

6. The custom status bar

This is the rounded bar that appears at the top center of the screen in full-screen mode, when the **Barra di stato personalizzata** (Customized Status Bar) option is enabled.

6.1 Text and colors

The text consists of: note (if any), menu key reminder, state. Example: `Server ufficio - (Ctrl+F11 menu) - --> 192.168.1.10:3389`.

Colors	Meaning
Green background, yellow text	Session connected and server reachable.
Yellow background, red text	Any other state: check in progress, connection in progress, connection lost, error.

6.2 Buttons

Button	Action
─ (yellow)	Minimizes.
□ (yellow)	Switches from full screen to window and vice versa.
X (red)	Same as Disconnetti & Exit: asks for confirmation if the session is connected, then closes.

6.3 Using the mouse

- **Dragging** with the left button: the bar can be moved anywhere on the screen and stays in the chosen position.
- **Right-click**: opens the quick menu.
- **Double-click**: hides the bar (like the Barra di stato menu item).

6.4 Hidden bar and automatic display

A bar hidden manually (double-click or menu) can be made to reappear in three ways:

- from the quick menu (Ctrl+F11), item **Barra di stato** (Status bar);
- by moving the mouse within **10 pixels of the top edge** of the screen, if the **Mostra barra al passaggio mouse in alto** (Show bar on mouse-over at top) option is enabled (it is enabled by default). In this case the bar hides again when the mouse moves more than 20 pixels below it;
- by leaving and re-entering full-screen mode, or by restoring the window after minimizing it.

7. The quick menu

7.1 How to open it

- **Ctrl+F11**: works only with the custom bar. The key combination is intercepted and does not reach the remote computer. When the native bar is active, it is disabled and is passed to the remote session.
- **Right-click the status bar** (in full screen).
- **Right-click the title bar** (in window mode), instead of the Windows system menu.

The menu closes when you click outside it, with the **Chiudi tendina** (Close menu) item, or with **Esc**. While the menu is open, the Esc key is not sent to the remote session.

7.2 Menu items

Item	Function
Note (in bold)	Present only if there is a note. Clicking it opens the "Nota di connessione" (Connection note) window to edit it. The new note applies to the current session and immediately updates the bar and title; it is not saved in the history.
Schermo ridotto / Schermo intero	Switches from full-screen mode to window and vice versa (chapter 9). (Reduced screen / Full screen)
Riduci a icona	Minimizes the session window.
Barra di stato	Shows or hides the status bar. Available only in full screen.
Mostra barra al passaggio mouse in alto	Turns automatic display of the bar on or off (section 6.4).
Barra RDP nativa	Switches to Microsoft's native connection bar, or back to the custom one (chapter 8).
Dati connessione...	Shows note, info (`-info` parameter), server, port, user, domain, state, RDP control in use with its version, copyright and program version.
Riconnetti	Closes the session if it is still open (waiting at most 5 seconds) and reopens it. Useful if the session is not responding.
Disconnetti & Exit	Asks "Disconnettere la sessione RDP e chiudere l'applicazione?" (Disconnect the RDP session and close the application?; default: No) and, if you confirm, disconnects and closes.
Chiudi tendina	Closes the menu without doing anything.

8. The native Microsoft connection bar

As an alternative to the AlbatrosRDP bar, you can use Microsoft's standard connection bar, the one of `mstsc.exe`.

8.1 Enabling it

- Before connecting: clear the **Barra di stato personalizzata** check box in the connection window. The choice is stored for that history entry.
- During the session: menu item **Barra RDP nativa** (Native RDP bar).

About one second after the connection is established, the RDP control switches to its own full screen and shows the Microsoft bar, pinned and with the Minimize, Restore and Pin buttons.

8.2 Differences in behavior

- **Ctrl+F11** is disabled: the key combination reaches the remote computer.
- The custom bar and its automatic display are disabled.
- **Minimize** on the Microsoft bar minimizes the whole session; reopen it from its icon on the taskbar.
- **Restore** on the Microsoft bar puts AlbatrosRDP in **window mode** and does not return to full screen by itself. From here, right-clicking the title bar opens the quick menu: **Schermo intero** (Full screen) returns to native full screen, while clearing **Barra RDP nativa** returns to the custom bar.
- **X** on the Microsoft bar closes the session. The question "La sessione RDP è stata disconnessa. Riconnettersi al server? (No = chiude l'applicazione)" (The RDP session has been disconnected. Reconnect to the server? (No = closes the application)) appears.

9. Window mode

With **Schermo ridotto** (Reduced screen, from the menu) or with the □ button on the bar, the session switches to a normal, resizable Windows window.

- The connection state (with note and menu reminder) is shown in the **window title**, instead of the status bar.
- The remote desktop keeps the resolution it was opened with and is scaled down to fit the window.
- **Right-clicking the title bar** opens the quick menu; Ctrl+F11 also keeps working (with the custom bar).
- To the left of the system buttons (minimize, maximize, close) there is an additional **Schermo intero** (Full screen) button that returns the session to full screen.

10. Interruptions, reconnection and errors

10.1 Server no longer reachable during the session

While the session is connected, every 2 seconds the program tries to open a TCP connection to the server's RDP port (timeout 1.5 seconds). If the test fails, the bar turns yellow with "Connessione persa su server:porta" (Connection lost on server:port), even if the RDP control has not yet detected the drop. It turns green again by itself when the server responds again. This is the typical case of a dropped SSH tunnel.

10.2 Automatic reconnection

In addition to the RDP control's own internal automatic reconnection, if the session is disconnected after having been connected at least once, AlbatrosRDP:

1. tries to reconnect at most every **5 seconds**, each time preceded by a quick TCP check (1 second);
2. after **3 consecutive failed attempts** it asks: "La riconnessione automatica non riesce (credenziali mancanti/annullate oppure server non disponibile). Continuare a riprovare?" (Automatic reconnection is failing (credentials missing/canceled or server unavailable). Keep retrying?). **Yes** resumes the attempts, **No** closes the program.

10.3 Watchdog (application not responding)

An independent check verifies that the user interface is responding. If it stays blocked for more than **15 seconds** (for example because of a network interruption during RDP authentication), the message "L'applicazione non risponde da diversi secondi... Vuoi forzare la chiusura dell'applicazione?" (The application has not been responding for several seconds... Do you want to force the application to close?) appears on top of every other window. **Yes** terminates the program, **No** keeps waiting. The check is suspended while the program's dialog boxes are open.

10.4 Unexpected errors

- **RDP control not available** or not working at startup: "Impossibile avviare la connessione RDP:" (Unable to start the RDP connection:) appears with the error details, then the program closes.
- **Unhandled exception**: the "AlbatrosRDP - Errore" message shows the error and asks "Continuare a usare l'applicazione?" (Continue using the application?). **Yes** lets you continue without losing the session, **No** closes. The error is always recorded in the log.

10.5 Closing

- Any manual closing while the session is connected (menu, X on the bar, X on the window, Alt+F4, taskbar) asks for confirmation. Answering No returns you exactly to the previous situation.
- When closing, the program disconnects the session and waits at most 1 second for the RDP control to close it.
- When closing starts from an error dialog, a safety stop is provided: if cleanup hangs, the process is terminated anyway after 8 seconds.

11. Starting from the command line

AlbatrosRDP can open a connection directly, without showing the connection window. Parameters can be passed in three ways: **in plain text**, **encrypted** in a single string, or in a **file** (plain text or encrypted).

11.1 Connection parameters

Parameter	Required	Meaning
`-ip=`	Yes	Server name or address. It also accepts `host:porta` and `[IPv6]:porta`.
`-port=`	No	TCP port (1-65535). If missing or invalid: 3389.
`-user=`	No	User name.
`-domain=`	No	Domain.
`-pwd=`	No	Password of the remote user. If missing, Windows asks for it.
`-nota=`	No	Note shown in the bar, title and menu.
`-info=`	No	Additional information shown in Dati connessione...

Parameter	Meaning
`-enc=`	Encrypted string (Base64) containing the parameters of the previous table.
`-file=`	Path of a file containing the parameters, in plain text or encrypted.
`-cryptpwd=`	Decryption password for `-enc` or `-file`. The special value `pipe` indicates that the password is delivered through a named pipe (section 11.6).
`-local=true`	Informational only: indicates that the content has been bound to the computer. It is ignored when reading.

General rules:

- Parameter names are case-insensitive; the leading hyphen is optional (`ip=` is the same as `-ip=`).
- Values containing spaces must be enclosed in double quotes, preferably the whole argument: `"-nota=Server ufficio"`.
- Order of priority: if `-file` is present, the file is used; otherwise, if `-enc` is present, the encrypted string; otherwise the individual parameters.
- Unknown parameters are ignored.
- If `-ip` is missing (or the specified file does not exist), the program behaves as if it had no parameters and opens the connection window.
- A connection started from the command line uses the custom bar and is **not** added to the history.

11.2 Plain-text parameters

```
AlbatrosRDP.exe -ip=192.168.1.10 -port=3389 -user=Administrator "-nota=Server ufficio"
```

> **Caution.** A password passed in plain text with `-pwd=` is visible to anyone who can read the processes' command lines (Task Manager, Process Explorer, WMI). To pass the password, use the encrypted form, preferably with the pipe.

11.3 Encrypted parameters

```
AlbatrosRDP.exe "-enc=<stringa Base64>" "-cryptpwd=<chiave>"
```

The `-enc` string is generated with the programming functions described in chapter 12 (`BuildCommandLineArgs`). The program has no interactive function to create it.

11.4 Parameters in a file

```
AlbatrosRDP.exe "-file=C:\Config\Clienti\Cliente1.rdpdat"
AlbatrosRDP.exe "-file=C:\Config\Clienti\Cliente1.rdpdat" "-cryptpwd=<chiave>"
```

The file (UTF-8) can contain the parameters **in plain text**, even on multiple lines and with or without the hyphen, or an **encrypted** string. The program detects the format by itself: if the content is plain text, any `-cryptpwd` is ignored. Example of a plain-text file written by hand:

```
-ip=192.168.1.10
-port=3389
-user=Administrator
"-nota=Server ufficio"
"-info=Contratto assistenza n. 42"
```

An encrypted file is created with `BuildCommandLineArgs` by specifying the path (chapter 12). If the file already exists, you are asked for confirmation before it is overwritten.

11.5 Missing or wrong decryption password

If the content is encrypted and `-cryptpwd` is missing or wrong, the **Password richiesta** (Password required) window appears: "I parametri di connessione sono protetti da password. Tentativo N di 3." (The connection parameters are password-protected. Attempt N of 3.), preceded by "Password errata." (Wrong password.) after an error.

- **3 attempts** are allowed.
- With **Annulla** (Cancel), or when the attempts are used up, the program **exits** without opening the connection window.
- Every decryption is verified (the result must contain at least `ip`): a wrong password cannot be mistaken for a correct one.

11.6 Password via named pipe

With `-cryptpwd=pipe` the real password never appears on the command line, not even for an instant. The program that starts AlbatrosRDP delivers it through a local named pipe:

- pipe name: `\\.\pipe\AlbatrosRDP_Secret_<PID>`, where PID is the process identifier of the AlbatrosRDP instance just started;
- the pipe is created by the calling program, is accessible only to the current Windows user and accepts a single connection;
- the secret is delivered only if the process connecting is exactly the expected one (client PID check);
- the text travels in UTF-8 (a BOM, if present, is tolerated);
- AlbatrosRDP waits at most **5 seconds**: if it receives nothing, it asks for the password with the window described in section 11.5.

The simplest way to use the pipe is the `StartProcessWithEncryptedArgsAndPipePasswordWait` function (chapter 12), which does everything in a single call.

11.7 Binding to a single computer

At creation time (`machineBound:=True`) the encrypted content can be bound to the current computer. In that case the actual encryption key consists of the computer's hardware ID followed by the password. The hardware ID is made up of:

- motherboard serial number;
- CPU identifier;
- serial number of the first physical disk.

When reading, nothing needs to be specified: the program first tries the password as it is (content valid on all computers) and then the combination with the local computer's hardware ID, including the variants due to the non-guaranteed order of disks (for example when a USB stick is plugged in).

> **Caution.** Bound content becomes unreadable if the motherboard, CPU or system disk is replaced, and of course on any other computer: in that case it must be regenerated.

12. Integration from other programs

The program's classes can be used by another VB.NET application, by adding a reference to `AlbatrosRDP.exe` (unprotected version) or by including the source files. The sample project **Test_Lancio_pipe** (console application) shows how to start the program with the password via pipe.

12.1 The RdpConnectionParams class

Property	Type	Description
`Ip`	String	Server (required).
`Port`	Integer	Port; 0 = default (3389).
`User`, `Domain`	String	User and domain.
`Password`	String	Password of the remote user.
`Nota`, `Info`	String	Note and additional information.
`IsValid`	Boolean	True if `Ip` has a value.
`Clone()`	Function	Returns a copy.

12.2 The RdpCommandLineManager class

Method (Shared)	Description
`BuildCommandLineArgs(prms, [encryptionPassword], [filePath], [machineBound])`	Builds the arguments. Without a password: plain text. With a password: `-enc` + `-cryptpwd`. With `filePath`: writes the file (plain text or encrypted, creates the folder, asks for confirmation if it exists) and returns `-file` [+ `-cryptpwd`]. The arguments are already quoted according to Windows rules.
`BuildCommandLineArgsFromFile(filePath, [encryptionPassword])`	Arguments for an existing file; if a password is specified, it first checks that the file can be decrypted. Throws an exception if the file does not exist or the password is wrong.
`StartProcessWithEncryptedArgsAndPipePasswordWait(exePath, prms, encryptionPassword, ByRef passwordDelivered, [machineBound], [pipeTimeoutMs=5000])`	Starts AlbatrosRDP with `-cryptpwd=pipe`, delivers the password through the pipe and waits for the delivery. `passwordDelivered` indicates the outcome. Suitable for launchers that exit immediately.
`StartProcessWithEncryptedArgsAndPipePassword(exePath, prms, encryptionPassword, [machineBound], [pipeTimeoutMs=5000])`	As above, but delivery takes place in the background and the method returns immediately. If the caller exits before delivery, the password does not arrive.
`ParseCommandLineArgs(args, [ByRef userAborted])`	Parses the received arguments (with an interactive password prompt if needed).
`ReadParamsFromFile(filePath, [cryptPwd])`	Reads a parameter file without dialog boxes; exception if the password is wrong.
`EncryptString(testo, password)` / `DecryptToOriginalString(blob, password)`	Basic encryption and decryption, without hardware binding.
`GetMachineHardwareId()`	Hardware ID of the current computer.

Example: start with the password via pipe from a launcher (the key is held in a variable, never written in the code):

```
Dim prms As New RdpConnectionParams With {
    .Ip = "192.168.1.10", .Port = 3389,
    .User = "Administrator", .Nota = "Server ufficio"}

Dim consegnata As Boolean = False
RdpCommandLineManager.StartProcessWithEncryptedArgsAndPipePasswordWait(
    "C:\Albatros\CompiledPrograms\AlbatrosRDP.exe",
    prms, chiave, consegnata)
```

Example: creating an encrypted file bound to the computer:

```
Dim argomenti As String = RdpCommandLineManager.BuildCommandLineArgs(
    prms, encryptionPassword:=chiave,
    filePath:="C:\Config\Clienti\Cliente1.rdpdat", machineBound:=True)
' -> "-file=C:\Config\Clienti\Cliente1.rdpdat" "-cryptpwd=..." "-local=true"
```

12.3 The SecretPipeTransfer class

Method (Shared)	Description
`SendSecretToChildProcessAndWait(processo, segreto, [timeoutMs])`	Caller side: creates the pipe for the child process's PID and waits for delivery. Returns True if delivered.
`SendSecretToChildProcess(processo, segreto, [timeoutMs])`	As above, in the background.
`ReceiveSecretForCurrentProcess([timeoutMs])`	AlbatrosRDP side: reads the secret from the pipe of its own PID.
`ReadSecretFromPipe(nomePipe, [timeoutMs])`	Reads from a pipe with an explicit name.
`WaitSeconds(n)` / `WaitMilliSeconds(n)`	Wait that keeps the user interface responsive.

12.4 Encryption format

Item	Value
Algorithm	AES-256, CBC mode, PKCS7 padding
Key derivation	PBKDF2-HMAC-SHA1, 50,000 iterations, random 16-byte salt
Format	Base64 of: salt (16 bytes) + IV (16 bytes) + encrypted data
Plain-text content	Parameters in the format `"-ip=..." "-user=..."` (UTF-8)
Compatibility	Identical to previous versions: strings and files created earlier remain readable, and vice versa

12.5 Customizations in code

Item	Description
`FrmRDP.New([nativeConnectionBar], [SafeMode])`	Session with connection window.
`FrmRDP.New(server, port, domain, userName, password, [nativeConnectionBar], [SafeMode])`	Direct session, without connection window.
`SafeMode`	If True, it first looks for the generic RDP control and limits the choice to versions up to 11.
`FrmRDP.MenuHotkey`	Quick menu key combination (default `Keys.Control Or Keys.F11`).

Item	Description
`FrmRDP.ConnectionNote` / `ConnectionInfo`	Session note and info.
`FrmRDP.ShowNativeConnectionBar`	Native bar yes/no; set it before `ShowDialog()`.
`Module1.PercorsoStorico`	Path of the history file.
`Module1.MaxCronologRDP`	Maximum number of history entries (default 20).

13. RDP settings applied

When each session is opened, the following settings are applied, in the format of `.rdp` files. They are defined in the code (`rdpSettingsString` string of FrmRDP); there is no external configuration file.

Setting	Effect
`session bpp:i:32`	32-bit color.
`compression:i:1`	Data compression enabled.
`disable wallpaper:i:1`	Remote desktop background not shown (less bandwidth).
`keyboardhook:i:2`	Windows key combinations sent to the remote computer only in full screen (default value).
`audiomode:i:0`	Remote audio played on the local computer.
`audiocapturemode:i:1`	Local microphone available in the remote session.
`redirectprinters:i:1`	Local printers available in the session.
`redirectsmartcards:i:1`	Local smart cards available.
`redirectclipboard:i:1`	Clipboard shared between local and remote.
`drivestoredirect:s:*`	All local drives visible in the remote session.
`negotiate security layer:i:1`	Automatic negotiation of the strongest security protocol.
`screen mode id`, `use multimon`	Ignored: full screen is handled by the program, on a single monitor.

Immediately afterwards, the program also sets:

- **automatic reconnection** of the RDP control enabled (replaces `autoreconnection enabled:i:0` in the string);
- **authentication level 0** and certificate warnings ignored (replaces `authentication level:i:2`): the server certificate is not verified and no warning appears;
- **CredSSP** enabled (required for NLA authentication);
- **connection timeout**: 8 seconds overall, 5 per single attempt.

The program can also interpret other `.rdp` keys (for example `alternate shell` and `shell working directory` to start a single program instead of the desktop, `connection type`, `networkautodetect`, `redirectcomports` and the RD Gateway settings `gatewayhostname`, `gatewayusagemethod` and similar): to use them, the string in the code must be changed and the program recompiled.

14. Security and privacy

- The remote user's **password** is never saved to disk: neither in the history nor in the log. After it is handed over to the RDP control, the copies in memory are cleared.
- The **log** records only the startup mode, connection states and errors: never passwords, keys or parameters.
- **Encryption** uses AES-256 with a key derived by PBKDF2. Buffers with sensitive data are zeroed after use.
- The **pipe** is accessible only to the current user, delivers the secret only to the expected process, and is single-use.
- The **server certificate is not verified** (chapter 13). Protection against eavesdropping therefore relies on the channel: trusted network, VPN or SSH tunnel. Consider whether to keep this setting.
- A password passed in plain text with `-pwd=` is visible in the process list (section 11.2).
- The reachability check during the session opens a TCP connection to the RDP port every 2 seconds: on the server this generates events in the RDP log (RdpCoreTS) and a little traffic in the tunnel.

15. Diagnostic log

The log is located in `%LOCALAPPDATA%\Albatros\AlbatrosRDP\AlbatrosRDP.log`. When it exceeds 1 MB it is renamed to `AlbatrosRDP.1.log` (replacing the previous copy) and a new one is started. Each line has the format:

```
2026-10-11 14:22:05.123 [4812] INFO  Stato RDP: connesso
```

that is, date and time, process PID, level (INFO, WARN, ERROR) and message. The following are recorded:

- application startup (version and number of arguments) and closing;
- command-line mode (plain text, encrypted, file) and outcome (valid or invalid parameters, password canceled or wrong);
- server, port, RDP control in use and type of bar;
- session state changes, with the extended disconnection reason code;
- failed reconnection attempts, watchdog interventions, errors and unhandled exceptions;
- session closing with the reason.

16. Troubleshooting

Problem	What to do
"Impossibile avviare la connessione RDP" appears at startup	The Windows RDP control is missing or not working. Check that Remote Desktop Connection (`mstsc.exe`) works and look at the log.
"Impossibile raggiungere il server"	Check the SSH tunnel, VPN, firewall, address and port. With a local tunnel, make sure it is active before connecting.
The program closes with "La connessione RDP non è stata stabilita"	Credentials canceled or wrong, or no network during authentication. Try again, checking user, domain and password.
Yellow bar with "Connessione persa su ..."	The server no longer responds on the RDP port: typically the tunnel has dropped. The bar turns green again by itself when the connection is restored.
Ctrl+F11 does not open the menu	The native Microsoft bar is active (Ctrl+F11 disabled). Right-click the title bar in window mode.
The status bar is not visible	It has been hidden (double-click or menu): move the mouse to the top edge or use Ctrl+F11 > Barra di stato. The bar is visible only if AlbatrosRDP is the active application.
Started with `-cryptpwd=pipe` and the password is requested	The password did not arrive within 5 seconds. The launcher probably exited before delivery: use `StartProcessWithEncryptedArgsAndPipePasswordWait`.
Correct password but "Password errata" with bound content	The hardware has changed (motherboard, CPU, disk) or you are using a different computer: regenerate the encrypted content.
With `-ip` present, the connection window opens anyway	The parameter was not recognized: check the use of double quotes and, with `-file`, that the file exists.
The history is not updated	Write permissions on the file in ProgramData are missing (section 2.3).
The history has disappeared	The file was unreadable: a copy `.corrupt-<data>.bak` has been saved in the same folder.
The remote desktop background does not appear (solid color)	This is intentional (`disable wallpaper:i:1`, chapter 13).
"L'applicazione non risponde da diversi secondi"	The program has been blocked for more than 15 seconds, usually because of a network drop during authentication. Yes closes the program, No keeps waiting.

Appendix A. Program messages

Message	Meaning and answers
Verifica raggiungibilità server:porta...	TCP test in progress before connecting. (Checking reachability of server:port...)
Connessione in corso...	The RDP control is establishing the session. (Connecting...)
--> server:porta (green bar)	Session connected.
Connessione persa su server:porta	The server does not respond to the periodic TCP test. (Connection lost on server:port)
Connessione RDP non attiva	Session disconnected; automatic reconnection in progress. (RDP connection not active)
Riconnessione in corso... / Disconnessione in corso...	Effect of the Riconnetti item or of closing. (Reconnecting... / Disconnecting...)
Errore di connessione / Errore di riconnessione	The RDP control rejected the connection request. (Connection error / Reconnection error)
Impossibile raggiungere il server ... Riprovare?	Yes = new check; No = close. (Unable to reach the server ... Retry?)
La connessione RDP non è stata stabilita ... L'applicazione verrà chiusa.	The first connection never succeeded (credentials or network). (The RDP connection was not established ... The application will be closed.)
La riconnessione automatica non riesce ... Continuare a riprovare?	After 3 failed attempts. Yes = continue; No = close. (Automatic reconnection is failing ... Keep retrying?)
La sessione RDP è stata disconnessa. Riconnettersi al server?	Session closed from the native bar or by the server. Yes = reconnect; No = close. (The RDP session has been disconnected. Reconnect to the server?)
Disconnettere la sessione RDP e chiudere l'applicazione?	Closing confirmation. Default: No. (Disconnect the RDP session and close the application?)
L'applicazione non risponde da diversi secondi ...	Watchdog. Yes = forced close; No = wait. (The application has not been responding for several seconds ...)
AlbatrosRDP - Errore ... Continuare a usare l'applicazione?	Unhandled exception. Yes = continue; No = close. (AlbatrosRDP - Error ... Continue using the application?)
Password richiesta - Tentativo N di 3	Encrypted parameters: enter the decryption password. (Password required - Attempt N of 3)
Il file ... esiste già. Sovrascrivere?	Creating a parameter file from code. (The file ... already exists. Overwrite?)

Appendix B. Quick reference

B.1 Keys and mouse

Command	Effect
Ctrl+F11	Opens the quick menu (custom bar only).
Esc with the menu open	Closes the menu.
Right-click the status bar	Opens the quick menu.
Right-click the title bar	Opens the quick menu (window mode).
Double-click the status bar	Hides the bar.
Mouse at the top edge	Makes the hidden bar reappear.
Dragging the status bar	Moves it.
Enter / Esc in the connection window	Connetti / Annulla (Connect / Cancel).

B.2 Command line

```
AlbatrosRDP.exe -ip=<server> [-port=<porta>] [-user=<utente>] [-domain=<dominio>]
                [-pwd=<password>] ["-nota=<testo>"] ["-info=<testo>"]

AlbatrosRDP.exe "-enc=<Base64>" "-cryptpwd=<chiave>|pipe"

AlbatrosRDP.exe "-file=<percorso>" ["-cryptpwd=<chiave>|pipe"]
```

B.3 Timing values

Check	Value
Initial reachability check	2.5 s
Check during the session	every 2 s, timeout 1.5 s
Minimum interval between reconnection attempts	5 s
Attempts before the question "Continuare a riprovare?" (Keep retrying?)	3
Initial wait before the connection is considered failed	15 s
Watchdog	15 s blocked (checked every 2 s)
Native bar activation after connecting	1 s
Wait for the password via pipe	5 s
Safety stop when closing	8 s

AlbatrosRDP

Client Bureau à distance

Manuel d'utilisation et d'intégration

Version 2.0.162.6127 — octobre 2026

© Raffaele Romano 2026

Sommaire

1. Introduction **31**
1.1 Fonctions principales 31
1.2 Version documentée 31
2. Configuration requise et installation **32**
2.1 Configuration requise 32
2.2 Fichiers à distribuer 32
2.3 Fichiers et dossiers utilisés par le programme 32
3. Démarrage rapide **33**
4. La fenêtre de connexion **34**
4.1 Champs et boutons 34
4.2 Contrôles avant la connexion 34
4.3 Fonctionnement de l'historique 34
5. La session à distance **36**
5.1 Ouverture de la session 36
5.2 Comportement en plein écran 36
6. La barre d'état personnalisée **37**
6.1 Texte et couleurs 37
6.2 Boutons 37
6.3 Utilisation avec la souris 37
6.4 Barre masquée et apparition automatique 37
7. Le menu rapide **38**
7.1 Comment l'ouvrir 38
7.2 Commandes du menu 38
8. La barre de connexion native Microsoft **39**
8.1 Activation 39
8.2 Différences de comportement 39
9. Le mode fenêtré **40**
10. Interruptions, reconnexion et erreurs **41**
10.1 Serveur devenu injoignable pendant la session 41
10.2 Reconnexion automatique 41
10.3 Watchdog (application bloquée) 41
10.4 Erreurs inattendues 41
10.5 Fermeture 41
11. Lancement depuis la ligne de commande **42**
11.1 Paramètres de connexion 42
11.2 Paramètres en clair 42
11.3 Paramètres chiffrés 42
11.4 Paramètres dans un fichier 43
11.5 Mot de passe de déchiffrement manquant ou erroné 43
11.6 Mot de passe via named pipe 43
11.7 Liaison à un seul ordinateur 43
12. Intégration depuis d'autres programmes **45**
12.1 La classe RdpConnectionParams 45
12.2 La classe RdpCommandLineManager 45
12.3 La classe SecretPipeTransfer 46
12.4 Format du chiffrement 46
12.5 Personnalisations par code 46
13. Paramètres RDP appliqués **48**
14. Sécurité et confidentialité **49**
15. Journal de diagnostic **50**
16. Dépannage **51**
Annexe A. Messages du programme **52**
Annexe B. Référence rapide **53**

B.1 Touches et souris....53
B.2 Ligne de commande....53
B.3 Valeurs temporelles....53

1. Introduction

AlbatrosRDP est un client Bureau à distance (RDP) pour Windows, développé en VB.NET sur .NET Framework 4.8. Il utilise le contrôle ActiveX de Microsoft (`mstscax.dll`), c'est-à-dire le même moteur que Connexion Bureau à distance (`mstsc.exe`), et y ajoute une série de fonctions conçues pour l'usage quotidien et pour les connexions à travers des tunnels SSH.

1.1 Fonctions principales

- Fenêtre de connexion avec **historique** des dernières connexions (le mot de passe n'est jamais enregistré) et une **note** libre pour chaque connexion.
- Session en **plein écran** avec une **barre d'état flottante** : colorée selon l'état, déplaçable, escamotable.
- En alternative, la **barre de connexion native** de Microsoft.
- **Menu rapide** accessible avec **Ctrl+F11**, par un clic droit sur la barre d'état ou sur la barre de titre.
- **Vérification de l'accessibilité** du serveur avant la connexion et, toutes les 2 secondes, pendant la session.
- **Reconnexion automatique** lorsque la session tombe.
- **Watchdog** : si l'application reste bloquée (par exemple à cause d'une coupure réseau pendant l'authentification), il propose la fermeture forcée.
- **Lancement direct depuis la ligne de commande**, avec des paramètres en clair, chiffrés (AES-256) ou lus dans un fichier. Le mot de passe de déchiffrement peut aussi être transmis via named pipe, sans jamais apparaître dans la ligne de commande.
- Liaison facultative des paramètres chiffrés à un **seul ordinateur** (ID matériel).
- **Journal de diagnostic** qui ne contient jamais de mots de passe, de clés ni de paramètres.

1.2 Version documentée

Élément	Valeur
Programme	AlbatrosRDP
Version	2.0.162.6127 (révision d'octobre 2026)
Plateforme	.NET Framework 4.8, Windows Forms, VB.NET
Moteur RDP	Contrôle ActiveX Microsoft RDP (MSTSCLib), versions 6 à 14
Auteur	© Raffaele Romano 2026

2. Configuration requise et installation

2.1 Configuration requise

- Windows avec le client Bureau à distance de Microsoft installé (`mstscax.dll`, présent en standard dans les versions bureau et serveur de Windows).
- .NET Framework 4.8.
- Accès réseau au serveur RDP sur le port TCP indiqué (par défaut **3389**), directement ou via un tunnel.

Au démarrage de la session, le programme recherche le contrôle RDP le plus récent enregistré sur le système (de `MsRdpClient14` jusqu'à `MsRdpClient6`). Chaque version est réellement créée et vérifiée : si elle ne fonctionne pas, elle est écartée et le programme passe à la précédente. La version utilisée est visible dans le menu **Dati connessione...** et dans le journal.

2.2 Fichiers à distribuer

Le programme ne nécessite pas d'installation : il suffit de le copier dans un dossier (par exemple `C:\Albatros\CompiledPrograms\`). Le projet produit deux versions :

Dossier de compilation	Contenu à copier
`bin\Release\AlbatrosRDP_Secure\`	Version protégée avec .NET Reactor. Les bibliothèques `Interop.MSTSCLib.dll`, `AxInterop.MSTSCLib.dll` et `Newtonsoft.Json.dll` sont incorporées : le seul fichier `AlbatrosRDP.exe` suffit. C'est la version conseillée pour la distribution.
`bin\Release\`	Version non protégée : copiez `AlbatrosRDP.exe`, `AlbatrosRDP.exe.config` et les trois DLL énumérées ci-dessus.

2.3 Fichiers et dossiers utilisés par le programme

Chemin	Utilisation
`C:\ProgramData\Albatros\Common\CronologRDP.txt`	Historique des connexions (JSON), commun à tous les utilisateurs de l'ordinateur.
`%LOCALAPPDATA%\Albatros\AlbatrosRDP\AlbatrosRDP.log`	Journal de diagnostic de l'utilisateur actuel ; la copie précédente est `AlbatrosRDP.1.log`.
`CronologRDP.txt.corrupt-<data>.bak`	Copie de sécurité de l'historique, créée uniquement si le fichier s'avère illisible.

> **Plusieurs utilisateurs sur le même ordinateur.** Avec les autorisations par défaut de ProgramData, le fichier d'historique créé par un utilisateur n'est pas modifiable par les autres : pour eux, l'historique ne se met pas à jour. Si nécessaire, un administrateur peut accorder l'autorisation de modification au groupe Utilisateurs avec : `icacls "C:\ProgramData\Albatros\Common" /grant *S-1-5-32-545:(OI)(CI)M`

3. Démarrage rapide

1. Lancez `AlbatrosRDP.exe` sans paramètres : la fenêtre de connexion s'ouvre.
2. Renseignez **Computer** (nom ou adresse du serveur), **Porta**, **Nome utente**, éventuellement **Dominio** et **Note**, puis la **Password**. Pour un serveur déjà utilisé, il suffit de le choisir dans la **Cronologia** (historique) et de saisir le mot de passe.
3. Appuyez sur **Connetti** (Se connecter) ou sur Entrée.
4. Le programme vérifie que le serveur est joignable et ouvre la session en plein écran. Si Windows demande les informations d'identification (NLA), saisissez-les dans la fenêtre du système.
5. La barre d'état apparaît en haut au centre : verte lorsque la session est active.
6. Pour le menu, appuyez sur **Ctrl+F11** (ou faites un clic droit sur la barre d'état).
7. Pour terminer, choisissez **Disconnetti & Exit** dans le menu, ou le **X** rouge de la barre, puis confirmez.

4. La fenêtre de connexion

Elle s'ouvre lorsque le programme démarre sans paramètres valides en ligne de commande. Elle rappelle le style de Connexion Bureau à distance de Windows.

> **Langue des libellés.** La fenêtre est traduite en anglais, italien, français et roumain, mais dans la version actuelle la langue est forcée en **anglais**. Le tableau indique aussi le libellé anglais qui apparaît à l'écran.

4.1 Champs et boutons

Champ	Libellé à l'écran	Description
Cronologia	History	Liste des dernières connexions, au format `server:porta {utente}` ; on peut seulement sélectionner, pas saisir. La première entrée, -- Nuova connessione --, vide les champs. À l'ouverture, la connexion la plus récente est sélectionnée.
✖ (à côté de l'historique)	—	Supprime de l'historique l'entrée sélectionnée, après confirmation.
Computer	Computer	Nom d'hôte, adresse IPv4 ou IPv6. Accepte aussi `host:porta` et `[IPv6]:porta` : le port indiqué ici est prioritaire sur le champ Porta. Une adresse IPv6 sans crochets est interprétée sans port.
Porta	Port	Chiffres uniquement, de 1 à 65535. S'il est vide, 3389 est utilisé.
Nome utente	User name	Utilisateur de la session à distance.
Dominio	Domain	Domaine de l'utilisateur (facultatif).
Note	Notes	Texte libre affiché dans la barre d'état, dans le titre de la fenêtre et en tête du menu. Il est enregistré dans l'historique.
Password	Password	Mot de passe de l'utilisateur distant. Il n'est jamais enregistré. S'il est laissé vide, Windows le demandera au moment de la connexion.
Mostra password	Show password	Affiche en clair le mot de passe saisi.
Barra di stato personalizzata	Customized Status Bar	Cochée (par défaut) : barre d'état d'AlbatrosRDP. Décochée : barre native de Microsoft (chapitre 8). Le choix est mémorisé pour chaque entrée de l'historique.
Connetti	Connect	Lance la connexion (touche Entrée).
Annulla	Cancel	Ferme le programme sans se connecter (touche Échap).

Si vous choisissez une entrée de l'historique, le curseur va directement sur le mot de passe ; sinon, sur le champ Computer. En bas à gauche figurent le copyright et la version.

4.2 Contrôles avant la connexion

- Computer vide : "Specificare l'indirizzo del computer."
- Port non valide dans le champ Computer (ex. `server:99999`) : "Porta non valida nel campo Computer: indicare un numero compreso tra 1 e 65535 (es. server:3389)."
- Port non valide dans le champ Porta : "Porta non valida: indicare un numero compreso tra 1 e 65535."

4.3 Fonctionnement de l'historique

- Une entrée est identifiée par **Serveur + Port + Nom d'utilisateur + Domaine**, sans distinction entre majuscules et minuscules.

- La note et le choix de la barre suivent l'entrée mais ne l'identifient pas : c'est toujours la dernière valeur utilisée qui s'applique.
- Une connexion déjà présente est déplacée en fin de liste, c'est-à-dire qu'elle devient la plus récente.
- Au maximum **20** entrées sont conservées : au-delà de ce nombre, les plus anciennes sont supprimées.
- L'enregistrement a lieu lorsque vous appuyez sur Connetti. Il est atomique et protégé par un verrou entre processus : deux instances ouvertes en même temps n'effacent pas mutuellement leurs entrées.
- Le mot de passe n'est jamais écrit dans le fichier.

5. La session à distance

5.1 Ouverture de la session

1. La fenêtre passe en **plein écran** sur le moniteur actuel, y compris la zone de la barre des tâches. Le titre de la fenêtre est la note, ou bien « AlbatrosRDP ».
2. Le bureau à distance est demandé avec la résolution du moniteur. Un seul moniteur est utilisé.
3. Vérification de l'accessibilité : une connexion TCP de test vers le serveur et le port, avec un délai d'expiration de 2,5 secondes (résolution DNS comprise ; adresses IPv4 et IPv6 essayées en parallèle). La barre affiche "Verifica raggiungibilità server:porta...".
4. Si le serveur ne répond pas, le message suivant apparaît : "Impossibile raggiungere il server ... (tunnel SSH non attivo oppure rete non disponibile). Riprovare?". **Sì** (Oui) répète la vérification, **No** (Non) ferme le programme.
5. Si le serveur répond, la connexion RDP démarre ("Connessione in corso..."). Si le serveur demande les informations d'identification, Windows affiche sa propre fenêtre : pendant cette phase, AlbatrosRDP suspend la gestion du clavier et ne reste pas au premier plan, pour ne pas la masquer.
6. Une fois la connexion établie, la barre devient verte et affiche `--> server:porta`.

Si la session n'atteint jamais l'état connecté (informations d'identification annulées ou erronées, réseau absent), le programme ne réessaie pas indéfiniment : il affiche "La connessione RDP non è stata stabilita (Credenziali mancanti/annullate oppure errore di rete). L'applicazione verrà chiusa." et se termine.

5.2 Comportement en plein écran

- La fenêtre reste au-dessus des autres **uniquement** lorsqu'elle est au premier plan : avec Alt+Tab ou un clic sur une autre application, vous passez normalement à d'autres programmes.
- La barre d'état n'est visible que lorsqu'AlbatrosRDP est l'application active.
- Le contenu distant s'adapte à la fenêtre (smart sizing) : en mode fenêtre réduite, le bureau à distance est rétréci proportionnellement, sans barres de défilement.

6. La barre d'état personnalisée

C'est la barre arrondie qui apparaît en haut au centre de l'écran en mode plein écran, lorsque l'option **Barra di stato personalizzata** est activée.

6.1 Texte et couleurs

Le texte se compose de : la note (si elle existe), le rappel de la touche du menu, l'état. Exemple : `Server ufficio - (Ctrl+F11 menu) - --> 192.168.1.10:3389.`

Couleurs	Signification
Fond vert, texte jaune	Session connectée et serveur joignable.
Fond jaune, texte rouge	Tout autre état : vérification en cours, connexion en cours, connexion perdue, erreur.

6.2 Boutons

Bouton	Action
─ (jaune)	Réduit la fenêtre.
□ (jaune)	Bascule entre plein écran et fenêtre, et inversement.
X (rouge)	Comme Disconnetti & Exit : demande confirmation si la session est connectée, puis ferme.

6.3 Utilisation avec la souris

- **Glisser** avec le bouton gauche : la barre peut être déplacée n'importe où sur l'écran et reste à la position choisie.
- **Bouton droit** : ouvre le menu rapide.
- **Double-clic** : masque la barre (comme la commande de menu Barra di stato).

6.4 Barre masquée et apparition automatique

Une barre masquée manuellement (double-clic ou menu) peut réapparaître de trois façons :

- depuis le menu rapide (Ctrl+F11), commande **Barra di stato** ;
- en amenant la souris à moins de **10 pixels du bord supérieur** de l'écran, si l'option **Mostra barra al passaggio mouse in alto** est activée (activée par défaut). Dans ce cas, la barre se masque à nouveau lorsque la souris s'éloigne de plus de 20 pixels en dessous d'elle ;
- en quittant puis en rétablissant le mode plein écran, ou en restaurant la fenêtre après une réduction.

7. Le menu rapide

7.1 Comment l'ouvrir

- **Ctrl+F11** : fonctionne uniquement avec la barre personnalisée. La combinaison est interceptée et n'arrive pas à l'ordinateur distant. Lorsque la barre native est active, elle est désactivée et transmise à la session à distance.
- **Clic droit sur la barre d'état** (en plein écran).
- **Clic droit sur la barre de titre** (en mode fenêtré), à la place du menu système de Windows.

Le menu se ferme par un clic à l'extérieur, avec la commande **Chiudi tendina** ou avec **Échap**. Tant que le menu est ouvert, la touche Échap n'est pas envoyée à la session à distance.

7.2 Commandes du menu

Commande	Fonction
Note (en gras)	Présente uniquement s'il existe une note. Un clic ouvre la fenêtre "Nota di connessione" pour la modifier. La nouvelle note s'applique à la session en cours et met immédiatement à jour la barre et le titre ; elle n'est pas enregistrée dans l'historique.
Schermo ridotto / Schermo intero	Bascule du mode plein écran vers la fenêtre et inversement (chapitre 9).
Riduci a icona	Réduit la fenêtre de la session.
Barra di stato	Affiche ou masque la barre d'état. Disponible uniquement en plein écran.
Mostra barra al passaggio mouse in alto	Active ou désactive l'apparition automatique de la barre (section 6.4).
Barra RDP nativa	Passe à la barre de connexion native de Microsoft, ou revient à la barre personnalisée (chapitre 8).
Dati connessione...	Affiche la note, les infos (paramètre `-info`), le serveur, le port, l'utilisateur, le domaine, l'état, le contrôle RDP utilisé avec sa version, le copyright et la version du programme.
Riconnetti	Ferme la session si elle est encore ouverte (attente maximale de 5 secondes) et la rouvre. Utile si la session ne répond pas.
Disconnetti & Exit	Demande "Disconnettere la sessione RDP e chiudere l'applicazione?" (par défaut : No) et, si vous confirmez, déconnecte et ferme.
Chiudi tendina	Ferme le menu sans rien faire.

8. La barre de connexion native Microsoft

Au lieu de la barre d'AlbatrosRDP, vous pouvez utiliser la barre de connexion standard de Microsoft, celle de `mstsc.exe`.

8.1 Activation

- Avant la connexion : décochez **Barra di stato personalizzata** dans la fenêtre de connexion. Le choix reste mémorisé pour cette entrée de l'historique.
- Pendant la session : commande de menu **Barra RDP nativa**.

Environ une seconde après l'établissement de la connexion, le contrôle RDP passe à son propre plein écran et affiche la barre Microsoft, épinglée et avec les boutons Réduire, Restaurer et Épingler.

8.2 Différences de comportement

- **Ctrl+F11** est désactivé : la combinaison arrive à l'ordinateur distant.
- La barre personnalisée et son apparition automatique sont désactivées.
- **Réduire** sur la barre Microsoft réduit toute la session ; elle se rouvre depuis l'icône de la barre des tâches.
- **Restaurer** sur la barre Microsoft fait passer AlbatrosRDP en **mode fenêtré** et ne revient pas tout seul au plein écran. À partir de là, un clic droit sur la barre de titre ouvre le menu rapide : **Schermo intero** revient au plein écran natif, tandis qu'en décochant **Barra RDP nativa** on revient à la barre personnalisée.
- **X** sur la barre Microsoft ferme la session. La question "La sessione RDP è stata disconnessa. Riconnettersi al server? (No = chiude l'applicazione)" apparaît.

9. Le mode fenêtré

Avec **Schermo ridotto** (menu) ou avec le bouton □ de la barre, la session passe dans une fenêtre Windows normale, redimensionnable.

- L'état de la connexion (avec la note et le rappel du menu) est affiché dans le **titre de la fenêtre**, à la place de la barre d'état.
- Le bureau à distance conserve la résolution avec laquelle il a été ouvert et est rétréci pour tenir dans la fenêtre.
- Le **clic droit sur la barre de titre** ouvre le menu rapide ; Ctrl+F11 continue également à fonctionner (avec la barre personnalisée).
- À gauche des boutons système (réduire, agrandir, fermer) apparaît un bouton supplémentaire **Schermo intero** qui remet la session en plein écran.

10. Interruptions, reconnexion et erreurs

10.1 Serveur devenu injoignable pendant la session

Tant que la session est connectée, le programme tente toutes les 2 secondes d'ouvrir une connexion TCP vers le port RDP du serveur (délai d'expiration de 1,5 seconde). Si le test échoue, la barre devient jaune avec "Connessione persa su server:porta", même si le contrôle RDP n'a pas encore détecté la coupure. Elle redevient verte d'elle-même lorsque le serveur répond de nouveau. C'est le cas typique d'un tunnel SSH tombé.

10.2 Reconnexion automatique

En plus de la reconnexion automatique interne du contrôle RDP, si la session est déconnectée après avoir été connectée au moins une fois, AlbatrosRDP :

1. tente de se reconnecter au maximum toutes les **5 secondes**, chaque fois précédé d'une vérification TCP rapide (1 seconde) ;
2. après **3 tentatives** consécutives échouées, demande : "La riconnessione automatica non riesce (credenziali mancanti/annullate oppure server non disponibile). Continuare a riprovare?". **Sì** reprend les tentatives, **No** ferme le programme.

10.3 Watchdog (application bloquée)

Un contrôle indépendant vérifie que l'interface répond. Si elle reste bloquée pendant plus de **15 secondes** (par exemple à cause d'une interruption réseau pendant l'authentification RDP), le message "L'applicazione non risponde da diversi secondi... Vuoi forzare la chiusura dell'applicazione?" apparaît au-dessus de toutes les autres fenêtres. **Sì** termine le programme, **No** continue d'attendre. Le contrôle est suspendu tant que des boîtes de dialogue du programme sont ouvertes.

10.4 Erreurs inattendues

- **Contrôle RDP non disponible** ou ne fonctionnant pas au démarrage : "Impossibile avviare la connessione RDP:" apparaît avec le détail de l'erreur, puis le programme se ferme.
- **Exception non gérée** : le message "AlbatrosRDP - Errore" indique l'erreur et demande "Continuare a usare l'applicazione?". **Sì** permet de continuer sans perdre la session, **No** ferme. L'erreur est toujours enregistrée dans le journal.

10.5 Fermeture

- Toute fermeture manuelle avec une session connectée (menu, X de la barre, X de la fenêtre, Alt+F4, barre des tâches) demande confirmation. En répondant No, vous revenez exactement à la situation précédente.
- À la fermeture, le programme déconnecte la session et attend au maximum 1 seconde que le contrôle RDP la ferme.
- Lorsque la fermeture part d'une boîte de dialogue d'erreur, un arrêt de sécurité est prévu : si le nettoyage se bloque, le processus est quand même terminé après 8 secondes.

11. Lancement depuis la ligne de commande

AlbatrosRDP peut ouvrir une connexion directement, sans afficher la fenêtre de connexion. Les paramètres peuvent être transmis de trois façons : **en clair**, **chiffrés** dans une chaîne unique, ou dans un **fichier** (en clair ou chiffré).

11.1 Paramètres de connexion

Paramètre	Obligatoire	Signification
`-ip=`	Oui	Nom ou adresse du serveur. Accepte aussi `host:porta` et `[IPv6]:porta`.
`-port=`	Non	Port TCP (1-65535). S'il est absent ou non valide : 3389.
`-user=`	Non	Nom d'utilisateur.
`-domain=`	Non	Domaine.
`-pwd=`	Non	Mot de passe de l'utilisateur distant. S'il est absent, Windows le demande.
`-nota=`	Non	Note affichée dans la barre, le titre et le menu.
`-info=`	Non	Information supplémentaire affichée dans Dati connessione...

Paramètre	Signification
`-enc=`	Chaîne chiffrée (Base64) contenant les paramètres du tableau précédent.
`-file=`	Chemin d'un fichier contenant les paramètres, en clair ou chiffrés.
`-cryptpwd=`	Mot de passe de déchiffrement de `-enc` ou `-file`. La valeur spéciale `pipe` indique que le mot de passe arrive via named pipe (section 11.6).
`-local=true`	Purement informatif : indique que le contenu a été lié à l'ordinateur. Il n'est pas pris en compte à la lecture.

Règles générales :

- Les noms des paramètres ne distinguent pas les majuscules et les minuscules ; le tiret initial est facultatif (`ip=` équivaut à `-ip=`).
- Les valeurs contenant des espaces doivent être placées entre guillemets doubles, de préférence l'argument entier : `"-nota=Server ufficio"`.
- Ordre de priorité : si `-file` est présent, le fichier est utilisé ; sinon, si `-enc` est présent, la chaîne chiffrée ; sinon les paramètres individuels.
- Les paramètres inconnus sont ignorés.
- Si `-ip` manque (ou si le fichier indiqué n'existe pas), le programme se comporte comme s'il n'avait pas de paramètres et ouvre la fenêtre de connexion.
- La connexion lancée depuis la ligne de commande utilise la barre personnalisée et **n'est pas** ajoutée à l'historique.

11.2 Paramètres en clair

```
AlbatrosRDP.exe -ip=192.168.1.10 -port=3389 -user=Administrator "-nota=Server ufficio"
```

> **Attention.** Un mot de passe transmis en clair avec `-pwd=` est visible par quiconque peut lire la ligne de commande des processus (Gestionnaire des tâches, Process Explorer, WMI). Pour transmettre le mot de passe, utilisez la forme chiffrée, de préférence avec la pipe.

11.3 Paramètres chiffrés

```
AlbatrosRDP.exe "-enc=<stringa Base64>" "-cryptpwd=<chiave>"
```

La chaîne `-enc` se génère avec les fonctions de programmation décrites au chapitre 12 (`BuildCommandLineArgs`). Le programme ne dispose pas d'une fonction interactive pour la créer.

11.4 Paramètres dans un fichier

```
AlbatrosRDP.exe "-file=C:\Config\Clienti\Cliente1.rdpdat"
AlbatrosRDP.exe "-file=C:\Config\Clienti\Cliente1.rdpdat" "-cryptpwd=<chiave>"
```

Le fichier (UTF-8) peut contenir les paramètres **en clair**, éventuellement sur plusieurs lignes et avec ou sans tiret, ou bien une chaîne **chiffrée**. Le programme reconnaît seul le format : si le contenu est en clair, l'éventuel `-cryptpwd` est ignoré. Exemple de fichier en clair écrit à la main :

```
-ip=192.168.1.10
-port=3389
-user=Administrator
"-nota=Server ufficio"
"-info=Contratto assistenza n. 42"
```

Un fichier chiffré se crée avec `BuildCommandLineArgs` en indiquant le chemin (chapitre 12). Si le fichier existe déjà, une confirmation est demandée avant de l'écraser.

11.5 Mot de passe de déchiffrement manquant ou erroné

Si le contenu est chiffré et que `-cryptpwd` manque ou est erroné, la fenêtre **Password richiesta** apparaît : "I parametri di connessione sono protetti da password. Tentativo N di 3." (précédé de "Password errata." après une erreur).

- Vous disposez de **3 tentatives**.
- Avec **Annulla**, ou une fois les tentatives épuisées, le programme **se termine** sans ouvrir la fenêtre de connexion.
- Chaque déchiffrement est vérifié (le résultat doit contenir au moins `ip`) : un mot de passe erroné ne peut pas être pris pour un bon.

11.6 Mot de passe via named pipe

Avec `-cryptpwd=pipe`, le mot de passe réel n'apparaît jamais dans la ligne de commande, pas même un instant. Le programme qui lance AlbatrosRDP le lui remet à travers une named pipe locale :

- nom de la pipe : `\\.\pipe\AlbatrosRDP_Secret_<PID>`, où PID est l'identifiant du processus AlbatrosRDP qui vient d'être lancé ;
- la pipe est créée par le programme appelant, n'est accessible qu'à l'utilisateur Windows actuel et n'accepte qu'une seule connexion ;
- le secret n'est remis que si c'est bien le processus attendu qui se connecte (vérification du PID du client) ;
- le texte transite en UTF-8 (un éventuel BOM est toléré) ;
- AlbatrosRDP attend au maximum **5 secondes** : s'il ne reçoit rien, il demande le mot de passe avec la fenêtre de la section 11.5.

Le moyen le plus simple d'utiliser la pipe est la fonction `StartProcessWithEncryptedArgsAndPipePasswordWait` (chapitre 12), qui fait tout en un seul appel.

11.7 Liaison à un seul ordinateur

Au moment de la création (`machineBound:=True`), il est possible de lier le contenu chiffré à l'ordinateur actuel. Dans ce cas, la clé de chiffrement effective est formée de l'ID matériel de l'ordinateur suivi du mot de passe. L'ID matériel se compose de :

- numéro de série de la carte mère ;
- identifiant du processeur ;
- numéro de série du premier disque physique.

À la lecture, il n'est rien nécessaire d'indiquer : le programme essaie d'abord le mot de passe tel quel (contenu valable sur tous les ordinateurs), puis la combinaison avec l'ID matériel de l'ordinateur local, y compris les variantes dues à l'ordre non garanti des disques (par exemple une clé USB insérée).

> **Attention.** Un contenu lié devient illisible si vous remplacez la carte mère, le processeur ou le disque système, et bien sûr sur tout autre ordinateur : dans ce cas, il doit être régénéré.

12. Intégration depuis d'autres programmes

Les classes du programme peuvent être utilisées par une autre application VB.NET, en ajoutant une référence à `AlbatrosRDP.exe` (version non protégée) ou en incluant les fichiers source. Le projet d'exemple **Test_Lancio_pipe** (application console) montre le lancement avec mot de passe via pipe.

12.1 La classe RdpConnectionParams

Propriété	Type	Description
`Ip`	String	Serveur (obligatoire).
`Port`	Integer	Port ; 0 = par défaut (3389).
`User`, `Domain`	String	Utilisateur et domaine.
`Password`	String	Mot de passe de l'utilisateur distant.
`Nota`, `Info`	String	Note et information supplémentaire.
`IsValid`	Boolean	True si `Ip` est renseigné.
`Clone()`	Fonction	Renvoie une copie.

12.2 La classe RdpCommandLineManager

Méthode (Shared)	Description
`BuildCommandLineArgs(prms, [encryptionPassword], [filePath], [machineBound])`	Construit les arguments. Sans mot de passe : en clair. Avec mot de passe : `-enc` + `-cryptpwd`. Avec `filePath` : écrit le fichier (en clair ou chiffré, crée le dossier, demande confirmation s'il existe) et renvoie `-file` [+ `-cryptpwd`]. Les arguments sont déjà mis entre guillemets selon les règles de Windows.
`BuildCommandLineArgsFromFile(filePath, [encryptionPassword])`	Arguments pour un fichier déjà existant ; si le mot de passe est indiqué, vérifie d'abord que le fichier se déchiffre. Lève une exception si le fichier n'existe pas ou si le mot de passe est erroné.
`StartProcessWithEncryptedArgsAndPipePasswordWait(exePath, prms, encryptionPassword, ByRef passwordDelivered, [machineBound], [pipeTimeoutMs=5000])`	Lance AlbatrosRDP avec `-cryptpwd=pipe`, remet le mot de passe via la pipe et attend la remise. `passwordDelivered` indique le résultat. Adapté aux lanceurs qui se terminent immédiatement.
`StartProcessWithEncryptedArgsAndPipePassword(exePath, prms, encryptionPassword, [machineBound], [pipeTimeoutMs=5000])`	Comme ci-dessus, mais la remise a lieu en arrière-plan et la méthode rend la main immédiatement. Si l'appelant se termine avant la remise, le mot de passe n'arrive pas.
`ParseCommandLineArgs(args, [ByRef userAborted])`	Interprète les arguments reçus (avec demande interactive du mot de passe si nécessaire).
`ReadParamsFromFile(filePath, [cryptPwd])`	Lit un fichier de paramètres sans boîtes de dialogue ; exception si le mot de passe est erroné.
`EncryptString(testo, password)` / `DecryptToOriginalString(blob, password)`	Chiffrement et déchiffrement de base, sans liaison matérielle.
`GetMachineHardwareId()`	ID matériel de l'ordinateur actuel.

Exemple : lancement avec mot de passe via pipe depuis un lanceur (la clé est contenue dans une variable, jamais écrite dans le code) :

```
Dim prms As New RdpConnectionParams With {
    .Ip = "192.168.1.10", .Port = 3389,
    .User = "Administrator", .Nota = "Server ufficio"}

Dim consegnata As Boolean = False
RdpCommandLineManager.StartProcessWithEncryptedArgsAndPipePasswordWait(
    "C:\Albatros\CompiledPrograms\AlbatrosRDP.exe",
    prms, chiave, consegnata)
```

Exemple : création d'un fichier chiffré lié à l'ordinateur :

```
Dim argomenti As String = RdpCommandLineManager.BuildCommandLineArgs(
    prms, encryptionPassword:=chiave,
    filePath:="C:\Config\Clienti\Cliente1.rdpdat", machineBound:=True)
' -> "-file=C:\Config\Clienti\Cliente1.rdpdat" "-cryptpwd=..." "-local=true"
```

12.3 La classe SecretPipeTransfer

Méthode (Shared)	Description
`SendSecretToChildProcessAndWait(processo, segreto, [timeoutMs])`	Côté appelant : crée la pipe pour le PID du processus enfant et attend la remise. Renvoie True si le secret a été remis.
`SendSecretToChildProcess(processo, segreto, [timeoutMs])`	Comme ci-dessus, en arrière-plan.
`ReceiveSecretForCurrentProcess([timeoutMs])`	Côté AlbatrosRDP : lit le secret depuis la pipe de son propre PID.
`ReadSecretFromPipe(nomePipe, [timeoutMs])`	Lecture depuis une pipe au nom explicite.
`WaitSeconds(n)` / `WaitMilliSeconds(n)`	Attente qui maintient l'interface réactive.

12.4 Format du chiffrement

Élément	Valeur
Algorithme	AES-256, mode CBC, remplissage PKCS7
Dérivation de la clé	PBKDF2-HMAC-SHA1, 50 000 itérations, sel aléatoire de 16 octets
Format	Base64 de : sel (16 octets) + IV (16 octets) + données chiffrées
Contenu en clair	Paramètres au format `"-ip=..." "-user=..."` (UTF-8)
Compatibilité	Identique aux versions précédentes : les chaînes et fichiers créés auparavant restent lisibles, et inversement

12.5 Personnalisations par code

Élément	Description
`FrmRDP.New([nativeConnectionBar], [SafeMode])`	Session avec fenêtre de connexion.
`FrmRDP.New(server, port, domain, userName, password, [nativeConnectionBar], [SafeMode])`	Session directe, sans fenêtre de connexion.
`SafeMode`	Si True, recherche d'abord le contrôle RDP générique et limite le choix aux versions jusqu'à la 11.
`FrmRDP.MenuHotkey`	Combinaison du menu rapide (par défaut `Keys.Control Or Keys.F11`).

Élément	Description
`FrmRDP.ConnectionNote` / `ConnectionInfo`	Note et infos de la session.
`FrmRDP.ShowNativeConnectionBar`	Barre native oui/non ; à définir avant `ShowDialog()`.
`Module1.PercorsoStorico`	Chemin du fichier d'historique.
`Module1.MaxCronologRDP`	Nombre maximal d'entrées dans l'historique (20 par défaut).

13. Paramètres RDP appliqués

À l'ouverture de chaque session, les paramètres suivants sont appliqués, au format des fichiers `.rdp`. Ils sont définis dans le code (chaîne `rdpSettingsString` de FrmRDP) ; il n'y a pas de fichier de configuration externe.

Paramètre	Effet
`session bpp:i:32`	Couleurs 32 bits.
`compression:i:1`	Compression des données activée.
`disable wallpaper:i:1`	Arrière-plan du bureau à distance non affiché (moins de bande passante).
`keyboardhook:i:2`	Combinaisons de touches Windows envoyées à l'ordinateur distant uniquement en plein écran (valeur par défaut).
`audiomode:i:0`	Audio distant lu sur l'ordinateur local.
`audiocapturemode:i:1`	Microphone local disponible dans la session à distance.
`redirectprinters:i:1`	Imprimantes locales disponibles dans la session.
`redirectsmartcards:i:1`	Cartes à puce locales disponibles.
`redirectclipboard:i:1`	Presse-papiers partagé entre local et distant.
`drivestoredirect:s:*`	Tous les lecteurs locaux visibles dans la session à distance.
`negotiate security layer:i:1`	Négociation automatique du protocole de sécurité le plus robuste.
`screen mode id`, `use multimon`	Ignorés : le plein écran est géré par le programme, sur un seul moniteur.

Juste après, le programme définit en outre :

- **reconnexion automatique** du contrôle RDP activée (remplace `autoreconnection enabled:i:0` de la chaîne) ;
- **niveau d'authentification 0** et avertissements de certificat ignorés (remplace `authentication level:i:2`) : le certificat du serveur n'est pas vérifié et aucun avertissement n'apparaît ;
- **CredSSP** activé (nécessaire pour l'authentification NLA) ;
- **délai d'expiration** de connexion : 8 secondes au total, 5 par tentative.

Le programme sait aussi interpréter d'autres clés `.rdp` (par exemple `alternate shell` et `shell working directory` pour lancer un seul programme à la place du bureau, `connection type`, `networkautodetect`, `redirectcomports` et les paramètres de la passerelle RD `gatewayhostname`, `gatewayusagemethod` et similaires) : pour les utiliser, il faut modifier la chaîne dans le code et recompiler le programme.

14. Sécurité et confidentialité

- Le **mot de passe** de l'utilisateur distant n'est jamais enregistré sur disque : ni dans l'historique, ni dans le journal. Après sa remise au contrôle RDP, les copies en mémoire sont effacées.
- Le **journal** enregistre uniquement le mode de lancement, les états de la connexion et les erreurs : jamais de mots de passe, de clés ni de paramètres.
- Le **chiffrement** utilise AES-256 avec une clé dérivée par PBKDF2. Les tampons contenant des données sensibles sont mis à zéro après usage.
- La **pipe** n'est accessible qu'à l'utilisateur actuel, ne remet le secret qu'au processus attendu et est à usage unique.
- Le **certificat du serveur n'est pas vérifié** (section 13). La protection contre les interceptions repose donc sur le canal : réseau de confiance, VPN ou tunnel SSH. Évaluez s'il convient de conserver ce paramètre.
- Un mot de passe transmis en clair avec `-pwd=` est visible dans la liste des processus (section 11.2).
- La vérification d'accessibilité pendant la session ouvre une connexion TCP vers le port RDP toutes les 2 secondes : sur le serveur, cela génère des événements dans le journal RDP (RdpCoreTS) et un peu de trafic dans le tunnel.

15. Journal de diagnostic

Le journal se trouve dans `%LOCALAPPDATA%\Albatros\AlbatrosRDP\AlbatrosRDP.log`. Lorsqu'il dépasse 1 Mo, il est renommé en `AlbatrosRDP.1.log` (en remplaçant la copie précédente) et un nouveau fichier est commencé. Chaque ligne a le format :

```
2026-10-11 14:22:05.123 [4812] INFO  Stato RDP: connesso
```

c'est-à-dire la date et l'heure, le PID du processus, le niveau (INFO, WARN, ERROR) et le message. Sont enregistrés :

- le démarrage (version et nombre d'arguments) et la fermeture de l'application ;
- le mode de la ligne de commande (en clair, chiffré, fichier) et le résultat (paramètres valides, non valides, mot de passe annulé ou erroné) ;
- le serveur, le port, le contrôle RDP utilisé et le type de barre ;
- les changements d'état de la session, avec le code étendu du motif de déconnexion ;
- les tentatives de reconnexion échouées, les interventions du watchdog, les erreurs et les exceptions non gérées ;
- la fermeture de la session avec son motif.

16. Dépannage

Problème	Que faire
Au démarrage apparaît "Impossibile avviare la connessione RDP"	Le contrôle RDP de Windows est absent ou ne fonctionne pas. Vérifiez que Connexion Bureau à distance (`mstsc.exe`) fonctionne et consultez le journal.
"Impossibile raggiungere il server"	Contrôlez le tunnel SSH, le VPN, le pare-feu, l'adresse et le port. Avec un tunnel local, vérifiez qu'il est actif avant de vous connecter.
Le programme se ferme avec "La connessione RDP non è stata stabilita"	Informations d'identification annulées ou erronées, ou réseau absent pendant l'authentification. Réessayez en contrôlant l'utilisateur, le domaine et le mot de passe.
Barre jaune avec "Connessione persa su ..."	Le serveur ne répond plus sur le port RDP : typiquement, le tunnel est tombé. La barre redevient verte d'elle-même au rétablissement.
Ctrl+F11 n'ouvre pas le menu	La barre native Microsoft est active (Ctrl+F11 désactivé). Utilisez le clic droit sur la barre de titre en mode fenêtré.
La barre d'état n'est pas visible	Elle a été masquée (double-clic ou menu) : amenez la souris sur le bord supérieur ou utilisez Ctrl+F11 > Barra di stato. La barre n'est visible que si AlbatrosRDP est l'application active.
Lancement avec `-cryptpwd=pipe` et demande du mot de passe	Le mot de passe n'est pas arrivé dans les 5 secondes. Le lanceur s'est probablement terminé avant la remise : utilisez `StartProcessWithEncryptedArgsAndPipePasswordWait`.
Mot de passe correct mais "Password errata" avec un contenu lié	Le matériel a changé (carte mère, processeur, disque) ou vous utilisez un autre ordinateur : régénérez le contenu chiffré.
Avec `-ip` présent, la fenêtre de connexion s'ouvre quand même	Le paramètre n'a pas été reconnu : contrôlez l'usage des guillemets doubles et, avec `-file`, que le fichier existe.
L'historique ne se met pas à jour	Les autorisations d'écriture sur le fichier dans ProgramData manquent (section 2.3).
L'historique a disparu	Le fichier était illisible : une copie `.corrupt-<data>.bak` en a été enregistrée dans le même dossier.
L'arrière-plan du bureau à distance n'apparaît pas (couleur unie)	C'est voulu (`disable wallpaper:i:1`, chapitre 13).
"L'applicazione non risponde da diversi secondi"	Le programme est bloqué depuis plus de 15 secondes, généralement à cause d'une coupure réseau pendant l'authentification. Sì ferme le programme, No continue d'attendre.

Annexe A. Messages du programme

Message	Signification et réponses
Verifica raggiungibilità server:porta...	Test TCP en cours avant la connexion.
Connessione in corso...	Le contrôle RDP est en train d'établir la session.
--> server:porta (barre verte)	Session connectée.
Connessione persa su server:porta	Le serveur ne répond pas au test TCP périodique.
Connessione RDP non attiva	Session déconnectée ; reconnexion automatique en cours.
Riconnessione in corso... / Disconnessione in corso...	Effet de la commande Riconnetti ou de la fermeture.
Errore di connessione / Errore di riconnessione	Le contrôle RDP a refusé la demande de connexion.
Impossibile raggiungere il server ... Riprovare?	Sì = nouvelle vérification ; No = fermeture.
La connessione RDP non è stata stabilita ... L'applicazione verrà chiusa.	Première connexion jamais réussie (informations d'identification ou réseau).
La riconnessione automatica non riesce ... Continuare a riprovare?	Après 3 tentatives échouées. Sì = continuer ; No = fermeture.
La sessione RDP è stata disconnessa. Riconnettersi al server?	Session fermée par la barre native ou par le serveur. Sì = reconnexion ; No = fermeture.
Disconnettere la sessione RDP e chiudere l'applicazione?	Confirmation de fermeture. Par défaut : No.
L'applicazione non risponde da diversi secondi ...	Watchdog. Sì = fermeture forcée ; No = attente.
AlbatrosRDP - Errore ... Continuare a usare l'applicazione?	Exception non gérée. Sì = continuer ; No = fermeture.
Password richiesta - Tentativo N di 3	Paramètres chiffrés : saisissez le mot de passe de déchiffrement.
Il file ... esiste già. Sovrascrivere?	Création d'un fichier de paramètres par code.

Annexe B. Référence rapide

B.1 Touches et souris

Commande	Effet
Ctrl+F11	Ouvre le menu rapide (barre personnalisée uniquement).
Échap avec le menu ouvert	Ferme le menu.
Clic droit sur la barre d'état	Ouvre le menu rapide.
Clic droit sur la barre de titre	Ouvre le menu rapide (mode fenêtré).
Double-clic sur la barre d'état	Masque la barre.
Souris sur le bord supérieur	Fait réapparaître la barre masquée.
Glisser la barre d'état	La déplace.
Entrée / Échap dans la fenêtre de connexion	Connetti / Annulla.

B.2 Ligne de commande

```
AlbatrosRDP.exe -ip=<server> [-port=<porta>] [-user=<utente>] [-domain=<dominio>]
                [-pwd=<password>] ["-nota=<testo>"] ["-info=<testo>"]

AlbatrosRDP.exe "-enc=<Base64>" "-cryptpwd=<chiave>|pipe"

AlbatrosRDP.exe "-file=<percorso>" ["-cryptpwd=<chiave>|pipe"]
```

B.3 Valeurs temporelles

Contrôle	Valeur
Vérification d'accessibilité initiale	2,5 s
Vérification pendant la session	toutes les 2 s, délai d'expiration 1,5 s
Intervalle minimal entre les tentatives de reconnexion	5 s
Tentatives avant la question "Continuare a riprovare?"	3
Attente initiale avant de considérer la connexion comme échouée	15 s
Watchdog	15 s de blocage (contrôle toutes les 2 s)
Activation de la barre native après la connexion	1 s
Attente du mot de passe via pipe	5 s
Arrêt de sécurité à la fermeture	8 s

AlbatrosRDP

Client Desktop Remoto

Manuale d'uso e di integrazione

Versione 2.0.162.6127 — ottobre 2026

© Raffaele Romano 2026

Indice

1. Introduzione **57**
1.1 Funzioni principali 57
1.2 Versione documentata 57
2. Requisiti e installazione **58**
2.1 Requisiti 58
2.2 File da distribuire 58
2.3 File e cartelle usati dal programma 58
3. Avvio rapido **59**
4. La finestra di connessione **60**
4.1 Campi e pulsanti 60
4.2 Controlli prima della connessione 60
4.3 Come funziona la cronologia 60
5. La sessione remota **62**
5.1 Apertura della sessione 62
5.2 Comportamento a tutto schermo 62
6. La barra di stato personalizzata **63**
6.1 Testo e colori 63
6.2 Pulsanti 63
6.3 Uso con il mouse 63
6.4 Barra nascosta e comparsa automatica 63
7. Il menu rapido **64**
7.1 Come aprirlo 64
7.2 Voci del menu 64
8. La barra di connessione nativa Microsoft **65**
8.1 Attivazione 65
8.2 Differenze di comportamento 65
9. La modalità finestra **66**
10. Interruzioni, riconnessione ed errori **67**
10.1 Server non più raggiungibile durante la sessione 67
10.2 Riconnessione automatica 67
10.3 Watchdog (applicazione bloccata) 67
10.4 Errori imprevisti 67
10.5 Chiusura 67
11. Avvio da riga di comando **68**
11.1 Parametri di connessione 68
11.2 Parametri in chiaro 68
11.3 Parametri cifrati 68
11.4 Parametri su file 69
11.5 Password di decifratura mancante o errata 69
11.6 Password tramite named pipe 69
11.7 Vincolo al singolo computer 69
12. Integrazione da altri programmi **71**
12.1 La classe RdpConnectionParams 71
12.2 La classe RdpCommandLineManager 71
12.3 La classe SecretPipeTransfer 72
12.4 Formato della cifratura 72
12.5 Personalizzazioni da codice 72
13. Impostazioni RDP applicate **74**
14. Sicurezza e riservatezza **75**
15. Log diagnostico **76**
16. Risoluzione dei problemi **77**
Appendice A. Messaggi del programma **78**
Appendice B. Riferimento rapido **79**

B.1 Tasti e mouse..... 79
B.2 Riga di comando..... 79
B.3 Valori temporali..... 79

1. Introduzione

AlbatrosRDP è un client Desktop Remoto (RDP) per Windows, sviluppato in VB.NET su .NET Framework 4.8. Usa il controllo ActiveX di Microsoft (`mstscax.dll`), cioè lo stesso motore di Connessione Desktop remoto (`mstsc.exe`), e vi aggiunge una serie di funzioni pensate per l'uso quotidiano e per i collegamenti attraverso tunnel SSH.

1.1 Funzioni principali

- Finestra di connessione con **cronologia** delle ultime connessioni (la password non viene mai salvata) e una **nota** libera per ogni connessione.
- Sessione a **tutto schermo** con una **barra di stato flottante**: colorata in base allo stato, trascinabile, a scomparsa.
- In alternativa, la **barra di connessione nativa** di Microsoft.
- **Menu rapido** richiamabile con **Ctrl+F11**, con il tasto destro sulla barra di stato o sulla barra del titolo.
- **Verifica di raggiungibilità** del server prima di connettersi e, ogni 2 secondi, durante la sessione.
- **Riconnessione automatica** quando la sessione cade.
- **Watchdog**: se l'applicazione resta bloccata (per esempio per una caduta di rete durante l'autenticazione) propone la chiusura forzata.
- **Avvio diretto da riga di comando**, con parametri in chiaro, cifrati (AES-256) o letti da file. La password di decifratura si può passare anche tramite named pipe, senza che compaia mai nella riga di comando.
- Vincolo opzionale dei parametri cifrati al **singolo computer** (ID hardware).
- **Log diagnostico** che non contiene mai password, chiavi o parametri.

1.2 Versione documentata

Voce	Valore
Programma	AlbatrosRDP
Versione	2.0.162.6127 (revisione di ottobre 2026)
Piattaforma	.NET Framework 4.8, Windows Forms, VB.NET
Motore RDP	Controllo ActiveX Microsoft RDP (MSTSCLib), versioni da 6 a 14
Autore	© Raffaele Romano 2026

2. Requisiti e installazione

2.1 Requisiti

- Windows con il client Desktop remoto di Microsoft installato (`mstscax.dll`, presente di serie nelle versioni desktop e server di Windows).
- .NET Framework 4.8.
- Accesso di rete al server RDP sulla porta TCP indicata (predefinita **3389**), direttamente o tramite tunnel.

All'avvio della sessione il programma cerca il controllo RDP più recente registrato sul sistema (da `MsRdpClient14` fino a `MsRdpClient6`). Ogni versione viene creata davvero e verificata: se non funziona viene scartata e si passa alla precedente. La versione agganciata è visibile nel menu **Dati connessione...** e nel log.

2.2 File da distribuire

Il programma non ha installazione: basta copiarlo in una cartella (per esempio `C:\Albatros\CompiledPrograms\`). Il progetto produce due versioni:

Cartella di compilazione	Contenuto da copiare
`bin\Release\AlbatrosRDP_Secure\`	Versione protetta con .NET Reactor. Le librerie `Interop.MSTSCLib.dll`, `AxInterop.MSTSCLib.dll` e `Newtonsoft.Json.dll` sono incorporate: basta il solo `AlbatrosRDP.exe`. È la versione consigliata per la distribuzione.
`bin\Release\`	Versione non protetta: copiare `AlbatrosRDP.exe`, `AlbatrosRDP.exe.config` e le tre DLL elencate sopra.

2.3 File e cartelle usati dal programma

Percorso	Uso
`C:\ProgramData\Albatros\Common\CronologRDP.txt`	Cronologia delle connessioni (JSON), comune a tutti gli utenti del computer.
`%LOCALAPPDATA%\Albatros\AlbatrosRDP\AlbatrosRDP.log`	Log diagnostico dell'utente corrente; la copia precedente è `AlbatrosRDP.1.log`.
`CronologRDP.txt.corrupt-<data>.bak`	Copia di sicurezza della cronologia, creata solo se il file risulta illeggibile.

> **Più utenti sullo stesso computer.** Con i permessi predefiniti di ProgramData, il file della cronologia creato da un utente non è modificabile dagli altri: per loro la cronologia non si aggiorna. Se serve, un amministratore può concedere la modifica al gruppo Utenti con: `icacls "C:\ProgramData\Albatros\Common" /grant *S-1-5-32-545:(OI)(CI)M`

3. Avvio rapido

1. Avviare `AlbatrosRDP.exe` senza parametri: si apre la finestra di connessione.
2. Compilare **Computer** (nome o indirizzo del server), **Porta**, **Nome utente**, eventualmente **Dominio** e **Note**, poi la **Password**. Per un server già usato basta sceglierlo dalla **Cronologia** e digitare la password.
3. Premere **Connetti** (oppure Invio).
4. Il programma verifica che il server sia raggiungibile e apre la sessione a tutto schermo. Se Windows chiede le credenziali (NLA), inserirle nella finestra di sistema.
5. In alto al centro compare la barra di stato: verde quando la sessione è attiva.
6. Per il menu premere **Ctrl+F11** (o fare clic destro sulla barra di stato).
7. Per terminare scegliere **Disconnetti & Exit** dal menu, oppure la **X** rossa della barra, e confermare.

4. La finestra di connessione

Si apre quando il programma parte senza parametri validi da riga di comando. Ricorda lo stile della Connessione Desktop remoto di Windows.

> **Lingua delle etichette.** La finestra è tradotta in inglese, italiano, francese e rumeno, ma nella versione attuale la lingua è forzata a **inglese**. Nella tabella è riportata anche l'etichetta inglese che appare a video.

4.1 Campi e pulsanti

Campo	Etichetta a video	Descrizione
Cronologia	History	Elenco delle ultime connessioni, nel formato `server:porta {utente}`; si può solo selezionare, non digitare. La prima voce, -- Nuova connessione --, svuota i campi. All'apertura è selezionata la connessione più recente.
✖ (accanto alla cronologia)	—	Rimuove dalla cronologia la voce selezionata, dopo conferma.
Computer	Computer	Nome host, indirizzo IPv4 o IPv6. Accetta anche `host:porta` e `[IPv6]:porta`: la porta scritta qui ha la precedenza sul campo Porta. Un IPv6 senza parentesi quadre è inteso senza porta.
Porta	Port	Solo cifre, da 1 a 65535. Se vuoto si usa 3389.
Nome utente	User name	Utente della sessione remota.
Dominio	Domain	Dominio dell'utente (facoltativo).
Note	Notes	Testo libero mostrato nella barra di stato, nel titolo della finestra e in testa al menu. Viene salvato in cronologia.
Password	Password	Password dell'utente remoto. Non viene mai salvata. Se lasciata vuota, la chiederà Windows al momento della connessione.
Mostra password	Show password	Mostra in chiaro la password digitata.
Barra di stato personalizzata	Customized Status Bar	Selezionata (predefinito): barra di stato di AlbatrosRDP. Deselezionata: barra nativa di Microsoft (capitolo 8). La scelta viene ricordata per ogni voce della cronologia.
Connetti	Connect	Avvia la connessione (tasto Invio).
Annulla	Cancel	Chiude il programma senza connettersi (tasto Esc).

Se si sceglie una voce dalla cronologia, il cursore va direttamente sulla password; altrimenti sul campo Computer. In basso a sinistra sono riportati copyright e versione.

4.2 Controlli prima della connessione

- Computer vuoto: "Specificare l'indirizzo del computer."
- Porta non valida nel campo Computer (es. `server:99999`): "Porta non valida nel campo Computer: indicare un numero compreso tra 1 e 65535 (es. server:3389)."
- Porta non valida nel campo Porta: "Porta non valida: indicare un numero compreso tra 1 e 65535."

4.3 Come funziona la cronologia

- Una voce è identificata da **Server + Porta + Nome utente + Dominio**, senza distinzione tra maiuscole e minuscole.
- Nota e scelta della barra seguono la voce ma non la identificano: vale sempre l'ultimo valore usato.

- Una connessione già presente viene spostata in fondo all'elenco, cioè diventa la più recente.
- Si conservano al massimo **20** voci: oltre questo numero si eliminano le più vecchie.
- Il salvataggio avviene alla pressione di Connetti. È atomico e protetto da un blocco tra processi: due istanze aperte insieme non si cancellano le voci a vicenda.
- La password non viene mai scritta nel file.

5. La sessione remota

5.1 Apertura della sessione

1. La finestra passa a **tutto schermo** sul monitor corrente, compresa l'area della barra delle applicazioni. Il titolo della finestra è la nota, oppure "AlbatrosRDP".
2. Il desktop remoto viene richiesto con la risoluzione del monitor. Si usa un solo monitor.
3. Verifica di raggiungibilità: una connessione TCP di prova verso server e porta, con timeout di 2,5 secondi (risoluzione DNS compresa; indirizzi IPv4 e IPv6 provati in parallelo). La barra mostra "Verifica raggiungibilità server:porta...".
4. Se il server non risponde compare: "Impossibile raggiungere il server ... (tunnel SSH non attivo oppure rete non disponibile). Riprovare?". **Sì** ripete la verifica, **No** chiude il programma.
5. Se il server risponde parte la connessione RDP ("Connessione in corso..."). Se il server richiede le credenziali, Windows mostra la propria finestra: in questa fase AlbatrosRDP sospende la gestione della tastiera e non resta in primo piano, per non coprirla.
6. A connessione stabilita la barra diventa verde e mostra `--> server:porta`.

Se la sessione non arriva mai allo stato connesso (credenziali annullate o errate, rete assente), il programma non riprova all'infinito: mostra "La connessione RDP non è stata stabilita (Credenziali mancanti/annullate oppure errore di rete). L'applicazione verrà chiusa." e termina.

5.2 Comportamento a tutto schermo

- La finestra resta sopra le altre **solo** quando è in primo piano: con Alt+Tab o con un clic su un'altra applicazione si passa normalmente ad altri programmi.
- La barra di stato è visibile solo quando AlbatrosRDP è l'applicazione attiva.
- Il contenuto remoto si adatta alla finestra (smart sizing): in modalità finestra ridotta il desktop remoto viene rimpicciolito proporzionalmente, senza barre di scorrimento.

6. La barra di stato personalizzata

È la barra arrotondata che compare in alto al centro dello schermo nella modalità a tutto schermo, quando è attiva l'opzione **Barra di stato personalizzata**.

6.1 Testo e colori

Il testo è composto da: nota (se presente), promemoria del tasto del menu, stato. Esempio: `Server ufficio - (Ctrl+F11 menu) - --> 192.168.1.10:3389`.

Colori	Significato
Sfondo verde, testo giallo	Sessione connessa e server raggiungibile.
Sfondo giallo, testo rosso	Qualsiasi altro stato: verifica in corso, connessione in corso, connessione persa, errore.

6.2 Pulsanti

Pulsante	Azione
─ (giallo)	Riduce a icona.
□ (giallo)	Passa da tutto schermo a finestra e viceversa.
X (rossa)	Come Disconnetti & Exit: chiede conferma se la sessione è connessa, poi chiude.

6.3 Uso con il mouse

- **Trascinamento** con il tasto sinistro: la barra si può spostare ovunque sullo schermo e resta nella posizione scelta.
- **Tasto destro**: apre il menu rapido.
- **Doppio clic**: nasconde la barra (come la voce di menu Barra di stato).

6.4 Barra nascosta e comparsa automatica

Una barra nascosta a mano (doppio clic o menu) si può far riapparire in tre modi:

- dal menu rapido (Ctrl+F11), voce **Barra di stato**;
- portando il mouse entro **10 pixel dal bordo superiore** dello schermo, se è attiva l'opzione **Mostra barra al passaggio mouse in alto** (attiva per impostazione predefinita). In questo caso la barra si nasconde di nuovo quando il mouse si allontana di oltre 20 pixel sotto di essa;
- uscendo e rientrando dalla modalità a tutto schermo, o ripristinando la finestra dopo una riduzione a icona.

7. Il menu rapido

7.1 Come aprirlo

- **Ctrl+F11**: funziona solo con la barra personalizzata. La combinazione viene intercettata e non arriva al computer remoto. Con la barra nativa attiva è disattivata e passa alla sessione remota.
- **Tasto destro sulla barra di stato** (a tutto schermo).
- **Tasto destro sulla barra del titolo** (in modalità finestra), al posto del menu di sistema di Windows.

Il menu si chiude con un clic all'esterno, con la voce **Chiudi tendina** oppure con **Esc**. Finché il menu è aperto, il tasto Esc non viene inviato alla sessione remota.

7.2 Voci del menu

Voce	Funzione
Nota (in grassetto)	Presente solo se c'è una nota. Con un clic si apre la finestra "Nota di connessione" per modificarla. La nuova nota vale per la sessione in corso e aggiorna subito barra e titolo; non viene salvata in cronologia.
Schermo ridotto / Schermo intero	Passa dalla modalità a tutto schermo alla finestra e viceversa (capitolo 9).
Riduci a icona	Riduce a icona la finestra della sessione.
Barra di stato	Mostra o nasconde la barra di stato. Disponibile solo a tutto schermo.
Mostra barra al passaggio mouse in alto	Attiva o disattiva la comparsa automatica della barra (paragrafo 6.4).
Barra RDP nativa	Passa alla barra di connessione nativa di Microsoft, o torna a quella personalizzata (capitolo 8).
Dati connessione...	Mostra nota, info (parametro `-info`), server, porta, utente, dominio, stato, controllo RDP agganciato con la sua versione, copyright e versione del programma.
Riconnetti	Chiude la sessione se è ancora aperta (attesa massima 5 secondi) e la riapre. Utile se la sessione non risponde.
Disconnetti & Exit	Chiede "Disconnettere la sessione RDP e chiudere l'applicazione?" (predefinito: No) e, se si conferma, disconnette e chiude.
Chiudi tendina	Chiude il menu senza fare nulla.

8. La barra di connessione nativa Microsoft

In alternativa alla barra di AlbatrosRDP si può usare la barra di connessione standard di Microsoft, quella di `mstsc.exe`.

8.1 Attivazione

- Prima della connessione: togliere la spunta a **Barra di stato personalizzata** nella finestra di connessione. La scelta resta memorizzata per quella voce della cronologia.
- Durante la sessione: voce di menu **Barra RDP nativa**.

Circa un secondo dopo che la connessione è stabilita, il controllo RDP passa al proprio schermo intero e mostra la barra Microsoft, fissata e con i pulsanti Riduci a icona, Ripristina e Blocca.

8.2 Differenze di comportamento

- **Ctrl+F11** è disattivato: la combinazione arriva al computer remoto.
- La barra personalizzata e la sua comparsa automatica sono disattivate.
- **Riduci a icona** sulla barra Microsoft riduce a icona l'intera sessione; si riapre dall'icona sulla barra delle applicazioni.
- **Ripristina** sulla barra Microsoft porta AlbatrosRDP in **modalità finestra** e non torna da solo a tutto schermo. Da qui, con il tasto destro sulla barra del titolo, si apre il menu rapido: **Schermo intero** torna allo schermo intero nativo, mentre togliendo la spunta a **Barra RDP nativa** si ritorna alla barra personalizzata.
- **X** sulla barra Microsoft chiude la sessione. Compare la domanda "La sessione RDP è stata disconnessa. Riconnettersi al server? (No = chiude l'applicazione)".

9. La modalità finestra

Con **Schermo ridotto** (menu) o con il pulsante □ della barra, la sessione passa in una normale finestra di Windows, ridimensionabile.

- Lo stato della connessione (con nota e promemoria del menu) viene mostrato nel **titolo della finestra**, al posto della barra di stato.
- Il desktop remoto conserva la risoluzione con cui è stato aperto e viene rimpicciolito per stare nella finestra.
- Il **tasto destro sulla barra del titolo** apre il menu rapido; anche Ctrl+F11 continua a funzionare (con la barra personalizzata).
- A sinistra dei pulsanti di sistema (riduci, ingrandisci, chiudi) compare un pulsante aggiuntivo **Schermo intero** che riporta la sessione a tutto schermo.

10. Interruzioni, riconnessione ed errori

10.1 Server non più raggiungibile durante la sessione

Mentre la sessione è connessa, ogni 2 secondi il programma prova ad aprire una connessione TCP verso la porta RDP del server (timeout 1,5 secondi). Se la prova fallisce, la barra diventa gialla con "Connessione persa su server:porta", anche se il controllo RDP non ha ancora rilevato la caduta. Torna verde da sola quando il server risponde di nuovo. È il caso tipico di un tunnel SSH caduto.

10.2 Riconnessione automatica

Oltre alla riconnessione automatica interna del controllo RDP, se la sessione risulta disconnessa dopo essere stata connessa almeno una volta, AlbatrosRDP:

1. prova a riconnettersi al massimo ogni **5 secondi**, ogni volta preceduto da una verifica TCP rapida (1 secondo);
2. dopo **3 tentativi** falliti consecutivi chiede: "La riconnessione automatica non riesce (credenziali mancanti/annullate oppure server non disponibile). Continuare a riprovare?". **Sì** riprende i tentativi, **No** chiude il programma.

10.3 Watchdog (applicazione bloccata)

Un controllo indipendente verifica che l'interfaccia risponda. Se resta bloccata per più di **15 secondi** (per esempio per un'interruzione di rete durante l'autenticazione RDP), compare sopra ogni altra finestra il messaggio "L'applicazione non risponde da diversi secondi... Vuoi forzare la chiusura dell'applicazione?". **Sì** termina il programma, **No** continua ad attendere. Il controllo è sospeso mentre sono aperti i dialoghi del programma.

10.4 Errori imprevisti

- **Controllo RDP non disponibile** o non funzionante all'avvio: compare "Impossibile avviare la connessione RDP:" con il dettaglio dell'errore, poi il programma si chiude.
- **Eccezione non gestita**: il messaggio "AlbatrosRDP - Errore" riporta l'errore e chiede "Continuare a usare l'applicazione?". **Sì** permette di proseguire senza perdere la sessione, **No** chiude. L'errore viene sempre registrato nel log.

10.5 Chiusura

- Qualunque chiusura manuale con sessione connessa (menu, X della barra, X della finestra, Alt+F4, barra delle applicazioni) chiede conferma. Rispondendo No si torna esattamente alla situazione di prima.
- In chiusura il programma disconnette la sessione e attende al massimo 1 secondo che il controllo RDP la chiuda.
- Quando la chiusura parte da un dialogo di errore, è previsto un arresto di sicurezza: se la pulizia si blocca, il processo viene comunque terminato dopo 8 secondi.

11. Avvio da riga di comando

AlbatrosRDP può aprire una connessione direttamente, senza mostrare la finestra di connessione. I parametri possono essere passati in tre modi: **in chiaro**, **cifrati** in un'unica stringa, oppure in un **file** (in chiaro o cifrato).

11.1 Parametri di connessione

Parametro	Obbligatorio	Significato
`-ip=`	Sì	Nome o indirizzo del server. Accetta anche `host:porta` e `[IPv6]:porta`.
`-port=`	No	Porta TCP (1-65535). Se assente o non valida: 3389.
`-user=`	No	Nome utente.
`-domain=`	No	Dominio.
`-pwd=`	No	Password dell'utente remoto. Se assente la chiede Windows.
`-nota=`	No	Nota mostrata in barra, titolo e menu.
`-info=`	No	Informazione aggiuntiva mostrata in Dati connessione...

Parametro	Significato
`-enc=`	Stringa cifrata (Base64) che contiene i parametri della tabella precedente.
`-file=`	Percorso di un file che contiene i parametri, in chiaro o cifrati.
`-cryptpwd=`	Password di decifratura di `-enc` o `-file`. Il valore speciale `pipe` indica che la password arriva tramite named pipe (paragrafo 11.6).
`-local=true`	Solo informativo: indica che il contenuto è stato vincolato al computer. In lettura non viene considerato.

Regole generali:

- I nomi dei parametri non distinguono maiuscole e minuscole; il trattino iniziale è facoltativo (`ip=` equivale a `-ip=`).
- I valori con spazi vanno racchiusi tra doppi apici, preferibilmente l'intero argomento: `"-nota=Server ufficio"`.
- Ordine di priorità: se c'è `-file` si usa il file; altrimenti, se c'è `-enc`, la stringa cifrata; altrimenti i singoli parametri.
- I parametri sconosciuti vengono ignorati.
- Se manca `-ip` (o il file indicato non esiste), il programma si comporta come se non avesse parametri e apre la finestra di connessione.
- La connessione avviata da riga di comando usa la barra personalizzata e **non** viene aggiunta alla cronologia.

11.2 Parametri in chiaro

```
AlbatrosRDP.exe -ip=192.168.1.10 -port=3389 -user=Administrator "-nota=Server ufficio"
```

> **Attenzione.** Una password passata con `-pwd=` in chiaro è visibile a chiunque possa leggere la riga di comando dei processi (Gestione attività, Process Explorer, WMI). Per passare la password usare la forma cifrata, meglio se con la pipe.

11.3 Parametri cifrati

```
AlbatrosRDP.exe "-enc=<stringa Base64>" "-cryptpwd=<chiave>"
```

La stringa `-enc` si genera con le funzioni di programmazione descritte al capitolo 12 (`BuildCommandLineArgs`). Il programma non ha una funzione interattiva per crearla.

11.4 Parametri su file

```
AlbatrosRDP.exe "-file=C:\Config\Clienti\Cliente1.rdpdat"
AlbatrosRDP.exe "-file=C:\Config\Clienti\Cliente1.rdpdat" "-cryptpwd=<chiave>"
```

Il file (UTF-8) può contenere i parametri **in chiaro**, anche su più righe e con o senza trattino, oppure una stringa **cifrata**. Il programma riconosce da solo il formato: se il contenuto è in chiaro, l'eventuale `-cryptpwd` viene ignorato. Esempio di file in chiaro scritto a mano:

```
-ip=192.168.1.10
-port=3389
-user=Administrator
"-nota=Server ufficio"
"-info=Contratto assistenza n. 42"
```

Un file cifrato si crea con `BuildCommandLineArgs` indicando il percorso (capitolo 12). Se il file esiste già, viene chiesta conferma prima di sovrascriverlo.

11.5 Password di decifratura mancante o errata

Se il contenuto è cifrato e `-cryptpwd` manca o è errata, compare la finestra **Password richiesta**: "I parametri di connessione sono protetti da password. Tentativo N di 3." (preceduto da "Password errata." dopo un errore).

- Sono concessi **3 tentativi**.
- Con **Annulla**, o esauriti i tentativi, il programma **termina** senza aprire la finestra di connessione.
- Ogni decifratura viene verificata (il risultato deve contenere almeno `ip`): una password errata non può essere scambiata per buona.

11.6 Password tramite named pipe

Con `-cryptpwd=pipe` la password reale non compare mai nella riga di comando, nemmeno per un istante. Il programma che avvia AlbatrosRDP gliela consegna attraverso una named pipe locale:

- nome della pipe: `\\.\pipe\AlbatrosRDP_Secret_<PID>`, dove PID è l'identificativo del processo AlbatrosRDP appena avviato;
- la pipe è creata dal programma chiamante, è accessibile al solo utente Windows corrente e accetta una sola connessione;
- il segreto viene consegnato solo se a collegarsi è proprio il processo atteso (verifica del PID del client);
- il testo viaggia in UTF-8 (un eventuale BOM viene tollerato);
- AlbatrosRDP attende al massimo **5 secondi**: se non riceve nulla, chiede la password con la finestra del paragrafo 11.5.

Il modo più semplice per usare la pipe è la funzione `StartProcessWithEncryptedArgsAndPipePasswordWait` (capitolo 12), che fa tutto in un'unica chiamata.

11.7 Vincolo al singolo computer

Al momento della creazione (`machineBound:=True`) si può vincolare il contenuto cifrato al computer corrente. In quel caso la chiave effettiva di cifratura è formata dall'ID hardware del computer seguito dalla password. L'ID hardware è composto da:

- numero di serie della scheda madre;
- identificativo della CPU;
- numero di serie del primo disco fisico.

In lettura non serve indicare nulla: il programma prova prima la password così com'è (contenuto valido su tutti i computer) e poi la combinazione con l'ID hardware del computer locale, comprese le varianti dovute all'ordine non garantito dei dischi (per esempio una chiavetta USB inserita).

> **Attenzione.** Un contenuto vincolato diventa illeggibile se si sostituiscono scheda madre, CPU o disco di sistema, e naturalmente su qualsiasi altro computer: in quel caso va rigenerato.

12. Integrazione da altri programmi

Le classi del programma possono essere usate da un'altra applicazione VB.NET, aggiungendo un riferimento ad `AlbatrosRDP.exe` (versione non protetta) oppure includendo i file sorgente. Il progetto di esempio **Test_Lancio_pipe** (applicazione console) mostra l'avvio con password tramite pipe.

12.1 La classe RdpConnectionParams

Proprietà	Tipo	Descrizione
`Ip`	String	Server (obbligatorio).
`Port`	Integer	Porta; 0 = predefinita (3389).
`User`, `Domain`	String	Utente e dominio.
`Password`	String	Password dell'utente remoto.
`Nota`, `Info`	String	Nota e informazione aggiuntiva.
`IsValid`	Boolean	True se `Ip` è valorizzato.
`Clone()`	Funzione	Restituisce una copia.

12.2 La classe RdpCommandLineManager

Metodo (Shared)	Descrizione
`BuildCommandLineArgs(prms, [encryptionPassword], [filePath], [machineBound])`	Costruisce gli argomenti. Senza password: in chiaro. Con password: `-enc` + `-cryptpwd`. Con `filePath`: scrive il file (in chiaro o cifrato, crea la cartella, chiede conferma se esiste) e restituisce `-file` [+ `-cryptpwd`]. Gli argomenti sono già quotati secondo le regole di Windows.
`BuildCommandLineArgsFromFile(filePath, [encryptionPassword])`	Argomenti per un file già esistente; se è indicata la password verifica prima che il file si decifri. Solleva un'eccezione se il file non esiste o la password è errata.
`StartProcessWithEncryptedArgsAndPipePasswordWait(exePath, prms, encryptionPassword, ByRef passwordDelivered, [machineBound], [pipeTimeoutMs=5000])`	Avvia AlbatrosRDP con `-cryptpwd=pipe`, consegna la password tramite pipe e attende la consegna. `passwordDelivered` indica l'esito. Adatto ai lanciatori che terminano subito.
`StartProcessWithEncryptedArgsAndPipePassword(exePath, prms, encryptionPassword, [machineBound], [pipeTimeoutMs=5000])`	Come sopra, ma la consegna avviene in background e il metodo ritorna subito. Se il chiamante termina prima della consegna, la password non arriva.
`ParseCommandLineArgs(args, [ByRef userAborted])`	Interpreta gli argomenti ricevuti (con richiesta interattiva della password se serve).
`ReadParamsFromFile(filePath, [cryptPwd])`	Legge un file di parametri senza dialoghi; eccezione se la password è errata.
`EncryptString(testo, password)` / `DecryptToOriginalString(blob, password)`	Cifratura e decifratura di base, senza vincolo hardware.
`GetMachineHardwareId()`	ID hardware del computer corrente.

Esempio: avvio con password tramite pipe da un lanciatore (la chiave è contenuta in una variabile, mai scritta nel codice):

```
Dim prms As New RdpConnectionParams With {
    .Ip = "192.168.1.10", .Port = 3389,
    .User = "Administrator", .Nota = "Server ufficio"}

Dim consegnata As Boolean = False
RdpCommandLineManager.StartProcessWithEncryptedArgsAndPipePasswordWait(
    "C:\Albatros\CompiledPrograms\AlbatrosRDP.exe",
    prms, chiave, consegnata)
```

Esempio: creazione di un file cifrato vincolato al computer:

```
Dim argomenti As String = RdpCommandLineManager.BuildCommandLineArgs(
    prms, encryptionPassword:=chiave,
    filePath:="C:\Config\Clienti\Cliente1.rdpdat", machineBound:=True)
' -> "-file=C:\Config\Clienti\Cliente1.rdpdat" "-cryptpwd=..." "-local=true"
```

12.3 La classe SecretPipeTransfer

Metodo (Shared)	Descrizione
`SendSecretToChildProcessAndWait(processo, segreto, [timeoutMs])`	Lato chiamante: crea la pipe per il PID del processo figlio e attende la consegna. Restituisce True se consegnato.
`SendSecretToChildProcess(processo, segreto, [timeoutMs])`	Come sopra, in background.
`ReceiveSecretForCurrentProcess([timeoutMs])`	Lato AlbatrosRDP: legge il segreto dalla pipe del proprio PID.
`ReadSecretFromPipe(nomePipe, [timeoutMs])`	Lettura da una pipe con nome esplicito.
`WaitSeconds(n)` / `WaitMilliSeconds(n)`	Attesa che mantiene reattiva l'interfaccia.

12.4 Formato della cifratura

Elemento	Valore
Algoritmo	AES-256, modalità CBC, padding PKCS7
Derivazione della chiave	PBKDF2-HMAC-SHA1, 50.000 iterazioni, salt casuale di 16 byte
Formato	Base64 di: salt (16 byte) + IV (16 byte) + dati cifrati
Contenuto in chiaro	Parametri nel formato `"-ip=..." "-user=..."` (UTF-8)
Compatibilità	Identico alle versioni precedenti: stringhe e file creati prima restano leggibili, e viceversa

12.5 Personalizzazioni da codice

Elemento	Descrizione
`FrmRDP.New([nativeConnectionBar], [SafeMode])`	Sessione con finestra di connessione.
`FrmRDP.New(server, port, domain, userName, password, [nativeConnectionBar], [SafeMode])`	Sessione diretta, senza finestra di connessione.
`SafeMode`	Se True, cerca prima il controllo RDP generico e limita la scelta alle versioni fino alla 11.
`FrmRDP.MenuHotkey`	Combinazione del menu rapido (predefinita `Keys.Control Or Keys.F11`).

Elemento	Descrizione
`FrmRDP.ConnectionNote` / `ConnectionInfo`	Nota e info della sessione.
`FrmRDP.ShowNativeConnectionBar`	Barra nativa sì/no; impostarla prima di `ShowDialog()`.
`Module1.PercorsoStorico`	Percorso del file di cronologia.
`Module1.MaxCronologRDP`	Numero massimo di voci in cronologia (predefinito 20).

13. Impostazioni RDP applicate

All'apertura di ogni sessione vengono applicate le seguenti impostazioni, nel formato dei file `.rdp`. Sono definite nel codice (stringa `rdpSettingsString` di FrmRDP); non c'è un file di configurazione esterno.

Impostazione	Effetto
`session bpp:i:32`	Colori a 32 bit.
`compression:i:1`	Compressione dei dati attiva.
`disable wallpaper:i:1`	Sfondo del desktop remoto non mostrato (meno banda).
`keyboardhook:i:2`	Combinazioni di tasti di Windows inviate al computer remoto solo a schermo intero (valore predefinito).
`audiomode:i:0`	Audio remoto riprodotto sul computer locale.
`audiocapturemode:i:1`	Microfono locale disponibile nella sessione remota.
`redirectprinters:i:1`	Stampanti locali disponibili nella sessione.
`redirectsmartcards:i:1`	Smart card locali disponibili.
`redirectclipboard:i:1`	Appunti condivisi tra locale e remoto.
`drivestoredirect:s:*`	Tutte le unità locali visibili nella sessione remota.
`negotiate security layer:i:1`	Negoziazione automatica del protocollo di sicurezza più robusto.
`screen mode id`, `use multimon`	Ignorate: lo schermo intero è gestito dal programma, su un solo monitor.

Subito dopo, il programma imposta inoltre:

- **riconnessione automatica** del controllo RDP attiva (sostituisce `autoreconnection enabled:i:0` della stringa);
- **livello di autenticazione 0** e avvisi sul certificato ignorati (sostituisce `authentication level:i:2`): il certificato del server non viene verificato e non compare alcun avviso;
- **CredSSP** attivo (necessario per l'autenticazione NLA);
- **timeout** di connessione: 8 secondi complessivi, 5 per singolo tentativo.

Il programma sa interpretare anche altre chiavi `.rdp` (per esempio `alternate shell` e `shell working directory` per avviare un solo programma al posto del desktop, `connection type`, `networkautodetect`, `redirectcomports` e le impostazioni del gateway RD `gatewayhostname`, `gatewayusagemethod` e simili): per usarle va modificata la stringa nel codice e ricompilato il programma.

14. Sicurezza e riservatezza

- La **password** dell'utente remoto non viene mai salvata su disco: né in cronologia né nel log. Dopo la consegna al controllo RDP, le copie in memoria vengono cancellate.
- Il **log** registra solo la modalità di avvio, gli stati della connessione e gli errori: mai password, chiavi o parametri.
- La **cifratura** usa AES-256 con chiave derivata da PBKDF2. I buffer con dati sensibili vengono azzerati dopo l'uso.
- La **pipe** è accessibile solo all'utente corrente, consegna il segreto al solo processo atteso, ed è monouso.
- Il **certificato del server non viene verificato** (paragrafo 13). La protezione da intercettazioni è quindi affidata al canale: rete fidata, VPN o tunnel SSH. Valutare se mantenere questa impostazione.
- Una password passata con `-pwd=` in chiaro è visibile nell'elenco dei processi (paragrafo 11.2).
- La verifica di raggiungibilità durante la sessione apre una connessione TCP verso la porta RDP ogni 2 secondi: sul server questo genera eventi nel registro di RDP (RdpCoreTS) e un po' di traffico nel tunnel.

15. Log diagnostico

Il log si trova in `%LOCALAPPDATA%\Albatros\AlbatrosRDP\AlbatrosRDP.log`. Quando supera 1 MB viene rinominato in `AlbatrosRDP.1.log` (sostituendo la copia precedente) e si ricomincia. Ogni riga ha il formato:

```
2026-10-11 14:22:05.123 [4812] INFO  Stato RDP: connesso
```

cioè data e ora, PID del processo, livello (INFO, WARN, ERROR) e messaggio. Vengono registrati:

- avvio (versione e numero di argomenti) e chiusura dell'applicazione;
- modalità della riga di comando (in chiaro, cifrata, file) ed esito (parametri validi, non validi, password annullata o errata);
- server, porta, controllo RDP agganciato e tipo di barra;
- cambi di stato della sessione, con il codice esteso del motivo di disconnessione;
- tentativi di riconnessione falliti, interventi del watchdog, errori ed eccezioni non gestite;
- chiusura della sessione con il motivo.

16. Risoluzione dei problemi

Problema	Cosa fare
All'avvio compare "Impossibile avviare la connessione RDP"	Il controllo RDP di Windows manca o non funziona. Verificare che Connessione Desktop remoto (`mstsc.exe`) funzioni e consultare il log.
"Impossibile raggiungere il server"	Controllare tunnel SSH, VPN, firewall, indirizzo e porta. Con un tunnel locale verificare che sia attivo prima di connettersi.
Il programma si chiude con "La connessione RDP non è stata stabilita"	Credenziali annullate o errate, oppure rete assente durante l'autenticazione. Riprovare controllando utente, dominio e password.
Barra gialla con "Connessione persa su ..."	Il server non risponde più sulla porta RDP: tipicamente il tunnel è caduto. La barra torna verde da sola al ripristino.
Ctrl+F11 non apre il menu	È attiva la barra nativa Microsoft (Ctrl+F11 disattivato). Usare il tasto destro sulla barra del titolo in modalità finestra.
La barra di stato non si vede	È stata nascosta (doppio clic o menu): portare il mouse sul bordo superiore o usare Ctrl+F11 > Barra di stato. La barra si vede solo se AlbatrosRDP è l'applicazione attiva.
Avvio con `-cryptpwd=pipe` e richiesta della password	La password non è arrivata entro 5 secondi. Probabilmente il lanciatore è terminato prima della consegna: usare `StartProcessWithEncryptedArgsAndPipePasswordWait`.
Password corretta ma "Password errata" con un contenuto vincolato	È cambiato l'hardware (scheda madre, CPU, disco) o si sta usando un altro computer: rigenerare il contenuto cifrato.
Con `-ip` presente si apre comunque la finestra di connessione	Il parametro non è stato riconosciuto: controllare l'uso dei doppi apici e, con `-file`, che il file esista.
La cronologia non si aggiorna	Mancano i permessi di scrittura sul file in ProgramData (paragrafo 2.3).
La cronologia è sparita	Il file era illeggibile: ne è stata salvata una copia `.corrupt-<data>.bak` nella stessa cartella.
Lo sfondo del desktop remoto non compare (tinta unita)	È voluto (`disable wallpaper:i:1`, capitolo 13).
"L'applicazione non risponde da diversi secondi"	Il programma è bloccato da oltre 15 secondi, di solito per una caduta di rete durante l'autenticazione. Sì chiude il programma, No continua ad attendere.

Appendice A. Messaggi del programma

Messaggio	Significato e risposte
Verifica raggiungibilità server:porta...	Prova TCP in corso prima della connessione.
Connessione in corso...	Il controllo RDP sta stabilendo la sessione.
--> server:porta (barra verde)	Sessione connessa.
Connessione persa su server:porta	Il server non risponde alla prova TCP periodica.
Connessione RDP non attiva	Sessione disconnessa; riconnessione automatica in corso.
Riconnessione in corso... / Disconnessione in corso...	Effetto della voce Riconnetti o della chiusura.
Errore di connessione / Errore di riconnessione	Il controllo RDP ha rifiutato la richiesta di connessione.
Impossibile raggiungere il server ... Riprovare?	Sì = nuova verifica; No = chiusura.
La connessione RDP non è stata stabilita ... L'applicazione verrà chiusa.	Prima connessione mai riuscita (credenziali o rete).
La riconnessione automatica non riesce ... Continuare a riprovare?	Dopo 3 tentativi falliti. Sì = continua; No = chiusura.
La sessione RDP è stata disconnessa. Riconnettersi al server?	Sessione chiusa dalla barra nativa o dal server. Sì = riconnessione; No = chiusura.
Disconnettere la sessione RDP e chiudere l'applicazione?	Conferma di chiusura. Predefinito: No.
L'applicazione non risponde da diversi secondi ...	Watchdog. Sì = chiusura forzata; No = attesa.
AlbatrosRDP - Errore ... Continuare a usare l'applicazione?	Eccezione non gestita. Sì = prosegue; No = chiusura.
Password richiesta - Tentativo N di 3	Parametri cifrati: inserire la password di decifratura.
Il file ... esiste già. Sovrascrivere?	Creazione di un file di parametri da codice.

Appendice B. Riferimento rapido

B.1 Tasti e mouse

Comando	Effetto
Ctrl+F11	Apre il menu rapido (solo barra personalizzata).
Esc con il menu aperto	Chiude il menu.
Tasto destro sulla barra di stato	Apre il menu rapido.
Tasto destro sulla barra del titolo	Apre il menu rapido (modalità finestra).
Doppio clic sulla barra di stato	Nasconde la barra.
Mouse sul bordo superiore	Fa ricomparire la barra nascosta.
Trascinamento della barra di stato	La sposta.
Invio / Esc nella finestra di connessione	Connetti / Annulla.

B.2 Riga di comando

```
AlbatrosRDP.exe -ip=<server> [-port=<porta>] [-user=<utente>] [-domain=<dominio>]
                [-pwd=<password>] ["-nota=<testo>"] ["-info=<testo>"]

AlbatrosRDP.exe "-enc=<Base64>" "-cryptpwd=<chiave>|pipe"

AlbatrosRDP.exe "-file=<percorso>" ["-cryptpwd=<chiave>|pipe"]
```

B.3 Valori temporali

Controllo	Valore
Verifica di raggiungibilità iniziale	2,5 s
Verifica durante la sessione	ogni 2 s, timeout 1,5 s
Intervallo minimo tra tentativi di riconnessione	5 s
Tentativi prima della domanda "Continuare a riprovare?"	3
Attesa iniziale prima di considerare fallita la connessione	15 s
Watchdog	15 s di blocco (controllo ogni 2 s)
Attivazione della barra nativa dopo la connessione	1 s
Attesa della password via pipe	5 s
Arresto di sicurezza in chiusura	8 s

AlbatrosRDP

Client Desktop la distanță

Manual de utilizare și de integrare

Versiunea 2.0.162.6127 — octombrie 2026

© Raffaele Romano 2026

Cuprins

1. Introducere....83
1.1 Funcții principale....83
1.2 Versiunea documentată....83
2. Cerințe și instalare....84
2.1 Cerințe....84
2.2 Fișiere de distribuit....84
2.3 Fișiere și foldere utilizate de program....84
3. Pornire rapidă....85
4. Fereastra de conectare....86
4.1 Câmpuri și butoane....86
4.2 Verificări înainte de conectare....86
4.3 Cum funcționează istoricul....86
5. Sesiunea la distanță....88
5.1 Deschiderea sesiunii....88
5.2 Comportamentul pe ecran complet....88
6. Bara de stare personalizată....89
6.1 Text și culori....89
6.2 Butoane....89
6.3 Utilizarea cu mouse-ul....89
6.4 Bara ascunsă și afișarea automată....89
7. Meniul rapid....90
7.1 Cum se deschide....90
7.2 Elementele meniului....90
8. Bara de conexiune nativă Microsoft....91
8.1 Activare....91
8.2 Diferențe de comportament....91
9. Modul fereastră....92
10. Întreruperi, reconectare și erori....93
10.1 Server care nu mai poate fi accesat în timpul sesiunii....93
10.2 Reconectare automată....93
10.3 Watchdog (aplicație blocată)....93
10.4 Erori neprevăzute....93
10.5 Închidere....93
11. Pornire din linia de comandă....94
11.1 Parametri de conectare....94
11.2 Parametri în clar....94
11.3 Parametri criptați....94
11.4 Parametri în fișier....95
11.5 Parolă de decriptare lipsă sau greșită....95
11.6 Parola prin named pipe....95
11.7 Legarea de un singur computer....95
12. Integrarea din alte programe....97
12.1 Clasa RdpConnectionParams....97
12.2 Clasa RdpCommandLineManager....97
12.3 Clasa SecretPipeTransfer....98
12.4 Formatul criptării....98
12.5 Personalizări din cod....98
13. Setări RDP aplicate....100
14. Securitate și confidențialitate....101
15. Jurnal de diagnosticare....102
16. Depanare....103
Anexa A. Mesajele programului....104
Anexa B. Referință rapidă....105

B.1 Taste și mouse.....105
B.2 Linia de comandă.....105
B.3 Valori de timp.....105

1. Introducere

AlbatrosRDP este un client Desktop la distanță (RDP) pentru Windows, dezvoltat în VB.NET pe .NET Framework 4.8. Folosește controlul ActiveX Microsoft (`mstscax.dll`), adică același motor ca Conexiune desktop la distanță (`mstsc.exe`), și adaugă o serie de funcții gândite pentru utilizarea zilnică și pentru conexiunile prin tuneluri SSH.

1.1 Funcții principale

- Fereastră de conectare cu **istoricul** ultimelor conexiuni (parola nu este salvată niciodată) și o **notă** liberă pentru fiecare conexiune.
- Sesiune pe **ecran complet** cu o **bară de stare flotantă**: colorată în funcție de stare, care poate fi glisată și ascunsă.
- Alternativ, **bara de conexiune nativă** Microsoft.
- **Meniu rapid** care se deschide cu **Ctrl+F11**, cu clic dreapta pe bara de stare sau pe bara de titlu.
- **Verificarea accesibilității** serverului înainte de conectare și, la fiecare 2 secunde, în timpul sesiunii.
- **Reconectare automată** atunci când sesiunea se întrerupe.
- **Watchdog**: dacă aplicația rămâne blocată (de exemplu din cauza unei căderi de rețea în timpul autentificării), propune închiderea forțată.
- **Pornire directă din linia de comandă**, cu parametri în clar, criptați (AES-256) sau citiți din fișier. Parola de decriptare poate fi transmisă și printr-un named pipe, fără să apară vreodată în linia de comandă.
- Legarea opțională a parametrilor criptați de un **singur computer** (ID hardware).
- **Jurnal de diagnosticare** care nu conține niciodată parole, chei sau parametri.

1.2 Versiunea documentată

Element	Valoare
Program	AlbatrosRDP
Versiune	2.0.162.6127 (revizia din octombrie 2026)
Platformă	.NET Framework 4.8, Windows Forms, VB.NET
Motor RDP	Controlul ActiveX Microsoft RDP (MSTSCLib), versiunile de la 6 la 14
Autor	© Raffaele Romano 2026

2. Cerințe și instalare

2.1 Cerințe

- Windows cu clientul Desktop la distanță Microsoft instalat (`mstscax.dll`, prezent implicit în versiunile desktop și server de Windows).
- .NET Framework 4.8.
- Acces de rețea la serverul RDP pe portul TCP indicat (implicit **3389**), direct sau printr-un tunel.

La pornirea sesiunii, programul caută cel mai recent control RDP înregistrat în sistem (de la `MsRdpClient14` până la `MsRdpClient6`). Fiecare versiune este creată efectiv și verificată: dacă nu funcționează, este eliminată și se trece la cea anterioară. Versiunea utilizată este vizibilă în meniul **Dati connessione...** și în jurnal.

2.2 Fișiere de distribuit

Programul nu necesită instalare: este suficient să îl copiați într-un folder (de exemplu `C:\Albatros\CompiledPrograms\`). Proiectul produce două versiuni:

Folder de compilare	Conținut de copiat
`bin\Release\AlbatrosRDP_Secure\`	Versiune protejată cu .NET Reactor. Bibliotecile `Interop.MSTSCLib.dll`, `AxInterop.MSTSCLib.dll` și `Newtonsoft.Json.dll` sunt încorporate: este suficient doar `AlbatrosRDP.exe`. Este versiunea recomandată pentru distribuire.
`bin\Release\`	Versiune neprotejată: copiați `AlbatrosRDP.exe`, `AlbatrosRDP.exe.config` și cele trei DLL-uri enumerate mai sus.

2.3 Fișiere și foldere utilizate de program

Cale	Utilizare
`C:\ProgramData\Albatros\Common\CronologRDP.txt`	Istoricul conexiunilor (JSON), comun tuturor utilizatorilor computerului.
`%LOCALAPPDATA%\Albatros\AlbatrosRDP\AlbatrosRDP.log`	Jurnalul de diagnosticare al utilizatorului curent; copia anterioară este `AlbatrosRDP.1.log`.
`CronologRDP.txt.corrupt-<data>.bak`	Copie de siguranță a istoricului, creată numai dacă fișierul nu poate fi citit.

> **Mai mulți utilizatori pe același computer.** Cu permisiunile implicite ale ProgramData, fișierul de istoric creat de un utilizator nu poate fi modificat de ceilalți: pentru aceștia istoricul nu se actualizează. Dacă este necesar, un administrator poate acorda dreptul de modificare grupului Utilizatori cu: `icacls "C:\ProgramData\Albatros\Common" /grant *S-1-5-32-545:(OI)(CI)M`

3. Pornire rapidă

1. Porniți `AlbatrosRDP.exe` fără parametri: se deschide fereastra de conectare.
2. Completați **Computer** (numele sau adresa serverului), **Porta**, **Nome utente**, eventual **Dominio** și **Note**, apoi **Password**. Pentru un server deja utilizat, este suficient să îl alegeți din **Cronologia** și să tastați parola.
3. Apăsați **Connetti** (Conectare) (sau Enter).
4. Programul verifică dacă serverul poate fi accesat și deschide sesiunea pe ecran complet. Dacă Windows solicită acreditările (NLA), introduceți-le în fereastra de sistem.
5. În partea de sus, la centru, apare bara de stare: verde când sesiunea este activă.
6. Pentru meniu apăsați **Ctrl+F11** (sau faceți clic dreapta pe bara de stare).
7. Pentru a încheia, alegeți **Disconnetti & Exit** din meniu sau **X**-ul roșu din bară și confirmați.

4. Fereastra de conectare

Se deschide atunci când programul pornește fără parametri valizi în linia de comandă. Amintește de stilul aplicației Conexiune desktop la distanță din Windows.

> **Limba etichetelor.** Fereastra este tradusă în engleză, italiană, franceză și română, dar în versiunea actuală limba este forțată la **engleză**. Tabelul indică și eticheta în engleză care apare pe ecran.

4.1 Câmpuri și butoane

Câmp	Eticheta de pe ecran	Descriere
Cronologia (Istoric)	History	Lista ultimelor conexiuni, în formatul `server:porta {utente}`; poate fi doar selectată, nu tastată. Primul element, -- Nuova connessione --, golește câmpurile. La deschidere este selectată cea mai recentă conexiune.
✖ (lângă istoric)	—	Elimină din istoric elementul selectat, după confirmare.
Computer	Computer	Nume de gazdă, adresă IPv4 sau IPv6. Acceptă și `host:porta` și `[IPv6]:porta`: portul scris aici are prioritate față de câmpul Porta. O adresă IPv6 fără paranteze pătrate este considerată fără port.
Porta (Port)	Port	Numai cifre, de la 1 la 65535. Dacă este gol, se folosește 3389.
Nome utente (Nume utilizator)	User name	Utilizatorul sesiunii la distanță.
Dominio (Domeniu)	Domain	Domeniul utilizatorului (opțional).
Note (Note)	Notes	Text liber afișat în bara de stare, în titlul ferestrei și în partea de sus a meniului. Este salvat în istoric.
Password (Parolă)	Password	Parola utilizatorului la distanță. Nu este salvată niciodată. Dacă este lăsată goală, o va solicita Windows în momentul conectării.
Mostra password (Afișare parolă)	Show password	Afișează în clar parola tastată.
Barra di stato personalizzata (Bară de stare personalizată)	Customized Status Bar	Bifată (implicit): bara de stare AlbatrosRDP. Debifată: bara nativă Microsoft (capitolul 8). Alegerea este memorată pentru fiecare element din istoric.
Connetti (Conectare)	Connect	Pornește conexiunea (tasta Enter).
Annulla (Anulare)	Cancel	Închide programul fără a se conecta (tasta Esc).

Dacă alegeți un element din istoric, cursorul trece direct la parolă; altfel, la câmpul Computer. În stânga jos sunt afișate drepturile de autor și versiunea.

4.2 Verificări înainte de conectare

- Câmpul Computer gol: "Specificare l'indirizzo del computer."
- Port nevalid în câmpul Computer (de ex. `server:99999`): "Porta non valida nel campo Computer: indicare un numero compreso tra 1 e 65535 (es. server:3389)."
- Port nevalid în câmpul Porta: "Porta non valida: indicare un numero compreso tra 1 e 65535."

4.3 Cum funcționează istoricul

- Un element este identificat prin **Server + Port + Nume utilizator + Domeniu**, fără a face distincție între majuscule și minuscule.

- Nota și alegerea barei urmează elementul, dar nu îl identifică: este valabilă întotdeauna ultima valoare utilizată.
- O conexiune deja existentă este mutată la sfârșitul listei, adică devine cea mai recentă.
- Se păstrează cel mult **20** de elemente: peste acest număr, cele mai vechi sunt eliminate.
- Salvarea are loc la apăsarea butonului Connetti. Este atomică și protejată printr-o blocare între procese: două instanțe deschise simultan nu își șterg reciproc elementele.
- Parola nu este scrisă niciodată în fișier.

5. Sesiunea la distanță

5.1 Deschiderea sesiunii

1. Fereastra trece pe **ecran complet** pe monitorul curent, inclusiv zona barei de activități. Titlul ferestrei este nota sau "AlbatrosRDP".
2. Desktopul la distanță este solicitat la rezoluția monitorului. Se folosește un singur monitor.
3. Verificarea accesibilității: o conexiune TCP de test către server și port, cu timeout de 2,5 secunde (inclusiv rezolvarea DNS; adresele IPv4 și IPv6 sunt încercate în paralel). Bara afișează "Verifica raggiungibilità server:porta...".
4. Dacă serverul nu răspunde, apare: "Impossibile raggiungere il server ... (tunnel SSH non attivo oppure rete non disponibile). Riprovare?". **Sì** (Da) repetă verificarea, **No** (Nu) închide programul.
5. Dacă serverul răspunde, pornește conexiunea RDP ("Connessione in corso..."). Dacă serverul solicită acreditările, Windows afișează propria fereastră: în această fază AlbatrosRDP suspendă gestionarea tastaturii și nu rămâne în prim-plan, pentru a nu o acoperi.
6. După stabilirea conexiunii, bara devine verde și afișează `--> server:porta`.

Dacă sesiunea nu ajunge niciodată în starea conectată (acreditări anulate sau greșite, rețea absentă), programul nu reîncearcă la nesfârșit: afișează "La connessione RDP non è stata stabilita (Credenziali mancanti/annullate oppure errore di rete). L'applicazione verrà chiusa." și se închide.

5.2 Comportamentul pe ecran complet

- Fereastra rămâne deasupra celorlalte **numai** atunci când este în prim-plan: cu Alt+Tab sau cu un clic pe altă aplicație se trece în mod normal la alte programe.
- Bara de stare este vizibilă numai atunci când AlbatrosRDP este aplicația activă.
- Conținutul la distanță se adaptează la fereastră (smart sizing): în modul fereastră redusă, desktopul la distanță este micșorat proporțional, fără bare de defilare.

6. Bara de stare personalizată

Este bara rotunjită care apare în partea de sus, la centrul ecranului, în modul ecran complet, atunci când este activă opțiunea **Barra di stato personalizzata**.

6.1 Text și culori

Textul este compus din: notă (dacă există), memento pentru tasta meniului, stare. Exemplu: `Server ufficio - (Ctrl+F11 menu) - --> 192.168.1.10:3389`.

Culori	Semnificație
Fundal verde, text galben	Sesiune conectată și server accesibil.
Fundal galben, text roșu	Orice altă stare: verificare în curs, conectare în curs, conexiune pierdută, eroare.

6.2 Butoane

Buton	Acțiune
─ (galben)	Minimizează.
□ (galben)	Comută între ecran complet și fereastră.
X (roșu)	Ca Disconnetti & Exit: cere confirmare dacă sesiunea este conectată, apoi închide.

6.3 Utilizarea cu mouse-ul

- **Glisare** cu butonul stâng: bara poate fi mutată oriunde pe ecran și rămâne în poziția aleasă.
- **Clic dreapta**: deschide meniul rapid.
- **Dublu clic**: ascunde bara (ca elementul de meniu Barra di stato).

6.4 Bara ascunsă și afișarea automată

O bară ascunsă manual (dublu clic sau meniu) poate fi reafișată în trei moduri:

- din meniul rapid (Ctrl+F11), elementul **Barra di stato**;
- aducând mouse-ul la mai puțin de **10 pixeli de marginea superioară** a ecranului, dacă este activă opțiunea **Mostra barra al passaggio mouse in alto** (activă implicit). În acest caz, bara se ascunde din nou când mouse-ul se îndepărtează la peste 20 de pixeli sub ea;
- ieșind și reintrând în modul ecran complet sau restaurând fereastra după o minimizare.

7. Meniul rapid

7.1 Cum se deschide

- **Ctrl+F11**: funcționează numai cu bara personalizată. Combinația este interceptată și nu ajunge la computerul la distanță. Cu bara nativă activă, este dezactivată și trece la sesiunea la distanță.
- **Clic dreapta pe bara de stare** (pe ecran complet).
- **Clic dreapta pe bara de titlu** (în modul fereastră), în locul meniului de sistem Windows.

Meniul se închide cu un clic în afara lui, cu elementul **Chiudi tendina** sau cu **Esc**. Cât timp meniul este deschis, tasta Esc nu este trimisă sesiunii la distanță.

7.2 Elementele meniului

Element	Funcție
Nota (Notă, cu caractere aldine)	Prezent numai dacă există o notă. Cu un clic se deschide fereastra "Nota di connessione" pentru a o modifica. Noua notă este valabilă pentru sesiunea curentă și actualizează imediat bara și titlul; nu este salvată în istoric.
Schermo ridotto / Schermo intero (Ecran redus / Ecran complet)	Comută între modul ecran complet și fereastră (capitolul 9).
Riduci a icona (Minimizare)	Minimizează fereastra sesiunii.
Barra di stato (Bară de stare)	Afișează sau ascunde bara de stare. Disponibil numai pe ecran complet.
Mostra barra al passaggio mouse in alto (Afișare bară la trecerea mouse-ului sus)	Activează sau dezactivează afișarea automată a barei (secțiunea 6.4).
Barra RDP nativa (Bară RDP nativă)	Trece la bara de conexiune nativă Microsoft sau revine la cea personalizată (capitolul 8).
Dati connessione... (Date conexiune...)	Afișează nota, informațiile (parametrul `-info`), serverul, portul, utilizatorul, domeniul, starea, controlul RDP utilizat cu versiunea sa, drepturile de autor și versiunea programului.
Riconnetti (Reconectare)	Închide sesiunea dacă este încă deschisă (așteptare maximă 5 secunde) și o redeschide. Util dacă sesiunea nu răspunde.
Disconnetti & Exit (Deconectare și ieșire)	Întreabă "Disconnettere la sessione RDP e chiudere l'applicazione?" (implicit: No) și, dacă confirmați, deconectează și închide.
Chiudi tendina (Închidere meniu)	Închide meniul fără a face nimic.

8. Bara de conexiune nativă Microsoft

Ca alternativă la bara AlbatrosRDP, se poate folosi bara de conexiune standard Microsoft, cea din `mstsc.exe`.

8.1 Activare

- Înainte de conectare: debifați **Barra di stato personalizzata** în fereastra de conectare. Alegerea rămâne memorată pentru acel element din istoric.
- În timpul sesiunii: elementul de meniu **Barra RDP nativa**.

La aproximativ o secundă după stabilirea conexiunii, controlul RDP trece la propriul ecran complet și afișează bara Microsoft, fixată și cu butoanele Minimizare, Restaurare și Blocare.

8.2 Diferențe de comportament

- **Ctrl+F11** este dezactivat: combinația ajunge la computerul la distanță.
- Bara personalizată și afișarea ei automată sunt dezactivate.
- **Minimizare** pe bara Microsoft minimizează întreaga sesiune; se redeschide din pictograma de pe bara de activități.
- **Restaurare** pe bara Microsoft trece AlbatrosRDP în **modul fereastră** și nu revine singur la ecran complet. De aici, cu clic dreapta pe bara de titlu, se deschide meniul rapid: **Schermo intero** revine la ecranul complet nativ, iar debifând **Barra RDP nativa** se revine la bara personalizată.
- **X** pe bara Microsoft închide sesiunea. Apare întrebarea "La sessione RDP è stata disconnessa. Riconnettersi al server? (No = chiude l'applicazione)".

9. Modul fereastră

Cu **Schermo ridotto** (meniu) sau cu butonul □ al barei, sesiunea trece într-o fereastră Windows obișnuită, redimensionabilă.

- Starea conexiunii (cu nota și mementoul meniului) este afișată în **titlul ferestrei**, în locul barei de stare.
- Desktopul la distanță păstrează rezoluția cu care a fost deschis și este micșorat pentru a încăpea în fereastră.
- Un **clic dreapta pe bara de titlu** deschide meniul rapid; și Ctrl+F11 continuă să funcționeze (cu bara personalizată).
- În stânga butoanelor de sistem (minimizare, maximizare, închidere) apare un buton suplimentar **Schermo intero** care readuce sesiunea pe ecran complet.

10. Întreruperi, reconectare și erori

10.1 Server care nu mai poate fi accesat în timpul sesiunii

Cât timp sesiunea este conectată, la fiecare 2 secunde programul încearcă să deschidă o conexiune TCP către portul RDP al serverului (timeout 1,5 secunde). Dacă încercarea eșuează, bara devine galbenă cu "Connessione persa su server:porta", chiar dacă controlul RDP nu a detectat încă întreruperea. Redevine verde singură când serverul răspunde din nou. Este cazul tipic al unui tunel SSH căzut.

10.2 Reconectare automată

Pe lângă reconectarea automată internă a controlului RDP, dacă sesiunea apare deconectată după ce a fost conectată cel puțin o dată, AlbatrosRDP:

1. încearcă să se reconecteze cel mult o dată la fiecare **5 secunde**, de fiecare dată după o verificare TCP rapidă (1 secundă);
2. după **3 încercări** consecutive eșuate întreabă: "La riconnessione automatica non riesce (credenziali mancanti/annullate oppure server non disponibile). Continuare a riprovare?". **Sì** reia încercările, **No** închide programul.

10.3 Watchdog (aplicație blocată)

Un control independent verifică dacă interfața răspunde. Dacă rămâne blocată mai mult de **15 secunde** (de exemplu din cauza unei întreruperi de rețea în timpul autentificării RDP), apare deasupra oricărei alte ferestre mesajul "L'applicazione non risponde da diversi secondi... Vuoi forzare la chiusura dell'applicazione?". **Sì** închide programul, **No** continuă să aștepte. Controlul este suspendat cât timp sunt deschise casetele de dialog ale programului.

10.4 Erori neprevăzute

- **Control RDP indisponibil** sau nefuncțional la pornire: apare "Impossibile avviare la connessione RDP:" cu detaliile erorii, apoi programul se închide.
- **Excepție netratată**: mesajul "AlbatrosRDP - Errore" indică eroarea și întreabă "Continuare a usare l'applicazione?". **Sì** permite continuarea fără pierderea sesiunii, **No** închide. Eroarea este întotdeauna înregistrată în jurnal.

10.5 Închidere

- Orice închidere manuală cu sesiunea conectată (meniu, X-ul barei, X-ul ferestrei, Alt+F4, bara de activități) cere confirmare. Răspunzând No, se revine exact la situația anterioară.
- La închidere, programul deconectează sesiunea și așteaptă cel mult 1 secundă ca controlul RDP să o închidă.
- Când închiderea pornește dintr-o casetă de dialog de eroare, este prevăzută o oprire de siguranță: dacă curățarea se blochează, procesul este oricum terminat după 8 secunde.

11. Pornire din linia de comandă

AlbatrosRDP poate deschide o conexiune direct, fără a afișa fereastra de conectare. Parametrii pot fi transmiși în trei moduri: **în clar**, **criptați** într-un singur șir sau într-un **fișier** (în clar sau criptat).

11.1 Parametri de conectare

Parametru	Obligatoriu	Semnificație
`-ip=`	Da	Numele sau adresa serverului. Acceptă și `host:porta` și `[IPv6]:porta`.
`-port=`	Nu	Port TCP (1-65535). Dacă lipsește sau nu este valid: 3389.
`-user=`	Nu	Nume utilizator.
`-domain=`	Nu	Domeniu.
`-pwd=`	Nu	Parola utilizatorului la distanță. Dacă lipsește, o solicită Windows.
`-nota=`	Nu	Notă afișată în bară, titlu și meniu.
`-info=`	Nu	Informație suplimentară afișată în Dati connessione...

Parametru	Semnificație
`-enc=`	Șir criptat (Base64) care conține parametrii din tabelul anterior.
`-file=`	Calea unui fișier care conține parametrii, în clar sau criptați.
`-cryptpwd=`	Parola de decriptare pentru `-enc` sau `-file`. Valoarea specială `pipe` indică faptul că parola sosește printr-un named pipe (secțiunea 11.6).
`-local=true`	Doar informativ: indică faptul că conținutul a fost legat de computer. La citire nu este luat în considerare.

Reguli generale:

- Numele parametrilor nu fac distincție între majuscule și minuscule; cratima inițială este opțională (`ip=` echivalează cu `-ip=`).
- Valorile cu spații trebuie încadrate între ghilimele duble, de preferință întregul argument: `"-nota=Server ufficio"`.
- Ordinea de prioritate: dacă există `-file`, se folosește fișierul; altfel, dacă există `-enc`, șirul criptat; altfel, parametrii individuali.
- Parametrii necunoscuți sunt ignorați.
- Dacă lipsește `-ip` (sau fișierul indicat nu există), programul se comportă ca și cum nu ar avea parametri și deschide fereastra de conectare.
- Conexiunea pornită din linia de comandă folosește bara personalizată și **nu** este adăugată în istoric.

11.2 Parametri în clar

```
AlbatrosRDP.exe -ip=192.168.1.10 -port=3389 -user=Administrator "-nota=Server ufficio"
```

> **Atenție.** O parolă transmisă în clar cu `-pwd=` este vizibilă oricui poate citi linia de comandă a proceselor (Manager activități, Process Explorer, WMI). Pentru a transmite parola, folosiți forma criptată, de preferință cu pipe-ul.

11.3 Parametri criptați

```
AlbatrosRDP.exe "-enc=<stringa Base64>" "-cryptpwd=<chiave>"
```

Șirul `-enc` se generează cu funcțiile de programare descrise în capitolul 12 (`BuildCommandLineArgs`). Programul nu are o funcție interactivă pentru crearea lui.

11.4 Parametri în fișier

```
AlbatrosRDP.exe "-file=C:\Config\Clienti\Cliente1.rdpdat"
AlbatrosRDP.exe "-file=C:\Config\Clienti\Cliente1.rdpdat" "-cryptpwd=<chiave>"
```

Fișierul (UTF-8) poate conține parametrii **în clar**, chiar și pe mai multe rânduri și cu sau fără cratimă, sau un șir **criptat**. Programul recunoaște singur formatul: dacă conținutul este în clar, eventualul `-cryptpwd` este ignorat. Exemplu de fișier în clar scris manual:

```
-ip=192.168.1.10
-port=3389
-user=Administrator
"-nota=Server ufficio"
"-info=Contratto assistenza n. 42"
```

Un fișier criptat se creează cu `BuildCommandLineArgs` indicând calea (capitolul 12). Dacă fișierul există deja, se cere confirmare înainte de suprascriere.

11.5 Parolă de decriptare lipsă sau greșită

Dacă conținutul este criptat și `-cryptpwd` lipsește sau este greșit, apare fereastra **Password richiesta**: "I parametri di connessione sono protetti da password. Tentativo N di 3." (precedat de "Password errata." după o eroare).

- Sunt permise **3 încercări**.
- Cu **Annulla** sau după epuizarea încercărilor, programul **se închide** fără a deschide fereastra de conectare.
- Fiecare decriptare este verificată (rezultatul trebuie să conțină cel puțin `ip`): o parolă greșită nu poate fi confundată cu una corectă.

11.6 Parola prin named pipe

Cu `-cryptpwd=pipe` parola reală nu apare niciodată în linia de comandă, nici măcar pentru o clipă. Programul care pornește AlbatrosRDP i-o transmite printr-un named pipe local:

- numele pipe-ului: `\\.\pipe\AlbatrosRDP_Secret_<PID>`, unde PID este identificatorul procesului AlbatrosRDP tocmai pornit;
- pipe-ul este creat de programul apelant, este accesibil numai utilizatorului Windows curent și acceptă o singură conexiune;
- secretul este transmis numai dacă se conectează exact procesul așteptat (verificarea PID-ului clientului);
- textul circulă în UTF-8 (un eventual BOM este tolerat);
- AlbatrosRDP așteaptă cel mult **5 secunde**: dacă nu primește nimic, cere parola cu fereastra din secțiunea 11.5.

Cel mai simplu mod de a folosi pipe-ul este funcția `StartProcessWithEncryptedArgsAndPipePasswordWait` (capitolul 12), care face totul într-un singur apel.

11.7 Legarea de un singur computer

La momentul creării (`machineBound:=True`), conținutul criptat poate fi legat de computerul curent. În acest caz, cheia efectivă de criptare este formată din ID-ul hardware al computerului urmat de parolă. ID-ul hardware este compus din:

- numărul de serie al plăcii de bază;
- identificatorul procesorului;

- numărul de serie al primului disc fizic.

La citire nu trebuie indicat nimic: programul încearcă mai întâi parola ca atare (conținut valabil pe toate computerele) și apoi combinația cu ID-ul hardware al computerului local, inclusiv variantele datorate ordinii negarantate a discurilor (de exemplu, o unitate flash USB introdusă).

> **Atenție.** Un conținut legat devine imposibil de citit dacă se înlocuiesc placa de bază, procesorul sau discul de sistem și, desigur, pe orice alt computer: în acest caz trebuie regenerat.

12. Integrarea din alte programe

Clasele programului pot fi folosite de o altă aplicație VB.NET, adăugând o referință la `AlbatrosRDP.exe` (versiunea neprotejată) sau incluzând fișierele sursă. Proiectul de exemplu **Test_Lancio_pipe** (aplicație consolă) arată pornirea cu parolă prin pipe.

12.1 Clasa RdpConnectionParams

Proprietate	Tip	Descriere
`Ip`	String	Server (obligatoriu).
`Port`	Integer	Port; 0 = implicit (3389).
`User`, `Domain`	String	Utilizator și domeniu.
`Password`	String	Parola utilizatorului la distanță.
`Nota`, `Info`	String	Notă și informație suplimentară.
`IsValid`	Boolean	True dacă `Ip` are o valoare.
`Clone()`	Funcție	Returnează o copie.

12.2 Clasa RdpCommandLineManager

Metodă (Shared)	Descriere
`BuildCommandLineArgs(prms, [encryptionPassword], [filePath], [machineBound])`	Construiește argumentele. Fără parolă: în clar. Cu parolă: `-enc` + `-cryptpwd`. Cu `filePath`: scrie fișierul (în clar sau criptat, creează folderul, cere confirmare dacă există) și returnează `-file` [+ `-cryptpwd`]. Argumentele sunt deja încadrate între ghilimele conform regulilor Windows.
`BuildCommandLineArgsFromFile(filePath, [encryptionPassword])`	Argumente pentru un fișier deja existent; dacă este indicată parola, verifică mai întâi că fișierul se decriptează. Generează o excepție dacă fișierul nu există sau parola este greșită.
`StartProcessWithEncryptedArgsAndPipePasswordWait(exePath, prms, encryptionPassword, ByRef passwordDelivered, [machineBound], [pipeTimeoutMs=5000])`	Pornește AlbatrosRDP cu `-cryptpwd=pipe`, transmite parola prin pipe și așteaptă livrarea. `passwordDelivered` indică rezultatul. Potrivit pentru lansatoarele care se închid imediat.
`StartProcessWithEncryptedArgsAndPipePassword(exePath, prms, encryptionPassword, [machineBound], [pipeTimeoutMs=5000])`	Ca mai sus, dar livrarea are loc în fundal și metoda revine imediat. Dacă apelantul se închide înainte de livrare, parola nu ajunge.
`ParseCommandLineArgs(args, [ByRef userAborted])`	Interpretează argumentele primite (cu solicitarea interactivă a parolei, dacă este necesar).
`ReadParamsFromFile(filePath, [cryptPwd])`	Citește un fișier de parametri fără casete de dialog; excepție dacă parola este greșită.
`EncryptString(testo, password)` / `DecryptToOriginalString(blob, password)`	Criptare și decriptare de bază, fără legare hardware.
`GetMachineHardwareId()`	ID-ul hardware al computerului curent.

Exemplu: pornire cu parolă prin pipe dintr-un lansator (cheia este conținută într-o variabilă, niciodată scrisă în cod):

```
Dim prms As New RdpConnectionParams With {
    .Ip = "192.168.1.10", .Port = 3389,
    .User = "Administrator", .Nota = "Server ufficio"}

Dim consegnata As Boolean = False
RdpCommandLineManager.StartProcessWithEncryptedArgsAndPipePasswordWait(
    "C:\Albatros\CompiledPrograms\AlbatrosRDP.exe",
    prms, chiave, consegnata)
```

Exemplu: crearea unui fișier criptat legat de computer:

```
Dim argomenti As String = RdpCommandLineManager.BuildCommandLineArgs(
    prms, encryptionPassword:=chiave,
    filePath:="C:\Config\Clienti\Cliente1.rdpdat", machineBound:=True)
' -> "-file=C:\Config\Clienti\Cliente1.rdpdat" "-cryptpwd=..." "-local=true"
```

12.3 Clasa SecretPipeTransfer

Metodă (Shared)	Descriere
`SendSecretToChildProcessAndWait(processo, segreto, [timeoutMs])`	Partea apelantului: creează pipe-ul pentru PID-ul procesului fiu și așteaptă livrarea. Returnează True dacă a fost livrat.
`SendSecretToChildProcess(processo, segreto, [timeoutMs])`	Ca mai sus, în fundal.
`ReceiveSecretForCurrentProcess([timeoutMs])`	Partea AlbatrosRDP: citește secretul din pipe-ul propriului PID.
`ReadSecretFromPipe(nomePipe, [timeoutMs])`	Citire dintr-un pipe cu nume explicit.
`WaitSeconds(n)` / `WaitMilliSeconds(n)`	Așteptare care menține interfața receptivă.

12.4 Formatul criptării

Element	Valoare
Algoritm	AES-256, mod CBC, padding PKCS7
Derivarea cheii	PBKDF2-HMAC-SHA1, 50.000 de iterații, salt aleatoriu de 16 octeți
Format	Base64 din: salt (16 octeți) + IV (16 octeți) + date criptate
Conținut în clar	Parametri în formatul `"-ip=..." "-user=..."` (UTF-8)
Compatibilitate	Identic cu versiunile anterioare: șirurile și fișierele create anterior rămân lizibile și invers

12.5 Personalizări din cod

Element	Descriere
`FrmRDP.New([nativeConnectionBar], [SafeMode])`	Sesiune cu fereastră de conectare.
`FrmRDP.New(server, port, domain, userName, password, [nativeConnectionBar], [SafeMode])`	Sesiune directă, fără fereastră de conectare.
`SafeMode`	Dacă este True, caută mai întâi controlul RDP generic și limitează alegerea la versiunile până la 11.
`FrmRDP.MenuHotkey`	Combinația pentru meniul rapid (implicit `Keys.Control Or Keys.F11`).

Element	Descriere
`FrmRDP.ConnectionNote` / `ConnectionInfo`	Nota și informațiile sesiunii.
`FrmRDP.ShowNativeConnectionBar`	Bară nativă da/nu; setați-o înainte de `ShowDialog()`.
`Module1.PercorsoStorico`	Calea fișierului de istoric.
`Module1.MaxCronologRDP`	Numărul maxim de elemente în istoric (implicit 20).

13. Setări RDP aplicate

La deschiderea fiecărei sesiuni se aplică următoarele setări, în formatul fișierelor `.rdp`. Sunt definite în cod (șirul `rdpSettingsString` din FrmRDP); nu există un fișier de configurare extern.

Setare	Efect
`session bpp:i:32`	Culori pe 32 de biți.
`compression:i:1`	Comprimarea datelor activă.
`disable wallpaper:i:1`	Fundalul desktopului la distanță nu este afișat (lățime de bandă mai mică).
`keyboardhook:i:2`	Combinațiile de taste Windows sunt trimise computerului la distanță numai pe ecran complet (valoare implicită).
`audiomode:i:0`	Sunetul la distanță este redat pe computerul local.
`audiocapturemode:i:1`	Microfonul local este disponibil în sesiunea la distanță.
`redirectprinters:i:1`	Imprimantele locale sunt disponibile în sesiune.
`redirectsmartcards:i:1`	Smart cardurile locale sunt disponibile.
`redirectclipboard:i:1`	Clipboard partajat între local și la distanță.
`drivestoredirect:s:*`	Toate unitățile locale sunt vizibile în sesiunea la distanță.
`negotiate security layer:i:1`	Negocierea automată a celui mai robust protocol de securitate.
`screen mode id`, `use multimon`	Ignorate: ecranul complet este gestionat de program, pe un singur monitor.

Imediat după aceea, programul mai setează:

- **reconectarea automată** a controlului RDP activă (înlocuiește `autoreconnection enabled:i:0` din șir);
- **nivelul de autentificare 0** și avertismentele privind certificatul ignorate (înlocuiește `authentication level:i:2`): certificatul serverului nu este verificat și nu apare niciun avertisment;
- **CredSSP** activ (necesar pentru autentificarea NLA);
- **timeout-ul** de conectare: 8 secunde în total, 5 pentru fiecare încercare.

Programul poate interpreta și alte chei `.rdp` (de exemplu `alternate shell` și `shell working directory` pentru a porni un singur program în locul desktopului, `connection type`, `networkautodetect`, `redirectcomports` și setările gateway-ului RD `gatewayhostname`, `gatewayusagemethod` și altele similare): pentru a le folosi, trebuie modificat șirul din cod și recompilat programul.

14. Securitate și confidențialitate

- **Parola** utilizatorului la distanță nu este salvată niciodată pe disc: nici în istoric, nici în jurnal. După transmiterea către controlul RDP, copiile din memorie sunt șterse.
- **Jurnalul** înregistrează doar modul de pornire, stările conexiunii și erorile: niciodată parole, chei sau parametri.
- **Criptarea** folosește AES-256 cu cheie derivată prin PBKDF2. Bufferele cu date sensibile sunt golite după utilizare.
- **Pipe-ul** este accesibil numai utilizatorului curent, transmite secretul numai procesului așteptat și este de unică folosință.
- **Certificatul serverului nu este verificat** (secțiunea 13). Protecția împotriva interceptărilor depinde, așadar, de canal: rețea de încredere, VPN sau tunel SSH. Evaluați dacă păstrați această setare.
- O parolă transmisă în clar cu `-pwd=` este vizibilă în lista proceselor (secțiunea 11.2).
- Verificarea accesibilității în timpul sesiunii deschide o conexiune TCP către portul RDP la fiecare 2 secunde: pe server aceasta generează evenimente în jurnalul RDP (RdpCoreTS) și puțin trafic în tunel.

15. Jurnal de diagnosticare

Jurnalul se află în `%LOCALAPPDATA%\Albatros\AlbatrosRDP\AlbatrosRDP.log`. Când depășește 1 MB, este redenumit în `AlbatrosRDP.1.log` (înlocuind copia anterioară) și se reia de la început. Fiecare rând are formatul:

```
2026-10-11 14:22:05.123 [4812] INFO  Stato RDP: connesso
```

adică data și ora, PID-ul procesului, nivelul (INFO, WARN, ERROR) și mesajul. Se înregistrează:

- pornirea (versiunea și numărul de argumente) și închiderea aplicației;
- modul liniei de comandă (în clar, criptat, fișier) și rezultatul (parametri valizi, nevalizi, parolă anulată sau greșită);
- serverul, portul, controlul RDP utilizat și tipul de bară;
- schimbările de stare ale sesiunii, cu codul extins al motivului deconectării;
- încercările de reconectare eșuate, intervențiile watchdog-ului, erorile și excepțiile netratate;
- închiderea sesiunii cu motivul.

16. Depanare

Problemă	Ce trebuie făcut
La pornire apare "Impossibile avviare la connessione RDP"	Controlul RDP Windows lipsește sau nu funcționează. Verificați dacă funcționează Conexiune desktop la distanță (`mstsc.exe`) și consultați jurnalul.
"Impossibile raggiungere il server"	Verificați tunelul SSH, VPN-ul, firewallul, adresa și portul. Cu un tunel local, verificați dacă este activ înainte de conectare.
Programul se închide cu "La connessione RDP non è stata stabilita"	Acreditări anulate sau greșite, sau rețea absentă în timpul autentificării. Reîncercați verificând utilizatorul, domeniul și parola.
Bară galbenă cu "Connessione persa su ..."	Serverul nu mai răspunde pe portul RDP: de obicei tunelul a căzut. Bara redevine verde singură la restabilire.
Ctrl+F11 nu deschide meniul	Este activă bara nativă Microsoft (Ctrl+F11 dezactivat). Folosiți clic dreapta pe bara de titlu în modul fereastră.
Bara de stare nu se vede	A fost ascunsă (dublu clic sau meniu): duceți mouse-ul la marginea superioară sau folosiți Ctrl+F11 > Barra di stato. Bara se vede numai dacă AlbatrosRDP este aplicația activă.
Pornire cu `-cryptpwd=pipe` și solicitarea parolei	Parola nu a sosit în 5 secunde. Probabil lansatorul s-a închis înainte de livrare: folosiți `StartProcessWithEncryptedArgsAndPipePasswordWait`.
Parolă corectă, dar "Password errata" cu un conținut legat	S-a schimbat hardware-ul (placa de bază, procesorul, discul) sau se folosește alt computer: regenerați conținutul criptat.
Cu `-ip` prezent se deschide totuși fereastra de conectare	Parametrul nu a fost recunoscut: verificați utilizarea ghilimelelor duble și, cu `-file`, existența fișierului.
Istoricul nu se actualizează	Lipsesc permisiunile de scriere pe fișierul din ProgramData (secțiunea 2.3).
Istoricul a dispărut	Fișierul nu putea fi citit: a fost salvată o copie `.corrupt-<data>.bak` în același folder.
Fundalul desktopului la distanță nu apare (culoare uniformă)	Este intenționat (`disable wallpaper:i:1`, capitolul 13).
"L'applicazione non risponde da diversi secondi"	Programul este blocat de peste 15 secunde, de obicei din cauza unei căderi de rețea în timpul autentificării. Sì închide programul, No continuă să aștepte.

Anexa A. Mesajele programului

Mesaj	Semnificație și răspunsuri
Verifica raggiungibilità server:porta... (Verificare accesibilitate server:port...)	Test TCP în curs înainte de conectare.
Connessione in corso... (Conectare în curs...)	Controlul RDP stabilește sesiunea.
--> server:porta (bară verde)	Sesiune conectată.
Connessione persa su server:porta (Conexiune pierdută pe server:port)	Serverul nu răspunde la testul TCP periodic.
Connessione RDP non attiva (Conexiune RDP inactivă)	Sesiune deconectată; reconectare automată în curs.
Riconnessione in corso... / Disconnessione in corso... (Reconectare în curs... / Deconectare în curs...)	Efectul elementului Riconnetti sau al închiderii.
Errore di connessione / Errore di riconnessione (Eroare de conectare / Eroare de reconectare)	Controlul RDP a refuzat cererea de conectare.
Impossibile raggiungere il server ... Riprovare? (Serverul nu poate fi accesat ... Reîncercați?)	Sì = verificare nouă; No = închidere.
La connessione RDP non è stata stabilita ... L'applicazione verrà chiusa. (Conexiunea RDP nu a fost stabilită ... Aplicația va fi închisă.)	Prima conexiune nu a reușit niciodată (acreditări sau rețea).
La riconnessione automatica non riesce ... Continuare a riprovare? (Reconectarea automată nu reușește ... Continuați să reîncercați?)	După 3 încercări eșuate. Sì = continuă; No = închidere.
La sessione RDP è stata disconnessa. Riconnettersi al server? (Sesiunea RDP a fost deconectată. Vă reconectați la server?)	Sesiune închisă din bara nativă sau de server. Sì = reconectare; No = închidere.
Disconnettere la sessione RDP e chiudere l'applicazione? (Deconectați sesiunea RDP și închideți aplicația?)	Confirmare de închidere. Implicit: No.
L'applicazione non risponde da diversi secondi ... (Aplicația nu răspunde de câteva secunde ...)	Watchdog. Sì = închidere forțată; No = așteptare.
AlbatrosRDP - Errore ... Continuare a usare l'applicazione? (AlbatrosRDP - Eroare ... Continuați să folosiți aplicația?)	Excepție netratată. Sì = continuă; No = închidere.
Password richiesta - Tentativo N di 3 (Parolă necesară - Încercarea N din 3)	Parametri criptați: introduceți parola de decriptare.
Il file ... esiste già. Sovrascrivere? (Fișierul ... există deja. Îl suprascrieți?)	Crearea unui fișier de parametri din cod.

Anexa B. Referință rapidă

B.1 Taste și mouse

Comandă	Efect
Ctrl+F11	Deschide meniul rapid (numai cu bara personalizată).
Esc cu meniul deschis	Închide meniul.
Clic dreapta pe bara de stare	Deschide meniul rapid.
Clic dreapta pe bara de titlu	Deschide meniul rapid (modul fereastră).
Dublu clic pe bara de stare	Ascunde bara.
Mouse-ul la marginea superioară	Reafișează bara ascunsă.
Glisarea barei de stare	O mută.
Enter / Esc în fereastra de conectare	Connetti / Annulla.

B.2 Linia de comandă

```
AlbatrosRDP.exe -ip=<server> [-port=<porta>] [-user=<utente>] [-domain=<dominio>]
                [-pwd=<password>] ["-nota=<testo>"] ["-info=<testo>"]

AlbatrosRDP.exe "-enc=<Base64>" "-cryptpwd=<chiave>|pipe"

AlbatrosRDP.exe "-file=<percorso>" ["-cryptpwd=<chiave>|pipe"]
```

B.3 Valori de timp

Control	Valoare
Verificarea inițială a accesibilității	2,5 s
Verificare în timpul sesiunii	la fiecare 2 s, timeout 1,5 s
Interval minim între încercările de reconectare	5 s
Încercări înainte de întrebarea "Continuare a riprovare?"	3
Așteptare inițială înainte de a considera conexiunea eșuată	15 s
Watchdog	15 s de blocare (verificare la fiecare 2 s)
Activarea barei native după conectare	1 s
Așteptarea parolei prin pipe	5 s
Oprire de siguranță la închidere	8 s

AlbatrosRDP

リモート デスクトップ クライアント

操作および統合マニュアル

バージョン 2.0.162.6127 — 2026 年 10 月

© Raffaele Romano 2026

目次

1. はじめに 109

1.1 主な機能 109

1.2 対象バージョン 109

2. 要件とインストール 110

2.1 要件 110

2.2 配布するファイル 110

2.3 プログラムが使用するファイルとフォルダー 110

3. クイック スタート 111

4. 接続ウィンドウ 112

4.1 フィールドとボタン 112

4.2 接続前のチェック 112

4.3 履歴のしくみ 113

5. リモート セッション 114

5.1 セッションの開始 114

5.2 全画面表示時の動作 114

6. カスタム ステータス バー 115

6.1 テキストと色 115

6.2 ボタン 115

6.3 マウスでの操作 115

6.4 バーの非表示と自動表示 115

7. クイック メニュー 116

7.1 開き方 116

7.2 メニュー項目 116

8. Microsoft のネイティブ接続バー 117

8.1 有効化 117

8.2 動作の違い 117

9. ウィンドウ モード 118

10. 中断、再接続、エラー 119

10.1 セッション中にサーバーに到達できなくなった場合 119

10.2 自動再接続 119

10.3 ウォッチドッグ (アプリケーションの応答停止)....119
10.4 予期しないエラー....119
10.5 終了....119

11. コマンド ラインからの起動....121

11.1 接続パラメーター....121
11.2 平文のパラメーター....121
11.3 暗号化されたパラメーター....122
11.4 ファイルによるパラメーター....122
11.5 復号パスワードがない、または間違っている場合....122
11.6 名前付きパイプによるパスワードの受け渡し....122
11.7 特定のコンピューターへの限定....123

12. 他のプログラムからの統合....124

12.1 RdpConnectionParams クラス....124
12.2 RdpCommandLineManager クラス....124
12.3 SecretPipeTransfer クラス....125
12.4 暗号化の形式....125
12.5 コードによるカスタマイズ....126

13. 適用される RDP 設定....127

14. セキュリティと機密性....128

15. 診断ログ....129

16. トラブルシューティング....130

付録 A. プログラムのメッセージ....131

付録 B. クイック リファレンス....132

B.1 キーとマウス....132
B.2 コマンド ライン....132
B.3 時間の値....132

1. はじめに

AlbatrosRDP は Windows 用のリモート デスクトップ (RDP) クライアントで、.NET Framework 4.8 上の VB.NET で開発されています。Microsoft の ActiveX コントロール (`mstscax.dll`)、つまりリモート デスクトップ接続 (`mstsc.exe`) と同じエンジンを使用し、日常的な利用や SSH トンネル経由の接続のための一連の機能を追加しています。

1.1 主な機能

- 最近の接続の**履歴** (パスワードは保存されません) と、接続ごとの自由記述の**メモ**を備えた接続ウィンドウ。
- **全画面**のセッションと**フローティング ステータス バー**: 状態に応じて色分けされ、ドラッグ可能で、自動的に隠れます。
- 代わりに、Microsoft の**ネイティブ接続バー**も使用できます。
- **クイック メニュー**: **Ctrl+F11**、ステータス バーまたはタイトル バーの右クリックで呼び出せます。
- **到達可能性の確認**: 接続前、およびセッション中は 2 秒ごとにサーバーへの到達可能性を確認します。
- **自動再接続**: セッションが切断されたときに自動的に再接続します。
- **ウォッチドッグ**: アプリケーションが応答しなくなった場合 (たとえば認証中のネットワーク切断など)、強制終了を提案します。
- **コマンド ラインからの直接起動**: 平文、暗号化 (AES-256)、またはファイルから読み込んだパラメーターを使用できます。復号パスワードは名前付きパイプ経由でも渡すことができ、その場合コマンド ラインに表示されることはありません。
- 暗号化されたパラメーターを**特定のコンピューター** (ハードウェア ID) に限定するオプション。
- **診断ログ**: パスワード、キー、パラメーターが記録されることはありません。

1.2 対象バージョン

項目	値
プログラム	AlbatrosRDP
バージョン	2.0.162.6127 (2026 年 10 月リビジョン)
プラットフォーム	.NET Framework 4.8、Windows Forms、VB.NET

項目	値
RDP エンジン	Microsoft RDP ActiveX コントロール (MSTSCLib)、バージョン 6 〜 14
作成者	© Raffaele Romano 2026

2. 要件とインストール

2.1 要件

- Microsoft リモート デスクトップ クライアントがインストールされた Windows (`mstscax.dll`。Windows のデスクトップ版およびサーバー版には標準で含まれています)。
- .NET Framework 4.8。
- 指定した TCP ポート (既定値 **3389**) で RDP サーバーに、直接またはトンネル経由でネットワーク アクセスできること。

セッション開始時に、プログラムはシステムに登録されている最新の RDP コントロールを検索します (`MsRdpClient14` から `MsRdpClient6` まで)。各バージョンは実際に作成されて検証され、動作しない場合は破棄されて 1 つ前のバージョンに進みます。使用されたバージョンは **Dati connessione...** メニューとログで確認できます。

2.2 配布するファイル

このプログラムにはインストールは不要で、フォルダー (たとえば `C:\Albatros\CompiledPrograms\`) にコピーするだけです。プロジェクトでは 2 つのバージョンが作成されます:

ビルド フォルダー	コピーする内容
`bin\Release\AlbatrosRDP_Secure\`	.NET Reactor で保護されたバージョン。ライブラリ `Interop.MSTSCLib.dll`、`AxInterop.MSTSCLib.dll`、`Newtonsoft.Json.dll` は埋め込まれているため、`AlbatrosRDP.exe` だけで動作します。配布にはこのバージョンを推奨します。
`bin\Release\`	保護されていないバージョン: `AlbatrosRDP.exe`、`AlbatrosRDP.exe.config`、および上記の 3 つの DLL をコピーします。

2.3 プログラムが使用するファイルとフォルダー

パス	用途
`C:\ProgramData\Albatros\Common\CronologRDP.txt`	接続履歴 (JSON)。コンピューターのすべてのユーザーで共通です。
`%LOCALAPPDATA%\Albatros\AlbatrosRDP\AlbatrosRDP.log`	現在のユーザーの診断ログ。1 つ前のコピーは `AlbatrosRDP.1.log` です。
`CronologRDP.txt.corrupt-<data>.bak`	履歴のバックアップ コピー。ファイルが読み取れない場合にのみ作成されます。

> **同じコンピューターで複数のユーザーが使用する場合。** ProgramData の既定のアクセス許可では、あるユーザーが作成した履歴ファイルを他のユーザーは変更できないため、他のユーザーの履歴は更新されません。必要に応じて、管理者は次のコマンドで Users グループに変更権限を付与できます: `icacls "C:\ProgramData\Albatros\Common" /grant *S-1-5-32-545:(OI)(CI)M`

3. クイック スタート

1. パラメーターを指定せずに `AlbatrosRDP.exe` を起動します。接続ウィンドウが開きます。
2. **Computer** (サーバーの名前またはアドレス)、**Porta**、**Nome utente**、必要に応じて **Dominio** と **Note** を入力し、最後に **Password** を入力します。以前に使用したサーバーの場合は、**Cronologia** から選択してパスワードを入力するだけです。
3. **Connetti** (接続) をクリックします (または Enter キーを押します)。
4. プログラムはサーバーに到達できることを確認し、全画面でセッションを開きます。Windows が資格情報を要求した場合 (NLA)、システムのウィンドウに入力します。
5. 画面上部中央にステータス バーが表示されます。セッションがアクティブなときは緑色です。
6. メニューを表示するには **Ctrl+F11** を押します (またはステータス バーを右クリックします)。
7. 終了するには、メニューから **Disconnetti & Exit** を選択するか、バーの赤い **X** をクリックして確認します。

4. 接続ウィンドウ

コマンド ラインに有効なパラメーターを指定せずにプログラムを起動すると開きます。Windows のリモート デスクトップ接続に似たスタイルです。

> **ラベルの言語。** このウィンドウは英語、イタリア語、フランス語、ルーマニア語に翻訳されていますが、現在のバージョンでは言語が**英語**に固定されています。表には画面に表示される英語のラベルも記載しています。

4.1 フィールドとボタン

フィールド	画面上のラベル	説明
Cronologia	History	最近の接続の一覧で、形式は `server:porta {utente}` です。選択のみ可能で、入力はできません。最初の項目 -- Nuova connessione -- を選ぶとフィールドが空になります。開いたときには最新の接続が選択されています。
✖ (履歴の横)	—	確認後、選択した項目を履歴から削除します。
Computer	Computer	ホスト名、IPv4 アドレス、または IPv6 アドレス。`host:porta` および `[IPv6]:porta` も指定でき、ここに書いたポートは Porta フィールドより優先されます。角かっこのない IPv6 はポートなしとして扱われます。
Porta	Port	数字のみ、1 ～ 65535。空の場合は 3389 が使用されます。
Nome utente	User name	リモート セッションのユーザー。
Dominio	Domain	ユーザーのドメイン (省略可能)。
Note	Notes	ステータス バー、ウィンドウのタイトル、メニューの先頭に表示される自由記述のテキスト。履歴に保存されます。
Password	Password	リモート ユーザーのパスワード。保存されることはありません。空のままにすると、接続時に Windows が要求します。
Mostra password	Show password	入力したパスワードを平文で表示します。
Barra di stato personalizzata	Customized Status Bar	オン (既定): AlbatrosRDP のステータス バー。オフ: Microsoft のネイティブ バー (第 8 章)。この選択は履歴の項目ごとに記憶されます。
Connetti	Connect	接続を開始します (Enter キー)。

フィールド	画面上のラベル	説明
Annulla	Cancel	接続せずにプログラムを終了します (Esc キー)。

履歴から項目を選択すると、カーソルはパスワードに直接移動します。それ以外の場合は Computer フィールドに移動します。左下には著作権表示とバージョンが表示されます。

4.2 接続前のチェック

- Computer が空: "Specificare l'indirizzo del computer." (コンピューターのアドレスを指定してください。)
- Computer フィールドのポートが無効 (例: `server:99999`): "Porta non valida nel campo Computer: indicare un numero compreso tra 1 e 65535 (es. server:3389)." (Computer フィールドのポートが無効です: 1 〜 65535 の数値を指定してください (例: server:3389)。)
- Porta フィールドのポートが無効: "Porta non valida: indicare un numero compreso tra 1 e 65535." (ポートが無効です: 1 〜 65535 の数値を指定してください。)

4.3 履歴のしくみ

- 項目は **サーバー + ポート + ユーザー名 + ドメイン** によって識別され、大文字と小文字は区別されません。
- メモとバーの選択は項目に付随しますが、項目の識別には使用されません。常に最後に使用した値が有効です。
- 既に存在する接続は一覧の末尾に移動され、最新の接続になります。
- 保持される項目は最大 **20** 件です。これを超えると古いものから削除されます。
- 保存は Connetti をクリックしたときに行われます。保存はアトミックで、プロセス間ロックによって保護されているため、同時に開いた 2 つのインスタンスが互いの項目を消してしまうことはありません。
- パスワードがファイルに書き込まれることはありません。

5. リモート セッション

5.1 セッションの開始

1. ウィンドウは現在のモニター上で、タスク バーの領域も含めて**全画面**表示になります。ウィンドウのタイトルはメモ、またはメモがない場合は "AlbatrosRDP" です。
2. リモート デスクトップはモニターの解像度で要求されます。使用されるモニターは 1 台のみです。
3. 到達可能性の確認: サーバーとポートに対してテスト用の TCP 接続を行います。タイムアウトは 2.5 秒です (DNS の名前解決を含み、IPv4 と IPv6 のアドレスは並行して試行されます)。バーには "Verifica raggiungibilità server:porta..." (サーバー:ポートの到達可能性を確認中...) と表示されます。
4. サーバーが応答しない場合は "Impossibile raggiungere il server ... (tunnel SSH non attivo oppure rete non disponibile). Riprovare?" (サーバー ... に到達できません (SSH トンネルが無効か、ネットワークが利用できません)。再試行しますか?) と表示されます。**はい** を選ぶと確認を繰り返し、**いいえ** を選ぶとプログラムが終了します。
5. サーバーが応答すると RDP 接続が開始されます ("Connessione in corso..." (接続中...))。サーバーが資格情報を要求すると、Windows が独自のウィンドウを表示します。この段階では、そのウィンドウを隠さないように、AlbatrosRDP はキーボード処理を一時停止し、最前面に表示されたままにはなりません。
6. 接続が確立されるとバーが緑色になり、`--> server:porta` と表示されます。

セッションが接続状態にまったく到達しない場合 (資格情報のキャンセルや誤り、ネットワークなし)、プログラムは無限に再試行することはしません。"La connessione RDP non è stata stabilita (Credenziali mancanti/annullate oppure errore di rete). L'applicazione verrà chiusa." (RDP 接続を確立できませんでした (資格情報がないかキャンセルされたか、ネットワーク エラーです)。アプリケーションを終了します。) と表示して終了します。

5.2 全画面表示時の動作

- ウィンドウが他のウィンドウより前面に表示されるのは、**アクティブなときだけ**です。Alt+Tab や他のアプリケーションのクリックで、通常どおり他のプログラムに切り替えられます。
- ステータス バーは、AlbatrosRDP がアクティブなアプリケーションのときにのみ表示されます。
- リモートの内容はウィンドウに合わせて調整されます (スマート サイズ変更)。縮小したウィンドウ モードでは、リモート デスクトップはスクロール バーなしで比例的に縮小されます。

6. カスタム ステータス バー

全画面モードで、**Barra di stato personalizzata** オプションが有効なときに、画面上部中央に表示される角の丸いバーです。

6.1 テキストと色

テキストは、メモ (ある場合)、メニュー キーの案内、状態で構成されます。例: `Server ufficio - (Ctrl+F11 menu) - --> 192.168.1.10:3389`。

色	意味
背景が緑、テキストが黄	セッションが接続済みで、サーバーに到達可能。
背景が黄、テキストが赤	その他のすべての状態: 確認中、接続中、接続の喪失、エラー。

6.2 ボタン

ボタン	動作
— (黄)	最小化します。
☐ (黄)	全画面とウィンドウを切り替えます。
X (赤)	Disconnetti & Exit と同じです。セッションが接続中の場合は確認を求めてから終了します。

6.3 マウスでの操作

- **ドラッグ** (左ボタン): バーを画面上の任意の位置に移動でき、選択した位置に留まります。
- **右クリック**: クイック メニューを開きます。
- **ダブルクリック**: バーを非表示にします (メニュー項目 Barra di stato と同じ)。

6.4 バーの非表示と自動表示

手動で (ダブルクリックまたはメニューで) 非表示にしたバーは、次の 3 つの方法で再表示できます:

- クイック メニュー (Ctrl+F11) の **Barra di stato** 項目から。

- **Mostra barra al passaggio mouse in alto** オプションが有効な場合 (既定で有効)、マウスを画面の**上端から 10 ピクセル以内**に移動する。この場合、マウスがバーの下 20 ピクセルを超えて離れると、バーは再び非表示になります。
- 全画面モードを終了して再度入る、または最小化したウィンドウを元に戻す。

7. クイック メニュー

7.1 開き方

- **Ctrl+F11**: カスタム バーでのみ機能します。このキーの組み合わせは横取りされ、リモート コンピューターには送られません。ネイティブ バーが有効な場合は無効になり、リモート セッションに渡されます。
- **ステータス バーの右クリック** (全画面時)。
- **タイトル バーの右クリック** (ウィンドウ モード時)。Windows のシステム メニューの代わりに表示されます。

メニューは、外側のクリック、**Chiudi tendina** 項目、または **Esc** キーで閉じます。メニューが開いている間、Esc キーはリモート セッションに送られません。

7.2 メニュー項目

項目	機能
メモ (太字)	メモがある場合にのみ表示されます。クリックすると、メモを編集するための "Nota di connessione" (接続メモ) ウィンドウが開きます。新しいメモは現在のセッションに適用され、バーとタイトルがすぐに更新されます。履歴には保存されません。
Schermo ridotto / Schermo intero	全画面モードとウィンドウを切り替えます (第 9 章)。
Riduci a icona	セッションのウィンドウを最小化します。
Barra di stato	ステータス バーの表示/非表示を切り替えます。全画面時のみ使用できます。
Mostra barra al passaggio mouse in alto	バーの自動表示を有効/無効にします (6.4 節)。
Barra RDP nativa	Microsoft のネイティブ接続バーに切り替えるか、カスタム バーに戻します (第 8 章)。
Dati connessione...	メモ、情報 (`-info` パラメーター)、サーバー、ポート、ユーザー、ドメイン、状態、使用中の RDP コントロールとそのバージョン、著作権表示、プログラムのバージョンを表示します。
Riconnetti	セッションがまだ開いている場合は閉じ (最大 5 秒待機)、再度開きます。セッションが応答しない場合に便利です。

項目	機能
Disconnetti & Exit	"Disconnettere la sessione RDP e chiudere l'applicazione?" (RDP セッションを切断してアプリケーションを終了しますか?) と確認し (既定: いいえ)、確認すると切断して終了します。
Chiudi tendina	何もせずにメニューを閉じます。

8. Microsoft のネイティブ接続バー

AlbatrosRDP のバーの代わりに、Microsoft の標準接続バー (`mstsc.exe` のもの) を使用できます。

8.1 有効化

- 接続前: 接続ウィンドウで **Barra di stato personalizzata** のチェックを外します。この選択は履歴のその項目に記憶されます。
- セッション中: メニュー項目 **Barra RDP nativa**。

接続が確立されてから約 1 秒後に、RDP コントロールが独自の全画面表示に切り替わり、Microsoft のバーが表示されます。バーは固定され、最小化、元に戻す、ピン留めの各ボタンがあります。

8.2 動作の違い

- **Ctrl+F11** は無効になり、このキーの組み合わせはリモート コンピューターに送られます。
- カスタム バーとその自動表示は無効になります。
- **最小化**: Microsoft のバーで最小化すると、セッション全体が最小化されます。タスク バーのアイコンから再度開きます。
- **元に戻す**: Microsoft のバーで元に戻すと、AlbatrosRDP は**ウィンドウ モード**になり、自動的に全画面に戻ることはありません。ここでタイトル バーを右クリックするとクイック メニューが開きます。**Schermo intero** でネイティブの全画面に戻り、**Barra RDP nativa** のチェックを外すとカスタム バーに戻ります。
- **X**: Microsoft のバーの X でセッションが閉じます。"La sessione RDP è stata disconnessa. Riconnettersi al server? (No = chiude l'applicazione)" (RDP セッションが切断されました。サーバーに再接続しますか? (いいえ = アプリケーションを終了)) という確認が表示されます。

9. ウィンドウ モード

Schermo ridotto (メニュー) またはバーの □ ボタンで、セッションはサイズ変更可能な通常の Windows のウィンドウに切り替わります。

- 接続の状態 (メモとメニューの案内を含む) は、ステータス バーの代わりに**ウィンドウのタイトル**に表示されます。
- リモート デスクトップは開いたときの解像度を維持し、ウィンドウに収まるように縮小されます。
- **タイトル バーの右クリック**でクイック メニューが開きます。Ctrl+F11 も引き続き機能します (カスタム バー使用時)。
- システム ボタン (最小化、最大化、閉じる) の左側に、セッションを全画面に戻す追加の **Schermo intero** ボタンが表示されます。

10. 中断、再接続、エラー

10.1 セッション中にサーバーに到達できなくなった場合

セッションが接続されている間、プログラムは 2 秒ごとにサーバーの RDP ポートへの TCP 接続を試みます (タイムアウト 1.5 秒)。試行に失敗すると、RDP コントロールがまだ切断を検出していなくても、バーは黄色になり "Connessione persa su server:porta" (サーバー:ポートへの接続が失われました) と表示されます。サーバーが再び応答すると自動的に緑色に戻ります。SSH トンネルが切断された場合の典型的な例です。

10.2 自動再接続

RDP コントロール内部の自動再接続に加えて、少なくとも 1 回接続された後にセッションが切断状態になると、AlbatrosRDP は次のように動作します:

1. 最大で **5 秒**ごとに再接続を試みます。毎回、事前に短い TCP チェック (1 秒) を行います。
2. **3 回**連続して失敗すると、"La riconnessione automatica non riesce (credenziali mancanti/annullate oppure server non disponibile). Continuare a riprovare?" (自動再接続に失敗しています (資格情報がないかキャンセルされたか、サーバーが利用できません)。再試行を続けますか?) と確認します。**はい** で試行を再開し、**いいえ** でプログラムを終了します。

10.3 ウォッチドッグ (アプリケーションの応答停止)

独立したチェックにより、インターフェイスが応答しているかどうかを確認します。**15 秒**を超えて応答しない場合 (たとえば RDP 認証中のネットワーク中断など)、すべてのウィンドウの前面に "L'applicazione non risponde da diversi secondi... Vuoi forzare la chiusura dell'applicazione?" (アプリケーションが数秒間応答していません... アプリケーションを強制終了しますか?) というメッセージが表示されます。**はい** でプログラムを終了し、**いいえ** で待機を続けます。プログラムのダイアログが開いている間、このチェックは一時停止します。

10.4 予期しないエラー

- **RDP コントロールが利用できない**、または起動時に動作しない場合: エラーの詳細とともに "Impossibile avviare la connessione RDP:" (RDP 接続を開始できません:) と表示され、プログラムが終了します。

- **ハンドルされない例外**: "AlbatrosRDP - Errore" メッセージにエラーが表示され、"Continuare a usare l'applicazione?" (アプリケーションの使用を続けますか?) と確認されます。**はい** を選ぶとセッションを失わずに続行でき、**いいえ** を選ぶと終了します。エラーは常にログに記録されます。

10.5 終了

- セッションが接続中に手動で終了する場合 (メニュー、バーの X、ウィンドウの X、Alt+F4、タスク バー)、必ず確認を求めます。「いいえ」と答えると、元の状態にそのまま戻ります。
- 終了時、プログラムはセッションを切断し、RDP コントロールがセッションを閉じるのを最大 1 秒待ちます。
- エラー ダイアログから終了する場合は安全停止機能があり、クリーンアップが停止しても 8 秒後にプロセスは強制的に終了されます。

11. コマンド ラインからの起動

AlbatrosRDP は、接続ウィンドウを表示せずに直接接続を開くことができます。パラメーターは、**平文**、1 つの文字列に**暗号化**、または**ファイル** (平文または暗号化) の 3 つの方法で渡すことができます。

11.1 接続パラメーター

パラメーター	必須	意味
`-ip=`	はい	サーバーの名前またはアドレス。`host:porta` および `[IPv6]:porta` も指定できます。
`-port=`	いいえ	TCP ポート (1 ～ 65535)。指定がないか無効な場合: 3389。
`-user=`	いいえ	ユーザー名。
`-domain=`	いいえ	ドメイン。
`-pwd=`	いいえ	リモート ユーザーのパスワード。指定がない場合は Windows が要求します。
`-nota=`	いいえ	バー、タイトル、メニューに表示されるメモ。
`-info=`	いいえ	Dati connessione... に表示される追加情報。

パラメーター	意味
`-enc=`	前の表のパラメーターを含む暗号化された文字列 (Base64)。
`-file=`	パラメーターを含むファイルのパス (平文または暗号化)。
`-cryptpwd=`	`-enc` または `-file` の復号パスワード。特別な値 `pipe` は、パスワードが名前付きパイプ経由で渡されることを示します (11.6 節)。
`-local=true`	情報提供のみ: 内容がコンピューターに限定されていることを示します。読み取り時には考慮されません。

一般的な規則:

- パラメーター名では大文字と小文字は区別されず、先頭のハイフンは省略可能です (`ip=` は `-ip=` と同じです)。
- スペースを含む値は二重引用符で囲みます。引数全体を囲むことを推奨します: `"-nota=Server ufficio"`。

- 優先順位: `-file` があればファイルを使用し、なければ `-enc` があれば暗号化文字列を、それもなければ個別のパラメーターを使用します。
- 不明なパラメーターは無視されます。
- `-ip` がない場合 (または指定したファイルが存在しない場合)、プログラムはパラメーターがないものとして動作し、接続ウィンドウを開きます。
- コマンド ラインから開始した接続はカスタム バーを使用し、履歴には追加され**ません**。

11.2 平文のパラメーター

```
AlbatrosRDP.exe -ip=192.168.1.10 -port=3389 -user=Administrator "-nota=Server ufficio"
```

> **注意。** `-pwd=` で平文で渡したパスワードは、プロセスのコマンド ラインを読み取れるすべてのユーザー (タスク マネージャー、Process Explorer、WMI) から見えます。パスワードを渡すには暗号化形式を使用し、できればパイプを併用してください。

11.3 暗号化されたパラメーター

```
AlbatrosRDP.exe "-enc=<stringa Base64>" "-cryptpwd=<chiave>"
```

`-enc` 文字列は、第 12 章で説明するプログラミング用の関数 (`BuildCommandLineArgs`) で生成します。プログラムには、この文字列を対話的に作成する機能はありません。

11.4 ファイルによるパラメーター

```
AlbatrosRDP.exe "-file=C:\Config\Clienti\Cliente1.rdpdat"
AlbatrosRDP.exe "-file=C:\Config\Clienti\Cliente1.rdpdat" "-cryptpwd=<chiave>"
```

ファイル (UTF-8) には、**平文**のパラメーター (複数行、ハイフンの有無を問わず) か、**暗号化**された文字列を記述できます。プログラムは形式を自動的に認識し、内容が平文の場合は `-cryptpwd` が指定されていても無視されます。手書きの平文ファイルの例:

```
-ip=192.168.1.10
-port=3389
-user=Administrator
"-nota=Server ufficio"
"-info=Contratto assistenza n. 42"
```

暗号化ファイルは、パスを指定して `BuildCommandLineArgs` で作成します (第 12 章)。ファイルが既に存在する場合は、上書きする前に確認を求めます。

11.5 復号パスワードがない、または間違っている場合

内容が暗号化されていて `-cryptpwd` がないか間違っている場合、**Password richiesta** (パスワードが必要) ウィンドウが表示されます: "I parametri di connessione sono protetti da password. Tentativo N di

3." (接続パラメーターはパスワードで保護されています。試行 N/3。) (誤入力の後は "Password errata." (パスワードが間違っています。) が前に付きます)。

- **3 回**まで試行できます。
- **Annulla** を選んだ場合、または試行回数を使い切った場合、プログラムは接続ウィンドウを開かずに**終了**します。
- 各復号は検証されます (結果に少なくとも `ip` が含まれている必要があります)。間違ったパスワードが正しいものと誤認されることはありません。

11.6 名前付きパイプによるパスワードの受け渡し

`-cryptpwd=pipe` を使用すると、実際のパスワードは一瞬たりともコマンド ラインに現れません。AlbatrosRDP を起動するプログラムが、ローカルの名前付きパイプを通じてパスワードを渡します:

- パイプ名: `\\.\pipe\AlbatrosRDP_Secret_<PID>`。PID は起動したばかりの AlbatrosRDP プロセスの識別子です。
- パイプは呼び出し元のプログラムによって作成され、現在の Windows ユーザーのみがアクセスでき、接続は 1 つだけ受け付けます。
- シークレットは、接続してきたのが想定どおりのプロセスである場合にのみ渡されます (クライアントの PID を確認)。
- テキストは UTF-8 で送信されます (BOM があっても許容されます)。
- AlbatrosRDP は最大 **5 秒**待機し、何も受信しなかった場合は 11.5 節のウィンドウでパスワードを要求します。

パイプを使用する最も簡単な方法は、すべてを 1 回の呼び出しで行う `StartProcessWithEncryptedArgsAndPipePasswordWait` 関数 (第 12 章) です。

11.7 特定のコンピューターへの限定

作成時 (`machineBound:=True`) に、暗号化された内容を現在のコンピューターに限定できます。その場合、実際の暗号化キーはコンピューターのハードウェア ID の後にパスワードを続けたものになります。ハードウェア ID は次の要素で構成されます:

- マザーボードのシリアル番号
- CPU の識別子
- 最初の物理ディスクのシリアル番号

読み取り時には何も指定する必要はありません。プログラムはまずパスワードそのもの (すべてのコンピューターで有効な内容) を試し、次にローカル コンピューターのハードウェア ID との組み合わせを試します。ディスクの順序が保証されないことによるバリエーション (たとえば USB メモリが挿入されている場合) も含めて試行します。

> **注意。** 限定された内容は、マザーボード、CPU、またはシステム ディスクを交換すると読み取れなくなります。当然、他のコンピューターでも読み取れません。その場合は再生成する必要があります。

12. 他のプログラムからの統合

プログラムのクラスは、`AlbatrosRDP.exe` (保護されていないバージョン) への参照を追加するか、ソース ファイルを含めることで、他の VB.NET アプリケーションから使用できます。サンプル プロジェクト **Test_Lancio_pipe** (コンソール アプリケーション) では、パイプ経由のパスワードによる起動を示しています。

12.1 RdpConnectionParams クラス

プロパティ	型	説明
`Ip`	String	サーバー (必須)。
`Port`	Integer	ポート。0 = 既定値 (3389)。
`User`、`Domain`	String	ユーザーとドメイン。
`Password`	String	リモート ユーザーのパスワード。
`Nota`、`Info`	String	メモと追加情報。
`IsValid`	Boolean	`Ip` に値が設定されている場合は True。
`Clone()`	関数	コピーを返します。

12.2 RdpCommandLineManager クラス

メソッド (Shared)	説明
`BuildCommandLineArgs(prms, [encryptionPassword], [filePath], [machineBound])`	引数を構築します。パスワードなし: 平文。パスワードあり: `-enc` + `-cryptpwd`。`filePath` あり: ファイルを書き込み (平文または暗号化。フォルダーを作成し、既存の場合は確認を求めます)、`-file` [+ `-cryptpwd`] を返します。引数は Windows の規則に従って既に引用符で囲まれています。
`BuildCommandLineArgsFromFile(filePath, [encryptionPassword])`	既存のファイル用の引数。パスワードが指定されている場合は、まずファイルを復号できることを確認します。ファイルが存在しないか、パスワードが間違っている場合は例外をスローします。

メソッド (Shared)	説明
`StartProcessWithEncryptedArgsAndPipePasswordWait(exePath, prms, encryptionPassword, ByRef passwordDelivered, [machineBound], [pipeTimeoutMs=5000])`	`-cryptpwd=pipe` を指定して AlbatrosRDP を起動し、パイプ経由でパスワードを渡して受け渡しの完了を待ちます。`passwordDelivered` は結果を示します。すぐに終了するランチャーに適しています。
`StartProcessWithEncryptedArgsAndPipePassword(exePath, prms, encryptionPassword, [machineBound], [pipeTimeoutMs=5000])`	上記と同じですが、受け渡しはバックグラウンドで行われ、メソッドはすぐに戻ります。受け渡し前に呼び出し元が終了すると、パスワードは届きません。
`ParseCommandLineArgs(args, [ByRef userAborted])`	受け取った引数を解釈します (必要に応じてパスワードを対話的に要求します)。
`ReadParamsFromFile(filePath, [cryptPwd])`	ダイアログなしでパラメーター ファイルを読み取ります。パスワードが間違っている場合は例外になります。
`EncryptString(testo, password)` / `DecryptToOriginalString(blob, password)`	ハードウェア限定なしの基本的な暗号化と復号。
`GetMachineHardwareId()`	現在のコンピューターのハードウェア ID。

例: ランチャーからパイプ経由のパスワードで起動する (キーは変数に格納し、コードには決して記述しません):

```
Dim prms As New RdpConnectionParams With {
  .Ip = "192.168.1.10", .Port = 3389,
  .User = "Administrator", .Nota = "Server ufficio"}

Dim consegnata As Boolean = False
RdpCommandLineManager.StartProcessWithEncryptedArgsAndPipePasswordWait(
  "C:\Albatros\CompiledPrograms\AlbatrosRDP.exe",
  prms, chiave, consegnata)
```

例: コンピューターに限定された暗号化ファイルを作成する:

```
Dim argomenti As String = RdpCommandLineManager.BuildCommandLineArgs(
  prms, encryptionPassword:=chiave,
  filePath:="C:\Config\Clienti\Cliente1.rdpdat", machineBound:=True)
' -> "-file=C:\Config\Clienti\Cliente1.rdpdat" "-cryptpwd=..." "-local=true"
```

12.3 SecretPipeTransfer クラス

メソッド (Shared)	説明
`SendSecretToChildProcessAndWait(processo, segreto, [timeoutMs])`	呼び出し側: 子プロセスの PID 用のパイプを作成し、受け渡しを待ちます。受け渡しが完了した場合は True を返します。
`SendSecretToChildProcess(processo, segreto, [timeoutMs])`	上記と同じで、バックグラウンドで実行します。

メソッド (Shared)	説明
`ReceiveSecretForCurrentProcess([timeoutMs])`	AlbatrosRDP 側: 自身の PID のパイプからシークレットを読み取ります。
`ReadSecretFromPipe(nomePipe, [timeoutMs])`	名前を明示したパイプから読み取ります。
`WaitSeconds(n)` / `WaitMilliSeconds(n)`	インターフェイスの応答性を保ったまま待機します。

12.4 暗号化の形式

項目	値
アルゴリズム	AES-256、CBC モード、PKCS7 パディング
キーの導出	PBKDF2-HMAC-SHA1、50,000 回の反復、16 バイトのランダムなソルト
形式	ソルト (16 バイト) + IV (16 バイト) + 暗号化データの Base64
平文の内容	`"-ip=..."` `"-user=..."` 形式のパラメーター (UTF-8)
互換性	以前のバージョンと同一: 以前に作成された文字列やファイルは引き続き読み取ることができ、その逆も同様です

12.5 コードによるカスタマイズ

項目	説明
`FrmRDP.New([nativeConnectionBar], [SafeMode])`	接続ウィンドウを使用するセッション。
`FrmRDP.New(server, port, domain, userName, password, [nativeConnectionBar], [SafeMode])`	接続ウィンドウを使用しない直接セッション。
`SafeMode`	True の場合、まず汎用の RDP コントロールを検索し、選択肢をバージョン 11 までに制限します。
`FrmRDP.MenuHotkey`	クイック メニューのキーの組み合わせ (既定値 `Keys.Control Or Keys.F11`)。
`FrmRDP.ConnectionNote` / `ConnectionInfo`	セッションのメモと情報。
`FrmRDP.ShowNativeConnectionBar`	ネイティブ バーを使用するかどうか。`ShowDialog()` の前に設定します。
`Module1.PercorsoStorico`	履歴ファイルのパス。

項目	説明
Module1.MaxCronologRDP	履歴の最大項目数 (既定値 20)。

13. 適用される RDP 設定

各セッションを開くときに、次の設定が `.rdp` ファイルの形式で適用されます。これらはコード内 (FrmRDP の `rdpSettingsString` 文字列) で定義されており、外部の構成ファイルはありません。

設定	効果
`session bpp:i:32`	32 ビット カラー。
`compression:i:1`	データ圧縮が有効。
`disable wallpaper:i:1`	リモート デスクトップの壁紙を表示しない (帯域幅を節約)。
`keyboardhook:i:2`	Windows のキーの組み合わせは、全画面時にのみリモート コンピューターに送信 (既定値)。
`audiomode:i:0`	リモートのオーディオをローカル コンピューターで再生。
`audiocaptureмode:i:1`	ローカルのマイクをリモート セッションで使用可能。
`redirectprinters:i:1`	ローカルのプリンターをセッションで使用可能。
`redirectsmartcards:i:1`	ローカルのスマート カードを使用可能。
`redirectclipboard:i:1`	クリップボードをローカルとリモートで共有。
`drivestoredirect:s:*`	すべてのローカル ドライブをリモート セッションで表示。
`negotiate security layer:i:1`	最も強力なセキュリティ プロトコルを自動的にネゴシエート。
`screen mode id`、`use multimon`	無視: 全画面表示はプログラムが 1 台のモニターで管理します。

その直後に、プログラムはさらに次の設定を行います:

- **RDP コントロールの自動再接続**を有効化 (文字列内の `autoreconnection enabled:i:0` を置き換えます)。
- **認証レベル 0** とし、証明書の警告を無視 (`authentication level:i:2` を置き換えます)。サーバーの証明書は検証されず、警告も表示されません。
- **CredSSP** を有効化 (NLA 認証に必要)。
- **接続タイムアウト**: 全体で 8 秒、1 回の試行あたり 5 秒。

プログラムは他の `.rdp` キーも解釈できます (たとえば、デスクトップの代わりに 1 つのプログラムだけを起動するための `alternate shell` と `shell working directory`、`connection type`、`networkautodetect`、`redirectcomports`、RD ゲートウェイの設定 `gatewayhostname`、

gatewayusagemethod など)。これらを使用するには、コード内の文字列を変更してプログラムを再コンパイルする必要があります。

14. セキュリティと機密性

- リモート ユーザーの**パスワード**は、履歴にもログにも、ディスクに保存されることはありません。RDP コントロールに渡した後、メモリ内のコピーは消去されます。
- **ログ**には、起動モード、接続の状態、エラーのみが記録され、パスワード、キー、パラメーターが記録されることはありません。
- **暗号化**には、PBKDF2 で導出したキーによる AES-256 を使用します。機密データを含むバッファーは使用後にゼロで消去されます。
- **パイプ**は現在のユーザーのみがアクセスでき、シークレットを想定どおりのプロセスにのみ渡し、1 回限りの使用です。
- **サーバーの証明書は検証されません** (第 13 章)。そのため、傍受からの保護はチャネル (信頼できるネットワーク、VPN、SSH トンネル) に依存します。この設定を維持するかどうかを検討してください。
- `-pwd=` で平文で渡したパスワードは、プロセスの一覧で見えてしまいます (11.2 節)。
- セッション中の到達可能性の確認では、2 秒ごとに RDP ポートへの TCP 接続を開きます。これにより、サーバーでは RDP のログ (RdpCoreTS) にイベントが生成され、トンネル内に若干のトラフィックが発生します。

15. 診断ログ

ログは `%LOCALAPPDATA%\Albatros\AlbatrosRDP\AlbatrosRDP.log` にあります。1 MB を超えると `AlbatrosRDP.1.log` に名前が変更され (以前のコピーは置き換えられます)、新しく記録が始まります。各行の形式は次のとおりです:

```
2026-10-11 14:22:05.123 [4812] INFO  Stato RDP: connesso
```

つまり、日付と時刻、プロセスの PID、レベル (INFO、WARN、ERROR)、メッセージです。記録される内容:

- アプリケーションの起動 (バージョンと引数の数) と終了
- コマンド ラインのモード (平文、暗号化、ファイル) と結果 (有効なパラメーター、無効なパラメーター、パスワードのキャンセルまたは誤り)
- サーバー、ポート、使用中の RDP コントロール、バーの種類
- セッションの状態の変化 (切断理由の拡張コードを含む)
- 失敗した再接続の試行、ウォッチドッグの介入、エラー、ハンドルされない例外
- セッションの終了とその理由

16. トラブルシューティング

問題	対処方法
起動時に "Impossibile avviare la connessione RDP" と表示される	Windows の RDP コントロールがないか、動作していません。リモート デスクトップ接続 (`mstsc.exe`) が動作することを確認し、ログを参照してください。
"Impossibile raggiungere il server"	SSH トンネル、VPN、ファイアウォール、アドレス、ポートを確認してください。ローカル トンネルを使用する場合は、接続する前にトンネルが有効であることを確認してください。
"La connessione RDP non è stata stabilita" と表示されてプログラムが終了する	資格情報がキャンセルされたか間違っている、または認証中にネットワークがありませんでした。ユーザー、ドメイン、パスワードを確認して再試行してください。
バーが黄色で "Connessione persa su ..." と表示される	サーバーが RDP ポートで応答しなくなっています。通常はトンネルが切断されています。復旧するとバーは自動的に緑色に戻ります。
Ctrl+F11 でメニューが開かない	Microsoft のネイティブ バーが有効になっています (Ctrl+F11 は無効)。ウィンドウ モードでタイトル バーを右クリックしてください。
ステータス バーが表示されない	バーが非表示にされています (ダブルクリックまたはメニュー)。マウスを上端に移動するか、Ctrl+F11 > Barra di stato を使用してください。バーは AlbatrosRDP がアクティブなアプリケーションの場合にのみ表示されます。
`-cryptpwd=pipe` で起動したのにパスワードを要求される	パスワードが 5 秒以内に届きませんでした。おそらくランチャーが受け渡しの前に終了しています。`StartProcessWithEncryptedArgsAndPipePasswordWait` を使用してください。
限定された内容で、パスワードが正しいのに "Password errata" と表示される	ハードウェア (マザーボード、CPU、ディスク) が変更されたか、別のコンピューターを使用しています。暗号化された内容を再生成してください。
`-ip` を指定しているのに接続ウィンドウが開く	パラメーターが認識されていません。二重引用符の使い方を確認し、`-file` の場合はファイルが存在することを確認してください。
履歴が更新されない	ProgramData 内のファイルに対する書き込み権限がありません (2.3 節)。

問題	対処方法
履歴が消えた	ファイルが読み取れなかったため、同じフォルダーに `.corrupt-<data>.bak` というコピーが保存されています。
リモート デスクトップの壁紙が表示されない (単色)	意図された動作です (`disable wallpaper:i:1`、第 13 章)。
"L'applicazione non risponde da diversi secondi"	プログラムが 15 秒以上応答していません。通常は認証中のネットワーク切断が原因です。「はい」でプログラムを終了し、「いいえ」で待機を続けます。

付録 A. プログラムのメッセージ

メッセージ	意味と応答
Verifica raggiungibilità server:porta...	接続前の TCP テストを実行中。
Connessione in corso...	RDP コントロールがセッションを確立中。
--> server:porta (緑のバー)	セッションが接続済み。
Connessione persa su server:porta	サーバーが定期的な TCP テストに応答しない。
Connessione RDP non attiva	セッションが切断され、自動再接続を実行中。
Riconnessione in corso... / Disconnessione in corso...	Riconnetti 項目または終了処理による表示。
Errore di connessione / Errore di riconnessione	RDP コントロールが接続要求を拒否した。
Impossibile raggiungere il server ... Riprovare?	はい = 再確認、いいえ = 終了。
La connessione RDP non è stata stabilita ... L'applicazione verrà chiusa.	最初の接続が一度も成功しなかった (資格情報またはネットワーク)。
La riconnessione automatica non riesce ... Continuare a riprovare?	3 回失敗した後。はい = 続行、いいえ = 終了。
La sessione RDP è stata disconnessa. Riconnettersi al server?	ネイティブ バーまたはサーバーによってセッションが閉じられた。はい = 再接続、いいえ = 終了。
Disconnettere la sessione RDP e chiudere l 'applicazione?	終了の確認。既定: いいえ。
L'applicazione non risponde da diversi secondi ...	ウォッチドッグ。はい = 強制終了、いいえ = 待機。
AlbatrosRDP - Errore ... Continuare a usare l'applicazione?	ハンドルされない例外。はい = 続行、いいえ = 終了。
Password richiesta - Tentativo N di 3	暗号化されたパラメーター: 復号パスワードを入力します。
Il file ... esiste già. Sovrascrivere?	コードからパラメーター ファイルを作成するとき。

付録 B. クイック リファレンス

B.1 キーとマウス

操作	効果
Ctrl+F11	クイック メニューを開く (カスタム バーのみ)。
メニューが開いているときの Esc	メニューを閉じる。
ステータス バーの右クリック	クイック メニューを開く。
タイトル バーの右クリック	クイック メニューを開く (ウィンドウ モード)。
ステータス バーのダブルクリック	バーを非表示にする。
マウスを上端に移動	非表示のバーを再表示する。
ステータス バーのドラッグ	バーを移動する。
接続ウィンドウでの Enter / Esc	Connetti / Annulla。

B.2 コマンド ライン

```
AlbatrosRDP.exe -ip=<server> [-port=<porta>] [-user=<utente>] [-domain=<dominio>]
        [-pwd=<password>] ["-nota=<testo>"] ["-info=<testo>"]

AlbatrosRDP.exe "-enc=<Base64>" "-cryptpwd=<chiave>|pipe"

AlbatrosRDP.exe "-file=<percorso>" ["-cryptpwd=<chiave>|pipe"]
```

B.3 時間の値

チェック	値
最初の到達可能性の確認	2.5 秒
セッション中の確認	2 秒ごと、タイムアウト 1.5 秒
再接続の試行間の最小間隔	5 秒
"Continuare a riprovare?" の確認が表示されるまでの試行回数	3
接続失敗と判断するまでの最初の待機時間	15 秒
ウォッチドッグ	15 秒間の応答停止 (2 秒ごとにチェック)
接続後のネイティブ バーの有効化	1 秒
パイプ経由のパスワードの待機	5 秒

チェック	値
終了時の安全停止	8 秒