WinSSH Manager

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 35

IT Italiano 69

RO Română 101

JA 日本語 134

DevService.net — Raffaele Romano

WinSSH Manager

User Manual

Management of the OpenSSH Server built into Windows

Windows 10/11 · Windows Server 2019, 2022, 2025

October 2026 edition

Contents

1. Introduction **5**
1.1 What WinSSH Manager is 5
1.2 Supported systems and requirements 5
1.3 How it works 5
1.4 Conventions used in this manual 6

2. Installation and first startup **7**
2.1 Copying the program 7
2.2 First startup 7
2.3 Where data is saved 8

3. The main window **9**
3.1 Window layout 9
3.2 Command bar buttons 9
3.3 Pending changes indicator 9
3.4 Warnings before applying 10
3.5 What happens when you apply 10

4. Stato tab **11**
4.1 Information shown 11
4.2 Buttons 12

5. Server tab **13**
5.1 Network 13
5.2 Authentication 14
5.3 Access control 14
5.4 Forwarding and session 15
5.5 Cryptography and logging 15
5.6 Advanced 15

6. Firewall tab **16**

7. Account tab **17**
7.1 Account list 17
7.2 Creating an account 17
7.3 Editing, enabling and disabling 19
7.4 Resetting the password 19
7.5 Deleting an account 19
7.6 Public keys 19
7.7 SFTP folder permissions 20

8. Sessioni tab **21**

9. Blocco IP tab **22**
9.1 How it works 22
9.2 Settings 22
9.3 Blocked IPs and log 23

10. Log tab **24**

11. Backup tab **25**
11.1 Exporting the settings 25
11.2 Importing the settings 25
11.3 Restoring sshd_config 25
11.4 Folders 25

12. Step-by-step procedures **26**
12.1 Recommended commissioning 26
12.2 Administrator with key and RDP/SQL tunnel 26
12.3 Supplier uploading files (SFTP only) 26
12.4 Read-only access 26
12.5 Changing the port without losing access 26
12.6 Switching to keys only 27
12.7 Migrating from Bitvise SSH Server 27

13. Text console and use from PowerShell **28**
13.1 Menu console 28
13.2 Module commands 28

14. Limitations to be aware of **30**

15. Troubleshooting **31**
15.1 In-depth debugging 31

16. Uninstallation **32**

Appendix A. Objects created in the system **33**

Appendix B. Glossary **34**

1. Introduction

1.1 What WinSSH Manager is

WinSSH Manager is a graphical control panel for the **OpenSSH Server built into Windows**. It lets you manage the port, authentication, accounts, SFTP access, firewall and automatic IP blocking from a single window, with a working model similar to that of Bitvise SSH Server: all settings are kept in a single file, and the server is reconfigured from that file.

The program uses only Microsoft components already present in the system: OpenSSH Server, Windows Firewall, Task Scheduler, local or Active Directory accounts, NTFS permissions. It does not install any services of its own and does not require third-party software.

- **SSH server** with shell (PowerShell, PowerShell 7 or Command Prompt), SFTP and SCP;
- **SFTP-only accounts** confined to a folder, optionally read-only;
- **tunnels** (port forwarding) allowed per account and restricted to specific destinations;
- **public keys** managed in a central store, valid for administrators too;
- **firewall** with a list of allowed IPs and **automatic blocking** of IPs that repeatedly fail to log on;
- **active sessions**, **logs**, **host key fingerprints**, **export and import** of the settings.

1.2 Supported systems and requirements

Requirement	Details
Operating system	Windows 10 (1809 or later), Windows 11, Windows Server 2019, 2022 and 2025
Components	.NET Framework 4.8 and Windows PowerShell 5.1, already present on all the systems listed
OpenSSH Server	Optional Windows feature. If it is missing, the program installs it (see chapter 2)
Privileges	The program must be run as **Administrator**: at startup Windows asks for UAC confirmation
Graphical interface	Requires the Desktop Experience. On Server Core, use the text console (chapter 13)

1.3 How it works

There is only one principle to keep in mind: **settings are saved in config.json and take effect only when you apply the configuration.**

1. You edit the fields in the **Server**, **Firewall** and **Blocco IP** (IP blocking) tabs and press **Salva impostazioni** (Save settings): the values are written to `config.json`. Accounts (**Account** tab), on the other hand, are saved to `config.json` as soon as you confirm their window.
2. You press **APPLICA CONFIGURAZIONE** (APPLY CONFIGURATION): the program generates a new `sshd_config` from `config.json`, checks it with `sshd -t` and, only if it is valid, puts it into use, aligns the firewall, keys, folders and IP blocking, and restarts the `sshd` service.

For this reason `sshd_config` **must not be edited by hand**: it is regenerated every time the configuration is applied, and manual changes would be lost. Directives that the GUI does not provide for are entered in the **Righe aggiuntive sshd_config** (Additional sshd_config lines) field of the Server tab (section 5.6).

> **Note:** The window always works on the machine on which it is running. To administer a remote server, use the GUI over Remote Desktop, or the text console over SSH.

1.4 Conventions used in this manual

- The names of buttons, tabs and fields are in **bold**, exactly as they appear on screen.
- File names, paths, commands and values to type are in `monospace font`.
- The **Note**, **Tip** and **Warning** boxes indicate, respectively, useful information, best practices, and situations in which you risk losing access to the server or losing data.

2. Installation and first startup

2.1 Copying the program

The program is a folder that contains `WinSshManagerGui.exe` and the `PowerShell` subfolder, which is the actual engine. It has no setup program.

1. Copy **the entire folder** to the server or PC, for example to `C:\Program Files\WinSshManager\`.
2. Make sure that the `PowerShell` subfolder is located next to `WinSshManagerGui.exe`. If it is missing, the message «Manca il motore PowerShell» (The PowerShell engine is missing) appears at startup and the program closes.
3. If another SSH server (for example Bitvise) is running on the same machine on the same port, stop it first, or configure OpenSSH on a different port for the trial period: two servers cannot listen on the same port.

2.2 First startup

Start `WinSshManagerGui.exe` and confirm the UAC prompt. At the first startup the program reads the state of the system and proposes the necessary operation:

Detected situation	What the program proposes
OpenSSH Server not installed	«OpenSSH Server non risulta installato su questo sistema. Installarlo e abilitarlo ora?» (OpenSSH Server does not appear to be installed on this system. Install and enable it now?). If you answer **Sì** (Yes), the optional feature is installed (on Windows Server 2025 it is already present and is only enabled). The operation may take a few minutes.
OpenSSH present, WinSSH Manager never initialized	«WinSSH Manager non è ancora inizializzato su questo sistema (manca config.json)» (WinSSH Manager is not yet initialized on this system (config.json is missing)). If you answer **Sì**, initialization is performed.
Already initialized	No question: the window opens on the **Stato** (Status) tab.

Installation or initialization performs these operations:

- sets the `sshd` service to automatic startup and starts it (at the first start OpenSSH generates the host keys);
- sets the `ssh-agent` service to manual startup;
- creates the data folder `C:\ProgramData\WinSshManager` and the key store `C:\ProgramData\ssh\managed_keys`, accessible only to SYSTEM and Administrators;
- creates `config.json` with the default values, **keeping the port** already configured in `sshd_config`, if any;
- saves a copy of the original `sshd_config` in `backup\sshd_config.originale.<date-time>`.

At the end, the message «OpenSSH Server installato e abilitato. Definire gli account e premere APPLICA CONFIGURAZIONE» (OpenSSH Server installed and enabled. Define the accounts and press APPLY CONFIGURATION) appears. The same procedure can be run again at any time with the **Installa / abilita OpenSSH** (Install / enable OpenSSH) button on the Stato tab.

> **Warning:** On Windows 10/11 and Windows Server 2019/2022, installation downloads the feature from Windows Update. In environments with WSUS and without a source for Features on Demand (FoD), installation may fail: in that case, first install **OpenSSH Server** from Settings → Apps → Optional features, then run **Installa / abilita OpenSSH** again.
>
> **Warning:** After initialization the access mode is **Users**, but there is still no account: until at least one is defined, the server accepts **any** valid Windows account. The Stato tab flags this in orange. Define the accounts immediately (chapter 7) and apply.

2.3 Where data is saved

Path	Content
`C:\ProgramData\WinSshManager\config.json`	Single source of all settings
`C:\ProgramData\WinSshManager\backup\`	Last 30 versions of `sshd_config` and `config.json`, plus the `sshd_config` file in its original version
`C:\ProgramData\WinSshManager\*.ps1, *.psm1`	Copy of the engine used by the IP blocking scheduled task, realigned every time the configuration is applied
`C:\ProgramData\WinSshManager\ipblocker-state.json`	IP blocking state (counters, blocked IPs, history)
`C:\ProgramData\WinSshManager\ipblocker.log`	Log of blocks and unblocks
`C:\ProgramData\ssh\sshd_config`	OpenSSH configuration, **generated** by the program
`C:\ProgramData\ssh\managed_keys\`	Central store of public keys, one file per account
`C:\ProgramData\ssh\administrators_authorized_keys`	Standard Microsoft file for administrator keys (managed by OpenSSH, respected by the program)
`C:\ProgramData\ssh\banner.txt`	Text of the pre-login banner

The `C:\ProgramData\WinSshManager` folder can be read and written only by SYSTEM and Administrators, because it contains scripts run as SYSTEM by the scheduled task.

3. The main window

3.1 Window layout

The main window («WinSSH Manager - OpenSSH Server per Windows») is divided into four areas, from top to bottom:

Area	Function
Tabs	Eight tabs: **Stato** (Status), **Server**, **Firewall**, **Account**, **Sessioni** (Sessions), **Blocco IP** (IP blocking), **Log**, **Backup**. They are described one by one in chapters 4–11.
Output operazioni (Operations output)	Dark panel with the messages produced by each operation, preceded by the time. Errors begin with «ERRORE:» (ERROR:). It is the first place to look if something goes wrong.
Command bar	The **Ricarica** (Reload), **Salva impostazioni** (Save settings), **Salva e applica** (Save and apply) and **APPLICA CONFIGURAZIONE** (APPLY CONFIGURATION) buttons and the pending changes indicator.
Status bar	Shows «Pronto» (Ready), or the description of the operation in progress with a progress bar.

Operations run in the background: while they are in progress, the tabs and the command bar are disabled, but the window remains responsive. The program cannot be closed during an operation.

3.2 Command bar buttons

Button	What it does
Ricarica (Reload)	Rereads `config.json` and refreshes the current tab. If there are unsaved changes, it asks whether to discard them.
Salva impostazioni (Save settings)	Checks the values in the **Server**, **Firewall** and **Blocco IP** tabs and writes them to `config.json`. It does not affect the running server. Accounts do not need this button: they are saved automatically.
Salva e applica (Save and apply)	Saves as above and immediately afterwards applies the configuration. Before proceeding, it shows warnings about risky changes (see 3.4).
APPLICA CONFIGURAZIONE (APPLY CONFIGURATION)	Generates `sshd_config` from `config.json`, checks it, puts it into use and restarts the service (see 3.5). If there are unsaved settings, it first asks whether to save them.

3.3 Pending changes indicator

Next to the buttons, the work status appears in orange:

Indicator	Meaning and what to do
«Impostazioni modificate e non salvate» (Settings changed and not saved)	Fields in Server, Firewall or Blocco IP have been changed. Press **Salva impostazioni** or **Salva e applica**.
«Modifiche salvate ma non ancora applicate» (Changes saved but not yet applied)	`config.json` contains settings different from those in use. Press **APPLICA CONFIGURAZIONE**.
(empty)	The server is using exactly the saved configuration.

When you close the window, the program asks for confirmation if there are changes that are unsaved, or saved but not applied.

3.4 Warnings before applying

Some changes can lock out the administrator. With **Salva e applica** the program lists them and asks for confirmation before proceeding:

- **password authentication disabled**: make sure the accounts have a public key;
- **port changed**: clients will have to connect to the new port;
- **firewall restricted** to a list of addresses: if you administer remotely, your own IP must be in the list.

> **Warning:** The warnings appear only with **Salva e applica**. If you save with **Salva impostazioni** and then press **APPLICA CONFIGURAZIONE**, the configuration is applied without this check. For port, authentication and firewall changes, always use **Salva e applica**.

3.5 What happens when you apply

APPLICA CONFIGURAZIONE performs, in order:

1. generates a candidate `sshd_config` from `config.json` and checks it with `sshd -t`. **If it is not valid, nothing is changed** and the error is shown, indicating the problematic line;
2. saves the `sshd_config` in use to the `backup` folder and writes the new one;
3. writes the banner, sets the default shell, protects the key store, creates the SFTP root folders with their permissions, updates the `SSH-SFTP-Only` group and the logon restrictions, updates the firewall rules and enables or disables the IP blocking task;
4. restarts the `sshd` service.

> **Note:** Restarting `sshd` may interrupt the SSH sessions in progress. If you are administering the server over SSH, be prepared to reconnect; the new rules apply in any case to all subsequent connections.

4. Stato tab

This is the tab that opens at startup, and it is refreshed every time you select it. It summarizes the state of the server.

4.1 Information shown

Item	Meaning
Installato (Installed)	«Sì» (Yes) in green if OpenSSH Server is present, «NO» in red otherwise
Versione (Version)	Detected version of OpenSSH for Windows
Eseguibile (Executable)	Path of `sshd.exe` (Windows feature or Microsoft MSI version)
Servizio sshd (sshd service)	Status and startup type of the service (e.g. «Running / Automatic»), in green if it is running
Porta, Indirizzi di ascolto (Port, Listen addresses)	Values saved in `config.json`
Shell predefinita (Default shell)	Shell set in the registry. If it is not set, «cmd.exe (default Windows)»
Account definiti (Defined accounts)	Number of accounts in the Account tab
Controllo accessi (Access control)	Mode **Users**, **Groups** or **Any**. In orange if it is **Any**, or **Users** without accounts: in both cases any valid Windows account can log on
Firewall	Status and profiles of the managed rule, or «regola gestita assente» (managed rule missing)
Blocco IP (IP blocking)	Status of the scheduled task and number of blocked IPs, or «disattivato» (disabled)
sshd_config	«Allineato alla configurazione» (Aligned with the configuration) in green, or «Differisce dalla configurazione: premere APPLICA CONFIGURAZIONE» (Differs from the configuration: press APPLY CONFIGURATION) in orange

4.2 Buttons

Button	Function
Aggiorna stato (Refresh status)	Rereads all the information
Installa / abilita OpenSSH (Install / enable OpenSSH)	Installs or enables OpenSSH Server and initializes WinSSH Manager (section 2.2). Does not overwrite `config.json` if it already exists
Avvia (Start), **Arresta** (Stop), **Riavvia (Restart)**	Control the `sshd` service. **Arresta** asks for confirmation because it closes all active SSH sessions
Anteprima sshd_config (sshd_config preview)	Shows the file that would be generated with the **saved** settings. It does not apply it. If there are unsaved changes on screen, the program warns that they are not included
sshd_config attuale (Current sshd_config)	Shows the file currently in use
Impronte chiavi host (Host key fingerprints)	Shows the SHA256, MD5 and Bubble Babble fingerprints for each host key

> **Tip:** At the first connection, the SSH client shows the fingerprint of the server key and asks you to confirm it. Before accepting, compare it with the **SHA256** fingerprint shown by **Impronte chiavi host**: this guarantees that you have connected to the right server.

5. Server tab

Contains the global settings of the SSH server. After making changes, press **Salva impostazioni** (or **Salva e applica**). Each field has a tooltip that appears when you hover the mouse over it.

5.1 Network

Field	Description	Default
Porta TCP (TCP port)	Port on which the server accepts connections (1–65535)	22
Indirizzi di ascolto (Listen addresses)	Local IP addresses on which to listen, separated by commas. `0.0.0.0` = all IPv4, `::` = all IPv6. CIDR networks are not allowed. If the field is left empty, both are used	`0.0.0.0, ::`
Connessioni non autenticate (Unauthenticated connections)	Directive `MaxStartups`: a number, or `start:rate:full`. With `10:30:100`, beyond 10 connections waiting for login, new ones are refused with a probability increasing from 30%, up to total refusal at 100	`10:30:100`
Sessioni per connessione (Sessions per connection)	Number of channels (shell, SFTP, tunnels) open on the same connection (1–100)	10
Keepalive (secondi, 0 = off) (Keepalive, seconds, 0 = off)	How often, in seconds, the server checks that the client is still present	60
Keepalive senza risposta (Unanswered keepalives)	After how many unanswered checks the connection is closed	3
Compressione (Compression)	Enables data compression	No

> **Note:** With the default values, an interrupted connection (network down, PC turned off) is closed by the server after about 3 minutes (60 s × 3).

5.2 Authentication

Field	Description	Default
Consenti autenticazione con password (Allow password authentication)	Logon with the Windows account password	Yes
Consenti autenticazione con chiave pubblica (Allow public key authentication)	Logon with the keys uploaded for each account (section 7.6)	Yes
Consenti password vuote (sconsigliato) (Allow empty passwords – not recommended)	Allows logon to accounts without a password	No
Tentativi per connessione (Attempts per connection)	Authentication attempts allowed before the connection is closed (1–20)	4
Tempo per il login (s) (Login time, s)	Seconds allowed to complete the login (10–600)	60
Banner pre-login (Pre-login banner)	Text shown by the client before the credentials prompt. Empty = no banner	empty

At least one of password and public key must remain enabled: the program does not allow saving if both are disabled. The method can then be restricted per account (section 7.2).

5.3 Access control

Field	Description
Chi può accedere (Who can log on)	**Users**: only the accounts defined in the Account tab (recommended, as in Bitvise). **Groups**: the members of the specified Windows groups. **Any**: any valid Windows account.
Gruppi ammessi (Allowed groups)	Groups mode only, separated by commas. Examples: `ssh-users`, `CONTOSO\ssh-group`. In Groups mode at least one group is required
Account sempre negati (Always denied accounts)	Accounts excluded in all cases, separated by commas. Accounts disabled in the Account tab are added automatically
Nega accesso interattivo e Desktop remoto agli account solo-SFTP (Deny interactive and Remote Desktop logon to SFTP-only accounts)	Local accounts in Solo SFTP (SFTP only) mode are added to the `SSH-SFTP-Only` group, which is denied console logon and Remote Desktop. Default: enabled

> **Warning:** In **Users** mode with no account defined, OpenSSH receives no restriction and accepts **all** valid Windows accounts.

> **Note:** The denial of interactive logon is set through the local security policy (`secedit`). On a domain-joined machine, a GPO that defines the same user rights takes precedence and can override it.

5.4 Forwarding and session

Field	Description	Default
Inoltro porte predefinito (Default port forwarding)	Value for accounts that do not redefine it: `no`, `yes` (local and remote), `local` (only from the client to the server), `remote` (only from the server to the client)	`no`
GatewayPorts	`no`: remote forwards listen only on the server's localhost. `yes`: on all interfaces. `clientspecified`: the client decides	`no`
Consenti inoltro dell'agent SSH (Allow SSH agent forwarding)	Allows the client's SSH agent to be used on the server	No
Shell predefinita (Default shell)	`powershell` (Windows PowerShell 5.1), `pwsh` (PowerShell 7, if installed), `cmd`, or the full path of an executable. Applies to all accounts. If the executable does not exist, the setting is ignored with a warning in the Output panel	`powershell`

5.5 Cryptography and logging

Field	Description	Default
Profilo algoritmi (Algorithm profile)	**Modern**: current algorithms only (curve25519, ML-KEM/sntrup if available, AES-GCM, ChaCha20, Ed25519, ECDSA and RSA-SHA2 keys). **Compatible**: adds NIST key exchanges, `diffie-hellman-group14-sha256`, `hmac-sha1` and `ssh-rsa` keys for older clients. **Default**: keeps the OpenSSH defaults. Algorithms not supported by the installed version are excluded automatically.	Modern
Livello log (Log level)	Level of detail of the messages in the event log: from `QUIET` to `DEBUG3`. `INFO` is sufficient for logons and IP blocking; `VERBOSE` adds the fingerprint of the key used at login	INFO

> **Tip:** Use **Compatible** only if some client can no longer connect (old versions of PuTTY, network devices, outdated SFTP libraries).

5.6 Advanced

The **Righe aggiuntive sshd_config** field accepts global OpenSSH directives that the GUI does not provide for, one per line. They are inserted as they are, before the per-user blocks, and checked with `sshd -t` when the configuration is applied: a wrong line prevents the configuration from being applied but does not damage the running server.

> **Warning:** Do not insert `Match` blocks here: they would be followed by the directives generated by the program and would alter their meaning.

6. Firewall tab

The program manages a Windows Firewall rule dedicated to the SSH server, equivalent to the «IP access rules» of Bitvise: connections from addresses not listed are dropped before they even reach OpenSSH.

Field	Description	Default
Gestisci il Windows Firewall per il server SSH (Manage Windows Firewall for the SSH server)	If disabled, the program does not touch the firewall (existing rules remain as they are)	Yes
Profili di rete (Network profiles)	**Dominio** (Domain), **Privato** (Private), **Pubblico** (Public): the profiles on which the port is open. If the firewall is managed, at least one is required	Dominio, Privato
IP / reti ammessi (Allowed IPs / networks)	One per line. Allowed: `Any`, `LocalSubnet`, single addresses (`203.0.113.10`), CIDR networks (`192.168.1.0/24`), ranges (`10.0.0.1-10.0.0.50`). If empty, it is equivalent to `Any`	`Any`
Disattiva le regole OpenSSH predefinite di Windows (Disable the default Windows OpenSSH rules)	Disables the inbound rule created by Microsoft at installation, which would open port 22 to everyone	Yes

Guidance on profiles:

- **Servers**: **Dominio** profile. Add **Pubblico** only if the exposed network adapter is classified as public.
- **PCs and laptops**: **Dominio** and **Privato**. On public networks (hotels, hotspots) the port stays closed, as it should.

Two rules are created:

Display name	Function
WinSSH Manager - SSH (TCP-In)	Allows connections to the SSH port from the allowed addresses, restricted to the executable `sshd.exe`
WinSSH Manager - IP bloccati	Blocks the IPs added by automatic blocking or manually (chapter 9). Applies to all profiles, only for the SSH port

> **Warning:** If you administer the server remotely over SSH, your own address (or network) must appear in **IP / reti ammessi**, otherwise at the first **Applica** (Apply) the next connection will be refused.

7. Account tab

Each SSH account corresponds to a **real Windows account**, local or Active Directory: OpenSSH for Windows does not support virtual accounts. The tab lists the allowed accounts and their rules.

> **Note:** Changes to accounts are saved in `config.json` as soon as you confirm; they take effect with **APPLICA CONFIGURAZIONE**.

7.1 Account list

Column	Content
Account	Name of the Windows account (`name` for a local account, `DOMAIN\name` for a domain account)
Attivo (Active)	«Sì» or «No». Disabled accounts are shown in gray
Accesso (Access)	«Shell» or «Solo SFTP» (SFTP only)
Cartella radice (Root folder)	SFTP folder of the account
Opzioni (Options)	«chroot» if the user is confined to the folder, «sola lettura» (read-only)
Inoltro (Forwarding)	Port forwarding permission
Autenticazione (Authentication)	Required authentication method
Da IP (From IP)	Addresses from which the account can connect
Descrizione (Description)	Free-form note

Buttons: **Nuovo...** (New...), **Modifica...** (Edit...; or double-click the row), **Chiavi pubbliche...** (Public keys...), **Abilita / disabilita** (Enable / disable), **Reimposta password...** (Reset password...), **Elimina...** (Delete...). All except **Nuovo...** act on the selected account.

7.2 Creating an account

Nuovo... opens the «Nuovo account SSH» (New SSH account) window, divided into sections.

Identità (Identity)

Field	Description
Account Windows (Windows account)	Local account: the name only (e.g. `mario`). Active Directory account: `DOMAIN\name`. Spaces, `@` and quotation marks are not allowed; the name of a local account cannot exceed 20 characters. After creation, the name can no longer be changed
Descrizione (Description)	Free-form note, also written as a comment in `sshd_config`
Account abilitato (Account enabled)	If disabled, the account remains in the configuration but is denied

Account Windows locale (Local Windows account)

Section present only at creation and only for local accounts.

Field	Description
Crea l'account Windows locale se non esiste (Create the local Windows account if it does not exist)	If the account does not exist, it is created with the specified password, with a password that never expires and cannot be changed by the user. Accounts in Shell mode are also added to the Users group
Password, Conferma password (Password, Confirm password)	Used only if the account must be created. The password is not saved in any configuration file and does not appear in the logs or in the process list

If you save a local account that does not exist and do not have it created, the program warns that logon will not be possible until the Windows account exists.

Tipo di accesso (Access type)

Option	Description
Shell completa (Full shell)	Terminal, SFTP, SCP and tunnels (if allowed). The user is not confined to any folder
Solo SFTP (SFTP only)	File transfer only. The user cannot open a terminal or use the agent; port forwarding is denied unless explicitly set otherwise
Cartella radice SFTP (SFTP root folder)	Solo SFTP only. Full **local** path (e.g. `D:\SFTP\mario`), selectable with **Sfoglia...** (Browse...). Network folders are not allowed. It is created when the configuration is applied if it does not exist
Confina nella cartella (chroot) (Confine to the folder)	Available if a folder is specified. The user sees the folder as `/` and cannot leave it. Without chroot, the folder is only the starting folder
Sola lettura (Read-only)	The user can download but cannot upload, modify or delete files

> **Warning:** The root folder must be a real local folder: network drives, junctions and symbolic links inside the folder do not work reliably with OpenSSH for Windows.

Inoltro porte (tunnel) (Port forwarding – tunnels)

Field	Description
Inoltro consentito (Forwarding allowed)	`default` (uses the global value of the Server tab), `no`, `local`, `remote`, `yes`
Destinazioni (locale) (Destinations – local)	Active with `local` or `yes`. Destinations reachable with local forwarding, in `host:port` format, separated by commas. E.g. `127.0.0.1:3389, sql01:1433`. Empty = all
Porte in ascolto (remoto) (Listening ports – remote)	Active with `remote` or `yes`. Ports that the user can open on the server, in `[host:]port` format. E.g. `8080`. Empty = all. Requires OpenSSH 7.8 or later

Sicurezza (Security)

Field	Description
Autenticazione (Authentication)	`default` (the global setting applies), `password`, `publickey`, `publickey+password` (**both** are required: first the key, then the password)
Accesso solo da (Access only from)	IPs or CIDR networks from which the account can connect, separated by commas. Empty = from any address

When you press **Salva** (Save), the account is registered. If the authentication method requires a public key, the program immediately opens the keys window so that you can add one.

7.3 Editing, enabling and disabling

- **Modifica...** (or a double-click) opens the same window with the account data; the name cannot be changed and the section for creating the Windows account does not appear.
- **Abilita / disabilita** toggles the state of the account. A disabled account is denied by OpenSSH after the configuration is applied, but the Windows account remains active for other uses.

7.4 Resetting the password

Reimposta password... asks for the new password for the selected **local** Windows account and sets it immediately, without the need to apply. For domain accounts, the program reminds you that the password is managed in Active Directory.

7.5 Deleting an account

Elimina... asks three questions in succession:

1. «Rimuovere l'account dalla configurazione SSH?» (Remove the account from the SSH configuration?) — removes the account from `config.json`;
2. «Eliminare anche le sue chiavi pubbliche dall'archivio centrale?» (Also delete its public keys from the central store?);
3. for local accounts only: «Eliminare anche l'account Windows locale?» (Also delete the local Windows account?). The operation is irreversible; the user profile remains on disk.

After deletion, press **APPLICA CONFIGURAZIONE**.

7.6 Public keys

Chiavi pubbliche... opens the list of keys of the selected account, with a sequential number and fingerprint (bits, SHA256, comment, type).

Button	Function
Incolla chiave... (Paste key...)	Paste one or more public keys, one per line, in the format `ssh-ed25519 AAAA… comment`
Importa file .pub... (Import .pub file...)	Select the public key file generated by the client
Elimina selezionata (Delete selected)	Removes the selected key, after confirmation
Chiudi (Close)	Closes the window

- Each key is checked with `ssh-keygen`: unrecognized lines are ignored with a warning, duplicates are skipped.

- A **private key** is always rejected. If you paste the wrong file by mistake, the program reports it.
- The keys are saved in `C:\ProgramData\ssh\managed_keys\<account>` (for domain accounts `managed_keys\domain\name`) with the permissions required by OpenSSH.
- The keys in the central store are valid **for administrators too**. For administrator accounts, on the other hand, OpenSSH ignores the `%USERPROFILE%\.ssh\authorized_keys` file: only `administrators_authorized_keys` and the central store apply.
- Added or deleted keys take effect immediately for new logons, without the need to apply (provided the configuration has already been applied at least once).

> **Tip:** On the client, the key pair is generated with `ssh-keygen -t ed25519`. Only the file ending in `.pub` must be uploaded to the server; the private key must never leave the client PC.

7.7 SFTP folder permissions

When the configuration is applied, the program creates the missing root folders and assigns NTFS permissions to the account:

Account type	Permissions assigned
Solo SFTP, read and write	On the root folder: read-only (the user cannot delete or rename it). On files and subfolders: modify
Solo SFTP, read-only	Read & execute on the whole tree

Permissions are added to the existing ones; they do not replace them. If the folder contains data reserved for other users, check the inherited permissions before assigning it.

8. Sessioni tab

Lists the active SSH connections on the server port, refreshed every time you open the tab.

Column	Content
Id	Process identifier of the session
Utente (User)	Connected account, or «(autenticazione in corso)» (authentication in progress) if the login is not yet complete
Remoto (Remote)	Address and port of the client
Inizio (Start)	Date and time the connection was opened

- **Aggiorna** (Refresh): rereads the list.
- **Disconnetti selezionata** (Disconnect selected): closes the selected session, after confirmation. The main service is never terminated.
- **Aggiorna ogni 10 secondi** (Refresh every 10 seconds): automatic refresh, active only while the tab is displayed.

9. Blocco IP tab

IP blocking, equivalent to Bitvise «IP blocking», detects addresses that repeatedly fail to log on and blocks them in the firewall for a set period.

9.1 How it works

- A scheduled task, `WinSSHManager-IPBlocker`, runs as SYSTEM: on every new event in the OpenSSH log, every 5 minutes (to let blocks expire) and at system startup.
- The following count as failures: wrong password or key, nonexistent user, exceeding the allowed attempts, unauthorized user («not allowed because»).
- When an IP exceeds the threshold within the set interval, it is added to the «WinSSH Manager - IP bloccati» firewall rule.
- When it expires, the block is removed automatically, within 5 minutes at the latest.
- The following are never blocked: `127.0.0.1`, `::1` and the addresses in the whitelist.

9.2 Settings

Left-hand panel. The settings are saved and applied with the buttons of the command bar at the bottom.

Field	Description	Default
Blocco automatico attivo (Automatic blocking enabled)	Enables or disables blocking. The scheduled task is already changed when you save	Yes
Fallimenti per bloccare (Failures before blocking)	Number of failed attempts that triggers the block (1–1000)	5
Nell'arco di (minuti) (Within, minutes)	Interval in which failures are counted (1–1440)	10
Durata blocco (minuti) (Block duration, minutes)	Duration of the temporary block (up to one year)	60
Permanente dopo N blocchi (Permanent after N blocks)	Number of blocks in 30 days after which the block becomes permanent. 0 = never	0
Chiudi le sessioni già aperte dall'IP bloccato (Close sessions already opened by the blocked IP)	When blocking, also closes the connections already established from that address	Yes
Mai bloccare (whitelist) (Never block)	IPs or CIDR networks, one per line	`127.0.0.1`, `::1`

> **Warning:** Make sure you **always** add the network from which you administer the server to the whitelist. A few password typing errors are enough to block yourself.

9.3 Blocked IPs and log

On the right are the **IP bloccati** (Blocked IPs) list (IP or network, from, until, reason; «permanente» for blocks with no expiry) and the **Registro blocchi** (Block log) with the last 300 lines of `ipblocker.log`. The log is rotated automatically beyond 1 MB.

Button	Function
Aggiorna (Refresh)	Rereads the list and the log
Blocca IP... (Block IP...)	Manually blocks an address or a CIDR network. Asks for the duration in minutes; `0` = permanent
Sblocca selezionato (Unblock selected)	Removes the block on the selected IP and resets its failures
Sblocca tutti (Unblock all)	Removes all blocks and resets all counters, after confirmation
Esegui un ciclo ora (Run a cycle now)	Analyzes the log immediately without waiting for the scheduled task

10. Log tab

Shows the events of the **OpenSSH/Operational** log, most recent first. It is loaded the first time the tab is opened.

- Successful logons are shown in **green**, failed or denied ones in **red**.
- **Double-clicking** a row opens the full text of the event.
- **Solo accessi falliti / negati** (Failed / denied logons only) filters the error events.
- **Eventi** (Events) sets how many events to show (10–5000, default 200).
- **Aggiorna** rereads the log with the specified criteria.
- **Apri Visualizzatore eventi** (Open Event Viewer) opens the OpenSSH/Operational log directly in Windows Event Viewer.

> **Tip:** When a user cannot log on, enable **Solo accessi falliti / negati** and look for the user's name: the message almost always indicates the cause (wrong password, key not accepted, user not authorized or connected from an IP that is not allowed).

11. Backup tab

11.1 Exporting the settings

Esporta... (Export...) creates a zip archive (suggested name `WinSshManager-YYYYMMDD.zip`) with:

- `config.json`;
- the public key store of the accounts;
- `administrators_authorized_keys`;
- only if **Includi le chiavi host** (Include host keys) is selected: the host keys of the server.

> **Warning:** Host keys are **private** keys: anyone who has the zip file can impersonate the server. Include them only to migrate the server to another machine while keeping the same fingerprints, and guard the file like a password.

11.2 Importing the settings

Importa... (Import...) reads a previously exported zip file:

- replaces `config.json` (a copy of the current version remains in `backup`);
- adds the public keys and `administrators_authorized_keys` contained in the zip file;
- if **Importa anche le chiavi host, se presenti nel file** (Also import host keys, if present in the file) is selected, replaces the host keys;
- at the end, asks whether to apply the configuration immediately.

11.3 Restoring sshd_config

Ripristina sshd_config da backup... (Restore sshd_config from backup...) lets you choose one of the versions saved in `C:\ProgramData\WinSshManager\backup`. The chosen file is checked with `sshd -t` and put into use, and the service is restarted.

> **Warning:** Restoring acts only on `sshd_config`. `config.json` remains as it is: at the next **Applica** its settings will be applied again. Use restore as an emergency remedy, then correct the settings in the tabs.

11.4 Folders

Apri cartella dati (Open data folder) opens `C:\ProgramData\WinSshManager`; **Apri cartella ssh** (Open ssh folder) opens `C:\ProgramData\ssh`.

12. Step-by-step procedures

The following procedures cover the most common cases. At the end of each one, press **APPLICA CONFIGURAZIONE** unless otherwise indicated.

12.1 Recommended commissioning

1. tab**Server**: port 22, or a high port if the server is exposed on the Internet (it reduces noise in the logs, but is not a security measure in itself); **Chi può accedere** = **Users**; **Profilo algoritmi** = **Modern**; shell `powershell` or `pwsh`.
2. tab**Firewall**: profiles suitable for the machine (chapter 6) and, in **IP / reti ammessi**, the local network plus the public IPs from which you connect.
3. tab**Blocco IP**: keep the default values and add the administration network to the whitelist.
4. **Salva e applica**.
5. tab**Account**: create the accounts (following sections) and apply.
6. Check from the server itself with `ssh username@localhost` and, for SFTP accounts, `sftp username@localhost`. From another PC, compare the fingerprint presented with **Stato → Impronte chiavi host**.

12.2 Administrator with key and RDP/SQL tunnel

1. **Nuovo...**, existing Windows account (e.g. the administrator's account).
2. **Shell completa**.
3. **Inoltro consentito** = `local`; **Destinazioni** = `127.0.0.1:3389, 127.0.0.1:1433`.
4. **Autenticazione** = `publickey`.
5. **Salva**, then add the public key in the window that opens.
6. Apply. From the client: `ssh -L 13389:127.0.0.1:3389 user@server`, then connect with Remote Desktop to `localhost:13389`.

12.3 Supplier uploading files (SFTP only)

1. **Nuovo...**, name of a dedicated local account (e.g. `supplier`), **Crea l'account Windows locale** with a strong password.
2. **Solo SFTP**; **Cartella radice** = `D:\SFTP\supplier`; enable **Confina nella cartella**.
3. **Autenticazione** = `password` (or `publickey`, if the supplier has a key).
4. **Accesso solo da** = the supplier's public IP.
5. Apply. The user sees the folder as `/` and can upload and manage the files inside it, but cannot delete the folder itself, nor access the console or Remote Desktop.

12.4 Read-only access

As in the previous case, also enabling **Sola lettura**. The user can only download: OpenSSH refuses writes and the NTFS permissions assigned are read-only.

12.5 Changing the port without losing access

1. If you are working remotely, make sure the new port number is reachable (router, perimeter firewall).
2. Change **Porta TCP** and press **Salva e applica**; confirm the warning.
3. The managed firewall rule is moved automatically to the new port.
4. Open a **new** connection on the new port (`ssh -p NEWPORT user@server`) **before** closing the existing one.

12.6 Switching to keys only

1. For each account, check in the **Chiavi pubbliche...** window that there is at least one key, and test logging on with the key.
2. tab**Server**: disable **Consenti autenticazione con password**.
3. **Salva e applica** and confirm the warning.

Alternatively, you can require the key only for some accounts, by setting **Autenticazione** = `publickey` on them.

12.7 Migrating from Bitvise SSH Server

1. In Bitvise, list the accounts and their permissions. Virtual accounts must be recreated as local Windows accounts (**Nuovo...** with **Crea l'account Windows locale**).
2. Export the client public keys from each Bitvise account and import them with **Chiavi pubbliche...**.
3. To prevent clients from seeing the fingerprint change warning, export the host keys from Bitvise in OpenSSH format (if the version in use allows it), copy them to `C:\ProgramData\ssh\` with the names `ssh_host_ed25519_key` / `ssh_host_rsa_key` and the corresponding `.pub` files. Otherwise, give the clients the new fingerprints.
4. Stop Bitvise and set its service to **Disabled**.
5. Apply the configuration, check that logons work, and only then uninstall Bitvise.

Feature mapping:

Bitvise SSH Server	WinSSH Manager
Centralized settings	`config.json`, applied with **APPLICA CONFIGURAZIONE**
Windows accounts / allowed groups	Server → **Chi può accedere** (Users / Groups)
Per-account IP access	Account → **Accesso solo da**
SFTP only, root folder, read-only mount	Account → **Solo SFTP**, **Cartella radice**, **Confina**, **Sola lettura**
Per-account forwarding permissions	Account → **Inoltro porte**
Per-account public keys	Account → **Chiavi pubbliche...**
IP access rules	tab**Firewall**
IP blocking	tab**Blocco IP**
Sessions, logs, host key fingerprints	tabs**Sessioni**, **Log** and **Stato**
Export / import settings	tab**Backup**

13. Text console and use from PowerShell

When the GUI is not available (SSH session, Server Core, emergencies), the same functions can be reached from a **PowerShell started as Administrator**.

13.1 Menu console

```
C:\ProgramData\WinSshManager\SshManager.ps1           # menu interattivo
C:\ProgramData\WinSshManager\SshManager.ps1 -Install  # installa/abilita OpenSSH
C:\ProgramData\WinSshManager\SshManager.ps1 -Apply    # applica la configurazione
C:\ProgramData\WinSshManager\SshManager.ps1 -Status   # stato sintetico
```

The main menu shows at the top the version, service status, port, number of accounts and IP blocking status, and indicates whether there are unapplied changes. The items are:

Item	Function	Item	Function
1	Stato dettagliato (Detailed status)	7	Log
2	Installa / abilita OpenSSH Server (Install / enable OpenSSH Server)	8	Impronte chiavi host (Host key fingerprints)
3	Impostazioni server (rete, autenticazione, accessi, firewall) (Server settings: network, authentication, access, firewall)	9	APPLICA CONFIGURAZIONE (APPLY CONFIGURATION)
4	Account e chiavi (Accounts and keys)	10	Anteprima sshd_config (sshd_config preview)
5	Sessioni attive (Active sessions)	11	Esporta / importa, modifica di config.json nel Blocco note (Export / import, editing config.json in Notepad)
6	Blocco IP (IP blocking)	12	Avvia / arresta servizio (Start / stop service)

At the prompts, pressing Enter keeps the value in square brackets; in lists, the `-` character clears the field. After each change, the console asks whether to apply it immediately.

13.2 Module commands

For automation, import the module directly:

```
Import-Module C:\ProgramData\WinSshManager\WinSshManager.psm1 -DisableNameChecking
Get-SshServerStatus
Set-SshManagedUser -Name mario -Mode Shell -AuthMethods publickey `
    -AllowTcpForwarding local -PermitOpen '127.0.0.1:3389'
Add-SshUserKey -Name mario -Path C:\temp\id_ed25519.pub
Update-SshServerConfiguration
Unblock-SshIp -Ip 203.0.113.9
```

Command	Function
`Install-SshManager`	Installs/enables OpenSSH and initializes
`Update-SshServerConfiguration`	Applies the configuration (`-NoRestart` to avoid restarting)
`Get-SshServerStatus`	Server status
`Get-SshManagedUser`, `Set-SshManagedUser`, `Remove-SshManagedUser`	Reading, creating/editing and removing accounts

Command	Function
`Get-SshUserKey`, `Add-SshUserKey`, `Remove-SshUserKey`	Public key management
`Get-SshSession`, `Stop-SshSession`	Active sessions
`Get-SshLog`	OpenSSH events (`-Last N`, `-FailuresOnly`)
`Get-SshBlockedIp`, `Block-SshIp`, `Unblock-SshIp`	Manual IP blocking (`Unblock-SshIp -Ip '*'` unblocks all)
`Enable-SshIpBlocker`, `Disable-SshIpBlocker`	Enabling the scheduled task
`Get-SshHostKeyFingerprint`	Host key fingerprints
`New-SshdConfigText -Config (Get-SshManagerConfig)`	Preview of `sshd_config`
`Export-SshManagerSettings`, `Import-SshManagerSettings`	Export and import (`-IncludeHostKeys`)

14. Limitations to be aware of

- **No virtual accounts**: every SSH user is a real Windows account. For SFTP-only access, it is advisable to create dedicated local accounts.
- **Only one folder per user**: the chroot is a single local folder; network drives, junctions and symbolic links inside it are not reliable.
- **Chroot for SFTP only**: in Shell mode the user is not confined (a limitation of OpenSSH for Windows).
- **Single shell**: the default shell applies to the whole server, not per account.
- **No FTPS**: SFTP and SCP only. SCP is available for Shell accounts, not for Solo SFTP accounts.
- **Local management only**: the GUI acts on the machine on which it is running.
- **OpenSSH updates**: they come from Windows Update; alternatively, you can install the Microsoft MSI version (`PowerShell/Win32-OpenSSH` project on GitHub), which is detected automatically.
- **On Windows 10/11** a sleeping PC does not respond: adjust the power options if it has to act as a server.
- **Domain controllers**: they have no local accounts; only domain accounts are used.

15. Troubleshooting

Problem	Probable cause and solution
«sshd -t ha rifiutato la configurazione generata» (sshd -t rejected the generated configuration)	The message indicates the line. Usually it is an option not supported by the installed version (try the **Default** algorithm profile) or a wrong line in **Righe aggiuntive sshd_config**. The running server has not been touched.
«Risposta non valida da PowerShell» (Invalid response from PowerShell)	Check that the `PowerShell` folder is next to the executable and that no GPO blocks `powershell.exe`. The full text of the error is in the Output operazioni panel.
The user cannot log on	tab**Log** with **Solo accessi falliti / negati**. Check that the account is in the Account tab and enabled, that the configuration has been applied, that the IP is allowed (Firewall and **Accesso solo da**) and that it is not blocked (Blocco IP tab).
Key logon refused	Often the key file has wrong permissions: apply the configuration again. For administrators, the key in `%USERPROFILE%\.ssh` is ignored: upload it with **Chiavi pubbliche...**. For domain accounts, check the first logon carefully.
SFTP with chroot does not work	The folder must exist, be local and not be a junction, and the user must have at least read permission on it.
You have locked yourself out	From the local console or via Remote Desktop: **Blocco IP** tab → **Sblocca selezionato**, then add your own network to the whitelist.
The server does not respond after a change	tab**Backup** → **Ripristina sshd_config da backup...**, then correct the settings.
OpenSSH installation failed	Install the **OpenSSH Server** optional feature from Settings → Apps → Optional features, or from the company FoD source, then **Installa / abilita OpenSSH**.

15.1 In-depth debugging

1. tab**Stato** → **Arresta**.
2. In an administrative PowerShell, run `& "$env:windir\System32\OpenSSH\sshd.exe" -d`. The server handles a single login and writes all the authentication steps on screen.
3. Try to log on from the client and read the reason for the refusal.
4. tab**Stato** → **Avvia**.

16. Uninstallation

From a PowerShell started as Administrator:

```
Import-Module C:\ProgramData\WinSshManager\WinSshManager.psm1 -DisableNameChecking
Disable-SshIpBlocker
Remove-NetFirewallRule -Name WinSSHManager-SSH-In, WinSSHManager-Blocklist -ErrorAction
SilentlyContinue
Enable-NetFirewallRule -Name OpenSSH-Server-In-TCP -ErrorAction SilentlyContinue
Remove-Item C:\ProgramData\WinSshManager -Recurse -Force
```

Before the last line, if you want to return to the original OpenSSH configuration, copy `backup\sshd_config.originale.*` to `C:\ProgramData\ssh\sshd_config`. Finally, delete the program folder.

OpenSSH Server, the Windows accounts, the `SSH-SFTP-Only` group and the keys in `C:\ProgramData\ssh` remain in place: remove them manually if they are no longer needed.

Appendix A. Objects created in the system

Object	Name	Notes
Service	`sshd`	Microsoft; set to automatic startup
Firewall rule	`WinSSHManager-SSH-In` («WinSSH Manager - SSH (TCP-In)»)	Access to the SSH port
Firewall rule	`WinSSHManager-Blocklist` («WinSSH Manager - IP bloccati»)	Blocked IPs
Scheduled task	`WinSSHManager-IPBlocker`	Run as SYSTEM
Local group	`SSH-SFTP-Only`	SFTP-only accounts, without interactive logon and RDP
Registry key	`HKLM\SOFTWARE\OpenSSH\DefaultShell`	Default shell
User rights	Deny log on locally / Deny log on through Remote Desktop Services	Assigned to the group `SSH-SFTP-Only`
Event log	Applications and Services Logs → OpenSSH → Operational	Microsoft; read by Log and Blocco IP

Appendix B. Glossary

Term	Meaning
sshd / sshd_config	The OpenSSH Server service and its configuration file
config.json	File in which WinSSH Manager keeps all the settings; it is used to generate `sshd_config`
Apply	Regenerate `sshd_config` from `config.json`, put it into use and restart the service
Host key	Key pair that identifies the server; its fingerprint allows the client to recognize it
Fingerprint	Short code that uniquely identifies a key (e.g. `SHA256:…`)
Public key	Publishable part of the client's key pair, uploaded to the server for passwordless logon
SFTP / SCP	File transfer protocols over SSH
Chroot	Confinement of the SFTP user to a folder, which the user sees as the root `/`
Port forwarding (tunnel)	Transport of a TCP connection through SSH: local (from the client to a destination reachable by the server) or remote (from the server to the client)
CIDR	IP network notation, e.g. `192.168.1.0/24` = from 192.168.1.0 to 192.168.1.255
Whitelist	List of addresses that are never blocked
UAC	Windows User Account Control: the confirmation prompt for running a program as administrator

WinSSH Manager

Manuel utilisateur

Gestion du serveur OpenSSH intégré à Windows

Windows 10/11 · Windows Server 2019, 2022, 2025

Édition octobre 2026

Sommaire

1. Introduction **38**
1.1 Qu'est-ce que WinSSH Manager 38
1.2 Systèmes pris en charge et configuration requise 38
1.3 Principe de fonctionnement 38
1.4 Conventions du manuel 39

2. Installation et premier démarrage **40**
2.1 Copie du programme 40
2.2 Premier démarrage 40
2.3 Emplacement d'enregistrement des données 41

3. La fenêtre principale **42**
3.1 Structure de la fenêtre 42
3.2 Boutons de la barre de commandes 42
3.3 Indicateur des modifications en attente 42
3.4 Avertissements avant l'application 43
3.5 Ce qui se passe lors de l'application 43

4. Onglet Stato **44**
4.1 Informations affichées 44
4.2 Boutons 45

5. Onglet Server **46**
5.1 Réseau 46
5.2 Authentification 47
5.3 Contrôle d'accès 47
5.4 Transferts et session 48
5.5 Chiffrement et journaux 48
5.6 Options avancées 48

6. Onglet Firewall **50**

7. Onglet Account **51**
7.1 Liste des comptes 51
7.2 Créer un compte 51
7.3 Modifier, activer et désactiver 53
7.4 Réinitialiser le mot de passe 53
7.5 Supprimer un compte 53
7.6 Clés publiques 53
7.7 Autorisations des dossiers SFTP 54

8. Onglet Sessioni **55**

9. Onglet Blocco IP **56**
9.1 Principe de fonctionnement 56
9.2 Paramètres 56
9.3 IP bloquées et registre 57

10. Onglet Log **58**

11. Onglet Backup **59**
11.1 Exporter les paramètres 59
11.2 Importer les paramètres 59
11.3 Restaurer sshd_config 59
11.4 Dossiers 59

12. Procédures guidées **60**
12.1 Mise en service conseillée 60
12.2 Administrateur avec clé et tunnel RDP/SQL 60
12.3 Fournisseur qui dépose des fichiers (SFTP uniquement) 60
12.4 Consultation en lecture seule 60
12.5 Changer le port sans perdre l'accès 60
12.6 Passer aux clés uniquement 61
12.7 Migrer depuis Bitvise SSH Server 61

13. Console texte et utilisation depuis PowerShell **62**
13.1 Console à menus 62
13.2 Commandes du module 62

14. Limites à connaître **64**

15. Résolution des problèmes **65**
15.1 Débogage approfondi 65

16. Désinstallation **66**

Annexe A. Objets créés dans le système **67**

Annexe B. Glossaire **68**

1. Introduction

1.1 Qu'est-ce que WinSSH Manager

WinSSH Manager est un panneau de configuration graphique pour le **serveur OpenSSH intégré à Windows**. Il permet de gérer le port, l'authentification, les comptes, les accès SFTP, le pare-feu et le blocage automatique des adresses IP depuis une seule fenêtre, selon un modèle de travail semblable à celui de Bitvise SSH Server : tous les paramètres se trouvent dans un seul fichier, et le serveur est reconfiguré à partir de ce fichier.

Le programme utilise exclusivement des composants Microsoft déjà présents dans le système : serveur OpenSSH, Pare-feu Windows, Planificateur de tâches, comptes locaux ou Active Directory, autorisations NTFS. Il n'installe aucun service propre et ne nécessite aucun logiciel tiers.

- **Serveur SSH** avec shell (PowerShell, PowerShell 7 ou Invite de commandes), SFTP et SCP ;
- **comptes SFTP uniquement** confinés dans un dossier, y compris en lecture seule ;
- **tunnels** (transfert de ports) autorisés par compte et limités à des destinations précises ;
- **clés publiques** gérées dans un magasin central, valables également pour les administrateurs ;
- **pare-feu** avec liste des adresses IP autorisées et **blocage automatique** des adresses IP qui échouent à plusieurs reprises lors de la connexion ;
- **sessions actives**, **journaux**, **empreintes des clés d'hôte**, **exportation et importation** des paramètres.

1.2 Systèmes pris en charge et configuration requise

Exigence	Détail
Système d'exploitation	Windows 10 (1809 ou version ultérieure), Windows 11, Windows Server 2019, 2022 et 2025
Composants	.NET Framework 4.8 et Windows PowerShell 5.1, déjà présents sur tous les systèmes énumérés
Serveur OpenSSH	Fonctionnalité facultative de Windows. Si elle est absente, le programme l'installe (voir chapitre 2)
Privilèges	Le programme doit être exécuté en tant qu'**administrateur** : au démarrage, Windows demande la confirmation UAC
Interface graphique	Nécessite l'Expérience utilisateur (Desktop Experience). Sur Server Core, on utilise la console texte (chapitre 13)

1.3 Principe de fonctionnement

Il n'y a qu'un seul principe à retenir : **les paramètres sont enregistrés dans config.json et ne prennent effet que lorsque la configuration est appliquée.**

1. Modifiez les champs des onglets **Server**, **Firewall** et **Blocco IP** et appuyez sur **Salva impostazioni** (Enregistrer les paramètres) : les valeurs sont écrites dans `config.json`. Les comptes (onglet **Account**) sont en revanche enregistrés dans `config.json` dès que vous validez leur fenêtre.
2. Appuyez sur **APPLICA CONFIGURAZIONE** (Appliquer la configuration) : le programme génère un nouveau `sshd_config` à partir de `config.json`, le vérifie avec `sshd -t` et, seulement s'il est valide, le met en service, aligne le pare-feu, les clés, les dossiers et le blocage IP, puis redémarre le service `sshd`.

C'est pourquoi `sshd_config` **ne doit pas être modifié à la main** : il est régénéré à chaque application et les modifications manuelles seraient perdues. Les directives que l'interface graphique ne prévoit pas se saisissent dans le champ **Righe aggiuntive sshd_config** (Lignes supplémentaires sshd_config) de l'onglet Server (paragraphe 5.6).

> **Remarque :** La fenêtre travaille toujours sur la machine sur laquelle elle est lancée. Pour administrer un serveur distant, utilisez l'interface graphique via le Bureau à distance, ou la console texte via SSH.

1.4 Conventions du manuel

- Les noms des boutons, onglets et champs sont en **gras**, exactement tels qu'ils apparaissent à l'écran.
- Les noms de fichiers, chemins, commandes et valeurs à saisir sont en `caractères à espacement fixe`.
- Les encadrés **Remarque**, **Conseil** et **Attention** signalent respectivement des informations utiles, des bonnes pratiques et des situations dans lesquelles vous risquez de perdre l'accès au serveur ou des données.

2. Installation et premier démarrage

2.1 Copie du programme

Le programme est un dossier qui contient `WinSshManagerGui.exe` et le sous-dossier `PowerShell`, qui constitue le moteur proprement dit. Il n'a pas de programme d'installation.

1. Copiez **l'ensemble du dossier** sur le serveur ou sur le PC, par exemple dans `C:\Program Files\WinSshManager\`.
2. Vérifiez que le sous-dossier `PowerShell` se trouve à côté de `WinSshManagerGui.exe`. S'il est absent, le message « Manca il motore PowerShell » (Moteur PowerShell manquant) apparaît au démarrage et le programme se ferme.
3. Si un autre serveur SSH (par exemple Bitvise) fonctionne sur la même machine et sur le même port, arrêtez-le d'abord, ou configurez OpenSSH sur un port différent pendant la période d'essai : deux serveurs ne peuvent pas écouter sur le même port.

2.2 Premier démarrage

Lancez `WinSshManagerGui.exe` et confirmez la demande UAC. Au premier démarrage, le programme lit l'état du système et propose l'opération nécessaire :

Situation détectée	Ce que propose le programme
Serveur OpenSSH non installé	« OpenSSH Server non risulta installato su questo sistema. Installarlo e abilitarlo ora? » (OpenSSH Server n'est pas installé sur ce système. L'installer et l'activer maintenant ?). Si vous répondez **Sì** (Oui), la fonctionnalité facultative est installée (sous Windows Server 2025, elle est déjà présente et est seulement activée). L'opération peut prendre quelques minutes.
OpenSSH présent, WinSSH Manager jamais initialisé	« WinSSH Manager non è ancora inizializzato su questo sistema (manca config.json) » (WinSSH Manager n'est pas encore initialisé sur ce système – config.json manquant). Si vous répondez **Sì**, l'initialisation est effectuée.
Déjà initialisé	Aucune question : la fenêtre s'ouvre sur l'onglet **Stato** (État).

L'installation ou l'initialisation effectue les opérations suivantes :

- configure le service `sshd` en démarrage automatique et le démarre (au premier démarrage, OpenSSH génère les clés d'hôte) ;
- configure le service `ssh-agent` en démarrage manuel ;
- crée le dossier de données `C:\ProgramData\WinSshManager` et le magasin de clés `C:\ProgramData\ssh\managed_keys`, accessibles uniquement à SYSTEM et Administrators ;
- crée `config.json` avec les valeurs par défaut, **en conservant le port** éventuellement déjà configuré dans `sshd_config` ;
- enregistre une copie du fichier `sshd_config` d'origine dans `backup\sshd_config.originale.<data-ora>`.

À la fin, le message « OpenSSH Server installato e abilitato. Definire gli account e premere APPLICA CONFIGURAZIONE » (OpenSSH Server installé et activé. Définissez les comptes et appuyez sur APPLICA CONFIGURAZIONE) apparaît. La même procédure peut être relancée à tout moment avec le bouton **Installa / abilita OpenSSH** (Installer / activer OpenSSH) de l'onglet Stato.

> **Attention :** Sous Windows 10/11 et Windows Server 2019/2022, l'installation télécharge la fonctionnalité depuis Windows Update. Dans les environnements avec WSUS et sans source pour les fonctionnalités à la demande (FoD), l'installation peut échouer : dans ce cas, installez d'abord **Serveur OpenSSH** depuis Paramètres → Applications → Fonctionnalités facultatives, puis relancez **Installa / abilita OpenSSH**.

> **Attention :** Après l'initialisation, le mode d'accès est **Users** mais il n'existe encore aucun compte : tant que vous n'en avez pas défini au moins un, le serveur accepte **n'importe quel** compte Windows valide. L'onglet Stato le signale en orange. Définissez immédiatement les comptes (chapitre 7) et appliquez.

2.3 Emplacement d'enregistrement des données

Chemin	Contenu
`C:\ProgramData\WinSshManager\config.json`	Source unique de tous les paramètres
`C:\ProgramData\WinSshManager\backup\`	Les 30 dernières versions de `sshd_config` et de `config.json`, plus le fichier `sshd_config` d'origine
`C:\ProgramData\WinSshManager\*.ps1, *.psm1`	Copie du moteur utilisée par la tâche planifiée du blocage IP, réalignée à chaque application
`C:\ProgramData\WinSshManager\ipblocker-state.json`	État du blocage IP (compteurs, IP bloquées, historique)
`C:\ProgramData\WinSshManager\ipblocker.log`	Registre des blocages et des déblocages
`C:\ProgramData\ssh\sshd_config`	Configuration d'OpenSSH, **générée** par le programme
`C:\ProgramData\ssh\managed_keys\`	Magasin central des clés publiques, un fichier par compte
`C:\ProgramData\ssh\administrators_authorized_keys`	Fichier standard de Microsoft pour les clés des administrateurs (géré par OpenSSH, respecté par le programme)
`C:\ProgramData\ssh\banner.txt`	Texte de la bannière avant connexion

Le dossier `C:\ProgramData\WinSshManager` n'est accessible en lecture et en écriture qu'à SYSTEM et Administrators, car il contient des scripts exécutés en tant que SYSTEM par la tâche planifiée.

3. La fenêtre principale

3.1 Structure de la fenêtre

La fenêtre principale (« WinSSH Manager - OpenSSH Server per Windows ») est divisée en quatre zones, de haut en bas :

Zone	Fonction
Onglets	Huit onglets : **Stato**, **Server**, **Firewall**, **Account**, **Sessioni**, **Blocco IP**, **Log**, **Backup**. Ils sont décrits un par un aux chapitres 4 à 11.
Sortie des opérations	Panneau sombre contenant les messages produits par chaque opération, précédés de l'heure. Les erreurs commencent par « ERRORE: ». C'est le premier endroit à consulter si quelque chose ne va pas.
Barre de commandes	Boutons **Ricarica** (Recharger), **Salva impostazioni**, **Salva e applica** (Enregistrer et appliquer), **APPLICA CONFIGURAZIONE** et l'indicateur des modifications en attente.
Barre d'état	Affiche « Pronto » (Prêt), ou la description de l'opération en cours avec une barre de progression.

Les opérations s'exécutent en arrière-plan : pendant leur exécution, les onglets et la barre de commandes sont désactivés, mais la fenêtre reste réactive. Il n'est pas possible de fermer le programme pendant une opération.

3.2 Boutons de la barre de commandes

Bouton	Action
Ricarica	Relit `config.json` et met à jour l'onglet courant. S'il existe des modifications non enregistrées, demande s'il faut les abandonner.
Salva impostazioni	Contrôle les valeurs des onglets **Server**, **Firewall** et **Blocco IP** et les écrit dans `config.json`. Ne modifie pas le serveur en fonctionnement. Les comptes n'ont pas besoin de ce bouton : ils s'enregistrent automatiquement.
Salva e applica	Enregistre comme ci-dessus, puis applique immédiatement la configuration. Avant de poursuivre, affiche les avertissements concernant les changements risqués (voir 3.4).
APPLICA CONFIGURAZIONE	Génère `sshd_config` à partir de `config.json`, le vérifie, le met en service et redémarre le service (voir 3.5). S'il existe des paramètres non enregistrés, demande d'abord s'il faut les enregistrer.

3.3 Indicateur des modifications en attente

À côté des boutons, l'état du travail apparaît en orange :

Indicateur	Signification et action à effectuer
« Impostazioni modificate e non salvate » (Paramètres modifiés et non enregistrés)	Des champs des onglets Server, Firewall ou Blocco IP ont été modifiés. Appuyez sur **Salva impostazioni** ou sur **Salva e applica**.
« Modifiche salvate ma non ancora applicate » (Modifications enregistrées mais pas encore appliquées)	`config.json` contient des paramètres différents de ceux en service. Appuyez sur **APPLICA CONFIGURAZIONE**.
(vide)	Le serveur utilise exactement la configuration enregistrée.

À la fermeture de la fenêtre, le programme demande confirmation s'il existe des modifications non enregistrées ou enregistrées mais non appliquées.

3.4 Avertissements avant l'application

Certaines modifications peuvent bloquer l'accès de l'administrateur lui-même. Avec **Salva e applica**, le programme les énumère et demande confirmation avant de poursuivre :

- **authentification par mot de passe désactivée** : vérifiez que les comptes disposent d'une clé publique ;
- **port modifié** : les clients devront se connecter au nouveau port ;
- **pare-feu restreint** à une liste d'adresses : si vous administrez à distance, votre propre adresse IP doit figurer dans la liste.

> **Attention :** Les avertissements n'apparaissent qu'avec **Salva e applica**. Si vous enregistrez avec **Salva impostazioni** puis appuyez sur **APPLICA CONFIGURAZIONE**, la configuration est appliquée sans ce contrôle. Pour les changements de port, d'authentification et de pare-feu, utilisez toujours **Salva e applica**.

3.5 Ce qui se passe lors de l'application

APPLICA CONFIGURAZIONE effectue, dans l'ordre :

1. génère un `sshd_config` candidat à partir de `config.json` et le vérifie avec `sshd -t`. **S'il n'est pas valide, rien n'est modifié** et l'erreur est affichée, avec l'indication de la ligne en cause ;
2. enregistre le fichier `sshd_config` en service dans le dossier `backup` et écrit le nouveau ;
3. écrit la bannière, définit le shell par défaut, protège le magasin de clés, crée les dossiers racine SFTP avec leurs autorisations, met à jour le groupe `SSH-SFTP-Only` et les restrictions d'accès, met à jour les règles du pare-feu et active ou désactive la tâche du blocage IP ;
4. redémarre le service `sshd`.

> **Remarque :** Le redémarrage de `sshd` peut interrompre les sessions SSH en cours. Si vous administrez le serveur via SSH, prévoyez de vous reconnecter ; les nouvelles règles s'appliquent de toute façon à toutes les connexions suivantes.

4. Onglet Stato

C'est l'onglet qui s'ouvre au démarrage ; il est mis à jour chaque fois que vous le sélectionnez. Il résume la situation du serveur.

4.1 Informations affichées

Élément	Signification
Installato (Installé)	« Sì » en vert si le serveur OpenSSH est présent, « NO » en rouge dans le cas contraire
Versione (Version)	Version d'OpenSSH for Windows détectée
Eseguibile (Exécutable)	Chemin de `sshd.exe` (fonctionnalité de Windows ou version MSI de Microsoft)
Servizio sshd (Service sshd)	État et type de démarrage du service (par ex. « Running / Automatic »), en vert s'il est en cours d'exécution
Porta, Indirizzi di ascolto (Port, Adresses d'écoute)	Valeurs enregistrées dans `config.json`
Shell predefinita (Shell par défaut)	Shell défini dans le Registre. S'il n'est pas défini, « cmd.exe (default Windows) »
Account definiti (Comptes définis)	Nombre de comptes dans l'onglet Account
Controllo accessi (Contrôle d'accès)	Mode **Users**, **Groups** ou **Any**. En orange s'il s'agit de **Any**, ou de **Users** sans compte : dans les deux cas, n'importe quel compte Windows valide peut se connecter
Firewall	État et profils de la règle gérée, ou « regola gestita assente » (règle gérée absente)
Blocco IP	État de la tâche planifiée et nombre d'IP bloquées, ou « disattivato » (désactivé)
sshd_config	« Allineato alla configurazione » (Aligné sur la configuration) en vert, ou « Differisce dalla configurazione: premere APPLICA CONFIGURAZIONE » (Diffère de la configuration : appuyez sur APPLICA CONFIGURAZIONE) en orange

4.2 Boutons

Bouton	Fonction
Aggiorna stato (Actualiser l'état)	Relit toutes les informations
Installa / abilita OpenSSH	Installe ou active le serveur OpenSSH et initialise WinSSH Manager (paragraphe 2.2). N'écrase pas un fichier `config.json` existant
Avvia, **Arresta**, **Riavvia**	Commandent le service `sshd` (Démarrer, Arrêter, Redémarrer). **Arresta** demande confirmation car il ferme toutes les sessions SSH actives
Anteprima sshd_config (Aperçu sshd_config)	Affiche le fichier qui serait généré avec les paramètres **enregistrés**. Ne l'applique pas. S'il existe à l'écran des modifications non enregistrées, le programme avertit qu'elles ne sont pas incluses
sshd_config attuale (sshd_config actuel)	Affiche le fichier actuellement en service
Impronte chiavi host (Empreintes des clés d'hôte)	Affiche pour chaque clé d'hôte les empreintes SHA256, MD5 et Bubble Babble

> **Conseil :** Lors de la première connexion, le client SSH affiche l'empreinte de la clé du serveur et demande de la confirmer. Comparez-la avec l'empreinte **SHA256** affichée par **Impronte chiavi host** avant de l'accepter : c'est la garantie que vous êtes connecté au bon serveur.

5. Onglet Server

Contient les paramètres globaux du serveur SSH. Après les modifications, appuyez sur **Salva impostazioni** (ou **Salva e applica**). Chaque champ dispose d'une info-bulle qui apparaît lorsque vous le survolez avec la souris.

5.1 Réseau

Champ	Description	Par défaut
Porta TCP (Port TCP)	Port sur lequel le serveur accepte les connexions (1–65535)	22
Indirizzi di ascolto (Adresses d'écoute)	Adresses IP locales sur lesquelles écouter, séparées par des virgules. `0.0.0.0` = toutes les adresses IPv4, `::` = toutes les adresses IPv6. Les réseaux CIDR ne sont pas admis. Si le champ reste vide, les deux sont utilisés	`0.0.0.0, ::`
Connessioni non autenticate (Connexions non authentifiées)	Directive `MaxStartups` : un nombre, ou `début:pourcentage:maximum`. Avec `10:30:100`, au-delà de 10 connexions en attente d'ouverture de session, les nouvelles sont refusées avec une probabilité croissante à partir de 30 %, jusqu'au refus total à 100	`10:30:100`
Sessioni per connessione (Sessions par connexion)	Nombre de canaux (shell, SFTP, tunnel) ouverts sur une même connexion (1–100)	10
Keepalive (secondi, 0 = off) (Keepalive en secondes, 0 = désactivé)	Intervalle en secondes auquel le serveur vérifie que le client est toujours présent	60
Keepalive senza risposta (Keepalive sans réponse)	Nombre de contrôles sans réponse après lequel la connexion est fermée	3
Compressione (Compression)	Active la compression des données	Non

> **Remarque :** Avec les valeurs par défaut, une connexion interrompue (réseau coupé, PC éteint) est fermée par le serveur après environ 3 minutes (60 s × 3).

5.2 Authentification

Champ	Description	Par défaut
Consenti autenticazione con password (Autoriser l'authentification par mot de passe)	Accès avec le mot de passe du compte Windows	Oui
Consenti autenticazione con chiave pubblica (Autoriser l'authentification par clé publique)	Accès avec les clés chargées pour chaque compte (paragraphe 7.6)	Oui
Consenti password vuote (sconsigliato) (Autoriser les mots de passe vides – déconseillé)	Permet l'accès à des comptes sans mot de passe	Non
Tentativi per connessione (Tentatives par connexion)	Tentatives d'authentification admises avant la fermeture de la connexion (1–20)	4
Tempo per il login (s) (Délai d'ouverture de session)	Secondes accordées pour terminer l'ouverture de session (10–600)	60
Banner pre-login (Bannière avant connexion)	Texte affiché par le client avant la demande d'identifiants. Vide = aucune bannière	vide

Au moins une des deux méthodes, mot de passe ou clé publique, doit rester active : le programme ne permet pas d'enregistrer si les deux sont désactivées. La méthode peut ensuite être restreinte pour chaque compte (paragraphe 7.2).

5.3 Contrôle d'accès

Champ	Description
Chi può accedere (Qui peut se connecter)	**Users** : uniquement les comptes définis dans l'onglet Account (conseillé, comme dans Bitvise). **Groups** : les membres des groupes Windows indiqués. **Any** : n'importe quel compte Windows valide.
Gruppi ammessi (Groupes autorisés)	Uniquement en mode Groups, séparés par des virgules. Exemples : `ssh-utenti`, `CONTOSO\gruppo-ssh`. En mode Groups, au moins un groupe est obligatoire
Account sempre negati (Comptes toujours refusés)	Comptes exclus dans tous les cas, séparés par des virgules. Les comptes désactivés dans l'onglet Account sont ajoutés automatiquement
Nega accesso interattivo e Desktop remoto agli account solo-SFTP (Refuser l'ouverture de session interactive et le Bureau à distance aux comptes SFTP uniquement)	Les comptes locaux en mode Solo SFTP sont placés dans le groupe `SSH-SFTP-Only`, auquel l'accès à la console et au Bureau à distance est refusé. Par défaut : activé

> **Attention :** En mode **Users** sans aucun compte défini, OpenSSH ne reçoit aucune restriction et accepte **tous** les comptes Windows valides.

> **Remarque :** Le refus de l'ouverture de session interactive est configuré au moyen de la stratégie de sécurité locale (`secedit`). Sur une machine membre d'un domaine, une GPO qui définit les mêmes droits utilisateur est prioritaire et peut l'annuler.

5.4 Transferts et session

Champ	Description	Par défaut
Inoltro porte predefinito (Transfert de ports par défaut)	Valeur pour les comptes qui ne la redéfinissent pas : `no`, `yes` (local et distant), `local` (uniquement du client vers le serveur), `remote` (uniquement du serveur vers le client)	`no`
GatewayPorts	`no` : les transferts distants n'écoutent que sur le localhost du serveur. `yes` : sur toutes les interfaces. `clientspecified` : c'est le client qui décide	`no`
Consenti inoltro dell'agent SSH (Autoriser le transfert de l'agent SSH)	Permet d'utiliser sur le serveur l'agent SSH du client	Non
Shell predefinita (Shell par défaut)	`powershell` (Windows PowerShell 5.1), `pwsh` (PowerShell 7, s'il est installé), `cmd`, ou le chemin complet d'un exécutable. S'applique à tous les comptes. Si l'exécutable n'existe pas, le paramètre est ignoré avec un avertissement dans le panneau Output	`powershell`

5.5 Chiffrement et journaux

Champ	Description	Par défaut
Profilo algoritmi (Profil d'algorithmes)	**Modern** : uniquement des algorithmes actuels (curve25519, ML-KEM/sntrup s'ils sont disponibles, AES-GCM, ChaCha20, clés Ed25519, ECDSA et RSA-SHA2). **Compatible** : ajoute les échanges NIST, `diffie-hellman-group14-sha256`, `hmac-sha1` et les clés `ssh-rsa` pour les clients anciens. **Default** : conserve les valeurs par défaut d'OpenSSH. Les algorithmes non pris en charge par la version installée sont exclus automatiquement.	Modern
Livello log (Niveau de journalisation)	Niveau de détail des messages dans le journal des événements : de `QUIET` à `DEBUG3`. `INFO` suffit pour les accès et le blocage IP ; `VERBOSE` ajoute l'empreinte de la clé utilisée lors de l'ouverture de session	INFO

> **Conseil :** N'utilisez **Compatible** que si certains clients ne parviennent plus à se connecter (anciennes versions de PuTTY, équipements réseau, bibliothèques SFTP anciennes).

5.6 Options avancées

Le champ **Righe aggiuntive sshd_config** accueille des directives globales d'OpenSSH que l'interface graphique ne prévoit pas, une par ligne. Elles sont insérées telles quelles, avant les blocs par utilisateur, et vérifiées avec `sshd -t` lors de l'application : une ligne erronée empêche l'application mais n'endommage pas le serveur en fonctionnement.

> **Attention :** N'insérez pas ici de blocs `Match` : ils seraient suivis des directives générées par le programme et en modifieraient la signification.

6. Onglet Firewall

Le programme gère une règle du Pare-feu Windows dédiée au serveur SSH, équivalente aux « IP access rules » de Bitvise : les connexions provenant d'adresses non répertoriées sont rejetées avant même d'atteindre OpenSSH.

Champ	Description	Par défaut
Gestisci il Windows Firewall per il server SSH (Gérer le Pare-feu Windows pour le serveur SSH)	S'il est désactivé, le programme ne modifie pas le pare-feu (les règles existantes restent telles quelles)	Oui
Profili di rete (Profils réseau)	**Dominio**, **Privato**, **Pubblico** (Domaine, Privé, Public) : les profils sur lesquels le port est ouvert. Si le pare-feu est géré, au moins un profil est obligatoire	Dominio, Privato
IP / reti ammessi (IP / réseaux autorisés)	Une par ligne. Valeurs admises : `Any`, `LocalSubnet`, adresses individuelles (`203.0.113.10`), réseaux CIDR (`192.168.1.0/24`), plages (`10.0.0.1-10.0.0.50`). Vide équivaut à `Any`	`Any`
Disattiva le regole OpenSSH predefinite di Windows (Désactiver les règles OpenSSH par défaut de Windows)	Désactive la règle de trafic entrant créée par Microsoft lors de l'installation, qui ouvrirait le port 22 à tous	Oui

Indications sur les profils :

- **Serveurs** : profil **Dominio**. N'ajoutez **Pubblico** que si la carte réseau exposée est classée comme publique.
- **PC et ordinateurs portables** : **Dominio** et **Privato**. Sur les réseaux publics (hôtels, points d'accès), le port reste fermé, comme il se doit.

Deux règles sont créées :

Nom complet	Fonction
WinSSH Manager - SSH (TCP-In)	Autorise les connexions au port SSH depuis les adresses autorisées, uniquement pour l'exécutable `sshd.exe`
WinSSH Manager - IP bloccati	Bloque les adresses IP ajoutées par le blocage automatique ou manuellement (chapitre 9). S'applique à tous les profils, uniquement pour le port SSH

> **Attention :** Si vous administrez le serveur à distance via SSH, votre propre adresse (ou votre propre réseau) doit figurer dans **IP / reti ammessi**, sinon, dès la première **Applica** (application), la connexion suivante sera refusée.

7. Onglet Account

Chaque compte SSH correspond à un **compte Windows réel**, local ou Active Directory : OpenSSH pour Windows ne prend pas en charge les comptes virtuels. L'onglet répertorie les comptes autorisés et leurs règles.

> **Remarque :** Les modifications des comptes sont enregistrées dans `config.json` dès que vous validez ; elles deviennent actives avec **APPLICA CONFIGURAZIONE**.

7.1 Liste des comptes

Colonne	Contenu
Account	Nom du compte Windows (`nome` pour un compte local, `DOMINIO\nome` pour un compte de domaine)
Attivo (Actif)	« Sì » ou « No ». Les comptes désactivés sont grisés
Accesso (Accès)	« Shell » ou « Solo SFTP » (SFTP uniquement)
Cartella radice (Dossier racine)	Dossier SFTP du compte
Opzioni (Options)	« chroot » si l'utilisateur est confiné dans le dossier, « sola lettura » (lecture seule)
Inoltro (Transfert)	Autorisation de transfert de ports
Autenticazione (Authentification)	Méthode d'authentification exigée
Da IP (Depuis IP)	Adresses depuis lesquelles le compte peut se connecter
Descrizione (Description)	Remarque libre

Boutons : **Nuovo...** (Nouveau), **Modifica...** (Modifier ; ou double-clic sur la ligne), **Chiavi pubbliche...** (Clés publiques), **Abilita / disabilita** (Activer / désactiver), **Reimposta password...** (Réinitialiser le mot de passe), **Elimina...** (Supprimer). Tous sauf **Nuovo...** agissent sur le compte sélectionné.

7.2 Créer un compte

Nuovo... ouvre la fenêtre « Nuovo account SSH » (Nouveau compte SSH), divisée en sections.

Identità (Identité)

Champ	Description
Account Windows (Compte Windows)	Compte local : uniquement le nom (par ex. `mario`). Compte Active Directory : `DOMINIO\nome`. Les espaces, `@` et les apostrophes ne sont pas admis ; le nom d'un compte local ne peut pas dépasser 20 caractères. Après la création, le nom n'est plus modifiable
Descrizione (Description)	Remarque libre, reportée également comme commentaire dans `sshd_config`
Account abilitato (Compte activé)	S'il est désactivé, le compte reste dans la configuration mais l'accès lui est refusé

Account Windows locale (Compte Windows local)

Section présente uniquement lors de la création et uniquement pour les comptes locaux.

Champ	Description
Crea l'account Windows locale se non esiste (Créer le compte Windows local s'il n'existe pas)	Si le compte n'existe pas, il est créé avec le mot de passe indiqué, un mot de passe qui n'expire jamais et que l'utilisateur ne peut pas modifier. Les comptes en mode Shell sont également placés dans le groupe Users
Password, Conferma password (Mot de passe, Confirmer le mot de passe)	Utilisés uniquement si le compte doit être créé. Le mot de passe n'est enregistré dans aucun fichier de configuration et n'apparaît ni dans les journaux ni dans la liste des processus

Si vous enregistrez un compte local qui n'existe pas sans le faire créer, le programme avertit que l'ouverture de session ne sera pas possible tant que le compte Windows n'existe pas.

Tipo di accesso (Type d'accès)

Option	Description
Shell completa (Shell complet)	Terminal, SFTP, SCP et tunnels (s'ils sont autorisés). L'utilisateur n'est confiné dans aucun dossier
Solo SFTP (SFTP uniquement)	Transfert de fichiers uniquement. L'utilisateur ne peut ni ouvrir de terminal ni utiliser l'agent ; le transfert de ports est interdit sauf paramétrage explicite contraire
Cartella radice SFTP (Dossier racine SFTP)	Uniquement pour Solo SFTP. Chemin **local** complet (par ex. `D:\SFTP\mario`), qu'il est possible de sélectionner avec **Sfoglia...** (Parcourir). Les dossiers réseau ne sont pas admis. Il est créé lors de l'application s'il n'existe pas
Confina nella cartella (chroot) (Confiner dans le dossier)	Disponible si un dossier est indiqué. L'utilisateur voit le dossier comme `/` et ne peut pas en sortir. Sans chroot, le dossier n'est que le dossier de départ
Sola lettura (Lecture seule)	L'utilisateur peut télécharger mais ne peut pas charger, modifier ou supprimer de fichiers

> **Attention :** Le dossier racine doit être un véritable dossier local : les lecteurs réseau, les jonctions et les liens symboliques à l'intérieur du dossier ne fonctionnent pas de manière fiable avec OpenSSH pour Windows.

Inoltro porte (tunnel) (Transfert de ports)

Champ	Description
Inoltro consentito (Transfert autorisé)	`default` (utilise la valeur globale de l'onglet Server), `no`, `local`, `remote`, `yes`
Destinazioni (locale) (Destinations – local)	Actif avec `local` ou `yes`. Destinations accessibles avec le transfert local, au format `hôte:port`, séparées par des virgules. Par ex. `127.0.0.1:3389, sql01:1433`. Vide = toutes
Porte in ascolto (remoto) (Ports en écoute – distant)	Actif avec `remote` ou `yes`. Ports que l'utilisateur peut ouvrir sur le serveur, au format `[hôte:]port`. Par ex. `8080`. Vide = tous. Nécessite OpenSSH 7.8 ou version ultérieure

Sicurezza (Sécurité)

Champ	Description
Autenticazione (Authentification)	`default` (le paramètre global s'applique), `password`, `publickey`, `publickey+password` (les **deux** sont nécessaires : d'abord la clé, puis le mot de passe)
Accesso solo da (Accès uniquement depuis)	Adresses IP ou réseaux CIDR depuis lesquels le compte peut se connecter, séparés par des virgules. Vide = depuis n'importe quelle adresse

Lorsque vous appuyez sur **Salva** (Enregistrer), le compte est enregistré. Si la méthode d'authentification exige une clé publique, le programme ouvre immédiatement la fenêtre des clés pour en ajouter une.

7.3 Modifier, activer et désactiver

- **Modifica...** (ou un double-clic) ouvre la même fenêtre avec les données du compte ; le nom n'est pas modifiable et la section de création du compte Windows n'apparaît pas.
- **Abilita / disabilita** inverse l'état du compte. Après l'application, un compte désactivé est refusé par OpenSSH, mais le compte Windows reste actif pour les autres usages.

7.4 Réinitialiser le mot de passe

Reimposta password... demande le nouveau mot de passe du compte Windows **local** sélectionné et le définit immédiatement, sans qu'il soit nécessaire d'appliquer. Pour les comptes de domaine, le programme rappelle que le mot de passe se gère dans Active Directory.

7.5 Supprimer un compte

Elimina... pose trois questions successives :

1. « Rimuovere l'account dalla configurazione SSH? » (Supprimer le compte de la configuration SSH ?) — retire le compte de `config.json` ;
2. « Eliminare anche le sue chiavi pubbliche dall'archivio centrale? » (Supprimer également ses clés publiques du magasin central ?) ;
3. uniquement pour les comptes locaux : « Eliminare anche l'account Windows locale? » (Supprimer également le compte Windows local ?). L'opération est irréversible ; le profil utilisateur reste sur le disque.

Après la suppression, appuyez sur **APPLICA CONFIGURAZIONE**.

7.6 Clés publiques

Chiavi pubbliche... ouvre la liste des clés du compte sélectionné, avec un numéro progressif et l'empreinte (bits, SHA256, commentaire, type).

Bouton	Fonction
Incolla chiave... (Coller une clé)	Permet de coller une ou plusieurs clés publiques, une par ligne, au format `ssh-ed25519 AAAA… commentaire`
Importa file .pub... (Importer un fichier .pub)	Permet de sélectionner le fichier de clé publique généré par le client
Elimina selezionata (Supprimer la sélection)	Supprime la clé sélectionnée, après confirmation
Chiudi (Fermer)	Ferme la fenêtre

- Chaque clé est vérifiée avec `ssh-keygen` : les lignes non reconnues sont ignorées avec un avertissement, les doublons sont ignorés.
- Une **clé privée** est toujours refusée. Si vous collez le mauvais fichier par erreur, le programme le signale.
- Les clés sont enregistrées dans `C:\ProgramData\ssh\managed_keys\<account>` (pour les comptes de domaine `managed_keys\dominio\nome`) avec les autorisations exigées par OpenSSH.
- Les clés du magasin central s'appliquent **également aux administrateurs**. Pour les comptes administrateurs, OpenSSH ignore en revanche le fichier `%USERPROFILE%\.ssh\authorized_keys` : seuls `administrators_authorized_keys` et le magasin central s'appliquent.
- Les clés ajoutées ou supprimées s'appliquent immédiatement aux nouvelles connexions, sans qu'il soit nécessaire d'appliquer (à condition que la configuration ait déjà été appliquée au moins une fois).

> **Conseil :** Sur le client, la paire de clés se génère avec `ssh-keygen -t ed25519`. Seul le fichier se terminant par `.pub` doit être chargé sur le serveur ; la clé privée ne doit jamais quitter le PC du client.

7.7 Autorisations des dossiers SFTP

Lors de l'application de la configuration, le programme crée les dossiers racine manquants et attribue au compte les autorisations NTFS suivantes :

Type de compte	Autorisations attribuées
SFTP uniquement, lecture et écriture	Sur le dossier racine : lecture seule (l'utilisateur ne peut ni le supprimer ni le renommer). Sur les fichiers et sous-dossiers : modification
SFTP uniquement, lecture seule	Lecture et exécution sur toute l'arborescence

Les autorisations sont ajoutées à celles existantes, elles ne les remplacent pas. Si le dossier contient des données réservées à d'autres utilisateurs, vérifiez les autorisations héritées avant de l'attribuer.

8. Onglet Sessioni

Répertorie les connexions SSH actives sur le port du serveur, mises à jour chaque fois que vous ouvrez l'onglet.

Colonne	Contenu
Id	Identifiant du processus de la session
Utente (Utilisateur)	Compte connecté, ou « (autenticazione in corso) » (authentification en cours) si l'ouverture de session n'est pas encore terminée
Remoto (Distant)	Adresse et port du client
Inizio (Début)	Date et heure d'ouverture de la connexion

- **Aggiorna** (Actualiser) : relit la liste.
- **Disconnetti selezionata** (Déconnecter la sélection) : ferme la session sélectionnée, après confirmation. Le service principal n'est jamais arrêté.
- **Aggiorna ogni 10 secondi** (Actualiser toutes les 10 secondes) : mise à jour automatique, active uniquement lorsque l'onglet est affiché.

9. Onglet Blocco IP

Le blocage IP, équivalent à l'« IP blocking » de Bitvise, détecte les adresses qui échouent à plusieurs reprises lors de la connexion et les bloque dans le pare-feu pendant une durée définie.

9.1 Principe de fonctionnement

- Une tâche planifiée, `WinSSHManager-IPBlocker`, s'exécute en tant que SYSTEM : à chaque nouvel événement du journal d'OpenSSH, toutes les 5 minutes (pour faire expirer les blocages) et au démarrage du système.
- Sont comptés comme échecs : mot de passe ou clé erronés, utilisateur inexistant, dépassement du nombre de tentatives admises, utilisateur non autorisé (« not allowed because »).
- Lorsqu'une adresse IP dépasse le seuil dans l'intervalle défini, elle est ajoutée à la règle de pare-feu « WinSSH Manager - IP bloccati ».
- À l'expiration, le blocage est supprimé automatiquement, au plus tard dans les 5 minutes.
- Ne sont jamais bloquées : `127.0.0.1`, `::1` et les adresses de la liste blanche.

9.2 Paramètres

Volet de gauche. Les paramètres s'enregistrent et s'appliquent avec les boutons de la barre de commandes en bas.

Champ	Description	Par défaut
Blocco automatico attivo (Blocage automatique actif)	Active ou désactive le blocage. La modification de la tâche planifiée a lieu dès l'enregistrement	Oui
Fallimenti per bloccare (Échecs avant blocage)	Nombre de tentatives échouées qui déclenche le blocage (1–1000)	5
Nell'arco di (minuti) (Sur une période de – minutes)	Intervalle pendant lequel les échecs sont comptés (1–1440)	10
Durata blocco (minuti) (Durée du blocage – minutes)	Durée du blocage temporaire (jusqu'à un an)	60
Permanente dopo N blocchi (Permanent après N blocages)	Nombre de blocages sur 30 jours au-delà duquel le blocage devient permanent. 0 = jamais	0
Chiudi le sessioni già aperte dall'IP bloccato (Fermer les sessions déjà ouvertes par l'IP bloquée)	Lors du blocage, ferme également les connexions déjà établies depuis cette adresse	Oui
Mai bloccare (whitelist) (Ne jamais bloquer – liste blanche)	Adresses IP ou réseaux CIDR, un par ligne	`127.0.0.1`, `::1`

> **Attention :** Ajoutez **toujours** à la liste blanche le réseau depuis lequel vous administrez le serveur. Quelques fautes de frappe dans le mot de passe suffisent pour vous bloquer vous-même.

9.3 IP bloquées et registre

À droite apparaissent la liste **IP bloccati** (IP bloquées : IP ou réseau, du, jusqu'au, motif ; « permanente » pour les blocages sans expiration) et le **Registro blocchi** (Registre des blocages) avec les 300 dernières lignes de `ipblocker.log`. Le registre fait l'objet d'une rotation automatique au-delà de 1 Mo.

Bouton	Fonction
Aggiorna (Actualiser)	Relit la liste et le registre
Blocca IP... (Bloquer une IP)	Bloque manuellement une adresse ou un réseau CIDR. Demande la durée en minutes ; `0` = permanent
Sblocca selezionato (Débloquer la sélection)	Supprime le blocage de l'adresse IP sélectionnée et remet à zéro ses échecs
Sblocca tutti (Tout débloquer)	Supprime tous les blocages et remet à zéro tous les compteurs, après confirmation
Esegui un ciclo ora (Exécuter un cycle maintenant)	Analyse immédiatement le journal sans attendre la tâche planifiée

10. Onglet Log

Affiche les événements du journal **OpenSSH/Operational**, du plus récent au plus ancien. Il est chargé à la première ouverture de l'onglet.

- En **vert** les connexions réussies, en **rouge** celles qui ont échoué ou ont été refusées.
- **Un double-clic** sur une ligne ouvre le texte complet de l'événement.
- **Solo accessi falliti / negati** (Uniquement les accès échoués / refusés) filtre les événements d'erreur.
- **Eventi** (Événements) détermine le nombre d'événements à afficher (10–5000, 200 par défaut).
- **Aggiorna** relit le journal avec les critères définis.
- **Apri Visualizzatore eventi** (Ouvrir l'Observateur d'événements) ouvre directement le journal OpenSSH/Operational dans l'Observateur d'événements de Windows.

> **Conseil :** Lorsqu'un utilisateur ne parvient pas à se connecter, activez **Solo accessi falliti / negati** et recherchez son nom : le message indique presque toujours la cause (mot de passe erroné, clé non acceptée, utilisateur non autorisé ou connecté depuis une adresse IP non autorisée).

11. Onglet Backup

11.1 Exporter les paramètres

Esporta... (Exporter) crée une archive zip (nom proposé `WinSshManager-AAAAMMGG.zip`) contenant :

- `config.json` ;
- le magasin des clés publiques des comptes ;
- `administrators_authorized_keys` ;
- uniquement si **Includi le chiavi host** (Inclure les clés d'hôte) est sélectionné : les clés d'hôte du serveur.

> **Attention :** Les clés d'hôte sont des clés **privées** : toute personne en possession du zip peut usurper l'identité du serveur. Ne les incluez que pour migrer le serveur sur une autre machine en conservant les mêmes empreintes, et conservez le fichier comme un mot de passe.

11.2 Importer les paramètres

Importa... (Importer) lit un zip exporté précédemment :

- remplace `config.json` (une copie de la version actuelle est conservée dans `backup`) ;
- ajoute les clés publiques et `administrators_authorized_keys` contenus dans le zip ;
- si **Importa anche le chiavi host, se presenti nel file** (Importer également les clés d'hôte, si elles sont présentes dans le fichier) est sélectionné, remplace les clés d'hôte ;
- à la fin, demande s'il faut appliquer immédiatement la configuration.

11.3 Restaurer sshd_config

Ripristina sshd_config da backup... (Restaurer sshd_config depuis une sauvegarde) permet de choisir l'une des versions enregistrées dans `C:\ProgramData\WinSshManager\backup`. Le fichier choisi est vérifié avec `sshd -t` et mis en service, puis le service est redémarré.

> **Attention :** La restauration n'agit que sur `sshd_config`. `config.json` reste inchangé : lors de la prochaine **Applica**, ses paramètres seront appliqués de nouveau. Utilisez la restauration comme solution d'urgence, puis corrigez les paramètres dans les onglets.

11.4 Dossiers

Apri cartella dati (Ouvrir le dossier de données) ouvre `C:\ProgramData\WinSshManager` ; **Apri cartella ssh** (Ouvrir le dossier ssh) ouvre `C:\ProgramData\ssh`.

12. Procédures guidées

Les procédures suivantes couvrent les cas les plus courants. À la fin de chacune, appuyez sur **APPLICA CONFIGURAZIONE** sauf indication contraire.

12.1 Mise en service conseillée

1. Onglet **Server** : port 22, ou un port élevé si le serveur est exposé sur Internet (cela réduit le bruit dans les journaux, mais ne constitue pas en soi une mesure de sécurité) ; **Chi può accedere** = **Users** ; **Profilo algoritmi** = **Modern** ; shell `powershell` ou `pwsh`.
2. Onglet **Firewall** : profils adaptés à la machine (chapitre 6) et, dans **IP / reti ammessi**, le réseau local plus les adresses IP publiques depuis lesquelles vous vous connectez.
3. Onglet **Blocco IP** : conservez les valeurs par défaut et ajoutez le réseau d'administration à la liste blanche.
4. **Salva e applica**.
5. Onglet **Account** : créez les comptes (paragraphes suivants) et appliquez.
6. Vérifiez depuis le serveur lui-même avec `ssh nomeutente@localhost` et, pour les comptes SFTP, `sftp nomeutente@localhost`. Depuis un autre PC, comparez l'empreinte présentée avec **Stato → Impronte chiavi host**.

12.2 Administrateur avec clé et tunnel RDP/SQL

1. **Nuovo...**, compte Windows existant (par ex. le compte de l'administrateur).
2. **Shell completa**.
3. **Inoltro consentito** = `local` ; **Destinazioni** = `127.0.0.1:3389, 127.0.0.1:1433`.
4. **Autenticazione** = `publickey`.
5. **Salva**, puis ajoutez la clé publique dans la fenêtre qui s'ouvre.
6. Appliquez. Depuis le client : `ssh -L 13389:127.0.0.1:3389 utente@server`, puis connectez-vous avec le Bureau à distance à `localhost:13389`.

12.3 Fournisseur qui dépose des fichiers (SFTP uniquement)

1. **Nuovo...**, nom d'un compte local dédié (par ex. `fornitore`), **Crea l'account Windows locale** avec un mot de passe robuste.
2. **Solo SFTP** ; **Cartella radice** = `D:\SFTP\fornitore` ; activez **Confina nella cartella**.
3. **Autenticazione** = `password` (ou `publickey`, si le fournisseur dispose d'une clé).
4. **Accesso solo da** = l'adresse IP publique du fournisseur.
5. Appliquez. L'utilisateur voit le dossier comme `/` ; il peut charger et gérer les fichiers qu'il contient, mais ne peut ni supprimer le dossier lui-même, ni accéder à la console ou au Bureau à distance.

12.4 Consultation en lecture seule

Comme dans le cas précédent, en activant également **Sola lettura**. L'utilisateur peut uniquement télécharger : OpenSSH refuse les écritures et les autorisations NTFS attribuées sont en lecture seule.

12.5 Changer le port sans perdre l'accès

1. Si vous travaillez à distance, assurez-vous que le nouveau numéro de port est accessible (routeur, pare-feu périmétrique).
2. Modifiez **Porta TCP** et appuyez sur **Salva e applica** ; confirmez l'avertissement.
3. La règle de pare-feu gérée est automatiquement déplacée sur le nouveau port.
4. Ouvrez une **nouvelle** connexion sur le nouveau port (`ssh -p NUOVAPORTA utente@server`) **avant** de fermer la connexion existante.

12.6 Passer aux clés uniquement

1. Pour chaque compte, vérifiez dans la fenêtre **Chiavi pubbliche...** qu'il existe au moins une clé et testez la connexion par clé.
2. Onglet **Server** : désactivez **Consenti autenticazione con password**.
3. **Salva e applica** et confirmez l'avertissement.

Vous pouvez également n'exiger la clé que pour certains comptes, en définissant pour ceux-ci **Autenticazione** = `publickey`.

12.7 Migrer depuis Bitvise SSH Server

1. Dans Bitvise, répertoriez les comptes et leurs autorisations. Les comptes virtuels doivent être recréés en tant que comptes Windows locaux (**Nuovo...** avec **Crea l'account Windows locale**).
2. Exportez les clés publiques des clients depuis chaque compte Bitvise et importez-les avec **Chiavi pubbliche...**.
3. Pour éviter que les clients voient l'avertissement de changement d'empreinte, exportez depuis Bitvise les clés d'hôte au format OpenSSH (si la version utilisée le permet), copiez-les dans `C:\ProgramData\ssh\` sous les noms `ssh_host_ed25519_key` / `ssh_host_rsa_key` avec les fichiers `.pub` correspondants. Sinon, communiquez les nouvelles empreintes aux clients.
4. Arrêtez Bitvise et configurez son service sur **Désactivé**.
5. Appliquez la configuration, vérifiez les accès et seulement ensuite désinstallez Bitvise.

Correspondance entre les fonctions :

Bitvise SSH Server	WinSSH Manager
Paramètres centralisés	`config.json`, appliqué avec **APPLICA CONFIGURAZIONE**
Windows accounts / groupes autorisés	Server → **Chi può accedere** (Users / Groups)
Accès depuis IP par compte	Account → **Accesso solo da**
SFTP uniquement, dossier racine, montage en lecture seule	Account → **Solo SFTP**, **Cartella radice**, **Confina**, **Sola lettura**
Autorisations de transfert par compte	Account → **Inoltro porte**
Clés publiques par compte	Account → **Chiavi pubbliche...**
IP access rules	Onglet **Firewall**
IP blocking	Onglet **Blocco IP**
Sessions, journaux, empreintes des clés d'hôte	Onglets **Sessioni**, **Log**, **Stato**
Export / import settings	Onglet **Backup**

13. Console texte et utilisation depuis PowerShell

Lorsque l'interface graphique n'est pas disponible (session SSH, Server Core, urgences), les mêmes fonctions sont accessibles depuis une **fenêtre PowerShell lancée en tant qu'administrateur**.

13.1 Console à menus

```
C:\ProgramData\WinSshManager\SshManager.ps1           # menu interattivo
C:\ProgramData\WinSshManager\SshManager.ps1 -Install  # installa/abilita OpenSSH
C:\ProgramData\WinSshManager\SshManager.ps1 -Apply    # applica la configurazione
C:\ProgramData\WinSshManager\SshManager.ps1 -Status   # stato sintetico
```

Le menu principal affiche en en-tête la version, l'état du service, le port, le nombre de comptes et l'état du blocage IP, et signale s'il existe des modifications non appliquées. Les options sont les suivantes :

Option	Fonction	Option	Fonction
1	Stato dettagliato (État détaillé)	7	Log
2	Installa / abilita OpenSSH Server (Installer / activer OpenSSH Server)	8	Impronte chiavi host (Empreintes des clés d'hôte)
3	Impostazioni server (rete, autenticazione, accessi, firewall) (Paramètres du serveur : réseau, authentification, accès, pare-feu)	9	APPLICA CONFIGURAZIONE (Appliquer la configuration)
4	Account e chiavi (Comptes et clés)	10	Anteprima sshd_config (Aperçu sshd_config)
5	Sessioni attive (Sessions actives)	11	Esporta / importa, modifica di config.json nel Blocco note (Exporter / importer, modification de config.json dans le Bloc-notes)
6	Blocco IP (Blocage IP)	12	Avvia / arresta servizio (Démarrer / arrêter le service)

Dans les questions, appuyer sur Entrée conserve la valeur indiquée entre crochets ; dans les listes, le caractère `-` vide le champ. Après chaque modification, la console demande s'il faut appliquer immédiatement.

13.2 Commandes du module

Pour l'automatisation, importez directement le module :

```
Import-Module C:\ProgramData\WinSshManager\WinSshManager.psm1 -DisableNameChecking
Get-SshServerStatus
Set-SshManagedUser -Name mario -Mode Shell -AuthMethods publickey `
    -AllowTcpForwarding local -PermitOpen '127.0.0.1:3389'
Add-SshUserKey -Name mario -Path C:\temp\id_ed25519.pub
Update-SshServerConfiguration
Unblock-SshIp -Ip 203.0.113.9
```

Commande	Fonction
`Install-SshManager`	Installe/active OpenSSH et initialise
`Update-SshServerConfiguration`	Applique la configuration (`-NoRestart` pour ne pas redémarrer)
`Get-SshServerStatus`	État du serveur

Commande	Fonction
`Get-SshManagedUser`, `Set-SshManagedUser`, `Remove-SshManagedUser`	Lecture, création/modification, suppression des comptes
`Get-SshUserKey`, `Add-SshUserKey`, `Remove-SshUserKey`	Gestion des clés publiques
`Get-SshSession`, `Stop-SshSession`	Sessions actives
`Get-SshLog`	Événements OpenSSH (`-Last N`, `-FailuresOnly`)
`Get-SshBlockedIp`, `Block-SshIp`, `Unblock-SshIp`	Blocage IP manuel (`Unblock-SshIp -Ip '*'` débloque tout)
`Enable-SshIpBlocker`, `Disable-SshIpBlocker`	Activation de la tâche planifiée
`Get-SshHostKeyFingerprint`	Empreintes des clés d'hôte
`New-SshdConfigText -Config (Get-SshManagerConfig)`	Aperçu de `sshd_config`
`Export-SshManagerSettings`, `Import-SshManagerSettings`	Exportation et importation (`-IncludeHostKeys`)

14. Limites à connaître

- **Aucun compte virtuel** : chaque utilisateur SSH est un compte Windows réel. Pour les accès SFTP uniquement, il est conseillé de créer des comptes locaux dédiés.
- **Un seul dossier par utilisateur** : le chroot est un seul dossier local ; les lecteurs réseau, les jonctions et les liens symboliques à l'intérieur ne sont pas fiables.
- **Chroot uniquement pour SFTP** : en mode Shell, l'utilisateur n'est pas confiné (limite d'OpenSSH pour Windows).
- **Shell unique** : le shell par défaut s'applique à l'ensemble du serveur, et non à chaque compte.
- **Pas de FTPS** : uniquement SFTP et SCP. SCP est disponible pour les comptes Shell, pas pour les comptes Solo SFTP.
- **Gestion locale uniquement** : l'interface graphique agit sur la machine sur laquelle elle est lancée.
- **Mises à jour d'OpenSSH** : elles arrivent par Windows Update ; vous pouvez également installer la version MSI de Microsoft (projet `PowerShell/Win32-OpenSSH` sur GitHub), qui est détectée automatiquement.
- **Sous Windows 10/11**, un PC en veille ne répond pas : ajustez les options d'alimentation s'il doit faire office de serveur.
- **Contrôleurs de domaine** : ils n'ont pas de comptes locaux ; seuls des comptes de domaine sont utilisés.

15. Résolution des problèmes

Problème	Cause probable et solution
« sshd -t ha rifiutato la configurazione generata » (sshd -t a refusé la configuration générée)	Le message indique la ligne. Il s'agit généralement d'une option non prise en charge par la version installée (essayez le profil d'algorithmes **Default**) ou d'une ligne erronée dans **Righe aggiuntive sshd_config**. Le serveur en fonctionnement n'a pas été modifié.
« Risposta non valida da PowerShell » (Réponse non valide de PowerShell)	Vérifiez que le dossier `PowerShell` se trouve à côté de l'exécutable et qu'aucune GPO ne bloque `powershell.exe`. Le texte complet de l'erreur figure dans le panneau Output operazioni.
L'utilisateur ne parvient pas à se connecter	Onglet **Log** avec **Solo accessi falliti / negati**. Vérifiez que le compte figure dans l'onglet Account et qu'il est activé, que la configuration a été appliquée, que l'adresse IP est autorisée (Firewall et **Accesso solo da**) et qu'elle n'est pas bloquée (onglet Blocco IP).
Connexion par clé refusée	Souvent, le fichier des clés a des autorisations erronées : appliquez de nouveau la configuration. Pour les administrateurs, la clé située dans `%USERPROFILE%\.ssh` est ignorée : chargez-la avec **Chiavi pubbliche...**. Pour les comptes de domaine, vérifiez attentivement la première connexion.
SFTP avec chroot ne fonctionne pas	Le dossier doit exister, être local et ne pas être une jonction, et l'utilisateur doit disposer au moins de l'autorisation de lecture.
Vous vous êtes bloqué vous-même	Depuis la console locale ou via le Bureau à distance : onglet **Blocco IP** → **Sblocca selezionato**, puis ajoutez votre propre réseau à la liste blanche.
Le serveur ne répond plus après une modification	Onglet **Backup** → **Ripristina sshd_config da backup...**, puis corrigez les paramètres.
Échec de l'installation d'OpenSSH	Installez la fonctionnalité facultative **Serveur OpenSSH** depuis Paramètres → Applications → Fonctionnalités facultatives, ou depuis la source FoD de l'entreprise, puis **Installa / abilita OpenSSH**.

15.1 Débogage approfondi

1. Onglet **Stato** → **Arresta**.
2. Dans une fenêtre PowerShell d'administration, exécutez `& "$env:windir\System32\OpenSSH\sshd.exe" -d`. Le serveur gère une seule ouverture de session et affiche à l'écran toutes les étapes de l'authentification.
3. Tentez la connexion depuis le client et lisez le motif du refus.
4. Onglet **Stato** → **Avvia**.

16. Désinstallation

Depuis une fenêtre PowerShell lancée en tant qu'administrateur :

```
Import-Module C:\ProgramData\WinSshManager\WinSshManager.psm1 -DisableNameChecking
Disable-SshIpBlocker
Remove-NetFirewallRule -Name WinSSHManager-SSH-In, WinSSHManager-Blocklist -ErrorAction
SilentlyContinue
Enable-NetFirewallRule -Name OpenSSH-Server-In-TCP -ErrorAction SilentlyContinue
Remove-Item C:\ProgramData\WinSshManager -Recurse -Force
```

Avant la dernière ligne, si vous souhaitez revenir à la configuration d'origine d'OpenSSH, copiez `backup\sshd_config.originale.*` dans `C:\ProgramData\ssh\sshd_config`. Supprimez enfin le dossier du programme.

Le serveur OpenSSH, les comptes Windows, le groupe `SSH-SFTP-Only` et les clés situées dans `C:\ProgramData\ssh` restent en place : supprimez-les manuellement s'ils ne sont plus nécessaires.

Annexe A. Objets créés dans le système

Objet	Nom	Remarques
Service	`sshd`	De Microsoft ; configuré en démarrage automatique
Règle de pare-feu	`WinSSHManager-SSH-In` (« WinSSH Manager - SSH (TCP-In) »)	Accès au port SSH
Règle de pare-feu	`WinSSHManager-Blocklist` (« WinSSH Manager - IP bloccati »)	IP bloquées
Tâche planifiée	`WinSSHManager-IPBlocker`	Exécutée en tant que SYSTEM
Groupe local	`SSH-SFTP-Only`	Comptes SFTP uniquement, sans ouverture de session interactive ni RDP
Clé de Registre	`HKLM\SOFTWARE\OpenSSH\DefaultShell`	Shell par défaut
Droits utilisateur	Interdire l'ouverture d'une session locale / par les services Bureau à distance	Attribués au groupe `SSH-SFTP-Only`
Journal des événements	Journaux des applications et des services → OpenSSH → Operational	De Microsoft ; lu par les onglets Log et Blocco IP

Annexe B. Glossaire

Terme	Signification
sshd / sshd_config	Le service OpenSSH Server et son fichier de configuration
config.json	Fichier dans lequel WinSSH Manager conserve tous les paramètres ; c'est à partir de lui qu'est généré `sshd_config`
Appliquer	Régénérer `sshd_config` à partir de `config.json`, le mettre en service et redémarrer le service
Clé d'hôte	Paire de clés qui identifie le serveur ; son empreinte permet au client de le reconnaître
Empreinte (fingerprint)	Code court qui identifie de manière unique une clé (par ex. `SHA256:…`)
Clé publique	Partie publiable de la paire de clés du client, chargée sur le serveur pour l'accès sans mot de passe
SFTP / SCP	Protocoles de transfert de fichiers sur SSH
Chroot	Confinement de l'utilisateur SFTP dans un dossier, qu'il voit comme la racine `/`
Transfert de ports (tunnel)	Transport d'une connexion TCP à travers SSH : local (du client vers une destination accessible depuis le serveur) ou distant (du serveur vers le client)
CIDR	Notation des réseaux IP, par ex. `192.168.1.0/24` = de 192.168.1.0 à 192.168.1.255
Liste blanche (whitelist)	Liste d'adresses qui ne sont jamais bloquées
UAC	Contrôle de compte d'utilisateur de Windows : la demande de confirmation pour exécuter un programme en tant qu'administrateur

WinSSH Manager

Manuale utente

Gestione dell'OpenSSH Server integrato in Windows

Windows 10/11 · Windows Server 2019, 2022, 2025

Edizione ottobre 2026

Indice

1. Introduzione **72**
1.1 Che cos'è WinSSH Manager 72
1.2 Sistemi supportati e requisiti 72
1.3 Come funziona 72
1.4 Convenzioni del manuale 73

2. Installazione e primo avvio **74**
2.1 Copia del programma 74
2.2 Primo avvio 74
2.3 Dove vengono salvati i dati 75

3. La finestra principale **76**
3.1 Struttura della finestra 76
3.2 Pulsanti della barra comandi 76
3.3 Indicatore delle modifiche in sospeso 76
3.4 Avvisi prima di applicare 77
3.5 Che cosa succede quando si applica 77

4. Scheda Stato **78**
4.1 Informazioni mostrate 78
4.2 Pulsanti 78

5. Scheda Server **79**
5.1 Rete 79
5.2 Autenticazione 79
5.3 Controllo accessi 80
5.4 Inoltri e sessione 80
5.5 Crittografia e log 81
5.6 Avanzate 81

6. Scheda Firewall **82**

7. Scheda Account **83**
7.1 Elenco degli account 83
7.2 Creare un account 83
7.3 Modificare, abilitare e disabilitare 85
7.4 Reimpostare la password 85
7.5 Eliminare un account 85
7.6 Chiavi pubbliche 85
7.7 Permessi delle cartelle SFTP 86

8. Scheda Sessioni **87**

9. Scheda Blocco IP **88**
9.1 Come funziona 88
9.2 Impostazioni 88
9.3 IP bloccati e registro 89

10. Scheda Log **90**

11. Scheda Backup **91**
11.1 Esportare le impostazioni 91
11.2 Importare le impostazioni 91
11.3 Ripristinare sshd_config 91
11.4 Cartelle 91

12. Procedure guidate **92**
12.1 Messa in servizio consigliata 92
12.2 Amministratore con chiave e tunnel RDP/SQL 92
12.3 Fornitore che deposita file (solo SFTP) 92
12.4 Consultazione in sola lettura 92
12.5 Cambiare la porta senza perdere l'accesso 92
12.6 Passare alle sole chiavi 93
12.7 Migrare da Bitvise SSH Server 93

13. Console testuale e uso da PowerShell **94**
13.1 Console a menu 94
13.2 Comandi del modulo 94

14. Limiti da conoscere **96**

15. Risoluzione dei problemi **97**
15.1 Debug approfondito 97

16. Disinstallazione **98**

Appendice A. Oggetti creati nel sistema **99**

Appendice B. Glossario **100**

1. Introduzione

1.1 Che cos'è WinSSH Manager

WinSSH Manager è un pannello di controllo grafico per l'**OpenSSH Server integrato in Windows**. Permette di gestire porta, autenticazione, account, accessi SFTP, firewall e blocco automatico degli IP da un'unica finestra, con un modello di lavoro simile a quello di Bitvise SSH Server: tutte le impostazioni stanno in un solo file, e il server viene riconfigurato a partire da quel file.

Il programma usa esclusivamente componenti Microsoft già presenti nel sistema: OpenSSH Server, Windows Firewall, Utilità di pianificazione, account locali o di Active Directory, permessi NTFS. Non installa servizi propri e non richiede software di terze parti.

- **Server SSH** con shell (PowerShell, PowerShell 7 o Prompt dei comandi), SFTP e SCP;
- **account solo SFTP** confinati in una cartella, anche in sola lettura;
- **tunnel** (inoltro porte) consentiti per singolo account e limitati a destinazioni precise;
- **chiavi pubbliche** gestite in un archivio centrale, valide anche per gli amministratori;
- **firewall** con elenco degli IP ammessi e **blocco automatico** degli IP che sbagliano ripetutamente l'accesso;
- **sessioni attive**, **log**, **impronte delle chiavi host**, **esportazione e importazione** delle impostazioni.

1.2 Sistemi supportati e requisiti

Requisito	Dettaglio
Sistema operativo	Windows 10 (1809 o successivo), Windows 11, Windows Server 2019, 2022 e 2025
Componenti	.NET Framework 4.8 e Windows PowerShell 5.1, già presenti su tutti i sistemi elencati
OpenSSH Server	Funzionalità facoltativa di Windows. Se manca, il programma la installa (vedi capitolo 2)
Privilegi	Il programma va eseguito come **Amministratore**: all'avvio Windows chiede la conferma UAC
Interfaccia grafica	Richiede l'Esperienza desktop. Su Server Core si usa la console testuale (capitolo 13)

1.3 Come funziona

Il principio da tenere presente è uno solo: **le impostazioni si salvano in config.json e diventano effettive solo quando si applica la configurazione.**

1. Si modificano i campi nelle schede **Server**, **Firewall** e **Blocco IP** e si preme **Salva impostazioni**: i valori vengono scritti in `config.json`. Gli account (scheda **Account**) vengono invece salvati in `config.json` appena si conferma la loro finestra.
2. Si preme **APPLICA CONFIGURAZIONE**: il programma genera un nuovo `sshd_config` a partire da `config.json`, lo verifica con `sshd -t` e solo se è valido lo mette in uso, allinea firewall, chiavi, cartelle e blocco IP e riavvia il servizio `sshd`.

Per questo motivo `sshd_config` **non va modificato a mano**: a ogni applicazione viene rigenerato e le modifiche manuali andrebbero perse. Le direttive che la GUI non prevede si inseriscono nel campo **Righe aggiuntive sshd_config** della scheda Server (paragrafo 5.6).

> **Nota:** La finestra lavora sempre sulla macchina su cui è avviata. Per amministrare un server remoto si usa la GUI via Desktop remoto, oppure la console testuale via SSH.

1.4 Convenzioni del manuale

- I nomi di pulsanti, schede e campi sono in **grassetto**, esattamente come compaiono a video.
- Nomi di file, percorsi, comandi e valori da digitare sono in `carattere a spaziatura fissa`.
- I riquadri **Nota**, **Consiglio** e **Attenzione** segnalano rispettivamente informazioni utili, buone pratiche e situazioni in cui si rischia di perdere l'accesso al server o dei dati.

2. Installazione e primo avvio

2.1 Copia del programma

Il programma è una cartella che contiene `WinSshManagerGui.exe` e la sottocartella `PowerShell`, che è il motore vero e proprio. Non ha un programma di installazione.

1. Copiare **l'intera cartella** sul server o sul PC, per esempio in `C:\Program Files\WinSshManager\`.
2. Verificare che la sottocartella `PowerShell` si trovi accanto a `WinSshManagerGui.exe`. Se manca, all'avvio compare il messaggio «Manca il motore PowerShell» e il programma si chiude.
3. Se sulla stessa macchina è in funzione un altro server SSH (per esempio Bitvise) sulla stessa porta, arrestarlo prima, oppure configurare per il periodo di prova OpenSSH su una porta diversa: due server non possono ascoltare sulla stessa porta.

2.2 Primo avvio

Avviare `WinSshManagerGui.exe` e confermare la richiesta UAC. Al primo avvio il programma legge lo stato del sistema e propone l'operazione necessaria:

Situazione rilevata	Cosa propone il programma
OpenSSH Server non installato	«OpenSSH Server non risulta installato su questo sistema. Installarlo e abilitarlo ora?». Rispondendo **Sì** viene installata la funzionalità facoltativa (su Windows Server 2025 è già presente e viene solo abilitata). L'operazione può richiedere alcuni minuti.
OpenSSH presente, WinSSH Manager mai inizializzato	«WinSSH Manager non è ancora inizializzato su questo sistema (manca config.json)». Rispondendo **Sì** viene eseguita l'inizializzazione.
Già inizializzato	Nessuna domanda: la finestra si apre sulla scheda **Stato**.

L'installazione o l'inizializzazione esegue queste operazioni:

- imposta il servizio `sshd` su avvio automatico e lo avvia (al primo avvio OpenSSH genera le chiavi host);
- imposta il servizio `ssh-agent` su avvio manuale;
- crea la cartella dati `C:\ProgramData\WinSshManager` e l'archivio delle chiavi `C:\ProgramData\ssh\managed_keys`, accessibili solo a SYSTEM e Administrators;
- crea `config.json` con i valori predefiniti, **conservando la porta** eventualmente già configurata in `sshd_config`;
- salva una copia dell'`sshd_config` originale in `backup\sshd_config.originale.<data-ora>`.

Al termine compare il messaggio «OpenSSH Server installato e abilitato. Definire gli account e premere APPLICA CONFIGURAZIONE». La stessa procedura si può rilanciare in qualsiasi momento con il pulsante **Installa / abilita OpenSSH** della scheda Stato.

> **Attenzione:** Su Windows 10/11 e Windows Server 2019/2022 l'installazione scarica la funzionalità da Windows Update. In ambienti con WSUS e senza sorgente per le funzionalità facoltative (FoD) l'installazione può fallire: in quel caso installare prima **OpenSSH Server** da Impostazioni → App → Funzionalità facoltative, poi rilanciare **Installa / abilita OpenSSH**.
>
> **Attenzione:** Dopo l'inizializzazione la modalità di accesso è **Users** ma non c'è ancora nessun account: finché non se ne definisce almeno uno, il server accetta **qualsiasi** account Windows valido. La scheda Stato lo segnala in arancione. Definire subito gli account (capitolo 7) e applicare.

2.3 Dove vengono salvati i dati

Percorso	Contenuto
`C:\ProgramData\WinSshManager\config.json`	Unica sorgente di tutte le impostazioni
`C:\ProgramData\WinSshManager\backup\`	Ultime 30 versioni di `sshd_config` e di `config.json`, più l'`sshd_config` originale
`C:\ProgramData\WinSshManager\*.ps1, *.psm1`	Copia del motore usata dall'attività pianificata del blocco IP, riallineata a ogni applicazione
`C:\ProgramData\WinSshManager\ipblocker-state.json`	Stato del blocco IP (contatori, IP bloccati, storico)
`C:\ProgramData\WinSshManager\ipblocker.log`	Registro dei blocchi e degli sblocchi
`C:\ProgramData\ssh\sshd_config`	Configurazione di OpenSSH, **generata** dal programma
`C:\ProgramData\ssh\managed_keys\`	Archivio centrale delle chiavi pubbliche, un file per account
`C:\ProgramData\ssh\administrators_authorized_keys`	File standard di Microsoft per le chiavi degli amministratori (gestito da OpenSSH, rispettato dal programma)
`C:\ProgramData\ssh\banner.txt`	Testo del banner pre-login

La cartella `C:\ProgramData\WinSshManager` è leggibile e scrivibile solo da SYSTEM e Administrators, perché contiene script eseguiti come SYSTEM dall'attività pianificata.

3. La finestra principale

3.1 Struttura della finestra

La finestra principale («WinSSH Manager - OpenSSH Server per Windows») è divisa in quattro zone, dall'alto verso il basso:

Zona	Funzione
Schede	Otto schede: **Stato**, **Server**, **Firewall**, **Account**, **Sessioni**, **Blocco IP**, **Log**, **Backup**. Sono descritte una per una nei capitoli 4–11.
Output operazioni	Pannello scuro con i messaggi prodotti da ogni operazione, preceduti dall'orario. Gli errori iniziano con «ERRORE:». È il primo posto da guardare se qualcosa non va.
Barra comandi	Pulsanti **Ricarica**, **Salva impostazioni**, **Salva e applica**, **APPLICA CONFIGURAZIONE** e l'indicatore delle modifiche in sospeso.
Barra di stato	Mostra «Pronto», oppure la descrizione dell'operazione in corso con una barra di avanzamento.

Le operazioni girano in background: mentre sono in corso schede e barra comandi sono disattivate, ma la finestra resta reattiva. Non è possibile chiudere il programma durante un'operazione.

3.2 Pulsanti della barra comandi

Pulsante	Cosa fa
Ricarica	Rilegge `config.json` e aggiorna la scheda corrente. Se ci sono modifiche non salvate chiede se scartarle.
Salva impostazioni	Controlla i valori delle schede **Server**, **Firewall** e **Blocco IP** e li scrive in `config.json`. Non tocca il server in funzione. Gli account non servono questo pulsante: si salvano da soli.
Salva e applica	Salva come sopra e subito dopo applica la configurazione. Prima di procedere mostra gli avvisi sui cambi rischiosi (vedi 3.4).
APPLICA CONFIGURAZIONE	Genera `sshd_config` da `config.json`, lo verifica, lo mette in uso e riavvia il servizio (vedi 3.5). Se ci sono impostazioni non salvate chiede prima di salvarle.

3.3 Indicatore delle modifiche in sospeso

Accanto ai pulsanti compare in arancione lo stato del lavoro:

Indicatore	Significato e cosa fare
«Impostazioni modificate e non salvate»	Sono stati cambiati campi di Server, Firewall o Blocco IP. Premere **Salva impostazioni** oppure **Salva e applica**.
«Modifiche salvate ma non ancora applicate»	`config.json` contiene impostazioni diverse da quelle in uso. Premere **APPLICA CONFIGURAZIONE**.
(vuoto)	Il server sta usando esattamente la configurazione salvata.

Alla chiusura della finestra il programma chiede conferma se esistono modifiche non salvate o salvate ma non applicate.

3.4 Avvisi prima di applicare

Alcune modifiche possono chiudere fuori l'amministratore stesso. Con **Salva e applica** il programma le elenca e chiede conferma prima di procedere:

- **autenticazione con password disattivata**: verificare che gli account abbiano una chiave pubblica;
- **porta cambiata**: i client dovranno collegarsi alla nuova porta;
- **firewall ristretto** a un elenco di indirizzi: se si amministra da remoto, il proprio IP deve essere nell'elenco.

> **Attenzione:** Gli avvisi compaiono solo con **Salva e applica**. Se si salva con **Salva impostazioni** e poi si preme **APPLICA CONFIGURAZIONE**, la configurazione viene applicata senza questo controllo. Per i cambi di porta, autenticazione e firewall usare sempre **Salva e applica**.

3.5 Che cosa succede quando si applica

APPLICA CONFIGURAZIONE esegue, nell'ordine:

1. genera un `sshd_config` candidato da `config.json` e lo verifica con `sshd -t`. **Se non è valido non modifica nulla** e mostra l'errore, che indica la riga problematica;
2. salva l'`sshd_config` in uso nella cartella `backup` e scrive quello nuovo;
3. scrive il banner, imposta la shell predefinita, protegge l'archivio chiavi, crea le cartelle radice SFTP con i loro permessi, aggiorna il gruppo `SSH-SFTP-Only` e le restrizioni di accesso, aggiorna le regole del firewall e attiva o disattiva l'attività del blocco IP;
4. riavvia il servizio `sshd`.

> **Nota:** Il riavvio di `sshd` può interrompere le sessioni SSH in corso. Se si sta amministrando il server via SSH, prevedere di ricollegarsi; le nuove regole valgono comunque per tutte le connessioni successive.

4. Scheda Stato

È la scheda che si apre all'avvio e viene aggiornata ogni volta che la si seleziona. Riassume la situazione del server.

4.1 Informazioni mostrate

Voce	Significato
Installato	«Sì» in verde se OpenSSH Server è presente, «NO» in rosso altrimenti
Versione	Versione di OpenSSH for Windows rilevata
Eseguibile	Percorso di `sshd.exe` (funzionalità di Windows o versione MSI di Microsoft)
Servizio sshd	Stato e tipo di avvio del servizio (es. «Running / Automatic»), in verde se è in esecuzione
Porta, Indirizzi di ascolto	Valori salvati in `config.json`
Shell predefinita	Shell impostata nel registro. Se non è impostata, «cmd.exe (default Windows)»
Account definiti	Numero di account nella scheda Account
Controllo accessi	Modalità **Users**, **Groups** o **Any**. In arancione se è **Any**, oppure **Users** senza account: in entrambi i casi entra qualsiasi account Windows valido
Firewall	Stato e profili della regola gestita, oppure «regola gestita assente»
Blocco IP	Stato dell'attività pianificata e numero di IP bloccati, oppure «disattivato»
sshd_config	«Allineato alla configurazione» in verde, oppure «Differisce dalla configurazione: premere APPLICA CONFIGURAZIONE» in arancione

4.2 Pulsanti

Pulsante	Funzione
Aggiorna stato	Rilegge tutte le informazioni
Installa / abilita OpenSSH	Installa o abilita OpenSSH Server e inizializza WinSSH Manager (paragrafo 2.2). Non sovrascrive un `config.json` esistente
Avvia, **Arresta**, **Riavvia**	Comandano il servizio `sshd`. **Arresta** chiede conferma perché chiude tutte le sessioni SSH attive
Anteprima sshd_config	Mostra il file che verrebbe generato con le impostazioni **salvate**. Non lo applica. Se a video ci sono modifiche non salvate, il programma avverte che non sono incluse
sshd_config attuale	Mostra il file attualmente in uso
Impronte chiavi host	Mostra per ogni chiave host le impronte SHA256, MD5 e Bubble Babble

> **Consiglio:** Alla prima connessione il client SSH mostra l'impronta della chiave del server e chiede di confermarla. Confrontarla con l'impronta **SHA256** mostrata da **Impronte chiavi host** prima di accettare: è la garanzia di essersi collegati al server giusto.

5. Scheda Server

Contiene le impostazioni globali del server SSH. Dopo le modifiche premere **Salva impostazioni** (o **Salva e applica**). Ogni campo ha un suggerimento che compare passandoci sopra con il mouse.

5.1 Rete

Campo	Descrizione	Predefinito
Porta TCP	Porta su cui il server accetta le connessioni (1–65535)	22
Indirizzi di ascolto	Indirizzi IP locali su cui ascoltare, separati da virgola. `0.0.0.0` = tutti gli IPv4, `::` = tutti gli IPv6. Non sono ammesse reti CIDR. Se il campo resta vuoto vengono usati entrambi	`0.0.0.0, ::`
Connessioni non autenticate	Direttiva `MaxStartups`: un numero, oppure `inizio:percentuale:massimo`. Con `10:30:100`, oltre 10 connessioni in attesa di login le nuove vengono rifiutate con probabilità crescente dal 30%, fino al rifiuto totale a 100	`10:30:100`
Sessioni per connessione	Numero di canali (shell, SFTP, tunnel) aperti su una stessa connessione (1–100)	10
Keepalive (secondi, 0 = off)	Ogni quanti secondi il server verifica che il client sia ancora presente	60
Keepalive senza risposta	Dopo quanti controlli senza risposta la connessione viene chiusa	3
Compressione	Abilita la compressione dei dati	No

> **Nota:** Con i valori predefiniti una connessione interrotta (rete caduta, PC spento) viene chiusa dal server dopo circa 3 minuti (60 s × 3).

5.2 Autenticazione

Campo	Descrizione	Predefinito
Consenti autenticazione con password	Accesso con la password dell'account Windows	Sì
Consenti autenticazione con chiave pubblica	Accesso con le chiavi caricate per ogni account (paragrafo 7.6)	Sì
Consenti password vuote (sconsigliato)	Permette l'accesso ad account senza password	No
Tentativi per connessione	Tentativi di autenticazione ammessi prima di chiudere la connessione (1–20)	4
Tempo per il login (s)	Secondi concessi per completare il login (10–600)	60
Banner pre-login	Testo mostrato dal client prima della richiesta di credenziali. Vuoto = nessun banner	vuoto

Almeno uno tra password e chiave pubblica deve restare attivo: il programma non permette di salvare se sono entrambi disattivati. Il metodo può poi essere ristretto per singolo account (paragrafo 7.2).

5.3 Controllo accessi

Campo	Descrizione
Chi può accedere	**Users**: solo gli account definiti nella scheda Account (consigliato, come in Bitvise). **Groups**: i membri dei gruppi Windows indicati. **Any**: qualsiasi account Windows valido.
Gruppi ammessi	Solo in modalità Groups, separati da virgola. Esempi: `ssh-utenti`, `CONTOSO\gruppo-ssh`. In modalità Groups è obbligatorio almeno un gruppo
Account sempre negati	Account esclusi in ogni caso, separati da virgola. Gli account disabilitati nella scheda Account vengono aggiunti automaticamente
Nega accesso interattivo e Desktop remoto agli account solo-SFTP	Gli account locali in modalità Solo SFTP vengono inseriti nel gruppo `SSH-SFTP-Only`, a cui vengono negati l'accesso alla console e il Desktop remoto. Predefinito: attivo

Attenzione: In modalità **Users** senza alcun account definito, OpenSSH non riceve nessuna restrizione e accetta **tutti** gli account Windows validi.

Nota: La negazione dell'accesso interattivo viene impostata tramite i criteri di sicurezza locali (`secedit`). Su una macchina in dominio, una GPO che definisce gli stessi diritti utente ha la precedenza e può annullarla.

5.4 Inoltri e sessione

Campo	Descrizione	Predefinito
Inoltro porte predefinito	Valore per gli account che non lo ridefiniscono: `no`, `yes` (locale e remoto), `local` (solo dal client verso il server), `remote` (solo dal server verso il client)	`no`
GatewayPorts	`no`: gli inoltri remoti ascoltano solo su localhost del server. `yes`: su tutte le interfacce. `clientspecified`: decide il client	`no`
Consenti inoltro dell'agent SSH	Permette di usare sul server l'agent SSH del client	No
Shell predefinita	`powershell` (Windows PowerShell 5.1), `pwsh` (PowerShell 7, se installata), `cmd`, oppure il percorso completo di un eseguibile. Vale per tutti gli account. Se l'eseguibile non esiste l'impostazione viene ignorata con un avviso nel pannello Output	`powershell`

5.5 Crittografia e log

Campo	Descrizione	Predefinito
Profilo algoritmi	**Modern**: solo algoritmi attuali (curve25519, ML-KEM/sntrup se disponibili, AES-GCM, ChaCha20, chiavi Ed25519, ECDSA e RSA-SHA2). **Compatible**: aggiunge scambi NIST, `diffie-hellman-group14-sha256`, `hmac-sha1` e chiavi `ssh-rsa` per client datati. **Default**: lascia i predefiniti di OpenSSH. Gli algoritmi non supportati dalla versione installata vengono esclusi automaticamente.	Modern
Livello log	Dettaglio dei messaggi nel registro eventi: da `QUIET` a `DEBUG3`. `INFO` è sufficiente per accessi e blocco IP; `VERBOSE` aggiunge l'impronta della chiave usata al login	INFO

Consiglio: Usare **Compatible** solo se qualche client non riesce più a collegarsi (versioni vecchie di PuTTY, apparati di rete, librerie SFTP datate).

5.6 Avanzate

Il campo **Righe aggiuntive sshd_config** accoglie direttive globali di OpenSSH che la GUI non prevede, una per riga. Vengono inserite così come sono, prima dei blocchi per utente, e verificate con `sshd -t` all'applicazione: una riga errata impedisce l'applicazione ma non danneggia il server in funzione.

Attenzione: Non inserire qui blocchi `Match`: verrebbero seguiti dalle direttive generate dal programma e ne altererebbero il significato.

6. Scheda Firewall

Il programma gestisce una regola di Windows Firewall dedicata al server SSH, equivalente alle «IP access rules» di Bitvise: le connessioni da indirizzi non elencati vengono scartate prima ancora di raggiungere OpenSSH.

Campo	Descrizione	Predefinito
Gestisci il Windows Firewall per il server SSH	Se disattivato il programma non tocca il firewall (le regole esistenti restano come sono)	Sì
Profili di rete	**Dominio**, **Privato**, **Pubblico**: i profili su cui la porta è aperta. Se il firewall è gestito, almeno uno è obbligatorio	Dominio, Privato
IP / reti ammessi	Uno per riga. Ammessi: `Any`, `LocalSubnet`, indirizzi singoli (`203.0.113.10`), reti CIDR (`192.168.1.0/24`), intervalli (`10.0.0.1-10.0.0.50`). Se vuoto equivale ad `Any`	`Any`
Disattiva le regole OpenSSH predefinite di Windows	Disattiva la regola in ingresso creata da Microsoft all'installazione, che aprirebbe la porta 22 a tutti	Sì

Indicazioni sui profili:

- **Server**: profilo **Dominio**. Aggiungere **Pubblico** solo se la scheda di rete esposta è classificata come pubblica.
- **PC e portatili**: **Dominio** e **Privato**. Sulle reti pubbliche (hotel, hotspot) la porta resta chiusa, come è giusto che sia.

Le regole create sono due:

Nome visualizzato	Funzione
WinSSH Manager - SSH (TCP-In)	Consente le connessioni alla porta SSH dagli indirizzi ammessi, limitatamente all'eseguibile `sshd.exe`
WinSSH Manager - IP bloccati	Blocca gli IP inseriti dal blocco automatico o a mano (capitolo 9). Vale su tutti i profili, solo per la porta SSH

> **Attenzione:** Se si amministra il server da remoto via SSH, il proprio indirizzo (o la propria rete) deve comparire in **IP / reti ammessi**, altrimenti al primo **Applica** la connessione successiva verrà rifiutata.

7. Scheda Account

Ogni account SSH corrisponde a un **account Windows reale**, locale o di Active Directory: OpenSSH per Windows non supporta account virtuali. La scheda elenca gli account ammessi e le loro regole.

> **Nota:** Le modifiche agli account vengono salvate in `config.json` appena si conferma; diventano attive con **APPLICA CONFIGURAZIONE**.

7.1 Elenco degli account

Colonna	Contenuto
Account	Nome dell'account Windows (`nome` per un account locale, `DOMINIO\nome` per un account di dominio)
Attivo	«Sì» o «No». Gli account disabilitati sono in grigio
Accesso	«Shell» oppure «Solo SFTP»
Cartella radice	Cartella SFTP dell'account
Opzioni	«chroot» se l'utente è confinato nella cartella, «sola lettura»
Inoltro	Permesso di inoltro porte
Autenticazione	Metodo di autenticazione richiesto
Da IP	Indirizzi da cui l'account può collegarsi
Descrizione	Nota libera

Pulsanti: **Nuovo...**, **Modifica...** (o doppio clic sulla riga), **Chiavi pubbliche...**, **Abilita / disabilita**, **Reimposta password...**, **Elimina...**. Tutti tranne **Nuovo...** agiscono sull'account selezionato.

7.2 Creare un account

Nuovo... apre la finestra «Nuovo account SSH», divisa in sezioni.

Identità

Campo	Descrizione
Account Windows	Account locale: solo il nome (es. `mario`). Account Active Directory: `DOMINIO\nome`. Non sono ammessi spazi, `@` e apici; il nome di un account locale non può superare 20 caratteri. Dopo la creazione il nome non è più modificabile
Descrizione	Nota libera, riportata anche come commento in `sshd_config`
Account abilitato	Se disattivato, l'account resta nella configurazione ma viene negato

Account Windows locale

Sezione presente solo alla creazione e solo per account locali.

Campo	Descrizione
Crea l'account Windows locale se non esiste	Se l'account non esiste viene creato con la password indicata, con password senza scadenza e non modificabile dall'utente. Gli account in modalità Shell vengono inseriti anche nel gruppo Users
Password, Conferma password	Usate solo se l'account va creato. La password non viene salvata in nessun file di configurazione e non compare nei log né nell'elenco dei processi

Se si salva un account locale che non esiste e non lo si fa creare, il programma avverte che il login non sarà possibile finché l'account Windows non esiste.

Tipo di accesso

Opzione	Descrizione
Shell completa	Terminale, SFTP, SCP e tunnel (se consentiti). L'utente non è confinato in alcuna cartella
Solo SFTP	Solo trasferimento file. Non può aprire un terminale né usare l'agent; l'inoltro porte è vietato salvo diversa impostazione esplicita
Cartella radice SFTP	Solo per Solo SFTP. Percorso **locale** completo (es. `D:\SFTP\mario`), selezionabile con **Sfoglia...**. Non sono ammesse cartelle di rete. Viene creata all'applicazione se non esiste
Confina nella cartella (chroot)	Disponibile se è indicata una cartella. L'utente vede la cartella come `/` e non può uscirne. Senza chroot la cartella è solo quella di partenza
Sola lettura	L'utente può scaricare ma non caricare, modificare o cancellare file

> **Attenzione:** La cartella radice deve essere una cartella locale reale: unità di rete, junction e collegamenti simbolici all'interno della cartella non funzionano in modo affidabile con OpenSSH per Windows.

Inoltro porte (tunnel)

Campo	Descrizione
Inoltro consentito	`default` (usa il valore globale della scheda Server), `no`, `local`, `remote`, `yes`
Destinazioni (locale)	Attivo con `local` o `yes`. Destinazioni raggiungibili con l'inoltro locale, formato `host:porta`, separate da virgola. Es. `127.0.0.1:3389, sql01:1433`. Vuoto = tutte
Porte in ascolto (remoto)	Attivo con `remote` o `yes`. Porte che l'utente può aprire sul server, formato `[host:]porta`. Es. `8080`. Vuoto = tutte. Richiede OpenSSH 7.8 o successivo

Sicurezza

Campo	Descrizione
Autenticazione	`default` (vale l'impostazione globale), `password`, `publickey`, `publickey+password` (servono **entrambe**: prima la chiave, poi la password)
Accesso solo da	IP o reti CIDR da cui l'account può collegarsi, separati da virgola. Vuoto = da qualsiasi indirizzo

Premendo **Salva** l'account viene registrato. Se il metodo di autenticazione richiede una chiave pubblica, il programma apre subito la finestra delle chiavi per aggiungerla.

7.3 Modificare, abilitare e disabilitare

- **Modifica...** (o doppio clic) apre la stessa finestra con i dati dell'account; il nome non è modificabile e la sezione per la creazione dell'account Windows non compare.
- **Abilita / disabilita** inverte lo stato dell'account. Un account disabilitato viene negato da OpenSSH dopo l'applicazione, ma l'account Windows resta attivo per gli altri usi.

7.4 Reimpostare la password

Reimposta password... chiede la nuova password per l'account Windows **locale** selezionato e la imposta subito, senza bisogno di applicare. Per gli account di dominio il programma ricorda che la password si gestisce in Active Directory.

7.5 Eliminare un account

Elimina... pone tre domande successive:

1. «Rimuovere l'account dalla configurazione SSH?» — toglie l'account da `config.json`;
2. «Eliminare anche le sue chiavi pubbliche dall'archivio centrale?»;
3. solo per account locali: «Eliminare anche l'account Windows locale?». L'operazione è irreversibile; il profilo utente resta su disco.

Dopo l'eliminazione premere **APPLICA CONFIGURAZIONE**.

7.6 Chiavi pubbliche

Chiavi pubbliche... apre l'elenco delle chiavi dell'account selezionato, con numero progressivo e impronta (bit, SHA256, commento, tipo).

Pulsante	Funzione
Incolla chiave...	Si incollano una o più chiavi pubbliche, una per riga, nel formato `ssh-ed25519 AAAA… commento`
Importa file .pub...	Si seleziona il file della chiave pubblica generato dal client
Elimina selezionata	Rimuove la chiave selezionata, previa conferma
Chiudi	Chiude la finestra

- Ogni chiave viene verificata con `ssh-keygen`: le righe non riconosciute vengono ignorate con un avviso, i duplicati vengono saltati.
- Una **chiave privata** viene sempre rifiutata. Se si incolla per errore il file sbagliato, il programma lo segnala.
- Le chiavi sono salvate in `C:\ProgramData\ssh\managed_keys\<account>` (per gli account di dominio `managed_keys\dominio\nome`) con i permessi richiesti da OpenSSH.

- Le chiavi dell'archivio centrale valgono **anche per gli amministratori**. Per gli account amministratori OpenSSH ignora invece il file `%USERPROFILE%\.ssh\authorized_keys`: valgono solo `administrators_authorized_keys` e l'archivio centrale.
- Le chiavi aggiunte o eliminate valgono subito per i nuovi accessi, senza bisogno di applicare (purché la configurazione sia già stata applicata almeno una volta).

> **Consiglio:** Sul client la coppia di chiavi si genera con `ssh-keygen -t ed25519`. Va caricato sul server solo il file che termina in `.pub`; la chiave privata non deve mai lasciare il PC del client.

7.7 Permessi delle cartelle SFTP

All'applicazione della configurazione il programma crea le cartelle radice mancanti e assegna all'account i permessi NTFS:

Tipo di account	Permessi assegnati
Solo SFTP, lettura e scrittura	Sulla cartella radice: sola lettura (l'utente non può cancellarla né rinominarla). Su file e sottocartelle: modifica
Solo SFTP, sola lettura	Lettura ed esecuzione su tutto l'albero

I permessi vengono aggiunti a quelli esistenti, non li sostituiscono. Se la cartella contiene dati riservati ad altri utenti, verificare i permessi ereditati prima di assegnarla.

8. Scheda Sessioni

Elenca le connessioni SSH attive sulla porta del server, aggiornate ogni volta che si apre la scheda.

Colonna	Contenuto
Id	Identificativo del processo della sessione
Utente	Account collegato, oppure «(autenticazione in corso)» se il login non è ancora completato
Remoto	Indirizzo e porta del client
Inizio	Data e ora di apertura della connessione

- **Aggiorna**: rilegge l'elenco.
- **Disconnetti selezionata**: chiude la sessione selezionata, previa conferma. Il servizio principale non viene mai terminato.
- **Aggiorna ogni 10 secondi**: aggiornamento automatico, attivo solo mentre la scheda è visualizzata.

9. Scheda Blocco IP

Il blocco IP, equivalente all'«IP blocking» di Bitvise, rileva gli indirizzi che sbagliano ripetutamente l'accesso e li blocca nel firewall per un periodo stabilito.

9.1 Come funziona

- Un'attività pianificata, `WinSSHManager-IPBlocker`, gira come SYSTEM: a ogni nuovo evento del log di OpenSSH, ogni 5 minuti (per far scadere i blocchi) e all'avvio del sistema.
- Conta come fallimento: password o chiave errata, utente inesistente, superamento dei tentativi ammessi, utente non autorizzato («not allowed because»).
- Quando un IP supera la soglia nell'intervallo stabilito viene aggiunto alla regola firewall «WinSSH Manager - IP bloccati».
- Alla scadenza il blocco viene rimosso automaticamente, al più tardi entro 5 minuti.
- Non vengono mai bloccati `127.0.0.1`, `::1` e gli indirizzi in whitelist.

9.2 Impostazioni

Riquadro a sinistra. Le impostazioni si salvano e si applicano con i pulsanti della barra comandi in basso.

Campo	Descrizione	Predefinito
Blocco automatico attivo	Attiva o disattiva il blocco. La modifica dell'attività pianificata avviene già al salvataggio	Sì
Fallimenti per bloccare	Numero di tentativi falliti che fa scattare il blocco (1–1000)	5
Nell'arco di (minuti)	Intervallo in cui vengono contati i fallimenti (1–1440)	10
Durata blocco (minuti)	Durata del blocco temporaneo (fino a un anno)	60
Permanente dopo N blocchi	Numero di blocchi in 30 giorni dopo cui il blocco diventa permanente. 0 = mai	0
Chiudi le sessioni già aperte dall'IP bloccato	Al blocco chiude anche le connessioni già stabilite da quell'indirizzo	Sì
Mai bloccare (whitelist)	IP o reti CIDR, uno per riga	`127.0.0.1`, `::1`

> **Attenzione:** Inserire **sempre** in whitelist la rete da cui si amministra il server. Bastano pochi errori di digitazione della password per bloccare se stessi.

9.3 IP bloccati e registro

A destra compaiono l'elenco **IP bloccati** (IP o rete, dal, fino a, motivo; «permanente» per i blocchi senza scadenza) e il **Registro blocchi** con le ultime 300 righe di `ipblocker.log`. Il registro viene ruotato automaticamente oltre 1 MB.

Pulsante	Funzione
Aggiorna	Rilegge elenco e registro
Blocca IP...	Blocca a mano un indirizzo o una rete CIDR. Chiede la durata in minuti; `0` = permanente
Sblocca selezionato	Rimuove il blocco dell'IP selezionato e ne azzera i fallimenti
Sblocca tutti	Rimuove tutti i blocchi e azzera tutti i contatori, previa conferma
Esegui un ciclo ora	Analizza subito il log senza attendere l'attività pianificata

10. Scheda Log

Mostra gli eventi del registro **OpenSSH/Operational**, dal più recente. Viene caricata alla prima apertura della scheda.

- In **verde** gli accessi riusciti, in **rosso** quelli falliti o negati.
- **Doppio clic** su una riga apre il testo completo dell'evento.
- **Solo accessi falliti / negati** filtra gli eventi di errore.
- **Eventi** stabilisce quanti eventi mostrare (10–5000, predefinito 200).
- **Aggiorna** rilegge il log con i criteri impostati.
- **Apri Visualizzatore eventi** apre direttamente il registro OpenSSH/Operational nel Visualizzatore eventi di Windows.

> **Consiglio:** Quando un utente non riesce ad accedere, attivare **Solo accessi falliti / negati** e cercare il suo nome: il messaggio indica quasi sempre la causa (password errata, chiave non accettata, utente non autorizzato o collegato da un IP non ammesso).

11. Scheda Backup

11.1 Esportare le impostazioni

Esporta... crea un archivio zip (nome proposto `WinSshManager-AAAAMMGG.zip`) con:

- `config.json`;
- l'archivio delle chiavi pubbliche degli account;
- `administrators_authorized_keys`;
- solo se è selezionato **Includi le chiavi host**: le chiavi host del server.

> **Attenzione:** Le chiavi host sono chiavi **private**: chi possiede lo zip può impersonare il server. Includerle solo per migrare il server su un'altra macchina mantenendo le stesse impronte, e custodire il file come una password.

11.2 Importare le impostazioni

Importa... legge uno zip esportato in precedenza:

- sostituisce `config.json` (della versione corrente resta una copia in `backup`);
- aggiunge le chiavi pubbliche e `administrators_authorized_keys` contenuti nello zip;
- se è selezionato **Importa anche le chiavi host, se presenti nel file**, sostituisce le chiavi host;
- al termine chiede se applicare subito la configurazione.

11.3 Ripristinare sshd_config

Ripristina sshd_config da backup... permette di scegliere una delle versioni salvate in `C:\ProgramData\WinSshManager\backup`. Il file scelto viene verificato con `sshd -t`, messo in uso e il servizio viene riavviato.

> **Attenzione:** Il ripristino agisce solo su `sshd_config`. `config.json` resta com'è: al prossimo **Applica** le sue impostazioni verranno riapplicate. Usare il ripristino come rimedio d'emergenza, poi correggere le impostazioni nelle schede.

11.4 Cartelle

Apri cartella dati apre `C:\ProgramData\WinSshManager`; **Apri cartella ssh** apre `C:\ProgramData\ssh`.

12. Procedure guidate

Le procedure che seguono coprono i casi più comuni. Al termine di ciascuna premere **APPLICA CONFIGURAZIONE** se non è indicato diversamente.

12.1 Messa in servizio consigliata

1. Scheda **Server**: porta 22, oppure una porta alta se il server è esposto su Internet (riduce il rumore nei log, ma non è di per sé una misura di sicurezza); **Chi può accedere** = **Users**; **Profilo algoritmi** = **Modern**; shell `powershell` o `pwsh`.
2. Scheda **Firewall**: profili adatti alla macchina (capitolo 6) e, in **IP / reti ammessi**, la rete locale più gli IP pubblici da cui ci si collega.
3. Scheda **Blocco IP**: lasciare i valori predefiniti e aggiungere in whitelist la rete di amministrazione.
4. **Salva e applica**.
5. Scheda **Account**: creare gli account (paragrafi seguenti) e applicare.
6. Verificare dal server stesso con `ssh nomeutente@localhost` e, per gli account SFTP, `sftp nomeutente@localhost`. Da un altro PC confrontare l'impronta presentata con **Stato → Impronte chiavi host**.

12.2 Amministratore con chiave e tunnel RDP/SQL

1. **Nuovo...**, account Windows esistente (es. l'account dell'amministratore).
2. **Shell completa**.
3. **Inoltro consentito** = `local`; **Destinazioni** = `127.0.0.1:3389, 127.0.0.1:1433`.
4. **Autenticazione** = `publickey`.
5. **Salva**, poi aggiungere la chiave pubblica nella finestra che si apre.
6. Applicare. Dal client: `ssh -L 13389:127.0.0.1:3389 utente@server`, poi collegarsi con Desktop remoto a `localhost:13389`.

12.3 Fornitore che deposita file (solo SFTP)

1. **Nuovo...**, nome di un account locale dedicato (es. `fornitore`), **Crea l'account Windows locale** con password robusta.
2. **Solo SFTP**; **Cartella radice** = `D:\SFTP\fornitore`; attivare **Confina nella cartella**.
3. **Autenticazione** = `password` (o `publickey`, se il fornitore ha una chiave).
4. **Accesso solo da** = l'IP pubblico del fornitore.
5. Applicare. L'utente vede la cartella come `/`, può caricare e gestire i file al suo interno ma non può cancellare la cartella stessa, né accedere alla console o al Desktop remoto.

12.4 Consultazione in sola lettura

Come il caso precedente, attivando anche **Sola lettura**. L'utente può solo scaricare: OpenSSH rifiuta le scritture e i permessi NTFS assegnati sono di sola lettura.

12.5 Cambiare la porta senza perdere l'accesso

1. Se si lavora da remoto, assicurarsi che il nuovo numero di porta sia raggiungibile (router, firewall perimetrale).
2. Cambiare **Porta TCP** e premere **Salva e applica**; confermare l'avviso.
3. La regola firewall gestita viene spostata automaticamente sulla nuova porta.
4. Aprire una **nuova** connessione sulla nuova porta (`ssh -p NUOVAPORTA utente@server`) **prima** di chiudere quella esistente.

12.6 Passare alle sole chiavi

1. Per ogni account verificare nella finestra **Chiavi pubbliche...** che ci sia almeno una chiave e provare l'accesso con chiave.
2. Scheda **Server**: disattivare **Consenti autenticazione con password**.
3. **Salva e applica** e confermare l'avviso.

In alternativa si può richiedere la chiave solo per alcuni account, impostando su di essi **Autenticazione** = `publickey`.

12.7 Migrare da Bitvise SSH Server

1. In Bitvise elencare gli account e i loro permessi. Gli account virtuali vanno ricreati come account Windows locali (**Nuovo...** con **Crea l'account Windows locale**).
2. Esportare le chiavi pubbliche dei client da ogni account Bitvise e importarle con **Chiavi pubbliche...**.
3. Per non far comparire ai client l'avviso di cambio impronta, esportare da Bitvise le chiavi host in formato OpenSSH (se la versione in uso lo consente), copiarle in `C:\ProgramData\ssh\` con i nomi `ssh_host_ed25519_key` / `ssh_host_rsa_key` e i rispettivi `.pub`. Altrimenti comunicare ai client le nuove impronte.
4. Arrestare Bitvise e impostarne il servizio su **Disabilitato**.
5. Applicare la configurazione, verificare gli accessi e solo allora disinstallare Bitvise.

Corrispondenza tra le funzioni:

Bitvise SSH Server	WinSSH Manager
Impostazioni centralizzate	`config.json`, applicato con **APPLICA CONFIGURAZIONE**
Windows accounts / gruppi ammessi	Server → **Chi può accedere** (Users / Groups)
Accesso da IP per account	Account → **Accesso solo da**
Solo SFTP, cartella radice, mount in sola lettura	Account → **Solo SFTP**, **Cartella radice**, **Confina**, **Sola lettura**
Permessi di inoltro per account	Account → **Inoltro porte**
Chiavi pubbliche per account	Account → **Chiavi pubbliche...**
IP access rules	Scheda **Firewall**
IP blocking	Scheda **Blocco IP**
Sessioni, log, impronte chiavi host	Schede **Sessioni**, **Log**, **Stato**
Export / import settings	Scheda **Backup**

13. Console testuale e uso da PowerShell

Quando la GUI non è disponibile (sessione SSH, Server Core, emergenze) le stesse funzioni sono raggiungibili da una **PowerShell avviata come Amministratore**.

13.1 Console a menu

```
C:\ProgramData\WinSshManager\SshManager.ps1           # menu interattivo
C:\ProgramData\WinSshManager\SshManager.ps1 -Install  # installa/abilita OpenSSH
C:\ProgramData\WinSshManager\SshManager.ps1 -Apply    # applica la configurazione
C:\ProgramData\WinSshManager\SshManager.ps1 -Status   # stato sintetico
```

Il menu principale mostra in testa versione, stato del servizio, porta, numero di account e stato del blocco IP, e segnala se ci sono modifiche non applicate. Le voci sono:

Voce	Funzione	Voce	Funzione
1	Stato dettagliato	7	Log
2	Installa / abilita OpenSSH Server	8	Impronte chiavi host
3	Impostazioni server (rete, autenticazione, accessi, firewall)	9	APPLICA CONFIGURAZIONE
4	Account e chiavi	10	Anteprima sshd_config
5	Sessioni attive	11	Esporta / importa, modifica di config.json nel Blocco note
6	Blocco IP	12	Avvia / arresta servizio

Nelle domande, premendo Invio si mantiene il valore tra parentesi quadre; nelle liste il carattere `-` svuota il campo. Dopo ogni modifica la console chiede se applicare subito.

13.2 Comandi del modulo

Per l'automazione si importa direttamente il modulo:

```
Import-Module C:\ProgramData\WinSshManager\WinSshManager.psm1 -DisableNameChecking
Get-SshServerStatus
Set-SshManagedUser -Name mario -Mode Shell -AuthMethods publickey `
    -AllowTcpForwarding local -PermitOpen '127.0.0.1:3389'
Add-SshUserKey -Name mario -Path C:\temp\id_ed25519.pub
Update-SshServerConfiguration
Unblock-SshIp -Ip 203.0.113.9
```

Comando	Funzione
`Install-SshManager`	Installa/abilita OpenSSH e inizializza
`Update-SshServerConfiguration`	Applica la configurazione (`-NoRestart` per non riavviare)
`Get-SshServerStatus`	Stato del server
`Get-SshManagedUser`, `Set-SshManagedUser`, `Remove-SshManagedUser`	Lettura, creazione/modifica, rimozione degli account
`Get-SshUserKey`, `Add-SshUserKey`, `Remove-SshUserKey`	Gestione delle chiavi pubbliche
`Get-SshSession`, `Stop-SshSession`	Sessioni attive

Comando	Funzione
`Get-SshLog`	Eventi OpenSSH (`-Last N`, `-FailuresOnly`)
`Get-SshBlockedIp`, `Block-SshIp`, `Unblock-SshIp`	Blocco IP manuale (`Unblock-SshIp -Ip '*'` sblocca tutti)
`Enable-SshIpBlocker`, `Disable-SshIpBlocker`	Attivazione dell'attività pianificata
`Get-SshHostKeyFingerprint`	Impronte delle chiavi host
`New-SshdConfigText -Config (Get-SshManagerConfig)`	Anteprima di `sshd_config`
`Export-SshManagerSettings`, `Import-SshManagerSettings`	Esportazione e importazione (`-IncludeHostKeys`)

14. Limiti da conoscere

- **Nessun account virtuale**: ogni utente SSH è un account Windows reale. Per gli accessi solo SFTP conviene creare account locali dedicati.
- **Una sola cartella per utente**: il chroot è una sola cartella locale; unità di rete, junction e collegamenti simbolici all'interno non sono affidabili.
- **Chroot solo per SFTP**: in modalità Shell l'utente non è confinato (limite di OpenSSH per Windows).
- **Shell unica**: la shell predefinita vale per tutto il server, non per singolo account.
- **Niente FTPS**: solo SFTP e SCP. SCP è disponibile per gli account Shell, non per quelli Solo SFTP.
- **Gestione solo locale**: la GUI agisce sulla macchina su cui è avviata.
- **Aggiornamenti di OpenSSH**: arrivano da Windows Update; in alternativa si può installare la versione MSI di Microsoft (progetto `PowerShell/Win32-OpenSSH` su GitHub), che viene rilevata automaticamente.
- **Su Windows 10/11** un PC in sospensione non risponde: regolare le opzioni di risparmio energetico se deve fare da server.
- **Domain Controller**: non hanno account locali; si usano solo account di dominio.

15. Risoluzione dei problemi

Problema	Causa probabile e soluzione
«sshd -t ha rifiutato la configurazione generata»	Il messaggio indica la riga. Di solito è un'opzione non supportata dalla versione installata (provare il profilo algoritmi **Default**) oppure una riga errata in **Righe aggiuntive sshd_config**. Il server in funzione non è stato toccato.
«Risposta non valida da PowerShell»	Verificare che la cartella `PowerShell` sia accanto all'eseguibile e che nessuna GPO blocchi `powershell.exe`. Il testo completo dell'errore è nel pannello Output operazioni.
L'utente non riesce ad accedere	Scheda **Log** con **Solo accessi falliti / negati**. Controllare che l'account sia nella scheda Account, abilitato, che la configurazione sia stata applicata, che l'IP sia ammesso (Firewall e **Accesso solo da**) e che non sia bloccato (scheda Blocco IP).
Accesso con chiave rifiutato	Spesso il file delle chiavi ha permessi errati: riapplicare la configurazione. Per gli amministratori la chiave in `%USERPROFILE%\.ssh` viene ignorata: caricarla con **Chiavi pubbliche...**. Per gli account di dominio verificare il primo accesso con attenzione.
SFTP con chroot non funziona	La cartella deve esistere, essere locale, non essere un junction, e l'utente deve avervi almeno la lettura.
Ci si è bloccati da soli	Dalla console locale o via Desktop remoto: scheda **Blocco IP** → **Sblocca selezionato**, poi aggiungere la propria rete alla whitelist.
Il server non risponde dopo una modifica	Scheda **Backup** → **Ripristina sshd_config da backup...**, poi correggere le impostazioni.
Installazione di OpenSSH fallita	Installare la funzionalità facoltativa **OpenSSH Server** da Impostazioni → App → Funzionalità facoltative, oppure dalla sorgente FoD aziendale, poi **Installa / abilita OpenSSH**.

15.1 Debug approfondito

1. Scheda **Stato** → **Arresta**.
2. In una PowerShell amministrativa eseguire `& "$env:windir\System32\OpenSSH\sshd.exe" -d`. Il server gestisce un solo login e scrive a video tutti i passaggi dell'autenticazione.
3. Tentare l'accesso dal client e leggere il motivo del rifiuto.
4. Scheda **Stato** → **Avvia**.

16. Disinstallazione

Da una PowerShell avviata come Amministratore:

```
Import-Module C:\ProgramData\WinSshManager\WinSshManager.psm1 -DisableNameChecking
Disable-SshIpBlocker
Remove-NetFirewallRule -Name WinSSHManager-SSH-In, WinSSHManager-Blocklist -ErrorAction
SilentlyContinue
Enable-NetFirewallRule -Name OpenSSH-Server-In-TCP -ErrorAction SilentlyContinue
Remove-Item C:\ProgramData\WinSshManager -Recurse -Force
```

Prima dell'ultima riga, se si vuole tornare alla configurazione originale di OpenSSH, copiare `backup\sshd_config.originale.*` in `C:\ProgramData\ssh\sshd_config`. Eliminare infine la cartella del programma.

OpenSSH Server, gli account Windows, il gruppo `SSH-SFTP-Only` e le chiavi in `C:\ProgramData\ssh` restano al loro posto: si rimuovono a mano se non servono più.

Appendice A. Oggetti creati nel sistema

Oggetto	Nome	Note
Servizio	`sshd`	Di Microsoft; impostato su avvio automatico
Regola firewall	`WinSSHManager-SSH-In` («WinSSH Manager - SSH (TCP-In)»)	Accesso alla porta SSH
Regola firewall	`WinSSHManager-Blocklist` («WinSSH Manager - IP bloccati»)	IP bloccati
Attività pianificata	`WinSSHManager-IPBlocker`	Eseguita come SYSTEM
Gruppo locale	`SSH-SFTP-Only`	Account solo SFTP, senza accesso interattivo e RDP
Chiave di registro	`HKLM\SOFTWARE\OpenSSH\DefaultShell`	Shell predefinita
Diritti utente	Nega accesso locale / tramite Desktop remoto	Assegnati al gruppo `SSH-SFTP-Only`
Registro eventi	Applications and Services Logs → OpenSSH → Operational	Di Microsoft; letto da Log e Blocco IP

Appendice B. Glossario

Termine	Significato
sshd / sshd_config	Il servizio OpenSSH Server e il suo file di configurazione
config.json	File in cui WinSSH Manager conserva tutte le impostazioni; da esso viene generato `sshd_config`
Applicare	Rigenerare `sshd_config` da `config.json`, metterlo in uso e riavviare il servizio
Chiave host	Coppia di chiavi che identifica il server; la sua impronta permette al client di riconoscerlo
Impronta (fingerprint)	Breve codice che identifica in modo univoco una chiave (es. `SHA256:…`)
Chiave pubblica	Parte pubblicabile della coppia di chiavi del client, caricata sul server per l'accesso senza password
SFTP / SCP	Protocolli di trasferimento file su SSH
Chroot	Confinamento dell'utente SFTP in una cartella, che vede come radice `/`
Inoltro porte (tunnel)	Trasporto di una connessione TCP attraverso SSH: locale (dal client verso una destinazione raggiungibile dal server) o remoto (dal server verso il client)
CIDR	Notazione delle reti IP, es. `192.168.1.0/24` = da 192.168.1.0 a 192.168.1.255
Whitelist	Elenco di indirizzi che non vengono mai bloccati
UAC	Controllo dell'account utente di Windows: la richiesta di conferma per eseguire un programma come amministratore

WinSSH Manager

Manual de utilizare

Gestionarea serverului OpenSSH integrat în Windows

Windows 10/11 · Windows Server 2019, 2022, 2025

Ediția octombrie 2026

Cuprins

1. Introducere 104
1.1 Ce este WinSSH Manager 104
1.2 Sisteme acceptate și cerințe 104
1.3 Cum funcționează 104
1.4 Convențiile manualului 105

2. Instalare și prima pornire 106
2.1 Copierea programului 106
2.2 Prima pornire 106
2.3 Unde sunt salvate datele 107

3. Fereastra principală 108
3.1 Structura ferestrei 108
3.2 Butoanele barei de comenzi 108
3.3 Indicatorul modificărilor în așteptare 108
3.4 Avertismente înainte de aplicare 109
3.5 Ce se întâmplă la aplicare 109

4. Fila Stato 110
4.1 Informații afișate 110
4.2 Butoane 111

5. Fila Server 112
5.1 Rețea 112
5.2 Autentificare 113
5.3 Controlul accesului 113
5.4 Redirecționări și sesiune 114
5.5 Criptografie și jurnal 114
5.6 Setări avansate 114

6. Fila Firewall 115

7. Fila Account 116
7.1 Lista conturilor 116
7.2 Crearea unui cont 116
7.3 Modificare, activare și dezactivare 118
7.4 Resetarea parolei 118
7.5 Ștergerea unui cont 118
7.6 Chei publice 118
7.7 Permisiunile folderelor SFTP 119

8. Fila Sessioni 120

9. Fila Blocco IP 121
9.1 Cum funcționează 121
9.2 Setări 121
9.3 IP-uri blocate și registru 122

10. Fila Log 123

11. Fila Backup 124
11.1 Exportarea setărilor 124
11.2 Importarea setărilor 124
11.3 Restaurarea sshd_config 124
11.4 Foldere 124

12. Proceduri ghidate 125
12.1 Punerea în funcțiune recomandată 125
12.2 Administrator cu cheie și tunel RDP/SQL 125
12.3 Furnizor care depune fișiere (doar SFTP) 125
12.4 Consultare doar în citire 125
12.5 Schimbarea portului fără a pierde accesul 125
12.6 Trecerea la autentificare doar cu chei 126
12.7 Migrarea de la Bitvise SSH Server 126

13. Consola text și utilizarea din PowerShell 127
13.1 Consola cu meniu 127
13.2 Comenzile modulului 127

14. Limitări de cunoscut 129

15. Rezolvarea problemelor 130
15.1 Depanare detaliată 130

16. Dezinstalare 131

Anexa A. Obiecte create în sistem 132

Anexa B. Glosar 133

1. Introducere

1.1 Ce este WinSSH Manager

WinSSH Manager este un panou de control grafic pentru **serverul OpenSSH integrat în Windows**. Permite gestionarea portului, autentificării, conturilor, accesurilor SFTP, paravanului de protecție și blocării automate a IP-urilor dintr-o singură fereastră, cu un model de lucru similar cu cel al Bitvise SSH Server: toate setările se află într-un singur fișier, iar serverul este reconfigurat pornind de la acel fișier.

Programul folosește exclusiv componente Microsoft deja prezente în sistem: OpenSSH Server, Paravanul de protecție Windows, Planificatorul de activități, conturi locale sau Active Directory, permisiuni NTFS. Nu instalează servicii proprii și nu necesită software de la terți.

- **Server SSH** cu shell (PowerShell, PowerShell 7 sau Linie de comandă), SFTP și SCP;
- **conturi doar SFTP** limitate la un folder, inclusiv doar în citire;
- **tuneluri** (redirecționare de porturi) permise pentru fiecare cont în parte și limitate la destinații precise;
- **chei publice** gestionate într-o arhivă centrală, valabile și pentru administratori;
- **paravan de protecție** cu lista IP-urilor admise și **blocare automată** a IP-urilor care greșesc în mod repetat autentificarea;
- **sesiuni active**, **jurnale**, **amprente ale cheilor gazdă**, **exportarea și importarea** setărilor.

1.2 Sisteme acceptate și cerințe

Cerință	Detalii
Sistem de operare	Windows 10 (1809 sau ulterior), Windows 11, Windows Server 2019, 2022 și 2025
Componente	.NET Framework 4.8 și Windows PowerShell 5.1, deja prezente pe toate sistemele enumerate
OpenSSH Server	Caracteristică opțională Windows. Dacă lipsește, programul o instalează (vedeți capitolul 2)
Privilegii	Programul trebuie rulat ca **Administrator**: la pornire, Windows cere confirmarea UAC
Interfață grafică	Necesită Experiența desktop. Pe Server Core se folosește consola text (capitolul 13)

1.3 Cum funcționează

Există un singur principiu de reținut: **setările se salvează în config.json și devin efective doar atunci când aplicați configurația.**

1. Modificați câmpurile din filele **Server**, **Firewall** și **Blocco IP** (Blocare IP) și apăsați **Salva impostazioni** (Salvare setări): valorile sunt scrise în `config.json`. Conturile (fila **Account**) sunt în schimb salvate în `config.json` imediat ce confirmați fereastra lor.
2. Apăsați **APPLICA CONFIGURAZIONE** (Aplicare configurație): programul generează un nou `sshd_config` pornind de la `config.json`, îl verifică cu `sshd -t` și doar dacă este valid îl pune în uz, aliniază paravanul de protecție, cheile, folderele și blocarea IP și repornește serviciul `sshd`.

Din acest motiv, `sshd_config` **nu trebuie modificat manual**: la fiecare aplicare este regenerat, iar modificările manuale s-ar pierde. Directivele pe care interfața grafică nu le prevede se introduc în câmpul **Righe aggiuntive sshd_config** (Rânduri suplimentare sshd_config) din fila Server (paragraful 5.6).

> **Notă:** Fereastra lucrează întotdeauna pe mașina pe care este pornită. Pentru a administra un server la distanță, folosiți interfața grafică prin Desktop la distanță sau consola text prin SSH.

1.4 Convențiile manualului

- Numele butoanelor, filelor și câmpurilor sunt scrise **aldin**, exact cum apar pe ecran.
- Numele de fișiere, căile, comenzile și valorile de tastat sunt scrise cu `caractere cu spațiere fixă`.
- Casetele **Notă**, **Sfat** și **Atenție** semnalează, respectiv, informații utile, bune practici și situații în care riscați să pierdeți accesul la server sau date.

2. Instalare și prima pornire

2.1 Copierea programului

Programul este un folder care conține `WinSshManagerGui.exe` și subfolderul `PowerShell`, care este motorul propriu-zis. Nu are un program de instalare.

1. Copiați **întregul folder** pe server sau pe PC, de exemplu în `C:\Program Files\WinSshManager\`.
2. Verificați ca subfolderul `PowerShell` să se afle lângă `WinSshManagerGui.exe`. Dacă lipsește, la pornire apare mesajul „Manca il motore PowerShell” (Lipsește motorul PowerShell) și programul se închide.
3. Dacă pe aceeași mașină rulează un alt server SSH (de exemplu Bitvise) pe același port, opriți-l mai întâi sau configurați, pentru perioada de test, OpenSSH pe un port diferit: două servere nu pot asculta pe același port.

2.2 Prima pornire

Porniți `WinSshManagerGui.exe` și confirmați solicitarea UAC. La prima pornire, programul citește starea sistemului și propune operația necesară:

Situație detectată	Ce propune programul
OpenSSH Server nu este instalat	„OpenSSH Server non risulta installato su questo sistema. Installarlo e abilitarlo ora?” (OpenSSH Server nu pare instalat pe acest sistem. Îl instalați și activați acum?). Dacă răspundeți **Sì** (Da), este instalată caracteristica opțională (pe Windows Server 2025 este deja prezentă și este doar activată). Operația poate dura câteva minute.
OpenSSH prezent, WinSSH Manager niciodată inițializat	„WinSSH Manager non è ancora inizializzato su questo sistema (manca config.json)” (WinSSH Manager nu este încă inițializat pe acest sistem – lipsește config.json). Dacă răspundeți **Sì**, este executată inițializarea.
Deja inițializat	Nicio întrebare: fereastra se deschide pe fila **Stato** (Stare).

Instalarea sau inițializarea execută următoarele operații:

- setează serviciul `sshd` pe pornire automată și îl pornește (la prima pornire, OpenSSH generează cheile gazdă);
- setează serviciul `ssh-agent` pe pornire manuală;
- creează folderul de date `C:\ProgramData\WinSshManager` și arhiva de chei `C:\ProgramData\ssh\managed_keys`, accesibile doar pentru SYSTEM și Administrators;
- creează `config.json` cu valorile implicite, **păstrând portul** eventual deja configurat în `sshd_config`;
- salvează o copie a fișierului `sshd_config` original în `backup\sshd_config.originale.<data-ora>`.

La final apare mesajul „OpenSSH Server installato e abilitato. Definire gli account e premere APPLICA CONFIGURAZIONE” (OpenSSH Server instalat și activat. Definiți conturile și apăsați APPLICA CONFIGURAZIONE). Aceeași procedură poate fi relansată oricând cu butonul **Installa / abilita OpenSSH** (Instalare / activare OpenSSH) din fila Stato.

> **Atenție:** Pe Windows 10/11 și Windows Server 2019/2022, instalarea descarcă caracteristica din Windows Update. În mediile cu WSUS și fără sursă pentru caracteristicile opționale (FoD), instalarea poate eșua: în acest caz, instalați mai întâi **OpenSSH Server** din Setări → Aplicații → Caracteristici opționale, apoi relansați **Installa / abilita OpenSSH**.
>
> **Atenție:** După inițializare, modul de acces este **Users**, dar încă nu există niciun cont: până când nu definiți cel puțin unul, serverul acceptă **orice** cont Windows valid. Fila Stato semnalează acest lucru cu portocaliu. Definiți imediat conturile (capitolul 7) și aplicați.

2.3 Unde sunt salvate datele

Cale	Conținut
`C:\ProgramData\WinSshManager\config.json`	Sursa unică a tuturor setărilor
`C:\ProgramData\WinSshManager\backup\`	Ultimele 30 de versiuni ale `sshd_config` și ale `config.json`, plus `sshd_config` original
`C:\ProgramData\WinSshManager\*.ps1, *.psm1`	Copie a motorului folosită de activitatea planificată a blocării IP, realiniată la fiecare aplicare
`C:\ProgramData\WinSshManager\ipblocker-state.json`	Starea blocării IP (contoare, IP-uri blocate, istoric)
`C:\ProgramData\WinSshManager\ipblocker.log`	Registrul blocărilor și deblocărilor
`C:\ProgramData\ssh\sshd_config`	Configurația OpenSSH, **generată** de program
`C:\ProgramData\ssh\managed_keys\`	Arhiva centrală a cheilor publice, câte un fișier pentru fiecare cont
`C:\ProgramData\ssh\administrators_authorized_keys`	Fișier standard Microsoft pentru cheile administratorilor (gestionat de OpenSSH, respectat de program)
`C:\ProgramData\ssh\banner.txt`	Textul bannerului afișat înainte de autentificare

Folderul `C:\ProgramData\WinSshManager` poate fi citit și scris doar de SYSTEM și Administrators, deoarece conține scripturi executate ca SYSTEM de activitatea planificată.

3. Fereastra principală

3.1 Structura ferestrei

Fereastra principală („WinSSH Manager - OpenSSH Server per Windows”) este împărțită în patru zone, de sus în jos:

Zonă	Funcție
File	Opt file: **Stato**, **Server**, **Firewall**, **Account**, **Sessioni**, **Blocco IP**, **Log**, **Backup**. Sunt descrise una câte una în capitolele 4–11.
Ieșirea operațiilor	Panou închis la culoare cu mesajele produse de fiecare operație, precedate de oră. Erorile încep cu „ERRORE:”. Este primul loc în care trebuie să vă uitați dacă ceva nu merge.
Bara de comenzi	Butoanele **Ricarica** (Reîncărcare), **Salva impostazioni**, **Salva e applica** (Salvare și aplicare), **APPLICA CONFIGURAZIONE** și indicatorul modificărilor în așteptare.
Bara de stare	Afișează „Pronto” (Gata) sau descrierea operației în curs, cu o bară de progres.

Operațiile rulează în fundal: cât timp sunt în curs, filele și bara de comenzi sunt dezactivate, dar fereastra rămâne receptivă. Nu este posibil să închideți programul în timpul unei operații.

3.2 Butoanele barei de comenzi

Buton	Ce face
Ricarica (Reîncărcare)	Recitește `config.json` și actualizează fila curentă. Dacă există modificări nesalvate, întreabă dacă trebuie abandonate.
Salva impostazioni (Salvare setări)	Verifică valorile din filele **Server**, **Firewall** și **Blocco IP** și le scrie în `config.json`. Nu afectează serverul în funcțiune. Conturile nu au nevoie de acest buton: se salvează singure.
Salva e applica (Salvare și aplicare)	Salvează ca mai sus și imediat după aceea aplică configurația. Înainte de a continua, afișează avertismentele privind modificările riscante (vedeți 3.4).
APPLICA CONFIGURAZIONE (Aplicare configurație)	Generează `sshd_config` din `config.json`, îl verifică, îl pune în uz și repornește serviciul (vedeți 3.5). Dacă există setări nesalvate, cere mai întâi salvarea lor.

3.3 Indicatorul modificărilor în așteptare

Lângă butoane apare cu portocaliu starea lucrului:

Indicator	Semnificație și ce trebuie făcut
„Impostazioni modificate e non salvate” (Setări modificate și nesalvate)	Au fost modificate câmpuri din Server, Firewall sau Blocco IP. Apăsați **Salva impostazioni** sau **Salva e applica**.
„Modifiche salvate ma non ancora applicate” (Modificări salvate, dar încă neaplicate)	`config.json` conține setări diferite de cele în uz. Apăsați **APPLICA CONFIGURAZIONE**.
(gol)	Serverul folosește exact configurația salvată.

La închiderea ferestrei, programul cere confirmarea dacă există modificări nesalvate sau salvate, dar neaplicate.

3.4 Avertismente înainte de aplicare

Unele modificări pot bloca accesul chiar și pentru administrator. Cu **Salva e applica** (Salvare și aplicare), programul le enumeră și cere confirmarea înainte de a continua:

- **autentificarea cu parolă dezactivată**: verificați ca toate conturile să aibă o cheie publică;
- **portul schimbat**: clienții vor trebui să se conecteze la noul port;
- **paravanul de protecție restricționat** la o listă de adrese: dacă administrați de la distanță, propriul IP trebuie să fie în listă.

> **Atenție:** Avertismentele apar doar cu **Salva e applica**. Dacă salvați cu **Salva impostazioni** și apoi apăsați **APPLICA CONFIGURAZIONE**, configurația este aplicată fără această verificare. Pentru schimbările de port, autentificare și paravan de protecție folosiți întotdeauna **Salva e applica**.

3.5 Ce se întâmplă la aplicare

APPLICA CONFIGURAZIONE execută, în ordine:

1. generează un `sshd_config` candidat din `config.json` și îl verifică cu `sshd -t`. **Dacă nu este valid, nu modifică nimic** și afișează eroarea, care indică rândul problematic;
2. salvează `sshd_config` în uz în folderul `backup` și îl scrie pe cel nou;
3. scrie bannerul, setează shell-ul implicit, protejează arhiva de chei, creează folderele rădăcină SFTP cu permisiunile lor, actualizează grupul `SSH-SFTP-Only` și restricțiile de acces, actualizează regulile paravanului de protecție și activează sau dezactivează activitatea de blocare IP;
4. repornește serviciul `sshd`.

> **Notă:** Repornirea `sshd` poate întrerupe sesiunile SSH în curs. Dacă administrați serverul prin SSH, prevedeți reconectarea; noile reguli se aplică oricum tuturor conexiunilor ulterioare.

4. Fila Stato

Este fila care se deschide la pornire și este actualizată de fiecare dată când o selectați. Rezumă situația serverului.

4.1 Informații afișate

Element	Semnificație
Installato (Instalat)	„Sì” (Da) cu verde dacă OpenSSH Server este prezent, „NO” cu roșu în caz contrar
Versione (Versiune)	Versiunea OpenSSH for Windows detectată
Eseguibile (Executabil)	Calea către `sshd.exe` (caracteristica Windows sau versiunea MSI de la Microsoft)
Servizio sshd (Serviciul sshd)	Starea și tipul de pornire ale serviciului (de ex. „Running / Automatic”), cu verde dacă rulează
Porta, Indirizzi di ascolto (Port, Adrese de ascultare)	Valori salvate în `config.json`
Shell predefinita (Shell implicit)	Shell-ul setat în registry. Dacă nu este setat, „cmd.exe (default Windows)”
Account definiti (Conturi definite)	Numărul de conturi din fila Account
Controllo accessi (Controlul accesului)	Modul **Users**, **Groups** sau **Any**. Cu portocaliu dacă este **Any** sau **Users** fără conturi: în ambele cazuri intră orice cont Windows valid
Firewall (Paravan de protecție)	Starea și profilurile regulii gestionate sau „regola gestita assente” (regula gestionată lipsește)
Blocco IP (Blocare IP)	Starea activității planificate și numărul de IP-uri blocate sau „disattivato” (dezactivat)
sshd_config	„Allineato alla configurazione” (Aliniat la configurație) cu verde sau „Differisce dalla configurazione: premere APPLICA CONFIGURAZIONE” (Diferă de configurație: apăsați APPLICA CONFIGURAZIONE) cu portocaliu

4.2 Butoane

Buton	Funcție
Aggiorna stato (Actualizare stare)	Recitește toate informațiile
Installa / abilita OpenSSH (Instalare / activare OpenSSH)	Instalează sau activează OpenSSH Server și inițializează WinSSH Manager (paragraful 2.2). Nu suprascrie un `config.json` existent
Avvia (Pornire), **Arresta (Oprire)**, **Riavvia (Repornire)**	Controlează serviciul `sshd`. **Arresta** cere confirmare, deoarece închide toate sesiunile SSH active
Anteprima sshd_config (Previzualizare sshd_config)	Afișează fișierul care ar fi generat cu setările **salvate**. Nu îl aplică. Dacă pe ecran există modificări nesalvate, programul avertizează că acestea nu sunt incluse
sshd_config attuale (sshd_config actual)	Afișează fișierul aflat în uz în prezent
Impronte chiavi host (Amprente chei gazdă)	Afișează, pentru fiecare cheie gazdă, amprentele SHA256, MD5 și Bubble Babble

> **Sfat:** La prima conectare, clientul SSH afișează amprenta cheii serverului și cere confirmarea ei. Comparați-o cu amprenta **SHA256** afișată de **Impronte chiavi host** înainte de a accepta: este garanția că v-ați conectat la serverul corect.

5. Fila Server

Conține setările globale ale serverului SSH. După modificări apăsați **Salva impostazioni** (sau **Salva e applica**). Fiecare câmp are un sfat care apare când treceți cu mouse-ul peste el.

5.1 Rețea

Câmp	Descriere	Implicit
Porta TCP (Port TCP)	Portul pe care serverul acceptă conexiunile (1–65535)	22
Indirizzi di ascolto (Adrese de ascultare)	Adresele IP locale pe care se ascultă, separate prin virgulă. `0.0.0.0` = toate adresele IPv4, `::` = toate adresele IPv6. Nu sunt admise rețele CIDR. Dacă câmpul rămâne gol, sunt folosite ambele	`0.0.0.0, ::`
Connessioni non autenticate (Conexiuni neautentificate)	Directiva `MaxStartups`: un număr sau `inizio:percentuale:massimo` (start:procent:maxim). Cu `10:30:100`, peste 10 conexiuni în așteptarea autentificării, cele noi sunt refuzate cu o probabilitate care crește de la 30%, până la refuzul total la 100	`10:30:100`
Sessioni per connessione (Sesiuni per conexiune)	Numărul de canale (shell, SFTP, tunel) deschise pe aceeași conexiune (1–100)	10
Keepalive (secondi, 0 = off) (Keepalive – secunde, 0 = dezactivat)	La câte secunde verifică serverul dacă clientul este încă prezent	60
Keepalive senza risposta (Keepalive fără răspuns)	După câte verificări fără răspuns este închisă conexiunea	3
Compressione (Compresie)	Activează compresia datelor	Nu

> **Notă:** Cu valorile implicite, o conexiune întreruptă (rețea căzută, PC oprit) este închisă de server după aproximativ 3 minute (60 s × 3).

5.2 Autentificare

Câmp	Descriere	Implicit
Consenti autenticazione con password (Permite autentificarea cu parolă)	Acces cu parola contului Windows	Da
Consenti autenticazione con chiave pubblica (Permite autentificarea cu cheie publică)	Acces cu cheile încărcate pentru fiecare cont (paragraful 7.6)	Da
Consenti password vuote (sconsigliato) (Permite parole goale – nerecomandat)	Permite accesul la conturi fără parolă	Nu
Tentativi per connessione (Încercări per conexiune)	Încercări de autentificare admise înainte de închiderea conexiunii (1–20)	4
Tempo per il login (s) (Timp pentru autentificare, s)	Secunde acordate pentru finalizarea autentificării (10–600)	60
Banner pre-login (Banner înainte de autentificare)	Text afișat de client înainte de solicitarea credențialelor. Gol = niciun banner	gol

Cel puțin una dintre metodele parolă și cheie publică trebuie să rămână activă: programul nu permite salvarea dacă ambele sunt dezactivate. Metoda poate fi apoi restricționată pentru fiecare cont în parte (paragraful 7.2).

5.3 Controlul accesului

Câmp	Descriere
Chi può accedere (Cine poate accesa)	**Users**: doar conturile definite în fila Account (recomandat, ca în Bitvise). **Groups**: membrii grupurilor Windows indicate. **Any**: orice cont Windows valid.
Gruppi ammessi (Grupuri admise)	Doar în modul Groups, separate prin virgulă. Exemple: `ssh-utenti`, `CONTOSO\gruppo-ssh`. În modul Groups este obligatoriu cel puțin un grup
Account sempre negati (Conturi refuzate întotdeauna)	Conturi excluse în orice caz, separate prin virgulă. Conturile dezactivate în fila Account sunt adăugate automat
Nega accesso interattivo e Desktop remoto agli account solo-SFTP (Refuză accesul interactiv și Desktop la distanță conturilor doar SFTP)	Conturile locale în modul Solo SFTP (Doar SFTP) sunt incluse în grupul `SSH-SFTP-Only`, căruia i se refuză accesul la consolă și Desktop la distanță. Implicit: activ

> **Atenție:** În modul **Users** fără niciun cont definit, OpenSSH nu primește nicio restricție și acceptă **toate** conturile Windows valide.

> **Notă:** Refuzarea accesului interactiv este setată prin politicile de securitate locale (`secedit`). Pe o mașină din domeniu, un GPO care definește aceleași drepturi de utilizator are prioritate și o poate anula.

5.4 Redirecționări și sesiune

Câmp	Descriere	Implicit
Inoltro porte predefinito (Redirecționare implicită a porturilor)	Valoare pentru conturile care nu o redefinesc: `no`, `yes` (locală și la distanță), `local` (doar de la client către server), `remote` (doar de la server către client)	`no`
GatewayPorts	`no`: redirecționările la distanță ascultă doar pe localhost-ul serverului. `yes`: pe toate interfețele. `clientspecified`: decide clientul	`no`
Consenti inoltro dell'agent SSH (Permite redirecționarea agentului SSH)	Permite folosirea pe server a agentului SSH al clientului	Nu
Shell predefinita (Shell implicit)	`powershell` (Windows PowerShell 5.1), `pwsh` (PowerShell 7, dacă este instalat), `cmd` sau calea completă a unui executabil. Este valabil pentru toate conturile. Dacă executabilul nu există, setarea este ignorată cu un avertisment în panoul Output	`powershell`

5.5 Criptografie și jurnal

Câmp	Descriere	Implicit
Profilo algoritmi (Profil algoritmi)	**Modern**: doar algoritmi actuali (curve25519, ML-KEM/sntrup dacă sunt disponibili, AES-GCM, ChaCha20, chei Ed25519, ECDSA și RSA-SHA2). **Compatible**: adaugă schimburi NIST, `diffie-hellman-group14-sha256`, `hmac-sha1` și chei `ssh-rsa` pentru clienți mai vechi. **Default**: păstrează valorile implicite OpenSSH. Algoritmii neacceptați de versiunea instalată sunt excluși automat.	Modern
Livello log (Nivel jurnal)	Nivelul de detaliu al mesajelor din jurnalul de evenimente: de la `QUIET` la `DEBUG3`. `INFO` este suficient pentru accese și blocarea IP; `VERBOSE` adaugă amprenta cheii folosite la autentificare	INFO

> **Sfat:** Folosiți **Compatible** doar dacă unii clienți nu se mai pot conecta (versiuni vechi de PuTTY, echipamente de rețea, biblioteci SFTP mai vechi).

5.6 Setări avansate

Câmpul **Righe aggiuntive sshd_config** primește directive globale OpenSSH pe care interfața grafică nu le prevede, câte una pe rând. Sunt inserate exact cum sunt, înaintea blocurilor per utilizator, și verificate cu `sshd -t` la aplicare: un rând greșit împiedică aplicarea, dar nu afectează serverul în funcțiune.

> **Atenție:** Nu inserați aici blocuri `Match`: ar fi urmate de directivele generate de program și le-ar altera semnificația.

6. Fila Firewall

Programul gestionează o regulă a Paravanului de protecție Windows dedicată serverului SSH, echivalentă cu „IP access rules” din Bitvise: conexiunile de la adrese care nu sunt în listă sunt eliminate înainte chiar de a ajunge la OpenSSH.

Câmp	Descriere	Implicit
Gestisci il Windows Firewall per il server SSH (Gestionează Paravanul de protecție Windows pentru serverul SSH)	Dacă este dezactivat, programul nu modifică paravanul de protecție (regulile existente rămân așa cum sunt)	Da
Profili di rete (Profiluri de rețea)	**Dominio (Domeniu)**, **Privato (Privat)**, **Pubblico (Public)**: profilurile pe care portul este deschis. Dacă paravanul de protecție este gestionat, cel puțin unul este obligatoriu	Dominio, Privato
IP / reti ammessi (IP-uri / rețele admise)	Câte unul pe rând. Admise: `Any`, `LocalSubnet`, adrese individuale (`203.0.113.10`), rețele CIDR (`192.168.1.0/24`), intervale (`10.0.0.1-10.0.0.50`). Dacă este gol, echivalează cu `Any`	`Any`
Disattiva le regole OpenSSH predefinite di Windows (Dezactivează regulile OpenSSH implicite din Windows)	Dezactivează regula de intrare creată de Microsoft la instalare, care ar deschide portul 22 pentru toți	Da

Indicații privind profilurile:

- **Server**: profilul **Dominio**. Adăugați **Pubblico** doar dacă placa de rețea expusă este clasificată ca publică.
- **PC-uri și laptopuri**: **Dominio** și **Privato**. Pe rețelele publice (hoteluri, hotspoturi) portul rămâne închis, așa cum este corect.

Regulile create sunt două:

Nume afișat	Funcție
WinSSH Manager - SSH (TCP-In)	Permite conexiunile la portul SSH de la adresele admise, limitat la executabilul `sshd.exe`
WinSSH Manager - IP bloccati	Blochează IP-urile introduse de blocarea automată sau manual (capitolul 9). Este valabilă pe toate profilurile, doar pentru portul SSH

> **Atenție:** Dacă administrați serverul de la distanță prin SSH, propria adresă (sau propria rețea) trebuie să apară în **IP / reti ammessi**, altfel, la prima **Applica**, conexiunea următoare va fi refuzată.

7. Fila Account

Fiecare cont SSH corespunde unui **cont Windows real**, local sau Active Directory: OpenSSH pentru Windows nu acceptă conturi virtuale. Fila listează conturile admise și regulile lor.

> **Notă:** Modificările conturilor sunt salvate în `config.json` imediat ce confirmați; devin active cu **APPLICA CONFIGURAZIONE**.

7.1 Lista conturilor

Coloană	Conținut
Account (Cont)	Numele contului Windows (`nume` pentru un cont local, `DOMENIU\nume` pentru un cont de domeniu)
Attivo (Activ)	„Sì” sau „No”. Conturile dezactivate sunt afișate cu gri
Accesso (Acces)	„Shell” sau „Solo SFTP”
Cartella radice (Folder rădăcină)	Folderul SFTP al contului
Opzioni (Opțiuni)	„chroot” dacă utilizatorul este limitat la folder, „sola lettura” (doar citire)
Inoltro (Redirecționare)	Permisiunea de redirecționare a porturilor
Autenticazione (Autentificare)	Metoda de autentificare cerută
Da IP (De la IP)	Adresele de la care se poate conecta contul
Descrizione (Descriere)	Notă liberă

Butoane: **Nuovo...** (Nou), **Modifica...** (Modificare; sau dublu clic pe rând), **Chiavi pubbliche...** (Chei publice), **Abilita / disabilita** (Activare / dezactivare), **Reimposta password...** (Resetare parolă), **Elimina...** (Ștergere). Toate, cu excepția **Nuovo...**, acționează asupra contului selectat.

7.2 Crearea unui cont

Nuovo... deschide fereastra „Nuovo account SSH” (Cont SSH nou), împărțită în secțiuni.

Identità (Identitate)

Câmp	Descriere
Account Windows (Cont Windows)	Cont local: doar numele (de ex. `mario`). Cont Active Directory: `DOMENIU\nume`. Nu sunt admise spațiile, `@` și apostrofurile; numele unui cont local nu poate depăși 20 de caractere. După creare, numele nu mai poate fi modificat
Descrizione (Descriere)	Notă liberă, inclusă și ca comentariu în `sshd_config`
Account abilitato (Cont activat)	Dacă este dezactivat, contul rămâne în configurație, dar este refuzat

Account Windows locale (Cont Windows local)

Secțiune prezentă doar la creare și doar pentru conturile locale.

Câmp	Descriere
Crea l'account Windows locale se non esiste (Creează contul Windows local dacă nu există)	Dacă contul nu există, este creat cu parola indicată, cu parolă fără expirare și care nu poate fi modificată de utilizator. Conturile în modul Shell sunt incluse și în grupul Users
Password, Conferma password (Parolă, Confirmare parolă)	Folosite doar dacă trebuie creat contul. Parola nu este salvată în niciun fișier de configurare și nu apare în jurnale și nici în lista proceselor

Dacă salvați un cont local care nu există și nu îl lăsați să fie creat, programul avertizează că autentificarea nu va fi posibilă până când contul Windows nu există.

Tipo di accesso (Tip de acces)

Opțiune	Descriere
Shell completa (Shell complet)	Terminal, SFTP, SCP și tuneluri (dacă sunt permise). Utilizatorul nu este limitat la niciun folder
Solo SFTP (Doar SFTP)	Doar transfer de fișiere. Nu poate deschide un terminal și nici folosi agentul; redirecționarea porturilor este interzisă, cu excepția unei setări explicite diferite
Cartella radice SFTP (Folder rădăcină SFTP)	Doar pentru Solo SFTP. Cale **locală** completă (de ex. `D:\SFTP\mario`), care poate fi selectată cu **Sfoglia...** (Răsfoire). Nu sunt admise foldere de rețea. Este creată la aplicare dacă nu există
Confina nella cartella (chroot) (Limitare la folder – chroot)	Disponibil dacă este indicat un folder. Utilizatorul vede folderul ca `/` și nu poate ieși din el. Fără chroot, folderul este doar cel de pornire
Sola lettura (Doar citire)	Utilizatorul poate descărca, dar nu poate încărca, modifica sau șterge fișiere

> **Atenție:** Folderul rădăcină trebuie să fie un folder local real: unitățile de rețea, joncțiunile și legăturile simbolice din interiorul folderului nu funcționează fiabil cu OpenSSH pentru Windows.

Inoltro porte (tunnel) (Redirecționarea porturilor – tunel)

Câmp	Descriere
Inoltro consentito (Redirecționare permisă)	`default` (folosește valoarea globală din fila Server), `no`, `local`, `remote`, `yes`
Destinazioni (locale) (Destinații – locală)	Activ cu `local` sau `yes`. Destinații accesibile prin redirecționarea locală, format `host:porta` (gazdă:port), separate prin virgulă. De ex. `127.0.0.1:3389, sql01:1433`. Gol = toate
Porte in ascolto (remoto) (Porturi de ascultare – la distanță)	Activ cu `remote` sau `yes`. Porturile pe care utilizatorul le poate deschide pe server, format `[host:]porta`. De ex. `8080`. Gol = toate. Necesită OpenSSH 7.8 sau ulterior

Sicurezza (Securitate)

Câmp	Descriere
Autenticazione (Autentificare)	`default` (se aplică setarea globală), `password`, `publickey`, `publickey+password` (sunt necesare **ambele**: mai întâi cheia, apoi parola)
Accesso solo da (Acces doar de la)	IP-uri sau rețele CIDR de la care se poate conecta contul, separate prin virgulă. Gol = de la orice adresă

Apăsând **Salva** (Salvare), contul este înregistrat. Dacă metoda de autentificare necesită o cheie publică, programul deschide imediat fereastra cheilor pentru a o adăuga.

7.3 Modificare, activare și dezactivare

- **Modifica...** (sau dublu clic) deschide aceeași fereastră cu datele contului; numele nu poate fi modificat, iar secțiunea pentru crearea contului Windows nu apare.
- **Abilita / disabilita** inversează starea contului. Un cont dezactivat este refuzat de OpenSSH după aplicare, dar contul Windows rămâne activ pentru celelalte utilizări.

7.4 Resetarea parolei

Reimposta password... cere noua parolă pentru contul Windows **local** selectat și o setează imediat, fără a fi nevoie de aplicare. Pentru conturile de domeniu, programul amintește că parola se gestionează în Active Directory.

7.5 Ștergerea unui cont

Elimina... pune trei întrebări succesive:

1. „Rimuovere l'account dalla configurazione SSH?” (Eliminați contul din configurația SSH?) — elimină contul din `config.json`;
2. „Eliminare anche le sue chiavi pubbliche dall'archivio centrale?” (Ștergeți și cheile sale publice din arhiva centrală?);
3. doar pentru conturile locale: „Eliminare anche l'account Windows locale?” (Ștergeți și contul Windows local?). Operația este ireversibilă; profilul utilizatorului rămâne pe disc.

După ștergere, apăsați **APPLICA CONFIGURAZIONE**.

7.6 Chei publice

Chiavi pubbliche... deschide lista cheilor contului selectat, cu număr progresiv și amprentă (biți, SHA256, comentariu, tip).

Buton	Funcție
Incolla chiave... (Lipire cheie)	Se lipesc una sau mai multe chei publice, câte una pe rând, în formatul `ssh-ed25519 AAAA… commento`
Importa file .pub... (Importare fișier .pub)	Se selectează fișierul cheii publice generat de client
Elimina selezionata (Ștergere cheie selectată)	Elimină cheia selectată, după confirmare
Chiudi (Închidere)	Închide fereastra

- Fiecare cheie este verificată cu `ssh-keygen`: rândurile nerecunoscute sunt ignorate cu un avertisment, duplicatele sunt omise.

- O **cheie privată** este întotdeauna refuzată. Dacă lipiți din greșeală fișierul greșit, programul semnalează acest lucru.
- Cheile sunt salvate în `C:\ProgramData\ssh\managed_keys\<account>` (pentru conturile de domeniu `managed_keys\dominio\nome`) cu permisiunile cerute de OpenSSH.
- Cheile din arhiva centrală sunt valabile **și pentru administratori**. Pentru conturile de administrator, OpenSSH ignoră în schimb fișierul `%USERPROFILE%\.ssh\authorized_keys`: sunt valabile doar `administrators_authorized_keys` și arhiva centrală.
- Cheile adăugate sau șterse sunt valabile imediat pentru noile accese, fără a fi nevoie de aplicare (cu condiția ca configurația să fi fost deja aplicată cel puțin o dată).

> **Sfat:** Pe client, perechea de chei se generează cu `ssh-keygen -t ed25519`. Pe server se încarcă doar fișierul care se termină cu `.pub`; cheia privată nu trebuie să părăsească niciodată PC-ul clientului.

7.7 Permisiunile folderelor SFTP

La aplicarea configurației, programul creează folderele rădăcină lipsă și atribuie contului permisiunile NTFS:

Tip de cont	Permisiuni atribuite
Doar SFTP, citire și scriere	Pe folderul rădăcină: doar citire (utilizatorul nu îl poate șterge și nici redenumi). Pe fișiere și subfoldere: modificare
Doar SFTP, doar citire	Citire și executare pe întregul arbore

Permisiunile sunt adăugate la cele existente, nu le înlocuiesc. Dacă folderul conține date rezervate altor utilizatori, verificați permisiunile moștenite înainte de a-l atribui.

8. Fila Sessioni

Listează conexiunile SSH active pe portul serverului, actualizate de fiecare dată când deschideți fila.

Coloană	Conținut
Id	Identificatorul procesului sesiunii
Utente (Utilizator)	Contul conectat sau „(autenticazione in corso)” (autentificare în curs) dacă autentificarea nu este încă finalizată
Remoto (La distanță)	Adresa și portul clientului
Inizio (Început)	Data și ora deschiderii conexiunii

- **Aggiorna** (Actualizare): recitește lista.
- **Disconnetti selezionata** (Deconectare sesiune selectată): închide sesiunea selectată, după confirmare. Serviciul principal nu este niciodată oprit.
- **Aggiorna ogni 10 secondi** (Actualizare la fiecare 10 secunde): actualizare automată, activă doar cât timp fila este afișată.

9. Fila Blocco IP

Blocarea IP, echivalentă cu „IP blocking” din Bitvise, detectează adresele care greșesc în mod repetat autentificarea și le blochează în paravanul de protecție pentru o perioadă stabilită.

9.1 Cum funcționează

- O activitate planificată, `WinSSHManager-IPBlocker`, rulează ca SYSTEM: la fiecare eveniment nou din jurnalul OpenSSH, la fiecare 5 minute (pentru expirarea blocărilor) și la pornirea sistemului.
- Se consideră eșec: parolă sau cheie greșită, utilizator inexistent, depășirea încercărilor admise, utilizator neautorizat („not allowed because”).
- Când un IP depășește pragul în intervalul stabilit, este adăugat la regula de paravan de protecție „WinSSH Manager - IP bloccati”.
- La expirare, blocarea este eliminată automat, cel târziu în 5 minute.
- Nu sunt blocate niciodată `127.0.0.1`, `::1` și adresele din lista albă (whitelist).

9.2 Setări

Caseta din stânga. Setările se salvează și se aplică prin butoanele barei de comenzi din partea de jos.

Câmp	Descriere	Implicit
Blocco automatico attivo (Blocare automată activă)	Activează sau dezactivează blocarea. Modificarea activității planificate are loc deja la salvare	Da
Fallimenti per bloccare (Eșecuri până la blocare)	Numărul de încercări eșuate care declanșează blocarea (1–1000)	5
Nell'arco di (minuti) (În decurs de – minute)	Intervalul în care sunt numărate eșecurile (1–1440)	10
Durata blocco (minuti) (Durata blocării – minute)	Durata blocării temporare (până la un an)	60
Permanente dopo N blocchi (Permanent după N blocări)	Numărul de blocări în 30 de zile după care blocarea devine permanentă. 0 = niciodată	0
Chiudi le sessioni già aperte dall'IP bloccato (Închide sesiunile deja deschise de IP-ul blocat)	La blocare, închide și conexiunile deja stabilite de la acea adresă	Da
Mai bloccare (whitelist) (Nu bloca niciodată – listă albă)	IP-uri sau rețele CIDR, câte unul pe rând	`127.0.0.1`, `::1`

> **Atenție:** Includeți **întotdeauna** în lista albă rețeaua din care administrați serverul. Sunt suficiente câteva greșeli de tastare a parolei pentru a vă bloca singur.

9.3 IP-uri blocate și registru

În dreapta apar lista **IP bloccati** (IP-uri blocate: IP sau rețea, de la, până la, motiv; „permanente” pentru blocările fără expirare) și **Registro blocchi** (Registrul blocărilor) cu ultimele 300 de rânduri din `ipblocker.log`. Registrul este rotit automat peste 1 MB.

Buton	Funcție
Aggiorna (Actualizare)	Recitește lista și registrul
Blocca IP... (Blocare IP)	Blochează manual o adresă sau o rețea CIDR. Cere durata în minute; `0` = permanent
Sblocca selezionato (Deblocare IP selectat)	Elimină blocarea IP-ului selectat și îi resetează eșecurile
Sblocca tutti (Deblocare toate)	Elimină toate blocările și resetează toate contoarele, după confirmare
Esegui un ciclo ora (Execută un ciclu acum)	Analizează imediat jurnalul, fără a aștepta activitatea planificată

10. Fila Log

Afișează evenimentele din jurnalul **OpenSSH/Operational**, de la cel mai recent. Este încărcată la prima deschidere a filei.

- Cu **verde** accesele reușite, cu **roșu** cele eșuate sau refuzate.
- **Dublu clic** pe un rând deschide textul complet al evenimentului.
- **Solo accessi falliti / negati** (Doar accese eșuate / refuzate) filtrează evenimentele de eroare.
- **Eventi** (Evenimente) stabilește câte evenimente sunt afișate (10–5000, implicit 200).
- **Aggiorna** recitește jurnalul cu criteriile setate.
- **Apri Visualizzatore eventi** (Deschide Vizualizatorul de evenimente) deschide direct jurnalul OpenSSH/Operational în Vizualizatorul de evenimente Windows.

> **Sfat:** Când un utilizator nu reușește să acceseze, activați **Solo accessi falliti / negati** și căutați-i numele: mesajul indică aproape întotdeauna cauza (parolă greșită, cheie neacceptată, utilizator neautorizat sau conectat de la un IP neadmis).

11. Fila Backup

11.1 Exportarea setărilor

Esporta... (Exportare) creează o arhivă zip (nume propus `WinSshManager-AAAAMMGG.zip`) cu:

- `config.json`;
- arhiva cheilor publice ale conturilor;
- `administrators_authorized_keys`;
- doar dacă este selectat **Includi le chiavi host** (Include cheile gazdă): cheile gazdă ale serverului.

> **Atenție:** Cheile gazdă sunt chei **private**: cine deține fișierul zip poate uzurpa identitatea serverului. Includeți-le doar pentru a migra serverul pe o altă mașină păstrând aceleași amprente și păstrați fișierul ca pe o parolă.

11.2 Importarea setărilor

Importa... (Importare) citește un fișier zip exportat anterior:

- înlocuiește `config.json` (din versiunea curentă rămâne o copie în `backup`);
- adaugă cheile publice și `administrators_authorized_keys` conținute în fișierul zip;
- dacă este selectat **Importa anche le chiavi host, se presenti nel file** (Importă și cheile gazdă, dacă sunt prezente în fișier), înlocuiește cheile gazdă;
- la final, întreabă dacă să aplice imediat configurația.

11.3 Restaurarea sshd_config

Ripristina sshd_config da backup... (Restaurare sshd_config din backup) permite alegerea uneia dintre versiunile salvate în `C:\ProgramData\WinSshManager\backup`. Fișierul ales este verificat cu `sshd -t`, pus în uz, iar serviciul este repornit.

> **Atenție:** Restaurarea acționează doar asupra `sshd_config`. `config.json` rămâne neschimbat: la următoarea **Applica** setările sale vor fi reaplicate. Folosiți restaurarea ca remediu de urgență, apoi corectați setările din file.

11.4 Foldere

Apri cartella dati (Deschide folderul de date) deschide `C:\ProgramData\WinSshManager`; **Apri cartella ssh** (Deschide folderul ssh) deschide `C:\ProgramData\ssh`.

12. Proceduri ghidate

Procedurile următoare acoperă cazurile cele mai frecvente. La finalul fiecăreia, apăsați **APPLICA CONFIGURAZIONE**, dacă nu se indică altfel.

12.1 Punerea în funcțiune recomandată

1. Fila **Server**: portul 22 sau un port înalt dacă serverul este expus pe Internet (reduce zgomotul din jurnale, dar nu este în sine o măsură de securitate); **Chi può accedere** = **Users**; **Profilo algoritmi** = **Modern**; shell `powershell` sau `pwsh`.
2. Fila **Firewall**: profiluri potrivite mașinii (capitolul 6) și, în **IP / reti ammessi**, rețeaua locală plus IP-urile publice de la care vă conectați.
3. Fila **Blocco IP**: lăsați valorile implicite și adăugați în lista albă rețeaua de administrare.
4. **Salva e applica**.
5. Fila **Account**: creați conturile (paragrafele următoare) și aplicați.
6. Verificați de pe serverul însuși cu `ssh nomeutente@localhost` și, pentru conturile SFTP, `sftp nomeutente@localhost`. De pe un alt PC, comparați amprenta prezentată cu **Stato → Impronte chiavi host**.

12.2 Administrator cu cheie și tunel RDP/SQL

1. **Nuovo...**, cont Windows existent (de ex. contul administratorului).
2. **Shell completa**.
3. **Inoltro consentito** = `local`; **Destinazioni** = `127.0.0.1:3389, 127.0.0.1:1433`.
4. **Autenticazione** = `publickey`.
5. **Salva**, apoi adăugați cheia publică în fereastra care se deschide.
6. Aplicați. De pe client: `ssh -L 13389:127.0.0.1:3389 utente@server`, apoi conectați-vă cu Desktop la distanță la `localhost:13389`.

12.3 Furnizor care depune fișiere (doar SFTP)

1. **Nuovo...**, numele unui cont local dedicat (de ex. `fornitore`), **Crea l'account Windows locale** cu o parolă puternică.
2. **Solo SFTP**; **Cartella radice** = `D:\SFTP\fornitore`; activați **Confina nella cartella**.
3. **Autenticazione** = `password` (sau `publickey`, dacă furnizorul are o cheie).
4. **Accesso solo da** = IP-ul public al furnizorului.
5. Aplicați. Utilizatorul vede folderul ca `/`, poate încărca și gestiona fișierele din interiorul lui, dar nu poate șterge folderul însuși și nici accesa consola sau Desktop la distanță.

12.4 Consultare doar în citire

Ca în cazul precedent, activând și **Sola lettura**. Utilizatorul poate doar descărca: OpenSSH refuză scrierile, iar permisiunile NTFS atribuite sunt doar de citire.

12.5 Schimbarea portului fără a pierde accesul

1. Dacă lucrați de la distanță, asigurați-vă că noul număr de port este accesibil (router, paravan de protecție perimetral).
2. Schimbați **Porta TCP** și apăsați **Salva e applica**; confirmați avertismentul.
3. Regula de paravan de protecție gestionată este mutată automat pe noul port.
4. Deschideți o conexiune **nouă** pe noul port (`ssh -p NUOVAPORTA utente@server`) **înainte** de a o închide pe cea existentă.

12.6 Trecerea la autentificare doar cu chei

1. Pentru fiecare cont, verificați în fereastra **Chiavi pubbliche...** că există cel puțin o cheie și încercați accesul cu cheie.
2. Fila **Server**: dezactivați **Consenti autenticazione con password**.
3. **Salva e applica** și confirmați avertismentul.

Ca alternativă, puteți cere cheia doar pentru unele conturi, setând pentru acestea **Autenticazione** = `publickey`.

12.7 Migrarea de la Bitvise SSH Server

1. În Bitvise, listați conturile și permisiunile lor. Conturile virtuale trebuie recreate ca și conturi Windows locale (**Nuovo...** cu **Crea l'account Windows locale**).
2. Exportați cheile publice ale clienților din fiecare cont Bitvise și importați-le cu **Chiavi pubbliche...**.
3. Pentru ca clienții să nu vadă avertismentul de schimbare a amprentei, exportați din Bitvise cheile gazdă în format OpenSSH (dacă versiunea folosită permite), copiați-le în `C:\ProgramData\ssh\` cu numele `ssh_host_ed25519_key` / `ssh_host_rsa_key` și fișierele `.pub` corespunzătoare. Altfel, comunicați clienților noile amprente.
4. Opriți Bitvise și setați serviciul său pe **Dezactivat**.
5. Aplicați configurația, verificați accesele și abia apoi dezinstalați Bitvise.

Corespondența dintre funcții:

Bitvise SSH Server	WinSSH Manager
Setări centralizate	`config.json`, aplicat cu **APPLICA CONFIGURAZIONE**
Windows accounts / grupuri admise	Server → **Chi può accedere** (Users / Groups)
Acces de la IP per cont	Account → **Accesso solo da**
Doar SFTP, folder rădăcină, montare doar în citire	Account → **Solo SFTP**, **Cartella radice**, **Confina**, **Sola lettura**
Permisiuni de redirecționare per cont	Account → **Inoltro porte**
Chei publice per cont	Account → **Chiavi pubbliche...**
IP access rules	Fila **Firewall**
IP blocking	Fila **Blocco IP**
Sesiuni, jurnale, amprente ale cheilor gazdă	Filele **Sessioni**, **Log**, **Stato**
Export / import settings	Fila **Backup**

13. Consola text și utilizarea din PowerShell

Când interfața grafică nu este disponibilă (sesiune SSH, Server Core, urgențe), aceleași funcții sunt accesibile dintr-un **PowerShell pornit ca Administrator**.

13.1 Consola cu meniu

```
C:\ProgramData\WinSshManager\SshManager.ps1           # menu interattivo
C:\ProgramData\WinSshManager\SshManager.ps1 -Install  # installa/abilita OpenSSH
C:\ProgramData\WinSshManager\SshManager.ps1 -Apply    # applica la configurazione
C:\ProgramData\WinSshManager\SshManager.ps1 -Status   # stato sintetico
```

Meniul principal afișează în partea de sus versiunea, starea serviciului, portul, numărul de conturi și starea blocării IP și semnalează dacă există modificări neaplicate. Elementele sunt:

Element	Funcție	Element	Funcție
1	Stato dettagliato (Stare detaliată)	7	Log (Jurnal)
2	Installa / abilita OpenSSH Server (Instalare / activare OpenSSH Server)	8	Impronte chiavi host (Amprente chei gazdă)
3	Impostazioni server (rete, autenticazione, accessi, firewall) (Setări server: rețea, autentificare, accese, paravan de protecție)	9	APPLICA CONFIGURAZIONE (Aplicare configurație)
4	Account e chiavi (Conturi și chei)	10	Anteprima sshd_config (Previzualizare sshd_config)
5	Sessioni attive (Sesiuni active)	11	Esporta / importa, modifica di config.json nel Blocco note (Exportare / importare, modificarea config.json în Notepad)
6	Blocco IP (Blocare IP)	12	Avvia / arresta servizio (Pornire / oprire serviciu)

La întrebări, apăsând Enter se păstrează valoarea dintre parantezele drepte; în liste, caracterul `-` golește câmpul. După fiecare modificare, consola întreabă dacă să aplice imediat.

13.2 Comenzile modulului

Pentru automatizare, se importă direct modulul:

```
Import-Module C:\ProgramData\WinSshManager\WinSshManager.psm1 -DisableNameChecking
Get-SshServerStatus
Set-SshManagedUser -Name mario -Mode Shell -AuthMethods publickey `
    -AllowTcpForwarding local -PermitOpen '127.0.0.1:3389'
Add-SshUserKey -Name mario -Path C:\temp\id_ed25519.pub
Update-SshServerConfiguration
Unblock-SshIp -Ip 203.0.113.9
```

Comandă	Funcție
`Install-SshManager`	Instalează/activează OpenSSH și inițializează
`Update-SshServerConfiguration`	Aplică configurația (`-NoRestart` pentru a nu reporni)
`Get-SshServerStatus`	Starea serverului

Comandă	Funcție
`Get-SshManagedUser`, `Set-SshManagedUser`, `Remove-SshManagedUser`	Citirea, crearea/modificarea și eliminarea conturilor
`Get-SshUserKey`, `Add-SshUserKey`, `Remove-SshUserKey`	Gestionarea cheilor publice
`Get-SshSession`, `Stop-SshSession`	Sesiuni active
`Get-SshLog`	Evenimente OpenSSH (`-Last N`, `-FailuresOnly`)
`Get-SshBlockedIp`, `Block-SshIp`, `Unblock-SshIp`	Blocare IP manuală (`Unblock-SshIp -Ip '*'` deblochează toate)
`Enable-SshIpBlocker`, `Disable-SshIpBlocker`	Activarea activității planificate
`Get-SshHostKeyFingerprint`	Amprentele cheilor gazdă
`New-SshdConfigText -Config (Get-SshManagerConfig)`	Previzualizarea `sshd_config`
`Export-SshManagerSettings`, `Import-SshManagerSettings`	Exportare și importare (`-IncludeHostKeys`)

14. Limitări de cunoscut

- **Niciun cont virtual**: fiecare utilizator SSH este un cont Windows real. Pentru accesele doar SFTP, este bine să creați conturi locale dedicate.
- **Un singur folder per utilizator**: chroot-ul este un singur folder local; unitățile de rețea, joncțiunile și legăturile simbolice din interior nu sunt fiabile.
- **Chroot doar pentru SFTP**: în modul Shell, utilizatorul nu este limitat (limitare a OpenSSH pentru Windows).
- **Shell unic**: shell-ul implicit este valabil pentru întregul server, nu pentru fiecare cont în parte.
- **Fără FTPS**: doar SFTP și SCP. SCP este disponibil pentru conturile Shell, nu și pentru cele Solo SFTP.
- **Gestionare doar locală**: interfața grafică acționează asupra mașinii pe care este pornită.
- **Actualizările OpenSSH**: vin din Windows Update; ca alternativă, se poate instala versiunea MSI de la Microsoft (proiectul `PowerShell/Win32-OpenSSH` de pe GitHub), care este detectată automat.
- **Pe Windows 10/11**, un PC în stare de repaus nu răspunde: ajustați opțiunile de economisire a energiei dacă trebuie să funcționeze ca server.
- **Controlere de domeniu**: nu au conturi locale; se folosesc doar conturi de domeniu.

15. Rezolvarea problemelor

Problemă	Cauză probabilă și soluție
„sshd -t ha rifiutato la configurazione generata” (sshd -t a refuzat configurația generată)	Mesajul indică rândul. De obicei este o opțiune neacceptată de versiunea instalată (încercați profilul de algoritmi **Default**) sau un rând greșit în **Righe aggiuntive sshd_config**. Serverul în funcțiune nu a fost afectat.
„Risposta non valida da PowerShell” (Răspuns nevalid de la PowerShell)	Verificați ca folderul `PowerShell` să fie lângă executabil și ca niciun GPO să nu blocheze `powershell.exe`. Textul complet al erorii se află în panoul Output operazioni.
Utilizatorul nu reușește să acceseze	Fila **Log** cu **Solo accessi falliti / negati**. Verificați dacă contul se află în fila Account, este activat, dacă configurația a fost aplicată, dacă IP-ul este admis (Firewall și **Accesso solo da**) și dacă nu este blocat (fila Blocco IP).
Acces cu cheie refuzat	Adesea fișierul cheilor are permisiuni greșite: reaplicați configurația. Pentru administratori, cheia din `%USERPROFILE%\.ssh` este ignorată: încărcați-o cu **Chiavi pubbliche...**. Pentru conturile de domeniu, verificați cu atenție primul acces.
SFTP cu chroot nu funcționează	Folderul trebuie să existe, să fie local, să nu fie o joncțiune, iar utilizatorul trebuie să aibă cel puțin permisiunea de citire asupra lui.
V-ați blocat singur	Din consola locală sau prin Desktop la distanță: fila **Blocco IP** → **Sblocca selezionato**, apoi adăugați propria rețea în lista albă.
Serverul nu răspunde după o modificare	Fila **Backup** → **Ripristina sshd_config da backup...**, apoi corectați setările.
Instalarea OpenSSH a eșuat	Instalați caracteristica opțională **OpenSSH Server** din Setări → Aplicații → Caracteristici opționale sau din sursa FoD a companiei, apoi **Installa / abilita OpenSSH**.

15.1 Depanare detaliată

1. Fila **Stato** → **Arresta**.
2. Într-un PowerShell administrativ, executați `& "$env:windir\System32\OpenSSH\sshd.exe" -d`. Serverul gestionează o singură autentificare și afișează pe ecran toți pașii autentificării.
3. Încercați accesul de pe client și citiți motivul refuzului.
4. Fila **Stato** → **Avvia**.

16. Dezinstalare

Dintr-un PowerShell pornit ca Administrator:

```
Import-Module C:\ProgramData\WinSshManager\WinSshManager.psm1 -DisableNameChecking
Disable-SshIpBlocker
Remove-NetFirewallRule -Name WinSSHManager-SSH-In, WinSSHManager-Blocklist -ErrorAction
SilentlyContinue
Enable-NetFirewallRule -Name OpenSSH-Server-In-TCP -ErrorAction SilentlyContinue
Remove-Item C:\ProgramData\WinSshManager -Recurse -Force
```

Înainte de ultimul rând, dacă doriți să reveniți la configurația originală OpenSSH, copiați `backup\sshd_config.originale.*` în `C:\ProgramData\ssh\sshd_config`. În final, ștergeți folderul programului.

OpenSSH Server, conturile Windows, grupul `SSH-SFTP-Only` și cheile din `C:\ProgramData\ssh` rămân la locul lor: se elimină manual dacă nu mai sunt necesare.

Anexa A. Obiecte create în sistem

Obiect	Nume	Note
Serviciu	`sshd`	De la Microsoft; setat pe pornire automată
Regulă de paravan de protecție	`WinSSHManager-SSH-In` („WinSSH Manager - SSH (TCP-In)”)	Acces la portul SSH
Regulă de paravan de protecție	`WinSSHManager-Blocklist` („WinSSH Manager - IP bloccati”)	IP-uri blocate
Activitate planificată	`WinSSHManager-IPBlocker`	Executată ca SYSTEM
Grup local	`SSH-SFTP-Only`	Conturi doar SFTP, fără acces interactiv și RDP
Cheie de registry	`HKLM\SOFTWARE\OpenSSH\DefaultShell`	Shell implicit
Drepturi de utilizator	Refuzare acces local / prin Desktop la distanță	Atribuite grupului `SSH-SFTP-Only`
Jurnal de evenimente	Jurnale de aplicații și servicii → OpenSSH → Operational	De la Microsoft; citit de Log și Blocco IP

Anexa B. Glosar

Termen	Semnificație
sshd / sshd_config	Serviciul OpenSSH Server și fișierul său de configurare
config.json	Fișierul în care WinSSH Manager păstrează toate setările; din el este generat `sshd_config`
Aplicare	Regenerarea `sshd_config` din `config.json`, punerea lui în uz și repornirea serviciului
Cheie gazdă	Pereche de chei care identifică serverul; amprenta sa permite clientului să îl recunoască
Amprentă (fingerprint)	Cod scurt care identifică în mod unic o cheie (de ex. `SHA256:…`)
Cheie publică	Partea care poate fi publicată din perechea de chei a clientului, încărcată pe server pentru accesul fără parolă
SFTP / SCP	Protocoale de transfer de fișiere prin SSH
Chroot	Limitarea utilizatorului SFTP la un folder, pe care îl vede ca rădăcină `/`
Redirecționarea porturilor (tunel)	Transportul unei conexiuni TCP prin SSH: local (de la client către o destinație accesibilă de pe server) sau la distanță (de la server către client)
CIDR	Notația rețelelor IP, de ex. `192.168.1.0/24` = de la 192.168.1.0 la 192.168.1.255
Listă albă (whitelist)	Listă de adrese care nu sunt blocate niciodată
UAC	Controlul contului de utilizator Windows: solicitarea de confirmare pentru a executa un program ca administrator

WinSSH Manager

ユーザー マニュアル

Windows に組み込まれた OpenSSH Server の管理

Windows 10/11 · Windows Server 2019, 2022, 2025

2026 年 10 月版

目次

1. はじめに 137

1.1 WinSSH Manager とは 137

1.2 サポートされるシステムと要件 137

1.3 動作のしくみ 137

1.4 本マニュアルの表記規則 138

2. インストールと初回起動 139

2.1 プログラムのコピー 139

2.2 初回起動 139

2.3 データの保存場所 140

3. メイン ウィンドウ 141

3.1 ウィンドウの構成 141

3.2 コマンド バーのボタン 141

3.3 保留中の変更のインジケーター 141

3.4 適用前の警告 142

3.5 適用時に行われる処理 142

4. Stato タブ 143

4.1 表示される情報 143

4.2 ボタン 144

5. Server タブ 145

5.1 ネットワーク 145

5.2 認証 146

5.3 アクセス制御 146

5.4 転送とセッション 147

5.5 暗号化とログ 147

5.6 詳細設定 148

6. Firewall タブ 149

7. Account タブ 150

7.1 アカウントの一覧 150

7.2 アカウントの作成 150
7.3 編集、有効化、無効化 152
7.4 パスワードのリセット 152
7.5 アカウントの削除 152
7.6 公開キー 153
7.7 SFTP フォルダーのアクセス許可 154

8. Sessioni タブ 155

9. Blocco IP タブ 156

9.1 動作のしくみ 156
9.2 設定 156
9.3 ブロックされた IP と記録 157

10. Log タブ 158

11. Backup タブ 159

11.1 設定のエクスポート 159
11.2 設定のインポート 159
11.3 sshd_config の復元 159
11.4 フォルダー 159

12. 手順ガイド 160

12.1 推奨される運用開始手順 160
12.2 キー認証の管理者と RDP/SQL トンネル 160
12.3 ファイルを預け入れる取引先 (SFTP のみ) 160
12.4 読み取り専用の閲覧 160
12.5 アクセスを失わずにポートを変更する 161
12.6 キー認証のみに移行する 161
12.7 Bitvise SSH Server からの移行 161

13. テキスト コンソールと PowerShell からの使用 163

13.1 メニュー形式のコンソール 163
13.2 モジュールのコマンド 163

14. 知っておくべき制限事項 165

15. トラブルシューティング 166

15.1 詳細なデバッグ 166

16. アンインストール 167

付録 A. システムに作成されるオブジェクト 168

付録 B. 用語集 169

1. はじめに

1.1 WinSSH Manager とは

WinSSH Manager は、**Windows に組み込まれた OpenSSH Server** 用のグラフィカルなコントロール パネルです。ポート、認証、アカウント、SFTP アクセス、ファイアウォール、IP の自動ブロックを 1 つのウィンドウから管理できます。動作モデルは Bitvise SSH Server と似ており、すべての設定が 1 つのファイルにまとめられ、サーバーはそのファイルを基に再構成されます。

このプログラムは、システムに既に存在する Microsoft のコンポーネント (OpenSSH Server、Windows ファイアウォール、タスク スケジューラ、ローカルまたは Active Directory のアカウント、NTFS アクセス許可) のみを使用します。独自のサービスはインストールせず、サードパーティ製ソフトウェアも必要ありません。

- **SSH サーバー**: シェル (PowerShell、PowerShell 7、またはコマンド プロンプト)、SFTP、SCP に対応。
- **SFTP 専用アカウント**: 1 つのフォルダー内に閉じ込められ、読み取り専用にすることもできます。
- **トンネル** (ポート転送): アカウントごとに許可し、特定の宛先に限定できます。
- **公開キー**: 中央のストアで管理され、管理者にも有効です。
- **ファイアウォール**: 許可する IP の一覧と、ログインに繰り返し失敗する IP の**自動ブロック**。
- **アクティブなセッション**、**ログ**、**ホスト キーのフィンガープリント**、設定の**エクスポートとインポート**。

1.2 サポートされるシステムと要件

要件	詳細
オペレーティング システム	Windows 10 (1809 以降)、Windows 11、Windows Server 2019、2022、2025
コンポーネント	.NET Framework 4.8 と Windows PowerShell 5.1 (上記のすべてのシステムに既に含まれています)
OpenSSH Server	Windows のオプション機能です。存在しない場合は、プログラムがインストールします (2 章を参照)
特権	プログラムは**管理者**として実行する必要があります。起動時に Windows が UAC の確認を求めます
グラフィカル インターフェイス	デスクトップ エクスペリエンスが必要です。Server Core ではテキスト コンソールを使用します (13 章)

1.3 動作のしくみ

覚えておくべき原則は 1 つだけです。**設定は config.json に保存され、構成を適用したときにのみ有効になります。**

1. 各タブ **Server** (サーバー)、**Firewall** (ファイアウォール)、**Blocco IP** (IP ブロック) でフィールドを変更し、**Salva impostazioni** (設定を保存) を押します。値は `config.json` に書き込まれます。一方、アカウント (**Account** タブ) は、そのウィンドウで確定した時点で `config.json` に保存されます。
2. **APPLICA CONFIGURAZIONE** (構成を適用) を押します。プログラムは `sshd_config` を `config.json` から新たに生成して `sshd -t` で検証し、有効な場合にのみ使用を開始します。さらに、ファイアウォール、キー、フォルダー、IP ブロックを同期し、`sshd` サービスを再起動します。

このため、`sshd_config` は**手動で編集しないでください**。適用するたびに再生成されるため、手動での変更は失われます。GUI にないディレクティブは、Server タブの **Righe aggiuntive sshd_config** (追加の sshd_config 行) フィールドに入力します (5.6 項)。

> **注:** ウィンドウは常に、起動したコンピューター上で動作します。リモート サーバーを管理するには、リモート デスクトップ経由で GUI を使用するか、SSH 経由でテキスト コンソールを使用します。

1.4 本マニュアルの表記規則

- ボタン、タブ、フィールドの名前は、画面に表示されるとおりに**太字**で示します。
- ファイル名、パス、コマンド、入力する値は等幅フォントで示します。
- **注**、**ヒント**、**注意** の囲みは、それぞれ役立つ情報、ベスト プラクティス、サーバーへのアクセスやデータを失うおそれがある状況を示します。

2. インストールと初回起動

2.1 プログラムのコピー

プログラムは、`WinSshManagerGui.exe` と、実際のエンジンであるサブフォルダー `PowerShell` を含むフォルダーです。インストーラーはありません。

1. **フォルダー全体**をサーバーまたは PC にコピーします (例: `C:\Program Files\WinSshManager\`)。
2. サブフォルダー `PowerShell` が `WinSshManagerGui.exe` と同じ場所にあることを確認します。ない場合は、起動時に「Manca il motore PowerShell」(PowerShell エンジンがありません) というメッセージが表示され、プログラムが終了します。
3. 同じコンピューターで別の SSH サーバー (例: Bitvise) が同じポートで動作している場合は、事前に停止するか、試用期間中は OpenSSH を別のポートに構成してください。2 つのサーバーが同じポートで待ち受けることはできません。

2.2 初回起動

`WinSshManagerGui.exe` を起動し、UAC の要求を承認します。初回起動時、プログラムはシステムの状態を読み取り、必要な操作を提示します。

検出された状況	プログラムが提示する内容
OpenSSH Server がインストールされていない	「OpenSSH Server non risulta installato su questo sistema. Installarlo e abilitarlo ora?」(このシステムには OpenSSH Server がインストールされていません。今すぐインストールして有効にしますか?)。**Sì** (はい) と答えるとオプション機能がインストールされます (Windows Server 2025 では既に存在するため、有効化のみ行われます)。この操作には数分かかる場合があります。
OpenSSH は存在するが、WinSSH Manager が一度も初期化されていない	「WinSSH Manager non è ancora inizializzato su questo sistema (manca config.json)」(このシステムでは WinSSH Manager がまだ初期化されていません (config.json がありません))。**Sì** と答えると初期化が実行されます。
初期化済み	質問は表示されず、ウィンドウは **Stato** (状態) タブで開きます。

インストールまたは初期化では、次の操作が実行されます。

- `sshd` サービスのスタートアップの種類を自動に設定して開始します (初回起動時に OpenSSH がホスト キーを生成します)。
- `ssh-agent` サービスのスタートアップの種類を手動に設定します。
- データ フォルダー `C:\ProgramData\WinSshManager` とキー ストア `C:\ProgramData\ssh\managed_keys` を作成します。これらには SYSTEM と Administrators のみがアクセスできます。
- `config.json` を既定値で作成します。その際、**ポートは維持されます** (`sshd_config` に既に構成されている場合)。
- 元の `sshd_config` のコピーを `backup\sshd_config.originale.<data-ora>` に保存します。

完了すると、「OpenSSH Server installato e abilitato. Definire gli account e premere APPLICA CONFIGURAZIONE」(OpenSSH Server がインストールされ、有効になりました。アカウントを定義して APPLICA CONFIGURAZIONE を押してください) というメッセージが表示されます。同じ手順は、Stato タブの **Installa / abilita OpenSSH** (OpenSSH のインストール/有効化) ボタンでいつでも再実行できます。

> **注意:** Windows 10/11 および Windows Server 2019/2022 では、インストール時に Windows Update から機能がダウンロードされます。WSUS を使用し、オプション機能 (FoD) のソースがない環境では、インストールが失敗する場合があります。その場合は、先に [設定] → [アプリ] → [オプション機能] から **OpenSSH Server** をインストールしてから、**Installa / abilita OpenSSH** を再実行してください。
>
> **注意:** 初期化後のアクセス モードは **Users** ですが、アカウントはまだありません。少なくとも 1 つ定義するまで、サーバーは有効な Windows アカウントであれば**どれでも**受け入れます。Stato タブでは、これがオレンジ色で示されます。すぐにアカウントを定義して (7 章) 適用してください。

2.3 データの保存場所

パス	内容
`C:\ProgramData\WinSshManager\config.json`	すべての設定の唯一のソース
`C:\ProgramData\WinSshManager\backup\`	`sshd_config` と `config.json` の最新 30 バージョン、および `sshd_config` の元のファイル
`C:\ProgramData\WinSshManager\*.ps1, *.psm1`	IP ブロックのスケジュールされたタスクが使用するエンジンのコピー。適用のたびに同期されます
`C:\ProgramData\WinSshManager\ipblocker-state.json`	IP ブロックの状態 (カウンター、ブロックされた IP、履歴)

パス	内容
C:\ProgramData\WinSshManager\ipblocker.log	ブロックとブロック解除の記録
C:\ProgramData\ssh\sshd_config	プログラムによって**生成される** OpenSSH の構成
C:\ProgramData\ssh\managed_keys\	公開キーの中央ストア (アカウントごとに 1 ファイル)
C:\ProgramData\ssh\administrators_authorized_keys	管理者のキー用の Microsoft 標準ファイル (OpenSSH が管理し、プログラムはこれを尊重します)
C:\ProgramData\ssh\banner.txt	ログイン前のバナーのテキスト

フォルダー C:\ProgramData\WinSshManager は、スケジュールされたタスクによって SYSTEM として実行されるスクリプトを含むため、SYSTEM と Administrators のみが読み書きできます。

3. メイン ウィンドウ

3.1 ウィンドウの構成

メイン ウィンドウ (「WinSSH Manager - OpenSSH Server per Windows」) は、上から順に 4 つの領域に分かれています。

領域	機能
タブ	8 つのタブ: **Stato** (状態)、**Server** (サーバー)、**Firewall** (ファイアウォール)、**Account** (アカウント)、**Sessioni** (セッション)、**Blocco IP** (IP ブロック)、**Log** (ログ)、**Backup** (バックアップ)。4 ～ 11 章で 1 つずつ説明します。
操作の出力	各操作で生成されたメッセージを時刻付きで表示する暗い色のパネルです。エラーは「ERRORE:」で始まります。問題が発生したときに最初に確認する場所です。
コマンド バー	**Ricarica** (再読み込み)、**Salva impostazioni** (設定を保存)、**Salva e applica** (保存して適用)、**APPLICA CONFIGURAZIONE** (構成を適用) の各ボタンと、保留中の変更のインジケーター。
ステータス バー	「Pronto」(準備完了)、または実行中の操作の説明と進行状況バーを表示します。

操作はバックグラウンドで実行されます。実行中はタブとコマンド バーが無効になりますが、ウィンドウは応答し続けます。操作中にプログラムを閉じることはできません。

3.2 コマンド バーのボタン

ボタン	動作
Ricarica	`config.json` を再読み込みし、現在のタブを更新します。保存されていない変更がある場合は、破棄するかどうかを確認します。
Salva impostazioni	**Server**、**Firewall**、**Blocco IP** の各タブの値をチェックし、`config.json` に書き込みます。動作中のサーバーには影響しません。アカウントにはこのボタンは不要です。自動的に保存されます。
Salva e applica	上記と同様に保存し、直後に構成を適用します。続行する前に、リスクのある変更に関する警告を表示します (3.4 を参照)。
APPLICA CONFIGURAZIONE	`config.json` から `sshd_config` を生成し、検証して使用を開始し、サービスを再起動します (3.5 を参照)。保存されていない設定がある場合は、先に保存するかどうかを確認します。

3.3 保留中の変更のインジケーター

ボタンの横に、作業の状態がオレンジ色で表示されます。

インジケーター	意味と対処
「Impostazioni modificate e non salvate」(設定が変更され、保存されていません)	Server、Firewall、または Blocco IP のフィールドが変更されています。**Salva impostazioni** または **Salva e applica** を押します。
「Modifiche salvate ma non ancora applicate」(変更は保存されましたが、まだ適用されていません)	`config.json` に、使用中のものとは異なる設定が含まれています。**APPLICA CONFIGURAZIONE** を押します。
(空)	サーバーは保存された構成をそのまま使用しています。

ウィンドウを閉じるときに、保存されていない変更、または保存済みで未適用の変更がある場合は、プログラムが確認を求めます。

3.4 適用前の警告

変更によっては、管理者自身が締め出される可能性があります。**Salva e applica** を使用すると、プログラムはそれらを一覧表示し、続行する前に確認を求めます。

- **パスワード認証の無効化**: アカウントに公開キーがあることを確認します。
- **ポートの変更**: クライアントは新しいポートに接続する必要があります。
- **アドレスの一覧へのファイアウォールの制限**: リモートで管理している場合は、自分の IP が一覧に含まれている必要があります。

> **注意:** 警告は **Salva e applica** の場合にのみ表示されます。**Salva impostazioni** で保存してから **APPLICA CONFIGURAZIONE** を押すと、このチェックなしで構成が適用されます。ポート、認証、ファイアウォールを変更する場合は、常に **Salva e applica** を使用してください。

3.5 適用時に行われる処理

APPLICA CONFIGURAZIONE は、次の処理を順に実行します。

1. `config.json` から候補となる `sshd_config` を生成し、`sshd -t` で検証します。**有効でない場合は何も変更せず**、問題のある行を示すエラーを表示します。
2. 使用中の `sshd_config` を `backup` フォルダーに保存し、新しいものを書き込みます。
3. バナーを書き込み、既定のシェルを設定し、キー ストアを保護し、SFTP のルート フォルダーをアクセス許可付きで作成し、`SSH-SFTP-Only` グループとアクセス制限を更新し、ファイアウォールの規則を更新し、IP ブロックのタスクを有効または無効にします。
4. `sshd` サービスを再起動します。

> **注:** `sshd` の再起動により、進行中の SSH セッションが中断される場合があります。SSH 経由でサーバーを管理している場合は、再接続に備えてください。新しい規則は、以降のすべての接続に適用されます。

4. Stato タブ

起動時に開くタブで、選択するたびに更新されます。サーバーの状況をまとめて表示します。

4.1 表示される情報

項目	意味
Installato (インストール済み)	OpenSSH Server が存在する場合は緑色で「Sì」、存在しない場合は赤色で「NO」
Versione (バージョン)	検出された OpenSSH for Windows のバージョン
Eseguibile (実行可能ファイル)	`sshd.exe` のパス (Windows の機能、または Microsoft の MSI 版)
Servizio sshd (sshd サービス)	サービスの状態とスタートアップの種類 (例: 「Running / Automatic」)。実行中の場合は緑色
Porta, Indirizzi di ascolto (ポート、待ち受けアドレス)	次に保存されている値: `config.json`
Shell predefinita (既定のシェル)	レジストリに設定されたシェル。設定されていない場合は「cmd.exe (default Windows)」
Account definiti (定義済みアカウント)	Account タブのアカウント数
Controllo accessi (アクセス制御)	モード **Users**、**Groups**、または **Any**。**Any** の場合、またはアカウントのない **Users** の場合はオレンジ色になります。どちらの場合も、有効な Windows アカウントであればどれでもログインできます
Firewall (ファイアウォール)	管理対象の規則の状態とプロファイル、または「regola gestita assente」(管理対象の規則なし)
Blocco IP (IP ブロック)	スケジュールされたタスクの状態とブロックされた IP の数、または「disattivato」(無効)

項目	意味
sshd_config	緑色で「Allineato alla configurazione」(構成と一致)、またはオレンジ色で「Differisce dalla configurazione: premere APPLICA CONFIGURAZIONE」(構成と異なります: APPLICA CONFIGURAZIONE を押してください)

4.2 ボタン

ボタン	機能
Aggiorna stato (状態の更新)	すべての情報を再読み込みします
Installa / abilita OpenSSH	OpenSSH Server をインストールまたは有効化し、WinSSH Manager を初期化します (2.2 項)。既存の `config.json` は上書きしません
Avvia (開始)、**Arresta** (停止)、**Riavvia (再起動)**	`sshd` サービスを操作します。**Arresta** は、アクティブな SSH セッションをすべて閉じるため確認を求めます
Anteprima sshd_config (sshd_config のプレビュー)	**保存済み**の設定で生成されるファイルを表示します。適用はしません。画面上に保存されていない変更がある場合は、それらが含まれていないことをプログラムが警告します
sshd_config attuale (現在の sshd_config)	現在使用中のファイルを表示します
Impronte chiavi host (ホストキーのフィンガープリント)	各ホスト キーについて、SHA256、MD5、Bubble Babble のフィンガープリントを表示します

> **ヒント:** 初回接続時、SSH クライアントはサーバーのキーのフィンガープリントを表示し、確認を求めます。承認する前に、**SHA256** のフィンガープリントを **Impronte chiavi host** で表示されるものと比較してください。これにより、正しいサーバーに接続していることを確認できます。

5. Server タブ

SSH サーバーの全体的な設定を含みます。変更後は **Salva impostazioni** (または **Salva e applica**) を押します。各フィールドには、マウスを重ねると表示されるヒントがあります。

5.1 ネットワーク

フィールド	説明	既定値
Porta TCP (TCP ポート)	サーバーが接続を受け付けるポート (1 〜 65535)	22
Indirizzi di ascolto (待ち受けアドレス)	待ち受けるローカル IP アドレス (コンマ区切り)。`0.0.0.0` = すべての IPv4、`::` = すべての IPv6。CIDR ネットワークは使用できません。空の場合は両方が使用されます	`0.0.0.0, ::`
Connessioni non autenticate (未認証の接続)	ディレクティブ `MaxStartups`: 数値、または `inizio:percentuale:massimo` (開始:割合:最大)。`10:30:100` の場合、ログイン待ちの接続が 10 を超えると、新しい接続は 30% から増加する確率で拒否され、100 で完全に拒否されます	`10:30:100`
Sessioni per connessione (接続あたりのセッション数)	同じ接続上で開かれるチャネル (シェル、SFTP、トンネル) の数 (1 〜 100)	10
Keepalive (secondi, 0 = off) (キープアライブ (秒、0 = オフ))	クライアントがまだ存在するかをサーバーが確認する間隔 (秒)	60
Keepalive senza risposta (応答のないキープアライブ)	応答のない確認が何回続いたら接続を閉じるか	3
Compressione (圧縮)	データの圧縮を有効にします	いいえ

> **注:** 既定値では、中断された接続 (ネットワークの切断、PC の電源オフ) は、約 3 分後 (60 秒 × 3) にサーバーによって閉じられます。

5.2 認証

フィールド	説明	既定値
Consenti autenticazione con password (パスワード認証を許可)	Windows アカウントのパスワードによるログイン	はい
Consenti autenticazione con chiave pubblica (公開キー認証を許可)	各アカウントに読み込まれたキーによるログイン (7.6 項)	はい
Consenti password vuote (sconsigliato) (空のパスワードを許可 (非推奨))	パスワードのないアカウントへのログインを許可します	いいえ
Tentativi per connessione (接続あたりの試行回数)	接続を閉じる前に許可される認証の試行回数 (1 〜 20)	4
Tempo per il login (s) (ログインの制限時間 (秒))	ログインを完了するために与えられる秒数 (10 〜 600)	60
Banner pre-login (ログイン前のバナー)	資格情報の要求前にクライアントが表示するテキスト。空 = バナーなし	空

パスワードと公開キーのうち、少なくとも一方は有効にしておく必要があります。両方が無効の場合、プログラムは保存を許可しません。その後、アカウントごとに方法を限定できます (7.2 項)。

5.3 アクセス制御

フィールド	説明
Chi può accedere (アクセスできるユーザー)	**Users**: Account タブで定義したアカウントのみ (推奨。Bitvise と同様)。 **Groups**: 指定した Windows グループのメンバー。 **Any**: 有効な任意の Windows アカウント。
Gruppi ammessi (許可するグループ)	Groups モードの場合のみ。コンマ区切りで指定します。例: `ssh-utenti`、`CONTOSO\gruppo-ssh`。Groups モードでは、少なくとも 1 つのグループが必須です
Account sempre negati (常に拒否するアカウント)	いかなる場合も除外するアカウント (コンマ区切り)。Account タブで無効にしたアカウントは自動的に追加されます
Nega accesso interattivo e Desktop remoto agli account solo-SFTP (SFTP 専用アカウントの対話型ログオンとリモート デスクトップを拒否)	Solo SFTP モードのローカル アカウントは `SSH-SFTP-Only` グループに追加され、このグループにはコンソールへのログオンとリモート デスクトップが拒否されます。既定値: 有効

> **注意:** **Users** モードでアカウントが 1 つも定義されていない場合、OpenSSH には制限が一切渡されず、有効な Windows アカウントが**すべて**受け入れられます。

> **注:** 対話型ログオンの拒否は、ローカル セキュリティ ポリシー (`secedit`) によって設定されます。ドメインに参加しているコンピューターでは、同じユーザー権利を定義する GPO が優先され、この設定を無効にする場合があります。

5.4 転送とセッション

フィールド	説明	既定値
Inoltro porte predefinito (既定のポート転送)	個別に再定義しないアカウントに適用される値: `no`、`yes` (ローカルとリモート)、`local` (クライアントからサーバー方向のみ)、`remote` (サーバーからクライアント方向のみ)	`no`
GatewayPorts	`no`: リモート転送はサーバーの localhost でのみ待ち受けます。`yes`: すべてのインターフェイスで待ち受けます。`clientspecified`: クライアントが決定します	`no`
Consenti inoltro dell'agent SSH (SSH エージェント転送を許可)	クライアントの SSH エージェントをサーバー上で使用できるようにします	いいえ
Shell predefinita (既定のシェル)	`powershell` (Windows PowerShell 5.1)、`pwsh` (PowerShell 7、インストールされている場合)、`cmd`、または実行可能ファイルの完全なパス。すべてのアカウントに適用されます。実行可能ファイルが存在しない場合、設定は無視され、Output パネルに警告が表示されます	`powershell`

5.5 暗号化とログ

フィールド	説明	既定値
Profilo algoritmi (アルゴリズム プロファイル)	**Modern**: 最新のアルゴリズムのみ (curve25519、利用可能な場合は ML-KEM/sntrup、AES-GCM、ChaCha20、Ed25519、ECDSA、RSA-SHA2 のキー)。 **Compatible**: 古いクライアント向けに、NIST の鍵交換、`diffie-hellman-group14-sha256`、`hmac-sha1`、および `ssh-rsa` キーを追加します。 **Default**: OpenSSH の既定値のままにします。 インストールされているバージョンでサポートされていないアルゴリズムは、自動的に除外されます。	Modern
Livello log (ログ レベル)	イベント ログのメッセージの詳細度: `QUIET` から `DEBUG3` まで。`INFO` はログインと IP ブロックには十分です。`VERBOSE` では、ログイン時に使用されたキーのフィンガープリントが追加されます	INFO

> **ヒント:** **Compatible** は、一部のクライアント (古いバージョンの PuTTY、ネットワーク機器、古い SFTP ライブラリ) が接続できなくなった場合にのみ使用してください。

5.6 詳細設定

Righe aggiuntive sshd_config フィールドには、GUI にない OpenSSH のグローバル ディレクティブを 1 行に 1 つずつ入力します。これらはユーザーごとのブロックの前にそのまま挿入され、適用時に `sshd -t` で検証されます。誤った行があると適用はできませんが、動作中のサーバーが損なわれることはありません。

> **注意:** ここに `Match` ブロックを入力しないでください。その後にプログラムが生成するディレクティブが続くことになり、意味が変わってしまいます。

6. Firewall タブ

プログラムは、SSH サーバー専用の Windows ファイアウォールの規則を管理します。これは Bitvise の「IP access rules」に相当し、一覧にないアドレスからの接続は OpenSSH に到達する前に破棄されます。

フィールド	説明	既定値
Gestisci il Windows Firewall per il server SSH (SSH サーバー用に Windows ファイアウォールを管理)	無効の場合、プログラムはファイアウォールに一切変更を加えません (既存の規則はそのまま残ります)	はい
Profili di rete (ネットワークプロファイル)	**Dominio** (ドメイン)、**Privato** (プライベート)、**Pubblico** (パブリック): ポートを開くプロファイル。ファイアウォールを管理する場合は、少なくとも 1 つが必須です	Dominio, Privato
IP / reti ammessi (許可する IP / ネットワーク)	1 行に 1 つ。使用できるもの: `Any`、`LocalSubnet`、単一のアドレス (`203.0.113.10`)、CIDR ネットワーク (`192.168.1.0/24`)、範囲 (`10.0.0.1-10.0.0.50`)。空の場合は次と同じです: `Any`	`Any`
Disattiva le regole OpenSSH predefinite di Windows (Windows の既定の OpenSSH 規則を無効化)	インストール時に Microsoft が作成する受信の規則を無効にします。この規則はポート 22 をすべてのアドレスに開きます	はい

プロファイルに関するガイドライン:

- **サーバー**: **Dominio** プロファイル。公開されているネットワーク アダプターがパブリックに分類されている場合にのみ、**Pubblico** を追加します。
- **PC とノート PC**: **Dominio** と **Privato**。パブリック ネットワーク (ホテル、ホットスポット) ではポートは閉じたままとなり、これが本来あるべき状態です。

作成される規則は 2 つです。

表示名	機能
WinSSH Manager - SSH (TCP-In)	許可するアドレスからの SSH ポートへの接続を許可します。対象は次の実行可能ファイルに限定されます: `sshd.exe`
WinSSH Manager - IP bloccati	自動ブロックまたは手動で追加された IP をブロックします (9章)。すべてのプロファイルで、SSH ポートに対してのみ適用されます

> **注意:** SSH 経由でリモートからサーバーを管理している場合は、自分のアドレス (またはネットワーク) を **IP / reti ammessi** に含める必要があります。含めないと、最初に **Applica** (適用) した後、次の接続が拒否されます。

7. Account タブ

各 SSH アカウントは、ローカルまたは Active Directory の**実際の Windows アカウント**に対応します。OpenSSH for Windows は仮想アカウントをサポートしていません。このタブには、許可されたアカウントとその規則が一覧表示されます。

> **注:** アカウントの変更は、確定した時点で `config.json` に保存され、**APPLICA CONFIGURAZIONE** で有効になります。

7.1 アカウントの一覧

列	内容
Account (アカウント)	Windows アカウントの名前 (ローカル アカウントの場合は `nome`、ドメイン アカウントの場合は `DOMINIO\nome`)
Attivo (有効)	「Sì」または「No」。無効なアカウントは灰色で表示されます
Accesso (アクセス)	「Shell」または「Solo SFTP」(SFTP のみ)
Cartella radice (ルート フォルダー)	アカウントの SFTP フォルダー
Opzioni (オプション)	ユーザーがフォルダーに閉じ込められている場合は「chroot」、読み取り専用の場合は「sola lettura」
Inoltro (転送)	ポート転送の許可
Autenticazione (認証)	必要な認証方法
Da IP (接続元 IP)	アカウントが接続できるアドレス
Descrizione (説明)	自由記述のメモ

ボタン: **Nuovo...** (新規)、**Modifica...** (編集。行をダブルクリックしても可)、**Chiavi pubbliche...** (公開キー)、**Abilita / disabilita** (有効化/無効化)、**Reimposta password...** (パスワードのリセット)、**Elimina...** (削除)。**Nuovo...** 以外はすべて、選択したアカウントに対して動作します。

7.2 アカウントの作成

Nuovo... をクリックすると、セクションに分かれた「Nuovo account SSH」(新しい SSH アカウント) ウィンドウが開きます。

Identità (ID)

フィールド	説明
Account Windows (Windows アカウント)	ローカル アカウント: 名前のみ (例: `mario`)。Active Directory アカウント: `DOMINIO\nome`。スペース、`@`、引用符は使用できません。ローカル アカウントの名前は 20 文字以内です。作成後は名前を変更できません
Descrizione (説明)	自由記述のメモ。コメントとして次にも記載されます: `sshd_config`
Account abilitato (アカウントを有効にする)	無効の場合、アカウントは構成に残りますが、拒否されます

Account Windows locale (ローカル Windows アカウント)

このセクションは、作成時かつローカル アカウントの場合にのみ表示されます。

フィールド	説明
Crea l'account Windows locale se non esiste (ローカル Windows アカウントが存在しない場合は作成する)	アカウントが存在しない場合は、指定したパスワードで作成されます。パスワードは無期限で、ユーザーは変更できません。Shell モードのアカウントは Users グループにも追加されます
Password, Conferma password (パスワード、パスワードの確認)	アカウントを作成する場合にのみ使用されます。パスワードはどの構成ファイルにも保存されず、ログやプロセスの一覧にも表示されません

存在しないローカル アカウントを作成せずに保存すると、Windows アカウントが存在するまでログインできないことをプログラムが警告します。

Tipo di accesso (アクセスの種類)

オプション	説明
Shell completa (フル シェル)	ターミナル、SFTP、SCP、トンネル (許可されている場合)。ユーザーはどのフォルダーにも閉じ込められません
Solo SFTP (SFTP のみ)	ファイル転送のみ。ターミナルを開くことも、エージェントを使用することもできません。明示的に別の設定をしない限り、ポート転送は禁止されます
Cartella radice SFTP (SFTP ルート フォルダー)	Solo SFTP の場合のみ。**ローカル**の完全なパス (例: `D:\SFTP\mario`)。**Sfoglia...** (参照) で選択できます。ネットワーク フォルダーは使用できません。存在しない場合は、適用時に作成されます
Confina nella cartella (chroot) (フォルダーに閉じ込める (chroot))	フォルダーが指定されている場合に使用できます。ユーザーにはフォルダーが `/` として表示され、そこから出ることはできません。chroot を使用しない場合、フォルダーは開始位置にすぎません
Sola lettura (読み取り専用)	ユーザーはダウンロードできますが、ファイルのアップロード、変更、削除はできません

> **注意:** ルート フォルダーは実際のローカル フォルダーである必要があります。ネットワーク ドライブ、ジャンクション、フォルダー内のシンボリック リンクは、OpenSSH for Windows では確実に動作しません。

Inoltro porte (tunnel) (ポート転送 (トンネル))

フィールド	説明
Inoltro consentito (許可する転送)	`default` (Server タブのグローバル値を使用)、`no`、`local`、`remote`、`yes`
Destinazioni (locale) (宛先 (ローカル))	`local` または `yes` の場合に有効です。ローカル転送で到達できる宛先を `host:porta` (ホスト:ポート) 形式でコンマ区切りで指定します。例: `127.0.0.1:3389, sql01:1433`。空 = すべて
Porte in ascolto (remoto) (待ち受けポート (リモート))	`remote` または `yes` の場合に有効です。ユーザーがサーバー上で開くことができるポートを `[host:]porta` 形式で指定します。例: `8080`。空 = すべて。OpenSSH 7.8 以降が必要です

Sicurezza (セキュリティ)

フィールド	説明
Autenticazione (認証)	`default` (グローバル設定を適用)、`password`、`publickey`、`publickey+password` (**両方**が必要: 最初にキー、次にパスワード)
Accesso solo da (アクセスを許可する接続元)	アカウントが接続できる IP または CIDR ネットワーク (コンマ区切り)。空 = 任意のアドレスから

Salva (保存) を押すと、アカウントが登録されます。認証方法に公開キーが必要な場合、プログラムはキーを追加するためのウィンドウをすぐに開きます。

7.3 編集、有効化、無効化

- **Modifica...** (またはダブルクリック) をクリックすると、アカウントのデータが入力された同じウィンドウが開きます。名前は変更できず、Windows アカウント作成のセクションは表示されません。
- **Abilita / disabilita** は、アカウントの状態を切り替えます。無効にしたアカウントは、適用後に OpenSSH によって拒否されますが、Windows アカウントは他の用途では有効なままです。

7.4 パスワードのリセット

Reimposta password... は、選択した**ローカル** Windows アカウントの新しいパスワードを要求し、適用を待たずにすぐに設定します。ドメイン アカウントの場合は、パスワードは Active Directory で管理することをプログラムが通知します。

7.5 アカウントの削除

Elimina... は、次の 3 つの質問を順に表示します。

1. 「Rimuovere l'account dalla configurazione SSH?」(SSH 構成からアカウントを削除しますか?) — `config.json` からアカウントを削除します。
2. 「Eliminare anche le sue chiavi pubbliche dall'archivio centrale?」(中央ストアからその公開キーも削除しますか?)
3. ローカル アカウントの場合のみ: 「Eliminare anche l'account Windows locale?」(ローカル Windows アカウントも削除しますか?)。この操作は元に戻せません。ユーザー プロファイルはディスク上に残ります。

削除後、**APPLICA CONFIGURAZIONE** を押します。

7.6 公開キー

Chiavi pubbliche... をクリックすると、選択したアカウントのキーの一覧が、連番とフィンガープリント (ビット数、SHA256、コメント、種類) 付きで開きます。

ボタン	機能
Incolla chiave... (キーの貼り付け)	1 つ以上の公開キーを 1 行に 1 つずつ貼り付けます。形式: `ssh-ed25519 AAAA··· commento`
Importa file .pub... (.pub ファイルのインポート)	クライアントで生成された公開キーのファイルを選択します
Elimina selezionata (選択したキーを削除)	確認後、選択したキーを削除します
Chiudi (閉じる)	ウィンドウを閉じます

- 各キーは `ssh-keygen` で検証されます。認識されない行は警告を表示して無視され、重複はスキップされます。
- **秘密キー**は常に拒否されます。誤って間違ったファイルを貼り付けた場合は、プログラムが通知します。
- キーは、OpenSSH が要求するアクセス許可付きで `C:\ProgramData\ssh\managed_keys\<account>` (ドメイン アカウントの場合は `managed_keys\dominio\nome`) に保存されます。
- 中央ストアのキーは**管理者にも**有効です。一方、管理者アカウントの場合、OpenSSH はファイル `%USERPROFILE%\.ssh\authorized_keys` を無視します。有効なのは `administrators_authorized_keys` と中央ストアのみです。
- 追加または削除したキーは、適用しなくても新しいログインにすぐに有効になります (構成が少なくとも 1 回適用済みであることが条件です)。

> **ヒント:** クライアントでは、キー ペアを `ssh-keygen -t ed25519` で生成します。サーバーには末尾が `.pub` のファイルのみをアップロードします。秘密キーはクライアントの PC から決して外に出さないでください。

7.7 SFTP フォルダーのアクセス許可

構成を適用すると、プログラムは存在しないルート フォルダーを作成し、アカウントに次の NTFS アクセス許可を割り当てます。

アカウントの種類	割り当てられるアクセス許可
Solo SFTP、読み取りと書き込み	ルート フォルダー: 読み取り専用 (ユーザーはフォルダーを削除したり名前を変更したりできません)。ファイルとサブフォルダー: 変更
Solo SFTP、読み取り専用	ツリー全体に対する読み取りと実行

アクセス許可は既存のものに追加され、置き換えられることはありません。フォルダーに他のユーザー専用のデータが含まれている場合は、割り当てる前に継承されたアクセス許可を確認してください。

8. Sessioni タブ

サーバーのポート上のアクティブな SSH 接続を一覧表示します。タブを開くたびに更新されます。

列	内容
Id (ID)	セッションのプロセス識別子
Utente (ユーザー)	接続しているアカウント。ログインがまだ完了していない場合は「(autenticazione in corso)」(認証中)
Remoto (リモート)	クライアントのアドレスとポート
Inizio (開始)	接続を開いた日時

- **Aggiorna** (更新): 一覧を再読み込みします。
- **Disconnetti selezionata** (選択したセッションを切断): 確認後、選択したセッションを閉じます。メイン サービスが終了されることはありません。
- **Aggiorna ogni 10 secondi** (10 秒ごとに更新): 自動更新です。タブが表示されている間のみ有効です。

9. Blocco IP タブ

IP ブロックは Bitvise の「IP blocking」に相当し、ログインに繰り返し失敗するアドレスを検出して、一定期間ファイアウォールでブロックします。

9.1 動作のしくみ

- スケジュールされたタスク `WinSSHManager-IPBlocker` が SYSTEM として実行されます。OpenSSH のログに新しいイベントが記録されるたび、5 分ごと (ブロックの期限切れ処理のため)、およびシステムの起動時に実行されます。
- 失敗としてカウントされるもの: パスワードまたはキーの誤り、存在しないユーザー、許可された試行回数の超過、許可されていないユーザー (「not allowed because」)。
- IP が指定した期間内にしきい値を超えると、ファイアウォールの規則「WinSSH Manager - IP bloccati」に追加されます。
- 期限が切れると、ブロックは遅くとも 5 分以内に自動的に解除されます。
- `127.0.0.1`、`::1`、およびホワイトリストのアドレスがブロックされることはありません。

9.2 設定

左側のパネルです。設定は、下部のコマンド バーのボタンで保存して適用します。

フィールド	説明	既定値
Blocco automatico attivo (自動ブロックを有効にする)	ブロックを有効または無効にします。スケジュールされたタスクの変更は、保存した時点で行われます	はい
Fallimenti per bloccare (ブロックまでの失敗回数)	ブロックが発動する失敗した試行の回数 (1 〜 1000)	5
Nell'arco di (minuti) (期間 (分))	失敗をカウントする期間 (1 〜 1440)	10
Durata blocco (minuti) (ブロック期間 (分))	一時的なブロックの期間 (最大 1 年)	60
Permanente dopo N blocchi (N 回のブロック後に永続化)	ブロックが永続的になるまでの 30 日間のブロック回数。0 = 永続化しない	0

フィールド	説明	既定値
Chiudi le sessioni già aperte dall'IP bloccato (ブロックした IP から既に開かれているセッションを閉じる)	ブロック時に、そのアドレスから既に確立されている接続も閉じます	はい
Mai bloccare (whitelist) (ブロックしない (ホワイトリスト))	IP または CIDR ネットワーク、1 行に 1 つ	`127.0.0.1`, `::1`

> **注意:** サーバーを管理するネットワークは、**必ず**ホワイトリストに追加してください。パスワードを数回入力ミスしただけで、自分自身がブロックされる可能性があります。

9.3 ブロックされた IP と記録

右側には、**IP bloccati** (ブロックされた IP) の一覧 (IP またはネットワーク、開始日時、終了日時、理由。期限のないブロックは「permanente」(永続)) と、**Registro blocchi** (ブロックの記録) が表示されます。記録には `ipblocker.log` の最新 300 行が表示されます。記録は 1 MB を超えると自動的にローテーションされます。

ボタン	機能
Aggiorna (更新)	一覧と記録を再読み込みします
Blocca IP... (IP をブロック)	アドレスまたは CIDR ネットワークを手動でブロックします。期間を分単位で入力します。`0` = 永続
Sblocca selezionato (選択した IP のブロックを解除)	選択した IP のブロックを解除し、その失敗回数をリセットします
Sblocca tutti (すべてのブロックを解除)	確認後、すべてのブロックを解除し、すべてのカウンターをリセットします
Esegui un ciclo ora (今すぐ 1 サイクル実行)	スケジュールされたタスクを待たずに、すぐにログを分析します

10. Log タブ

OpenSSH/Operational ログのイベントを新しい順に表示します。タブを初めて開いたときに読み込まれます。

- 成功したログインは**緑色**、失敗または拒否されたログインは**赤色**で表示されます。
- **ダブルクリック**した行のイベントの全文が開きます。
- **Solo accessi falliti / negati** (失敗/拒否されたアクセスのみ) は、エラー イベントを抽出します。
- **Eventi** (イベント) では、表示するイベントの数を指定します (10 ～ 5000、既定値 200)。
- **Aggiorna** は、設定した条件でログを再読み込みします。
- **Apri Visualizzatore eventi** (イベント ビューアーを開く) は、Windows のイベント ビューアーで OpenSSH/Operational ログを直接開きます。

> **ヒント:** ユーザーがログインできない場合は、**Solo accessi falliti / negati** を有効にしてそのユーザー名を検索します。ほとんどの場合、メッセージに原因 (パスワードの誤り、キーが受け入れられない、ユーザーが許可されていない、許可されていない IP からの接続) が示されています。

11. Backup タブ

11.1 設定のエクスポート

Esporta... (エクスポート) は、次の内容を含む zip アーカイブ (提案される名前は `WinSshManager-AAAAMMGG.zip`) を作成します。

- `config.json`
- アカウントの公開キーのストア
- `administrators_authorized_keys`
- **Includi le chiavi host** (ホスト キーを含める) が選択されている場合のみ: サーバーのホスト キー。

> **注意:** ホスト キーは**秘密**キーです。zip を所有する者は誰でもサーバーになりすますことができます。同じフィンガープリントを維持したまま別のコンピューターにサーバーを移行する場合にのみ含め、ファイルはパスワードと同様に厳重に保管してください。

11.2 設定のインポート

Importa... (インポート) は、以前にエクスポートした zip を読み込みます。

- `config.json` を置き換えます (現在のバージョンのコピーが `backup` に残ります)。
- zip に含まれる公開キーと `administrators_authorized_keys` を追加します。
- **Importa anche le chiavi host, se presenti nel file** (ファイルにホスト キーが含まれている場合はそれもインポートする) が選択されている場合は、ホスト キーを置き換えます。
- 完了すると、すぐに構成を適用するかどうかを確認します。

11.3 sshd_config の復元

Ripristina sshd_config da backup... (バックアップから sshd_config を復元) では、`C:\ProgramData\WinSshManager\backup` に保存されたバージョンのいずれかを選択できます。選択したファイルは `sshd -t` で検証されて使用が開始され、サービスが再起動されます。

> **注意:** 復元は `sshd_config` にのみ作用します。`config.json` はそのまま残るため、次に **Applica** すると、その設定が再び適用されます。復元は緊急時の対処として使用し、その後、各タブで設定を修正してください。

11.4 フォルダー

Apri cartella dati (データ フォルダーを開く) は `C:\ProgramData\WinSshManager` を開き、**Apri cartella ssh** (ssh フォルダーを開く) は `C:\ProgramData\ssh` を開きます。

12. 手順ガイド

以下の手順は、最も一般的なケースを対象としています。特に指示がない限り、各手順の最後に **APPLICA CONFIGURAZIONE** を押します。

12.1 推奨される運用開始手順

1. **Server** タブ: ポートは 22、またはサーバーがインターネットに公開されている場合は大きい番号のポート (ログのノイズは減りますが、それ自体はセキュリティ対策ではありません)。**Chi può accedere** = **Users**、**Profilo algoritmi** = **Modern**、シェルは `powershell` または `pwsh`。
2. **Firewall** タブ: コンピューターに適したプロファイル (6 章) を選択し、**IP / reti ammessi** にローカルネットワークと接続元のパブリック IP を指定します。
3. **Blocco IP** タブ: 既定値のままにし、管理用のネットワークをホワイトリストに追加します。
4. **Salva e applica** を実行します。
5. **Account** タブ: アカウントを作成し (以降の項を参照)、適用します。
6. サーバー自体で `ssh nomeutente@localhost` を使用して確認し、SFTP アカウントの場合は `sftp nomeutente@localhost` も使用します。別の PC からは、提示されたフィンガープリントを **Stato** → **Impronte chiavi host** と比較します。

12.2 キー認証の管理者と RDP/SQL トンネル

1. **Nuovo...** で、既存の Windows アカウント (例: 管理者のアカウント) を指定します。
2. **Shell completa** を選択します。
3. **Inoltro consentito** = `local`、**Destinazioni** = `127.0.0.1:3389, 127.0.0.1:1433`。
4. **Autenticazione** = `publickey`。
5. **Salva** を押し、開いたウィンドウで公開キーを追加します。
6. 適用します。クライアントから: `ssh -L 13389:127.0.0.1:3389 utente@server` を実行し、リモートデスクトップで `localhost:13389` に接続します。

12.3 ファイルを預け入れる取引先 (SFTP のみ)

1. **Nuovo...** で、専用のローカル アカウントの名前 (例: `fornitore`) を指定し、強力なパスワードで **Crea l'account Windows locale** を選択します。
2. **Solo SFTP**、**Cartella radice** = `D:\SFTP\fornitore`、**Confina nella cartella** を有効にします。

3. **Autenticazione** = `password` (取引先がキーを持っている場合は `publickey`)。
4. **Accesso solo da** = 取引先のパブリック IP。
5. 適用します。ユーザーにはフォルダーが `/` として表示され、その中でファイルをアップロードおよび管理できますが、フォルダー自体を削除することはできず、コンソールやリモート デスクトップにもアクセスできません。

12.4 読み取り専用の閲覧

前のケースと同様にし、さらに **Sola lettura** を有効にします。ユーザーはダウンロードのみ可能です。OpenSSH が書き込みを拒否し、割り当てられる NTFS アクセス許可も読み取り専用です。

12.5 アクセスを失わずにポートを変更する

1. リモートで作業している場合は、新しいポート番号に到達できること (ルーター、境界ファイアウォール) を確認します。
2. **Porta TCP** を変更して **Salva e applica** を押し、警告を承認します。
3. 管理対象のファイアウォール規則は、自動的に新しいポートに移行されます。
4. 既存の接続を閉じる**前に**、新しいポートで `ssh -p NUOVAPORTA utente@server` を使用して**新しい**接続を開きます。

12.6 キー認証のみに移行する

1. 各アカウントについて、**Chiavi pubbliche...** ウィンドウで少なくとも 1 つのキーがあることを確認し、キーでのログインを試します。
2. **Server** タブ: **Consenti autenticazione con password** を無効にします。
3. **Salva e applica** を押し、警告を承認します。

代わりに、一部のアカウントでのみキーを必須にすることもできます。その場合は、該当するアカウントで **Autenticazione** = `publickey` を設定します。

12.7 Bitvise SSH Server からの移行

1. Bitvise でアカウントとそのアクセス許可を一覧にします。仮想アカウントは、ローカル Windows アカウントとして作成し直す必要があります (**Nuovo...** で **Crea l'account Windows locale** を選択)。
2. 各 Bitvise アカウントからクライアントの公開キーをエクスポートし、**Chiavi pubbliche...** でインポートします。

3. クライアントにフィンガープリント変更の警告が表示されないようにするには、Bitvise からホストキーを OpenSSH 形式でエクスポートし (使用中のバージョンで可能な場合)、`C:\ProgramData\ssh\` に `ssh_host_ed25519_key` / `ssh_host_rsa_key` という名前と、それぞれの `.pub` でコピーします。それ以外の場合は、新しいフィンガープリントをクライアントに通知します。
4. Bitvise を停止し、そのサービスのスタートアップの種類を **無効** に設定します。
5. 構成を適用し、ログインを確認してから、Bitvise をアンインストールします。

機能の対応:

Bitvise SSH Server	WinSSH Manager
一元化された設定	`config.json`、適用は **APPLICA CONFIGURAZIONE**
Windows accounts / 許可するグループ	Server → **Chi può accedere** (Users / Groups)
アカウントごとの接続元 IP 制限	Account → **Accesso solo da**
SFTP のみ、ルート フォルダー、読み取り専用マウント	Account → **Solo SFTP**、**Cartella radice**、**Confina**、**Sola lettura**
アカウントごとの転送の許可	Account → **Inoltro porte**
アカウントごとの公開キー	Account → **Chiavi pubbliche...**
IP access rules	タブ: **Firewall**
IP blocking	タブ: **Blocco IP**
セッション、ログ、ホスト キーのフィンガープリント	タブ: **Sessioni**、**Log**、**Stato**
Export / import settings	タブ: **Backup**

13. テキスト コンソールと PowerShell からの使用

GUI を使用できない場合 (SSH セッション、Server Core、緊急時) でも、**管理者として起動した PowerShell** から同じ機能を利用できます。

13.1 メニュー形式のコンソール

```
C:\ProgramData\WinSshManager\SshManager.ps1      # menu interattivo
C:\ProgramData\WinSshManager\SshManager.ps1 -Install # installa/abilita OpenSSH
C:\ProgramData\WinSshManager\SshManager.ps1 -Apply   # applica la configurazione
C:\ProgramData\WinSshManager\SshManager.ps1 -Status  # stato sintetico
```

メイン メニューの上部には、バージョン、サービスの状態、ポート、アカウント数、IP ブロックの状態が表示され、未適用の変更がある場合は通知されます。項目は次のとおりです。

項目	機能	項目	機能
1	詳細な状態	7	ログ
2	OpenSSH Server のインストール/有効化	8	ホスト キーのフィンガープリント
3	サーバーの設定 (ネットワーク、認証、アクセス、ファイアウォール)	9	APPLICA CONFIGURAZIONE
4	アカウントとキー	10	sshd_config のプレビュー
5	アクティブなセッション	11	エクスポート/インポート、メモ帳での config.json の編集
6	IP ブロック	12	サービスの開始/停止

質問では、Enter キーを押すと角かっこ内の値が維持されます。一覧では、文字 - でフィールドを空にします。変更のたびに、コンソールはすぐに適用するかどうかを確認します。

13.2 モジュールのコマンド

自動化のためには、モジュールを直接インポートします。

```
Import-Module C:\ProgramData\WinSshManager\WinSshManager.psm1 -DisableNameChecking
Get-SshServerStatus
Set-SshManagedUser -Name mario -Mode Shell -AuthMethods publickey `
  -AllowTcpForwarding local -PermitOpen '127.0.0.1:3389'
Add-SshUserKey -Name mario -Path C:\temp\id_ed25519.pub
Update-SshServerConfiguration
Unblock-SshIp -Ip 203.0.113.9
```

コマンド	機能
`Install-SshManager`	OpenSSH をインストール/有効化して初期化します
`Update-SshServerConfiguration`	構成を適用します (`-NoRestart` を指定すると再起動しません)
`Get-SshServerStatus`	サーバーの状態
`Get-SshManagedUser`, `Set-SshManagedUser`, `Remove-SshManagedUser`	アカウントの読み取り、作成/変更、削除
`Get-SshUserKey`, `Add-SshUserKey`, `Remove-SshUserKey`	公開キーの管理
`Get-SshSession`, `Stop-SshSession`	アクティブなセッション
`Get-SshLog`	OpenSSH のイベント (`-Last N`、`-FailuresOnly`)
`Get-SshBlockedIp`, `Block-SshIp`, `Unblock-SshIp`	手動の IP ブロック (`Unblock-SshIp -Ip '*'` ですべてのブロックを解除)
`Enable-SshIpBlocker`, `Disable-SshIpBlocker`	スケジュールされたタスクの有効化
`Get-SshHostKeyFingerprint`	ホスト キーのフィンガープリント
`New-SshdConfigText -Config (Get-SshManagerConfig)`	プレビュー: `sshd_config`
`Export-SshManagerSettings`, `Import-SshManagerSettings`	エクスポートとインポート (`-IncludeHostKeys`)

14. 知っておくべき制限事項

- **仮想アカウントなし**: 各 SSH ユーザーは実際の Windows アカウントです。SFTP のみのアクセスには、専用のローカル アカウントを作成することをお勧めします。
- **ユーザーごとに 1 つのフォルダー**: chroot は 1 つのローカル フォルダーのみです。ネットワーク ドライブ、ジャンクション、内部のシンボリック リンクは信頼性がありません。
- **chroot は SFTP のみ**: Shell モードでは、ユーザーは閉じ込められません (OpenSSH for Windows の制限)。
- **シェルは 1 つのみ**: 既定のシェルはサーバー全体に適用され、アカウントごとには設定できません。
- **FTPS は非対応**: SFTP と SCP のみです。SCP は Shell アカウントで使用でき、Solo SFTP アカウントでは使用できません。
- **ローカルでの管理のみ**: GUI は、起動したコンピューターに対して動作します。
- **OpenSSH の更新**: Windows Update から提供されます。代わりに Microsoft の MSI 版 (GitHub の `PowerShell/Win32-OpenSSH` プロジェクト) をインストールすることもでき、自動的に検出されます。
- **Windows 10/11 では**、スリープ状態の PC は応答しません。サーバーとして使用する場合は、電源オプションを調整してください。
- **ドメイン コントローラー**: ローカル アカウントがないため、ドメイン アカウントのみを使用します。

15. トラブルシューティング

問題	考えられる原因と解決策
「sshd -t ha rifiutato la configurazione generata」(sshd -t が生成された構成を拒否しました)	メッセージに行が示されます。通常は、インストールされているバージョンでサポートされていないオプション (アルゴリズム プロファイル **Default** を試してください)、または **Righe aggiuntive sshd_config** の誤った行が原因です。動作中のサーバーには変更が加えられていません。
「Risposta non valida da PowerShell」(PowerShell からの応答が無効です)	`PowerShell` フォルダーが実行可能ファイルと同じ場所にあること、および GPO が `powershell.exe` をブロックしていないことを確認します。エラーの全文は「Output operazioni」パネルにあります。
ユーザーがログインできない	**Log** タブで **Solo accessi falliti / negati** を使用します。アカウントが Account タブにあって有効であること、構成が適用済みであること、IP が許可されていること (Firewall と **Accesso solo da**)、およびブロックされていないこと (Blocco IP タブ) を確認します。
キーによるログインが拒否される	多くの場合、キー ファイルのアクセス許可が正しくありません。構成を再適用してください。管理者の場合、`%USERPROFILE%\.ssh` 内のキーは無視されます。**Chiavi pubbliche...** で読み込んでください。ドメイン アカウントの場合は、初回ログインを慎重に確認してください。
chroot を使用した SFTP が機能しない	フォルダーが存在し、ローカルであり、ジャンクションでないこと、およびユーザーが少なくとも読み取り権限を持っていることが必要です。
自分自身をブロックしてしまった	ローカル コンソールまたはリモート デスクトップから: **Blocco IP** タブ → **Sblocca selezionato** を実行し、自分のネットワークをホワイトリストに追加します。
変更後にサーバーが応答しない	**Backup** タブ → **Ripristina sshd_config da backup...** を実行し、その後設定を修正します。

問題	考えられる原因と解決策
OpenSSH のインストールに失敗した	オプション機能 **OpenSSH Server** を [設定] → [アプリ] → [オプション機能] から、または社内の FoD ソースからインストールし、その後 **Installa / abilita OpenSSH** を実行します。

15.1 詳細なデバッグ

1. **Stato** タブ → **Arresta** を実行します。
2. 管理者として実行した PowerShell で `& "$env:windir\System32\OpenSSH\sshd.exe" -d` を実行します。サーバーは 1 回のログインのみを処理し、認証のすべての手順を画面に出力します。
3. クライアントからログインを試み、拒否の理由を確認します。
4. **Stato** タブ → **Avvia** を実行します。

16. アンインストール

管理者として起動した PowerShell から:

```
Import-Module C:\ProgramData\WinSshManager\WinSshManager.psm1 -DisableNameChecking
Disable-SshIpBlocker
Remove-NetFirewallRule -Name WinSSHManager-SSH-In, WinSSHManager-Blocklist -ErrorAction
SilentlyContinue
Enable-NetFirewallRule -Name OpenSSH-Server-In-TCP -ErrorAction SilentlyContinue
Remove-Item C:\ProgramData\WinSshManager -Recurse -Force
```

OpenSSH の元の構成に戻す場合は、最後の行の前に `backup\sshd_config.originale.*` を `C:\ProgramData\ssh\sshd_config` にコピーします。最後に、プログラムのフォルダーを削除します。

OpenSSH Server、Windows アカウント、`SSH-SFTP-Only` グループ、および `C:\ProgramData\ssh` 内のキーはそのまま残ります。不要になった場合は手動で削除してください。

付録 A. システムに作成されるオブジェクト

オブジェクト	名前	備考
サービス	`sshd`	Microsoft 製。スタートアップの種類は自動に設定されます
ファイアウォール規則	`WinSSHManager-SSH-In` (「WinSSH Manager - SSH (TCP-In)」)	SSH ポートへのアクセス
ファイアウォール規則	`WinSSHManager-Blocklist` (「WinSSH Manager - IP bloccati」)	ブロックされた IP
スケジュールされたタスク	`WinSSHManager-IPBlocker`	SYSTEM として実行
ローカル グループ	`SSH-SFTP-Only`	SFTP 専用アカウント。対話型ログオンと RDP なし
レジストリ キー	`HKLM\SOFTWARE\OpenSSH\DefaultShell`	既定のシェル
ユーザー権利	ローカル ログオンを拒否 / リモート デスクトップ サービスを使ったログオンを拒否	割り当て先グループ: `SSH-SFTP-Only`
イベント ログ	アプリケーションとサービス ログ → OpenSSH → Operational	Microsoft 製。Log と Blocco IP が読み取ります

付録 B. 用語集

用語	意味
sshd / sshd_config	OpenSSH Server サービスとその構成ファイル
config.json	WinSSH Manager がすべての設定を保持するファイル。このファイルから次が生成されます: `sshd_config`
適用	`config.json` から `sshd_config` を再生成し、使用を開始してサービスを再起動すること
ホスト キー	サーバーを識別するキー ペア。そのフィンガープリントにより、クライアントはサーバーを認識できます
フィンガープリント (fingerprint)	キーを一意に識別する短いコード (例: `SHA256:…`)
公開キー	クライアントのキー ペアのうち公開可能な部分。パスワードなしでログインするためにサーバーにアップロードします
SFTP / SCP	SSH 上のファイル転送プロトコル
chroot	SFTP ユーザーを 1 つのフォルダーに閉じ込めること。ユーザーにはそのフォルダーがルートとして表示されます: `/`
ポート転送 (トンネル)	SSH を介した TCP 接続の転送。ローカル (クライアントから、サーバーが到達できる宛先へ) またはリモート (サーバーからクライアントへ)
CIDR	IP ネットワークの表記。例: `192.168.1.0/24` = 192.168.1.0 〜 192.168.1.255
ホワイトリスト	決してブロックされないアドレスの一覧
UAC	Windows のユーザー アカウント制御。プログラムを管理者として実行する際の確認要求