

RDP Session Scanner

Version 2.0

User's Manual

For Administrators and Users

Software by: TC Consulting

Platform: Windows · Interface: Web Browser

Table of Contents

1. Introduction	4
Key Capabilities	4
2. System Requirements	4
Host Machine (where the app runs)	4
Client Machines (what is probed)	4
User Workstations	5
3. Installation	5
Using the Compiled Executable (Recommended)	5
Running as a Startup Service (Optional)	5
4. Accessing the Application	6
Browser Certificate Warning	6
Logging In	6
What You See After Logging In	7
5. Configure Page	7
Configuration Password	7
Changing Your Password	8
Company Name	8
Listening Port	8
Bind Address	8
RDP Hosts Tab	8
Groups Tab	9
User Profiles Tab	9
Audit Log Tab	9
Closing Configure	10
6. Host Fields Reference	10
User Profile Fields Reference	11
7. Scanning Hosts	11
Group Display on the Dashboard	11
8. Status Indicators	12
9. Connecting to a Host	12
What Happens When You Click Connect	12
One-Time Client Setup — Connect and Shadow from Any PC	13
Downloading the Setup Package	13
RdpHandler Security	13
When the Connect Button Is Disabled	14
10. Shadowing a Session	14
Shadow vs. Connect	14
When to Use Shadow	14
When to Use Connect	15
Group Policy Requirement	15
Session ID	15
Credentials for Shadow	15

11. Security	15
Dashboard Authentication.....	15
HTTPS / TLS Encryption	16
Rate Limiting.....	16
Configuration Change Audit Log	16
Encryption Key Isolation	16
API Password Protection.....	16
Bind Address Restriction.....	17
12. Firewall & Port Forwarding.....	17
What Works Through a Firewall	17
Exposing the Dashboard to External Users.....	17
Cisco ASA 5506	18
Juniper SRX300	18
Verifying Access	18
Session Detection Firewall Rules (quser / qwinsta)	19
Cisco ASA 5506 — Session Detection Rules	19
Juniper SRX300 — Session Detection Rules	19
Windows Firewall on Target PCs.....	19
13. Required Permissions	20
14. Troubleshooting.....	20
Machine shows Offline but I can ping it	20
RDP Enabled shows Disabled but I can connect manually.....	20
Logged-in Users shows Unknown	20
Users show as Free after I connect	21
Connect or Shadow button does nothing	21
Shadow fails with an access-denied error	21
Login page shows "Too many attempts"	21
Browser shows certificate warning on every visit	21
hosts.json, settings.json, or users.json not found	21
15. Data Files	22
hosts.json.....	22
groups.json	22
users.json.....	22
settings.json.....	22
secret.key.....	22
connections.log.....	22
config_changes.log	23

1. Introduction

RDP Session Scanner is a lightweight, browser-based web application that runs on a Windows machine inside your network. It provides a single dashboard where you can see the status of every configured RDP host at a glance — whether the machine is online, whether RDP is responding, and whether anyone is currently logged in.

From the same dashboard you can launch a full Remote Desktop connection or shadow an active session with a single click, without opening the Windows Remote Desktop client manually or remembering IP addresses and port numbers.

✓ Minimal setup — RDP Session Scanner is web-based. Users access the dashboard through any modern browser with no installation. To use the Connect and Shadow buttons from a remote PC, a one-time setup (install_rdp_handlers.bat) is required on that PC. The dashboard itself — scanning, status, and host management — works in any browser with no setup at all.

Key Capabilities

- Probe any number of hosts in parallel and display results in seconds.
- Detect online/offline status, RDP availability, and active user sessions.
- Distinguish local console sessions from remote RDP sessions.
- Launch mstsc.exe on the user's own PC with the correct port and resolution (requires one-time RdpHandler setup).
- Shadow any active session (local or remote) with a single click.
- Require a username and password to log in to the dashboard — each person uses their own User Profile credentials.
- Organize hosts into named, collapsible groups on the dashboard for easier navigation.
- Support machines behind firewalls via separate probe and connect addresses.
- Display a company name in the page header for easy branding.
- Encrypt all traffic between the browser and the server using HTTPS (TLS).

2. System Requirements

Host Machine (where the app runs)

- Windows 10 / Windows Server 2016 or later
- Network access to the machines you want to probe

Client Machines (what is probed)

- Windows with Remote Desktop enabled
- ICMP (ping) allowed from the host machine, or RDP port reachable

- For session detection: TCP 445 (SMB), TCP 135 (RPC Endpoint Mapper), and TCP 49152–65535 (dynamic RPC) open from the host machine to each target; the host machine's Windows account must have remote query rights on the target

User Workstations

The dashboard itself works in any browser with no installation. To use the Connect and Shadow buttons from a remote PC, a one-time setup is required on that PC (see One-Time Client Setup in the Connecting to a Host chapter):

- Any modern browser: Chrome, Edge, Firefox, or Safari
- Network access to the machine running SessionScanner.exe
- For Connect and Shadow: Windows PC with RdpHandler.exe installed — download RdpHandler_Setup.zip from the dashboard, extract, and run install_rdp_handlers.bat as Administrator (once per PC)
- For Connect and Shadow: Administrator rights required on the PC during setup (to copy RdpHandler.exe to C:\Windows\System32)

3. Installation

Using the Compiled Executable (Recommended)

- Copy SessionScanner.exe to a permanent folder on the host machine, for example C:\Tools\SessionScanner\
- Double-click SessionScanner.exe. A console window confirms the server is running and shows the URL (e.g. https://localhost:5000). Keep this window open while using the dashboard.
- Open a browser and go to https://localhost:5000 (or the port shown in the console). From other machines on the same network use the host IP: https://<host-ip>:5000
- On first launch, accept the browser security warning for the self-signed TLS certificate (see Section 11 — Security for details).
- Log in with your username and password. If no User Profiles have been created yet, leave the username blank and enter the configuration password.

i Data file location: hosts.json, settings.json, groups.json, and users.json are stored in the same folder as the executable. The encryption key (secret.key) is stored separately in %LOCALAPPDATA%\SessionScanner\. Keep the executable in a folder where the running account has write access.

Running as a Startup Service (Optional)

To start automatically with Windows, create a scheduled task that runs SessionScanner.exe at logon or system startup, or use NSSM (Non-Sucking Service Manager) to wrap it as a Windows service.

4. Accessing the Application

Once SessionScanner.exe is running, open any web browser on the same network and navigate to the application URL. All traffic is encrypted using HTTPS with a self-signed TLS certificate.

Scenario	URL
On the same machine as the executable	https://localhost:5000 (replace 5000 with your configured port)
From another PC on the same network	https://<server-ip>:5000 (e.g. https://10.20.30.40:5000)

i The default listening port is 5000. You can change it in the Configure panel under Listening Port. A restart of SessionScanner.exe is required for the new port to take effect. The console window always shows the actual port the server is listening on.

i Replace <server-ip> with the IP address of the Windows machine running SessionScanner.exe. You can find it by running ipconfig in a command prompt on that machine.

Browser Certificate Warning

Because the TLS certificate is self-signed (not issued by a public certificate authority), your browser will display a security warning on first access. This is expected and safe within your local network. To proceed:

- Chrome / Edge: click Advanced, then Proceed to <ip> (unsafe).
- Firefox: click Advanced, then Accept the Risk and Continue.

i You only need to accept the certificate once per browser. After acceptance, the padlock icon appears normally on all future visits.

Logging In

After navigating to the URL, a login page appears. Enter your username and password to access the dashboard.

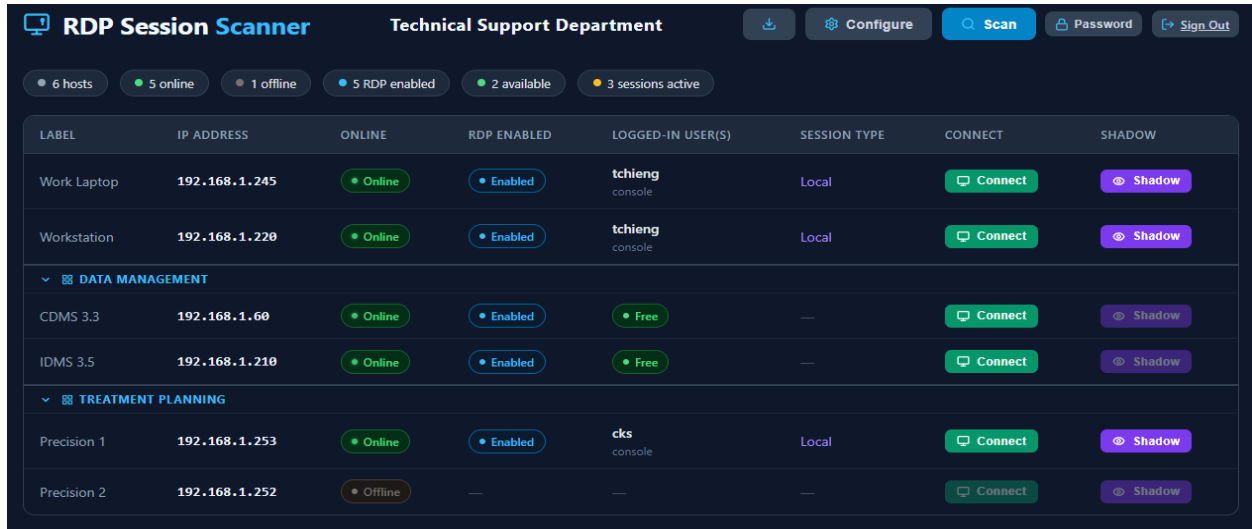
Login method	How to log in
User Profile account	Enter the username and password configured on your User Profile in the Configure panel.
Admin (config password)	Leave the username field blank and enter the configuration password. Use this if no User Profiles have been created yet, or if all profile passwords have been lost.

i Sessions expire after 12 hours of inactivity. You will be redirected to the login page when your session expires.

⚠ After 5 failed login attempts from the same IP address, that address is locked out for 15 minutes. Wait for the lockout to expire, or ask an administrator to restart the application to clear it immediately.

What You See After Logging In

If at least one RDP host has been configured, the dashboard loads and immediately begins scanning. The results appear within a few seconds. The example below shows a typical dashboard after a scan completes.



LABEL	IP ADDRESS	ONLINE	RDP ENABLED	LOGGED-IN USER(S)	SESSION TYPE	CONNECT	SHADOW
Work Laptop	192.168.1.245	Online	Enabled	tchieng console	Local	Connect	Shadow
Workstation	192.168.1.220	Online	Enabled	tchieng console	Local	Connect	Shadow
DATA MANAGEMENT							
CDMS 3.3	192.168.1.60	Online	Enabled	Free	—	Connect	Shadow
IDMS 3.5	192.168.1.210	Online	Enabled	Free	—	Connect	Shadow
TREATMENT PLANNING							
Precision 1	192.168.1.253	Online	Enabled	eks console	Local	Connect	Shadow
Precision 2	192.168.1.252	Offline	—	—	—	Connect	Shadow

Figure 1 — RDP Session Scanner dashboard showing six configured hosts after a scan.

If no hosts have been configured yet, a message prompts you to click Configure and add hosts first.

5. Configure Page

Click the Configure button in the top-right corner of the dashboard to open the configuration panel. All settings are saved immediately to the server. The panel has four tabs: RDP Hosts, Groups, User Profiles, and Audit Log.

Configuration Password

The configuration password is used as the admin fallback on the login page (leave the username blank). It also protects the Change Configuration Password bar inside the Configure panel. It is not shared with any User Profile account.

ℹ The default password is ChangeMe! — change it the first time you open Configure. The password is stored as a secure PBKDF2-SHA256 hash in settings.json; the original password cannot be recovered from the stored value.

⚠ If the admin password is lost, stop SessionScanner, delete the config_password entry from settings.json, and restart. The application will re-seed the default password (ChangeMe!) on next startup. Log in with the default password and change it immediately.

Changing Your Password

Any logged-in user can change their own password from the header. Click the Password button (lock icon) in the top-right corner of the dashboard. A dialog prompts for your current password, a new password, and confirmation. Click Change Password to save.

- User Profile accounts: the new password is saved to users.json for that profile.
- Admin (blank-username) account: the new password updates the config_password in settings.json.

ℹ Administrators can also change the configuration password from inside the Configure panel using the Change Configuration Password bar.

Company Name

Enter your organization's name in the Company Name field and click Save. It appears centered in the main page header. Leave it blank to hide it.

Listening Port

The Listening Port field controls which TCP port SessionScanner.exe binds to when it starts. The default is 5000. To use a different port, enter the new value and click Save, then restart SessionScanner.exe. The console window always shows the port the server is currently using.

ℹ If you change the port, update any browser bookmarks, firewall rules, and port-forwarding rules to match the new port number.

Bind Address

The Bind Address field controls which network interface SessionScanner.exe listens on. The default is 0.0.0.0 (all interfaces). To restrict the dashboard to a specific network interface, enter its IP address (e.g. 192.168.1.10) and click Save, then restart SessionScanner.exe.

ℹ Setting the bind address to 127.0.0.1 (localhost) makes the dashboard accessible only from the machine running SessionScanner.exe. This is the most restrictive option.

RDP Hosts Tab

Manage the list of machines to probe and connect to. Each host has its own set of fields (see section 6). Host credentials are used by the server to query session status — they are not used to authenticate your RDP connection.

- Add Host — fill in the form at the bottom of the tab and click Save Host.
- Edit Host — click Edit on any row; the form populates with that host's current values.

- Delete Host — click Delete on the row and confirm. The host is removed permanently.

Groups Tab

Groups let you organise hosts into named categories that are displayed as collapsible sections on the dashboard. Groups are optional — hosts not assigned to a group appear at the top of the dashboard under an ungrouped section.

- Add Group — enter a Group Name in the form at the bottom of the tab and click Save Group.
- Edit Group — click Edit on any row; the name field populates for editing.
- Delete Group — click Delete on the row and confirm. Any hosts assigned to that group are moved to Ungrouped automatically; no host data is lost.
- Host Count — the Groups table shows how many hosts are currently assigned to each group.

User Profiles Tab

User profiles serve two purposes: they allow each person to sign in to the dashboard with their own username and password, and they store optional Windows credentials used by the server to query session status on each scan.

- Add Profile — fill in the form and click Save Profile.
- Edit Profile — click Edit on any row.
- Delete Profile — click Delete on the row and confirm.

i Each person logs in to the dashboard using the username and password stored on their User Profile. The admin fallback (leave username blank) uses the configuration password and does not require a User Profile.

Audit Log Tab

The Audit Log tab shows a record of every Connect and Shadow action initiated from the dashboard, including which dashboard user made it, plus every user Login (Success or Failed) and Logout. Login and Logout entries have no host or target; the Detail column shows Success or Failed. It is read-only. The log is loaded fresh each time you open the tab.

Column	Description
Timestamp	Date and time the action was initiated (server time).
Action	CONNECT (blue badge) or SHADOW (purple badge).
User	The dashboard user who made the connection. Logins with the configuration password are recorded as admin. Entries logged before this column was added show a blank user.
Source IP	The IP address of the browser that clicked the button.
Host	The label of the target host as configured.
Target	The Connect IP and port used for the connection.

Detail	For Shadow actions, the RDP session ID that was shadowed.
--------	---

Click the Refresh button to reload the log from the server, showing any entries added since the tab was last opened.

Closing Configure

Click **×** or click outside the panel. The dashboard waits 5 seconds (to allow any stored credentials to register) and then runs a fresh scan against the updated host list.

6. Host Fields Reference

Field	Required	Description
Label	Optional	A friendly display name shown in the main table. E.g. Reception PC or Treatment Room 3.
Group	Optional	The group this host belongs to. Hosts in the same group are displayed together in a collapsible section on the dashboard. Leave blank for Ungrouped.
Probe Address	Required	The IP address used to probe the machine — ping, RDP port check, and session query. Must be reachable from the scanner host.
Probe Port	Optional	The TCP port used for the RDP Enabled check and session probing. Defaults to 3389.
Connect IP	Optional	A different IP used only when clicking Connect or Shadow. Use for machines behind a firewall. Leave blank to use the Probe Address.
Connect Port	Optional	The TCP port passed to mstsc when connecting. Defaults to the Probe Port when left blank.
Resolution	Optional	Screen resolution passed to mstsc.exe. Defaults to 1920x1200. Options: 1024x768 up to 2560x1440.
Default Username	Optional	Windows account used by the server to query session status on this host. Accepts DOMAIN\user or user@domain format. Not used to authenticate your RDP connection.
Default Password	Optional	Password for the Default Username above, used by the server for session scanning only. Stored encrypted in hosts.json.

User Profile Fields Reference

Field	Required	Description
Display Name	Recommended	Human-readable label shown in the User Profiles list. E.g. Jane Smith or Admin - John.
Username	Required	The username used to log in to the dashboard.
Password	Required	The password used to log in to the dashboard. Stored encrypted in users.json.

i Host and user profile passwords are encrypted at rest using Fernet symmetric encryption (AES-128-CBC + HMAC-SHA256). The encryption key is stored in secret.key under %LOCALAPPDATA%\SessionScanner\ — separate from the data files. Keep that folder accessible to the running account; losing secret.key means stored passwords must be re-entered.

7. Scanning Hosts

The dashboard runs a scan automatically in three situations:

- When the page first loads and at least one host is configured.
- When the Configure panel is closed (after a 5-second delay to allow stored credentials to register).
- Three seconds after a successful Connect or Shadow action.

You can trigger a manual scan at any time by clicking the Scan button. All configured hosts are probed in parallel, so the total scan time equals the slowest host's response time.

A progress bar is displayed during the scan. Summary chips show counts of hosts scanned, online, offline, RDP-enabled, available, and active sessions.

Group Display on the Dashboard

When groups have been configured, hosts are organised into collapsible sections on the dashboard:

- Ungrouped hosts — displayed first, sorted alphabetically by label (or probe address if no label is set).
- Named groups — displayed below the ungrouped section, sorted alphabetically by group name. Each group has a header row showing the group name and the number of hosts in the group.
- Hosts within each group — sorted alphabetically by label.

Click any group header row to collapse or expand that group. Collapse states are preserved across scans.

✓ Tip: For large numbers of hosts the scan completes faster when all machines are powered on. Offline machines wait the full 1-second ping timeout, but this happens in parallel across all hosts simultaneously.

8. Status Indicators

Column	Badge / Value	Meaning
Online	Online (green)	Machine responded to a ping (ICMP echo).
Online	Offline (grey)	No ping response within 1 second. Powered off, unreachable, or blocking ICMP.
RDP Enabled	Enabled (blue)	TCP connection to the configured RDP port succeeded.
RDP Enabled	Disabled (grey)	RDP port refused or timed out.
Logged-in Users	Free (green)	RDP is available and no user sessions were detected.
Logged-in Users	Unknown (grey)	The session query was denied — typically wrong credentials, insufficient remote permissions, or a firewall blocking RPC. The machine may or may not have active users.
Logged-in Users	Username shown	One or more users are logged in.
Session Type	Remote (orange)	Session established via RDP (session name begins with rdp-tcp).
Session Type	Local (purple)	Local console session — user is physically at the machine.

9. Connecting to a Host

The Connect button is enabled when a host is Online, RDP Enabled, and does not have an active remote session. A local console session does not block the button.

What Happens When You Click Connect

- The browser calls `http://localhost:9876/connect` on your own PC — no file is downloaded and no browser prompt appears.
- `RdpHandler.exe` (running silently in the background on your PC) receives the request and launches `mstsc.exe` with the correct host address, port, and resolution.
- The RDP window opens on your own PC — not on the server running SessionScanner.
- Windows will prompt for your RDP credentials on first connect to each host. Tick "Remember my credentials" to save them in your local Windows Credential Manager — future connects to the same host will be silent.

One-Time Client Setup — Connect and Shadow from Any PC

Both the Connect and Shadow buttons work by calling a small background helper (RdpHandler.exe) that runs on the user's own PC. A setup package can be downloaded directly from the dashboard — no manual file copying required.

Downloading the Setup Package

Click the RDP Handler button (download icon) in the top-right corner of the dashboard. The browser downloads RdpHandler_Setup.zip, which contains two files:

File	Purpose
RdpHandler.exe	Pre-compiled background helper. The installer copies this to C:\Windows\System32\.
install_rdp_handlers.bat	Run once on each user's PC. Copies RdpHandler.exe to C:\Windows\System32, registers it to start automatically at login, and starts it immediately.

- Download RdpHandler_Setup.zip from the dashboard and extract both files to any folder.
- Right-click install_rdp_handlers.bat and choose Run as administrator.
- The installer copies RdpHandler.exe to C:\Windows\System32\RdpHandler.exe, registers it to auto-start at login, and starts it immediately.
- No reboot is needed. Connect and Shadow work immediately after installation.

✓ Once RdpHandler is installed, Connect and Shadow launch instantly with no browser dialog or prompt of any kind. RdpHandler runs silently in the background and starts automatically every time the user logs in.

❗ If Connect or Shadow shows an error message saying "RdpHandler not running", the helper is not installed or was stopped on that PC. Run install_rdp_handlers.bat on that machine and try again.

RdpHandler Security

Control	How it works
Shared secret token	On page load the dashboard fetches a 256-bit random token from the SessionScanner server and sends it to RdpHandler as a bootstrap ping. Every subsequent Connect and Shadow request must carry that token. Requests without a valid token are rejected with HTTP 403 before any process is launched.
Origin locking	The bootstrap ping also passes the SessionScanner page origin. RdpHandler locks its CORS Allow-Origin header to that specific origin, so browser requests from any other site are blocked by the browser's same-origin policy.

Parameter validation	All query parameters are strictly validated before use: IP/hostname must match a safe character whitelist, port must be 1–65535, resolution must be one of the supported values, and the shadow session ID must be a non-negative integer.
Constant-time token check	The token check uses a byte-by-byte comparison that takes the same time regardless of where a mismatch occurs, preventing timing-based token guessing attacks.

⚠ The shared token is stored in settings.json. Secure the SessionScanner folder so that only authorised administrators have read access to it — anyone who can read settings.json can extract the token and call RdpHandler directly.

When the Connect Button Is Disabled

Tooltip	Reason
Host is offline	Ping failed — machine is unreachable.
RDP not available	RDP port check failed.
Remote session in use	Another user is already connected via RDP.

10. Shadowing a Session

The Shadow button appears whenever a user — local or remote — is logged in to a host. Clicking it launches mstsc.exe in shadow mode, letting you view and control the active session.

Shadow vs. Connect

Connect opens a new, independent RDP session for you. Shadow attaches to an existing session. Both parties share keyboard and mouse control in Shadow mode.

When to Use Shadow

- Remote support — a user reports an error or unexpected behaviour. Shadow lets you see their exact screen at the moment the problem occurs.
- Live training — demonstrate a procedure while the user watches your mouse and keyboard in real time.
- Diagnosing a running application — the application or error is already open in their session.
- Verifying what a user is seeing — confirm the display, layout, or system state from their perspective.

When to Use Connect

- Performing administrative tasks, running scripts, or installing software without disturbing an active user session.
- Doing your own work on the server — your session is fully private and isolated.
- No user is currently logged in and you simply need access to the machine.

Group Policy Requirement

⚠ RDP shadowing requires the following Group Policy setting on each target machine: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections > Set rules for remote control of Remote Desktop Services user sessions. Set to Enabled and choose "Full Control with user's permission" (prompts the user) or "Full Control without user's permission" (silent). Without this setting the shadow connection will be refused.

Session ID

The session ID is obtained automatically from query user or qwinsta during the scan and passed to RdpHandler.exe. No manual entry is required.

Credentials for Shadow

Shadow launches mstsc on the user's local PC. The credentials configured in the app are used for session scanning only — they are not passed to mstsc. Windows handles RDP authentication using credentials stored in your local Windows Credential Manager.

11. Security

RDP Session Scanner includes the following security controls to protect the dashboard and its data.

Dashboard Authentication

The dashboard requires a username and password to access. Credentials are verified before any page is served.

- User Profile accounts: each user logs in with a username and password configured on their profile.
- Admin fallback: leave the username blank on the login page and enter the configuration password. This account is intended for initial setup and administrator access only.
- Each logged-in user can change their own password at any time using the Password button in the dashboard header.
- Sessions are maintained via an encrypted server-side cookie and expire after 12 hours.

HTTPS / TLS Encryption

All traffic between the browser and the server is encrypted using TLS. A self-signed certificate is generated automatically on first run and stored in %LOCALAPPDATA%\SessionScanner\. The certificate is valid for 10 years and includes the server's bind address as a Subject Alternative Name.

i Because the certificate is self-signed, browsers display a security warning on first access. Accept the warning once per browser. The certificate protects the connection from eavesdropping despite the warning.

Rate Limiting

The login page is protected against brute-force password guessing:

- After 5 consecutive failed login attempts from the same IP address, that address is locked out for 15 minutes.
- The lockout counter resets automatically on a successful login.
- Restarting SessionScanner.exe clears all active lockouts immediately.

Configuration Change Audit Log

Every change made through the Configure panel is recorded in config_changes.log alongside the data files. Each entry records the timestamp, the type of change (HOST_ADDED, HOST_MODIFIED, HOST_DELETED, GROUP_*, USER_*, PASSWORD_CHANGED, or SETTINGS_CHANGED), the source IP of the browser, and the label of the affected record.

i The config_changes.log file is append-only and not exposed through the dashboard. Review it directly on the server to audit configuration history.

Encryption Key Isolation

The Fernet encryption key used to encrypt passwords in hosts.json and users.json is stored in a separate location from the data files:

- Key location: %LOCALAPPDATA%\SessionScanner\secret.key
- Data files: the folder containing SessionScanner.exe

This separation means that access to the data folder alone is insufficient to decrypt stored passwords. An attacker would need access to both locations.

API Password Protection

The REST API never returns decrypted passwords to the browser:

- GET /api/hosts and GET /api/users always return an empty string in the password field.
- POST /api/hosts and POST /api/users preserve the existing encrypted password if the client submits an empty string, preventing accidental password erasure.

Bind Address Restriction

The Bind Address setting in the Configure panel controls which network interface the server listens on. Restricting it to a specific IP address or to 127.0.0.1 (localhost only) reduces the network attack surface. See the Bind Address section in the Configure Page chapter for details.

12. Firewall & Port Forwarding

RDP Session Scanner is designed to run inside the same network as the machines it probes. The four address/port fields let you separate probing from connecting, which is useful when the scanner sits outside a firewall or on a different network segment.

Field	Used for
Probe Address	Ping, RDP port check, and query user session detection. Use the IP reachable from the scanner host (typically the internal IP).
Probe Port	TCP port used for the RDP Enabled check and session probing. Defaults to 3389. Set to the forwarded port when probing through a firewall.
Connect IP	mstsc.exe launch only. Use the external / NAT IP or hostname. Leave blank to use the Probe Address.
Connect Port	TCP port passed to mstsc when connecting. Leave blank to use the Probe Port. Set to the external forwarded port when it differs from the probe port.

What Works Through a Firewall

- YES Online check — works if ICMP is allowed, or if the RDP port is open.
- YES RDP Enabled — works if the forwarded RDP port is reachable from the scanner host.
- NO Session detection — requires TCP 445, TCP 135, and dynamic RPC ports (49152–65535). These ports are rarely forwarded through a perimeter firewall.
- YES Connect / Shadow — works as long as mstsc can reach the external IP on the forwarded port.

Exposing the Dashboard to External Users

To allow users outside the local network to access the SessionScanner dashboard, create a port-forwarding (static NAT) rule on the perimeter firewall that maps the external interface to the SessionScanner host on its listening port (default 5000). Access is restricted to the remote desktop user group already defined on your firewall.

i The host IP 192.168.193.2 used in the examples is for illustration only. Replace it with the actual internal IP of the machine running SessionScanner.exe.

⚠ The SessionScanner dashboard now requires authentication and all traffic is encrypted via HTTPS. Restrict inbound firewall access to your authorised remote users group.

Cisco ASA 5506

The following commands create the OBJ_SESSION_SCANNER host object, add a static NAT entry, and add an inbound ACL entry restricting access to the existing RemoteDesktopAccess group. Paste in the ASA CLI (enable mode), then save:

```
! -- Host object for SessionScanner -----
! Replace 192.168.193.2 with the IP where SessionScanner.exe runs.
object network OBJ_SESSION_SCANNER
  host 192.168.193.2
! -- Static NAT: forward outside TCP 5000 -> OBJ_SESSION_SCANNER:5000 --
object network OBJ_SESSION_SCANNER
  nat (inside,outside) static interface service tcp 5000 5000
! -- Inbound ACL: RemoteDesktopAccess -> OBJ_SESSION_SCANNER:5000 -----
access-list outside_access_in extended permit tcp object-group RemoteDesktopAccess object
OBJ_SESSION_SCANNER eq 5000
! -- Save -----
write memory
```

Juniper SRX300

The following commands add OBJ_SESSION_SCANNER to the trust zone address book, add a static NAT rule, and add a security policy. Enter configuration mode (cli → configure) and paste:

i The IP address 10.20.30.40 used in the commands below is for illustration only. Replace it with the actual public IP address of your Juniper SRX firewall's external interface.

```
# -- Trust-zone address for SessionScanner -----
set security zones security-zone trust address-book address OBJ_SESSION_SCANNER 192.168.193.2/32
# -- Static NAT -----
set security nat static rule-set ProductRules rule SessionScanner5000 match destination-address
10.20.30.40/32
set security nat static rule-set ProductRules rule SessionScanner5000 match destination-port 5000
set security nat static rule-set ProductRules rule SessionScanner5000 then static-nat prefix
192.168.193.2/32 mapped-port 5000
# -- Custom application -----
set applications application APP_SESSION_SCANNER protocol tcp destination-port 5000
# -- Security policy -----
set security policies from-zone untrust to-zone trust policy ALLOW_SESSION_SCANNER_IN match source-
address Planning_Access
set security policies from-zone untrust to-zone trust policy ALLOW_SESSION_SCANNER_IN match
destination-address OBJ_SESSION_SCANNER
set security policies from-zone untrust to-zone trust policy ALLOW_SESSION_SCANNER_IN match
application APP_SESSION_SCANNER
set security policies from-zone untrust to-zone trust policy ALLOW_SESSION_SCANNER_IN then permit
# -- Commit -----
commit
```

Verifying Access

After applying the rules, open a browser from a machine in the RemoteDesktopAccess / Planning_Access group and navigate to <https://<external-ip>:5000>. Accept the certificate warning, then log in. If the login page does not appear:

- Confirm SessionScanner.exe is running and the console shows it is listening on the expected port.
- On the ASA: run packet-tracer input outside tcp <your-source-ip> 12345 <outside-interface-ip> 5000 detail.

- On the SRX: run show security flow session destination-port 5000.
- Check that no Windows Firewall rule on the SessionScanner host is blocking inbound TCP on the configured port.

Session Detection Firewall Rules (quser / qwinsta)

When the SessionScanner server and the target PCs are separated by a firewall, session detection requires outbound rules permitting the following TCP ports from the SessionScanner server to each target PC:

Port	Protocol	Purpose
445	TCP	SMB — named pipe transport used by the Remote Desktop Services query API.
135	TCP	RPC Endpoint Mapper — used to negotiate the dynamic port for the RPC call.
49152–65535	TCP	Dynamic RPC ports — the actual session query runs on a port negotiated via port 135.

Cisco ASA 5506 — Session Detection Rules

```
access-list inside_access_out extended permit tcp object OBJ_SESSION_SCANNER object-group RemoteDesktopAccess eq 445
access-list inside_access_out extended permit tcp object OBJ_SESSION_SCANNER object-group RemoteDesktopAccess eq 135
access-list inside_access_out extended permit tcp object OBJ_SESSION_SCANNER object-group RemoteDesktopAccess range 49152 65535
write memory
```

Juniper SRX300 — Session Detection Rules

```
set applications application APP_SMB protocol tcp destination-port 445
set applications application APP_RPC_EPM protocol tcp destination-port 135
set applications application APP_RPC_DYNAMIC protocol tcp destination-port 49152-65535
set applications application-set APP_SET_QUSER application APP_SMB
set applications application-set APP_SET_QUSER application APP_RPC_EPM
set applications application-set APP_SET_QUSER application APP_RPC_DYNAMIC
set security policies from-zone trust to-zone untrust policy ALLOW_QUSER_OUTBOUND match source-address OBJ_SESSION_SCANNER
set security policies from-zone trust to-zone untrust policy ALLOW_QUSER_OUTBOUND match destination-address Planning_Access
set security policies from-zone trust to-zone untrust policy ALLOW_QUSER_OUTBOUND match application APP_SET_QUSER
set security policies from-zone trust to-zone untrust policy ALLOW_QUSER_OUTBOUND then permit
commit
```

Windows Firewall on Target PCs

Each target PC must allow inbound connections on these ports through its local Windows Firewall:

Windows Firewall Rule	Ports covered
-----------------------	---------------

File and Printer Sharing (SMB-In)	TCP 445
Remote Desktop - Shadow (TCP-In)	TCP 135, dynamic RPC
Windows Management Instrumentation (WMI-In)	TCP 135, dynamic RPC

13. Required Permissions

Capability	Required Access
Ping	No special privileges — ICMP must be allowed by the target's firewall.
RDP port check	No special privileges — standard TCP connect.
Session detection	Scanning account must have Remote Interactive Logon rights or be a member of the Remote Desktop Users group on each target, or be a domain administrator.
Connect (mstsc)	The configured username must have RDP rights on the target.
Shadow	Configured username must have Remote Control permission, and the Group Policy setting in section 10 must be enabled.

14. Troubleshooting

Machine shows Offline but I can ping it

The scanner's ping uses a 1-second timeout. If the machine is slow to respond or ICMP is rate-limited, it may intermittently show as offline. Check whether a host-based firewall on the target is blocking ICMP.

RDP Enabled shows Disabled but I can connect manually

Verify that the IP Address and RDP Port fields match exactly what you type into the Windows RDP client. If a VPN or proxy is involved, the scanning machine may reach the port differently than your workstation.

Logged-in Users shows Unknown

Unknown means the session query (query user / qwinsta) ran against the target but was denied with an access error. Common causes:

- Wrong credentials — verify the Username and Password on the host are correct, using DOMAIN\user format for domain accounts.
- Insufficient remote permissions — the querying account must be a member of the local Administrators or Remote Desktop Users group on the target.

- UAC Remote Token Filtering — on the target, create the DWORD registry value LocalAccountTokenFilterPolicy = 1 under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Note that a domain Group Policy may override this setting.
- Firewall blocking RPC — TCP 135 and dynamic RPC ports (49152–65535) must be open from the scanning server to the target in addition to the RDP port.

Users show as Free after I connect

Session detection requires TCP 445 (SMB), TCP 135 (RPC Endpoint Mapper), and dynamic RPC ports (TCP 49152–65535) from the scanning machine to the target. Check that all three are open and that the scanning account has remote query rights on the target.

Connect or Shadow button does nothing

RdpHandler.exe is not running on this PC, or the installer has not been run yet. The Connect and Shadow buttons call `http://localhost:9876/` on the user's own PC. Run `install_rdp_handlers.bat` on the PC where the browser is open, then try again.

Shadow fails with an access-denied error

The Group Policy setting for remote control is not configured on the target. See section 10. Also confirm the connecting account has the Remote Control permission in the local security policy.

Login page shows "Too many attempts"

Five consecutive failed login attempts from the same IP address trigger a 15-minute lockout. Wait for the lockout period to expire, or restart SessionScanner.exe on the server to clear all lockouts immediately.

Browser shows certificate warning on every visit

Click Advanced and accept the self-signed certificate once per browser. After acceptance, the browser remembers the exception and the warning will not reappear for that URL. If the server's IP address changes, a new certificate is generated and the warning will appear again.

hosts.json, settings.json, or users.json not found

These files are created automatically the first time you save a host, company name, or user profile. They are stored in the same folder as SessionScanner.exe. Ensure the process has write permission to that folder.

15. Data Files

The application writes the following files. Data files are stored next to the executable; the encryption key is stored separately in %LOCALAPPDATA%\SessionScanner\.

hosts.json

Stores the list of configured RDP hosts. Each entry is a JSON object with the fields described in section 6, plus an auto-generated id. Default Username and Password are used by the server for session scanning only. Passwords are stored encrypted using Fernet symmetric encryption.

groups.json

Stores the list of named host groups. Each entry contains an auto-generated id and the group name. Hosts reference a group by its id. Deleting a group from the Configure panel automatically clears the group assignment on any hosts that referenced it — no host data is lost.

users.json

Stores per-user credential profiles used for dashboard authentication. Each entry contains a Display Name, Username, Password hash, and an auto-generated id. Dashboard login verifies the submitted password against the stored hash. Passwords are stored encrypted using Fernet symmetric encryption.

settings.json

Stores global application settings: the company name, listening port (default 5000), bind address (default 0.0.0.0), the configuration panel password hash, the RdpHandler shared secret token, and the Flask session secret. The configuration password is stored as a PBKDF2-SHA256 hash. Secure this file so only authorised administrators can read it.

secret.key

Contains the Fernet symmetric encryption key used to encrypt and decrypt passwords in hosts.json and users.json. Generated automatically on first run. Stored in %LOCALAPPDATA%\SessionScanner\ (separate from the data files) to isolate it from the application data folder. If it is lost, all stored passwords must be re-entered. Do not share it outside your server.

connections.log

A plain-text log file appended to each time a Connect or Shadow action is initiated from the dashboard. Each line records the server timestamp, action (CONNECT or SHADOW), the dashboard username of the person who made the connection (admin for the configuration-password login, with spaces replaced by underscores), source IP of the browser, host label, target IP:port, and (for Shadow) the RDP session ID. Can be viewed from the Audit Log tab in the Configure panel.

config_changes.log

A plain-text audit log appended to each time a configuration change is made through the Configure panel. Each line records the server timestamp, the change type, the source IP of the browser, and the label of the affected record.

Change Type	When logged
HOST_ADDED	A new RDP host was saved.
HOST_MODIFIED	An existing host's fields were changed.
HOST_DELETED	A host was removed.
GROUP_ADDED	A new group was created.
GROUP_MODIFIED	A group name was changed.
GROUP_DELETED	A group was removed.
USER_ADDED	A new user profile was created.
USER_MODIFIED	A user profile was updated.
USER_DELETED	A user profile was removed.
PASSWORD_CHANGED	A user's own password was changed via the Password button.
SETTINGS_CHANGED	A setting (company name, port, bind address, etc.) was saved.

i config_changes.log is append-only and is not accessible through the dashboard. Review it directly on the server to audit who changed what and when.

All data files can be copied to a new machine alongside the executable to migrate your configuration. The secret.key file must also be copied from %LOCALAPPDATA%\SessionScanner\ to the same path on the new machine.