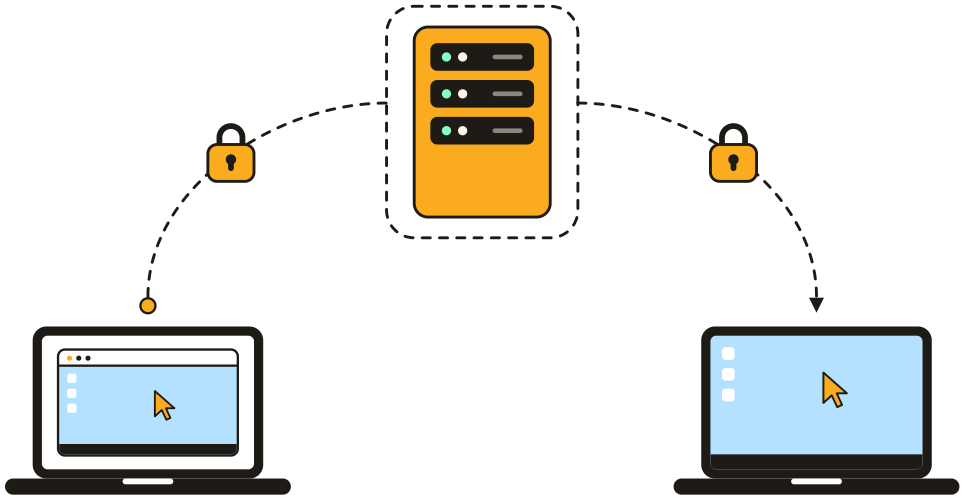
Remote Utilities®

TECHNICAL OVERVIEW

Security Whitepaper

How Remote Utilities protects connections, credentials and stored data.



DOCUMENT

Version 1.0
November 2026

APPLIES TO

Remote Utilities for Windows 7.9, for macOS and Linux 2.1, mobile Viewer 14.3, RU Server 3.5.6

AUDIENCE

IT administrators, security teams and technical evaluators

Contents

1	Security at a Glance	3
2	Components and Channels	4
3	Encryption of the Viewer–Host Connection	5
4	Authentication and Access Control on the Host	8
5	Self-Hosted Server	10
6	Protection of Stored Data	13
7	Software Integrity	13
8	Logging and Audit Trail	14
9	Platform Availability	14
10	Recommended Configuration	15
A	Where to Find the Settings	16
B	Glossary	16

About this document

This whitepaper explains how Remote Utilities secures remote access: how connections are encrypted, how technicians are authenticated and what they are allowed to do, how passwords and address books are stored, and which controls an administrator has at hand.

It is written for IT administrators, security teams and anyone evaluating Remote Utilities for use in their organization. A glossary at the end explains the cryptographic terms.

The description was prepared by the Remote Utilities development team from the source code of the product versions listed here. Where a feature exists only on some platforms, the text says so, and section 9 gives the full matrix.

PRODUCT VERSIONS COVERED

Viewer, Host and Agent for Windows	**7.9**
Viewer, Host and Agent for macOS and Linux	**2.1**
Mobile Viewer for iOS and Android	**14.3**
Remote Utilities Server (RU Server)	**3.5.6**

1 Security at a Glance

Remote Utilities is remote desktop software for IT support and administration. Its security rests on a few principles that hold in every connection mode, on every license and on every platform.

Encryption is always on

All data between Viewer and Host is encrypted, on every license including the free one. There is no setting that turns encryption off.

Two layers of protection

Authentication takes place inside TLS 1.2 or 1.3. After sign-in, the session is encrypted with a one-time AES-256 key.

End-to-end encryption

A relay server, ours or your own, only forwards encrypted packets. It sees neither passwords nor the content of a session.

Host identity check

The Viewer remembers the certificate of every Host and warns the technician if the certificate ever changes.

Authentication is mandatory

Four methods, in any combination. There are no default or blank passwords: a Host with no method enabled accepts no connections.

No passwords in clear text

Access passwords and server account passwords are stored only as hashes and travel over the network only inside TLS.

Permissions per user and mode

Rights are granted to each user or group for each connection mode. The Host enforces them, not the Viewer.

Your network, your server

No account with us is needed. The whole system, including the server, can run inside your own network without Internet access.

PLATFORM NOTE

The Host for Windows has the widest set of controls. Two-factor authentication, the IP filter, brute-force protection and authentication with Windows accounts are features of the Host for Windows. Section 9 lists what is available on each platform.

2 Components and Channels

A Remote Utilities deployment has up to three kinds of participants:

- **Viewer** is the technician's program. It runs on Windows, macOS, Linux, iOS and Android.
- **Host** is the program on the remote computer. It runs as a service and allows unattended access. **Agent** is the variant of the Host that runs without installation, for a one-off support session.
- **Server** is an optional intermediary. It is either our public Internet-ID service or Remote Utilities Server (RU Server), which you install on your own premises.

Remote Utilities works without registration and keeps no central record of your users or computers. Access passwords and permissions are stored on your Hosts or on your own server, not with us. Our public Internet-ID servers only route connections: they hold no user accounts, no address books and no license keys.

A Viewer reaches a Host in one of two ways. A **direct connection** goes straight to the address of the Host, usually inside a local network or a VPN. An **Internet-ID connection** is brokered by a server: the Host keeps an outgoing connection to it, so the remote network needs no public address and no open inbound ports.

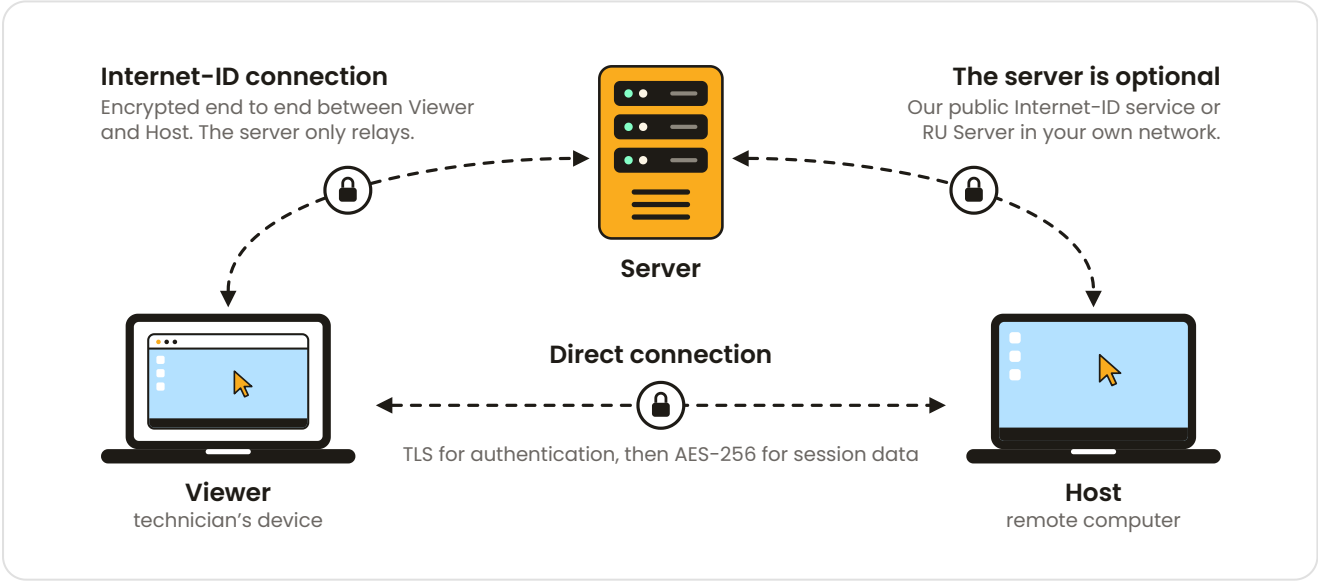


Figure 1. The two connection paths. Both are encrypted between the Viewer and the Host. A direct connection involves no server at all.

Table 1. Communication channels and how each one is protected

Channel	What it carries	Protection
Viewer and Host: authentication	Credentials, the two-factor code, the session key	TLS 1.2 or 1.3, Host certificate
Viewer and Host: connection modes	Screen, keyboard and mouse, files, terminal, clipboard and all other session data	AES-256 with the session key
Viewer and Host through Internet-ID	The same, relayed by the server	The same encryption from Viewer to Host. The server sees routing data only
Viewer and RU Server	Account sign-in, address books, license keys	TLS 1.2 or 1.3, server certificate
Host and RU Server	Checks of a user and the user's permissions	TLS 1.2 or 1.3, server certificate
Service connection of a Host or Viewer to the Internet-ID server	ID, program version, license information	Routing data only. Access passwords and session content never pass through it

3 Encryption of the Viewer–Host Connection

3.1 Three stages of every connection

Every connection passes the three stages shown in Figure 2, whether it is direct or goes through Internet-ID, and whichever platforms the Viewer and the Host run on.

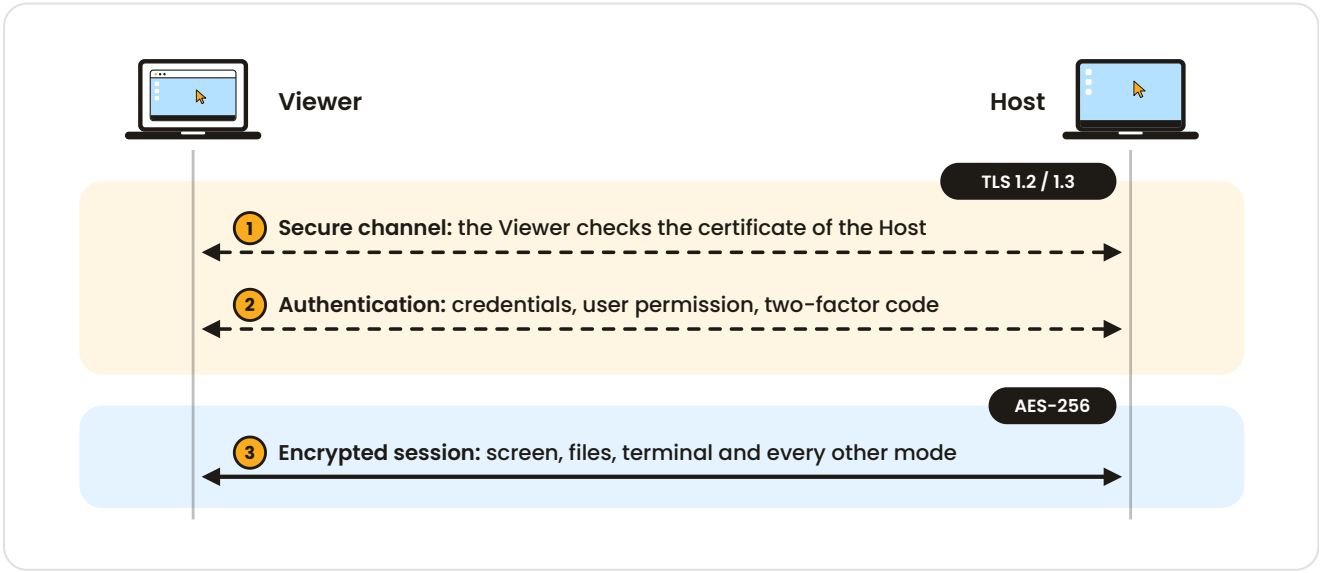


Figure 2. The three stages of a connection. The permission prompt and the two-factor code are optional.

Two properties matter most. First, a password and the session key travel only inside TLS, after the Viewer has checked the Host certificate. Second, only a Viewer that has authenticated successfully receives the session key, and the key is required for every connection mode: without it nobody can join someone else's session.

3.2 Cryptographic parameters

Table 2. Encryption parameters of the Viewer–Host connection

Element	Implementation
Protection of authentication	TLS 1.2 or TLS 1.3. Earlier protocol versions are not accepted. The implementation uses the OpenSSL 3 library.
Host certificate	Self-signed, with an RSA 2048-bit key and a SHA-256 signature. The Host creates it at first start. In the Host for Windows it can be viewed, exported and re-issued in the **Host identity** tab of the settings.
Session key	AES, 256 bits. Random, created anew for every sign-in, delivered only inside TLS and never stored.
Encryption of session data	AES-256 with the one-time session key.
One implementation	Windows, macOS, Linux, iOS and Android use the same encryption code. There are no differences between platforms.

3.3 Verifying the identity of the Host

A Host certificate is not issued by a certificate authority. Remote Utilities uses the trust-on-first-use model, familiar from SSH:

- At the first connection the Viewer saves the Host certificate in the properties of the connection in the address book.
- At every later connection it compares the certificate it receives with the saved one, before any password is sent.
- If the certificate is different, the technician sees a warning and decides whether to trust the new one. Legitimate reasons are a reinstalled Host or a certificate re-issued by hand. If neither took place, the change may mean that the Host has been replaced or the connection intercepted.

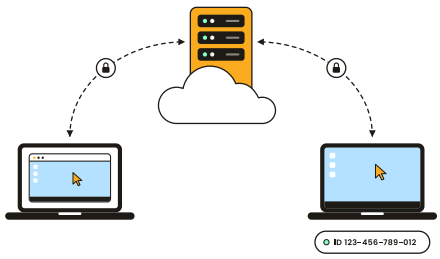
The Viewers for macOS and Linux and the mobile Viewer work the same way.

THE FIRST CONNECTION

The very first time there is nothing to compare with, and the certificate is accepted on trust. Where full assurance is required, compare the certificate fingerprint by hand: the Host for Windows shows it in the **Host identity** tab.

3.4 Connections through Internet-ID

The Host keeps an outgoing service connection to the Internet-ID server. The Viewer asks the server for the Host with a given ID, the server pairs the two, and from then on it simply forwards bytes in both directions. TLS and the session key are established between the Viewer and the Host through the relay, exactly as in a direct connection. This is true of our public servers and of a self-hosted RU Server alike.



SERVER SEES

- The ID
- IP addresses of both sides
- Program versions
- Volume and time of the exchange

SERVER NEVER SEES

- Passwords
- Two-factor codes
- The screen, files and clipboard
- Any other session content

Figure 3. What an Internet-ID server learns about a session that it relays.

Knowing an ID is not enough. An ID is an address, not a password: authentication on the Host is required in every case. And if someone put a different computer behind the same ID, the Viewer would notice it by the certificate (section 3.3).

3.5 Special cases

RDP mode. Remote Utilities can carry a standard Microsoft RDP session to the remote computer through its own connection. Entering the mode requires the same authentication. The RDP stream itself is protected by the encryption of the RDP protocol, which Windows provides.

Earlier versions. A current Host does not accept Viewers that use the legacy protocol from before TLS was introduced. The Viewer for Windows can still connect to Hosts of earlier versions and then works with the protection those versions provide. The Viewers for macOS and Linux and the mobile Viewer support the current scheme only. To have the protection described here on every connection, keep all Hosts up to date.

4 Authentication and Access Control on the Host

4.1 Four authentication methods

Any combination of methods can be enabled on one Host. As long as none is enabled, nobody can connect to the Host. Blank or factory-set passwords do not exist.

Table 3. Authentication methods, named as in the Host settings

Method	What the technician provides	Who verifies it	Permissions
Single password security	One password	The Host	Full access
Remote Utilities security	The username and password of a user created in the Host settings	The Host	Set for each user
Windows security	A Windows or domain account. Signing in under the current account without typing a password is possible	Windows itself. The password is not passed to the Host	Set for each Windows user or group
Custom server security	Nothing at connection time: the technician is already signed in on RU Server	RU Server confirms the user and works out the permissions (section 5.4)	Set on the Host for users and groups of the server

4.2 What is checked at every connection

1. **Source address.** Brute-force block list and IP filter (Host for Windows, section 4.5).
2. **Identity of the Host.** The connection is protected by TLS, and the Viewer checks the Host certificate.
3. **Credentials.** Verified by the Host, by Windows or by RU Server, depending on the authentication method.
4. **Permission of the remote user.** If enabled, a prompt appears on the remote computer.
5. **Two-factor code.** If enabled.
6. **Permissions.** Whenever a connection mode is opened, the Host checks that this user is allowed to use that mode.

4.3 Permissions and connection modes

With every method except the single password, permissions are granted to each user or group separately:

- **Remote Control** and **View Only**
- **File Transfer**
- **Redirect**: connecting onward to other computers through this Host
- **Remote Access Features**: terminal, registry, inventory, RDP, remote printing and other service modes
- **Communication Features**: text chat, voice and video chat
- **Power Control**
- **Remote Update** and **Remote Settings**

In addition, the **Modes** tab of the Host settings can switch off any connection mode for all users and all authentication methods at once.

All these checks are performed by the Host, not by the Viewer. A modified Viewer cannot get round a restriction.

4.4 Two-factor authentication

HOST FOR WINDOWS

- Standard time-based one-time passwords (TOTP): six digits, a new code every 30 seconds. Any authenticator app will do, for example Google Authenticator or Microsoft Authenticator.
- Two-factor authentication is set up per Host and applies to all users and to all four authentication methods.
- The code is requested after the password has been verified and, if the permission prompt is on, after the remote user has accepted the connection.
- The Host accepts the code of the current 30-second interval, so the clocks of the Host and of the phone have to be accurate.

4.5 Brute-force protection and IP filter

HOST FOR WINDOWS

Brute-force protection. The Host counts failed sign-in attempts from each IP address. After a series of failures it blocks the address. The block is lifted a short time after the last attempt, and every new attempt restarts the timer, so an attack that continues keeps its own address blocked. A successful sign-in resets the counter. Every block is recorded in the Host log.

IP filter. An allow list or a deny list of IPv4 addresses and ranges. The filter applies to direct connections. Connections that arrive through Internet-ID are not filtered by address: they are governed by the authentication methods and, on a self-hosted server, by the access restrictions of the server (section 5.5).

4.6 Ask user permission

With **Ask user permission** turned on, a prompt appears on the remote computer after the password check, and the person at that computer accepts or rejects the connection. The waiting time and the answer applied when nobody responds are configurable. With Remote Utilities security the prompt can also be turned on for individual users. The feature is available on all Host platforms.

4.7 Agent

At first start the Agent turns on single password security by itself and generates a numeric password. The password is shown in the Agent window next to the ID, and it stays the same until the user generates a new one. The remote user tells the technician the ID and the password. In all other respects authentication works as on the Host.

4.8 Protection of the Host settings

HOST FOR WINDOWS

Settings protection is a separate password that locks the settings window of the Host. Optionally it also locks the Internet-ID and callback connection settings. It prevents a local user from changing the configuration and has nothing to do with the authentication of Viewers.

5 Self-Hosted Server

5.1 Roles of the server

Remote Utilities Server (RU Server) is a program that you install in your own network. It has four roles, and only some of them need a server account.

Table 4. Roles of RU Server

Role	Who connects	Server account	Protection
Internet-ID routing	Hosts and Viewers	Not needed. Use can be limited by a PIN code or to listed users (section 5.5)	End-to-end encryption between Viewer and Host
Address book synchronization	Viewers	Required	TLS, permissions on address books
Authentication server	Viewers and Hosts	Required for the technician. The Host connects without an account	TLS, verification at every connection
License key distribution	Viewers	Required	TLS, permissions on each key

Our public Internet-ID servers perform the first role only.

5.2 Signing in on the server

- An account is the login and password of a user created in the Admin Console (**File › Address book manager**). The same account serves address books, license keys and authentication on Hosts.
- The connection is protected by TLS 1.2 or 1.3. The server has its own self-signed certificate, created automatically. Viewer and Host remember it at the first connection and show a warning with the certificate fingerprint if it changes. A Host that runs unattended simply refuses to connect to the server in that case.
- The password travels only inside TLS. User passwords are not kept on the server in clear text.

5.3 Permissions on the server

The server has users and groups. Every object (an address book, a folder, a single connection, a license key, the use of Internet-ID routing) has its own list of permissions. The rules are simple:

- ✓ What is not explicitly allowed is denied.
- ✓ A denial outweighs a permission.
- ✓ A disabled account gets no access anywhere.
- ✓ A user sees only the address books, folders and connections that they have permission to read. Permission to modify is granted separately.

5.4 Custom server security

The idea of this method is that the Host neither stores the passwords of technicians nor verifies them itself. It asks the server whether the person connecting really is the user they claim to be, and what that user is allowed to do.

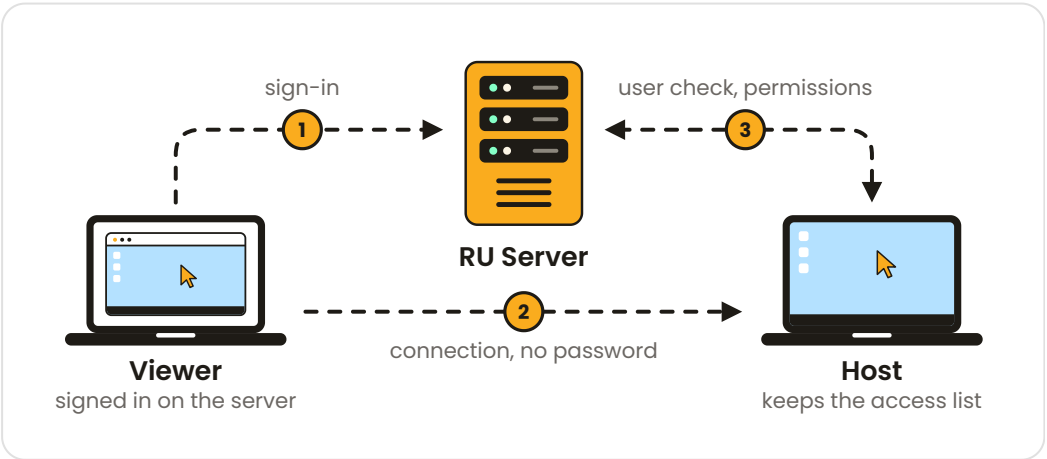


Figure 4. Custom server security. All of these exchanges travel over connections protected by TLS.

1. The technician signs in on the server in the Viewer beforehand, with login and password (section 5.2).
2. The technician connects to a Host. No password is sent to the Host.
3. The Host asks the server to confirm that the Viewer is signed in as this user, and receives the permissions of the user. If the user has none for this Host, access is denied.

What follows from this design:

- ✓ The server password never reaches the Host.
- ✓ Management is central. The list of who may do what is kept on the Host in terms of server users and groups, while the membership of the groups is kept on the server. Remove a person from a group or disable their account on the server, and they lose access to all Hosts at once.
- ✓ The server has to be reachable by both the Viewer and the Host at the moment of connection. The check is made anew every time; there are no long-lived tokens.
- ✓ If **Force custom server security** is turned on for a user on the server, the Viewer of that user authenticates on Hosts by this method only.

5.5 Who may use the Internet-ID routing of the server

By default, the routing of a self-hosted server can be used by any Host and Viewer that knows its address. Two settings of the server restrict this:

- **PIN code**. Hosts connect to the server only if the same PIN is entered in their settings. With **Require PIN on Viewer**, Viewers need the PIN as well.
- **Enable permission-based Internet-ID access**. Only Viewers that are signed in on the server as a user with this permission can connect through the server.

These settings protect the server itself from outsiders. Access to any particular Host is guarded by the authentication of that Host in every case.

5.6 License keys and the Admin Console

- The server gives out license keys only to users who are signed in, and only the keys they have permission for. A key can be forced on Viewers, and storing it on the Viewer side can be forbidden.
- The Admin Console connects to the server service locally, on the same computer. Remote connection of the Console is off by default and requires a separate password.

6 Protection of Stored Data

Table 5. What is stored on each device and how it is protected

Stored data	Protection
Access passwords on the Host	Stored only as hashes. On Windows the settings are kept in a registry key that only administrators and the operating system can access. On macOS and Linux they are kept in a settings file in a system directory.
Passwords of RU Server users	Stored only as hashes.
Connection passwords saved in the address book of the Viewer	Stored in an obfuscated form. This guards against a casual glance, not against a person who has obtained the address book file. The real protection is address book encryption or, on a phone, the app lock.
Address book encryption in the Viewer for Windows	The whole address book file is encrypted with AES-256, with a key derived from the passphrase of the user. Without the passphrase the book cannot be opened, and a forgotten passphrase cannot be recovered.
Address books on RU Server	Access is controlled by the permissions of the server and by the operating system of the server computer. The local copies on the Viewers can be encrypted as described above.
Mobile Viewer	App lock with a PIN or biometrics. Repeated wrong attempts are followed by pauses that grow longer each time. The lock data is kept in the Keychain on iOS and under an Android Keystore key on Android.

7 Software Integrity

PROGRAMS FOR WINDOWS

- ✓ All programs are digitally signed. At start-up the Host and the Viewer verify the signatures of their own modules.
- ✓ The Host does not start if its program folder contains executable files or libraries that do not belong to it.
- ✓ Packages for remote update of the Host, for update of the Viewer and for conversion of an Agent into a Host are checked for a valid digital signature before they are run.
- ✓ The online MSI Configurator signs the installation packages that it builds.

8 Logging and Audit Trail

- **Host.** Successful and failed sign-ins with the IP address and the username, blocked addresses, refused connection modes. On Windows the log is written to a file, which is on by default, and optionally to the Windows event log. On macOS and Linux it is written to a file.
- **RU Server.** User sign-ins with the IP address.
- **Viewer.** A log of connections. In the Viewer for Windows it has to be turned on.

9 Platform Availability

Table 6. Security features of the Host

Host feature	Windows	macOS, Linux
Encryption of the channel (TLS and AES-256), Host certificate	✓	✓
Single password security	✓	✓
Remote Utilities security (username and password)	✓	✓
Custom server security	✓	✓
Permissions per user, switching modes off for everyone	✓	✓
Ask user permission	✓	✓
Windows security	✓	–
Two-factor authentication	✓	–
Brute-force protection	✓	–
IP filter	✓	–
Password protection of the settings	✓	–

All Viewers check the Host certificate and can sign in on RU Server to synchronize address books. Encryption of address books with a passphrase is a feature of the Viewer for Windows. The app lock with a PIN or biometrics is a feature of the mobile Viewer.

10 Recommended Configuration

The protections described above are built in. How strong a particular deployment is also depends on choices that are yours. This checklist sums up the settings we recommend.

ON EVERY HOST

- ✓ Prefer the methods with individual users (Remote Utilities security, Windows security, Custom server security) to one shared password, and give each user only the permissions they need.
- ✓ Use long, unique passwords.
- ✓ Turn on two-factor authentication on Hosts for Windows.
- ✓ Switch off the connection modes you do not use in the **Modes** tab.
- ✓ For direct connections, limit the source addresses with the IP filter and your firewall. Do not expose the Host port to the Internet without need.
- ✓ Turn on **Ask user permission** where a person works at the remote computer.
- ✓ Protect the Host settings with a password.

ON THE DEVICES OF TECHNICIANS

- ✓ Encrypt address books in the Viewer for Windows, above all on laptops and with the Portable Viewer.
- ✓ Turn on the app lock in the mobile Viewer.
- ✓ On macOS and Linux, protect the user account and encrypt the disk.
- ✓ Treat an unexpected Host identity warning as a security event. Do not accept the new certificate until you know why it changed.
- ✓ For sensitive machines, compare the certificate fingerprint at the first connection.

ON A SELF-HOSTED SERVER

- ✓ Restrict the Internet-ID routing with a PIN code or with permission-based access.
- ✓ Grant access through groups, and disable the account of a person who leaves at once.
- ✓ Turn on **Force custom server security** for technicians who must authenticate through the server only.
- ✓ Keep the Admin Console local. If you allow remote connection of the Console, set a strong password and limit access with a firewall.
- ✓ Protect the server computer itself: few administrators, disk encryption, backups.

IN DAY-TO-DAY OPERATION

- ✓ Keep Viewers, Hosts and the server on current versions, so that every connection uses the current protocol.
- ✓ Leave the Host log on. On Windows, also write events to the Windows event log and collect them centrally.
- ✓ Review failed sign-ins and blocked addresses regularly.
- ✓ Remove Hosts, users and saved connections that are no longer needed.

A Where to Find the Settings

Setting	Location
Authentication methods, users and their permissions	Settings for Host › Authentication
Two-factor authentication	Settings for Host › Two-factor authentication
Permission prompt for the remote user	Settings for Host › Confirmation
Allow list and deny list of addresses	Settings for Host › IP-filter
Switching connection modes off for everyone	Settings for Host › Modes
Password on the settings window	Settings for Host › Settings protection
Host certificate, its fingerprint, re-issue	Settings for Host › Host identity
Address book encryption	Viewer for Windows › Tools › Options › Protection
Sign-in on the server	Viewer › Sign in. The list of servers: Manage › Server manager
Users, groups and permissions of the server	Admin Console › File › Address book manager
PIN code, permission-based Internet-ID access	Admin Console › server configuration › Communication

B Glossary

TLS
The standard protocol for protected connections, the same one that https uses. Versions 1.2 and 1.3 are the current ones.

AES-256
A standard symmetric cipher with a 256-bit key: the same key encrypts and decrypts the data.

Session key
An AES key that is valid for one session and is not stored anywhere.

Certificate
The identity document of a program: a public key and details of its owner. A self-signed certificate is not vouched for by a third party, which is why it is remembered at the first connection and compared afterwards.

Certificate fingerprint
A short string by which two certificates can be compared by eye.

Trust on first use
A model in which an identity is accepted at the first contact and every later contact is checked against it.

End-to-end encryption
Data is encrypted from the Viewer to the Host. Intermediaries on the way cannot decrypt it.

Hash
An irreversible imprint of a password. A hash is enough to check a password that has been entered, but the password cannot be read from it.

TOTP
A one-time code that an authenticator app computes from a shared secret and the current time.

Internet-ID
A connection type in which a server pairs a Viewer with a Host by the ID of the Host, without a public address or open inbound ports on the remote side.

Questions and Security Reports

For questions about this document or about the security of Remote Utilities, write to **support@remoteutilities.com** or open a ticket in the Support Center at **www.remoteutilities.com/support/**.

To report a suspected vulnerability, use the same address. Please name the program and its version and describe the steps that reproduce the problem, and give us the opportunity to investigate and fix it before it is made public.

DOCUMENT INFORMATION

Version	**1.0**
Published	**November 2026**
Classification	**Public**
Publisher	**Remote Utilities Pte. Ltd.**

© 2026 Remote Utilities Pte. Ltd. This document is provided for information. It describes the product versions listed on page 2; later versions may differ. Windows, macOS, iOS, Android and other product names mentioned here may be trademarks of their respective owners.