



Remote Service Platform built by ApplicGate RSP

A new approach to secure networks...



Plant Supplier

Plant



Secure

Flexible

Remote Service Platform by ApplicGate

Access controllable
by plant operator



Plant Operator

Easy to install

Easy to operate

Fast

Cheap

Reliable

Redundant
configuration

High
availability

Access from
anywhere

Remote Service Platform by ApplicGate

Remote Service Platform – Goals and Challenges

Standardisation

- Convince the plant owner to use your (standardized) remote access solution
- → easy, secure installation with full control

Automatization

- Easy configuration and rollout

Self-Service

- Delegate configuration to local admins and project managers
- Adaption of privileges by project managers

Remote Service Platform - Overview

Goals

- Remote control of plants by partners (e.g. supplier)
- Secure authentication and data transmission
- Full control by plant operator
- No additional hardware necessary

Prerequisites for remote site (plant)

- Any Windows system (Windows 10,11, Windows Server) with .NET 4.8 Framework or .NET 8 or higher or any Linux system with .NET 8 or higher
- From this system outgoing sessions (TCP,TLS) to one specific public Internet address (central RSP installation) must be allowed (can be routed via web Proxy at plant)
- Works with dynamic IP addresses, no fixed IP address needed!

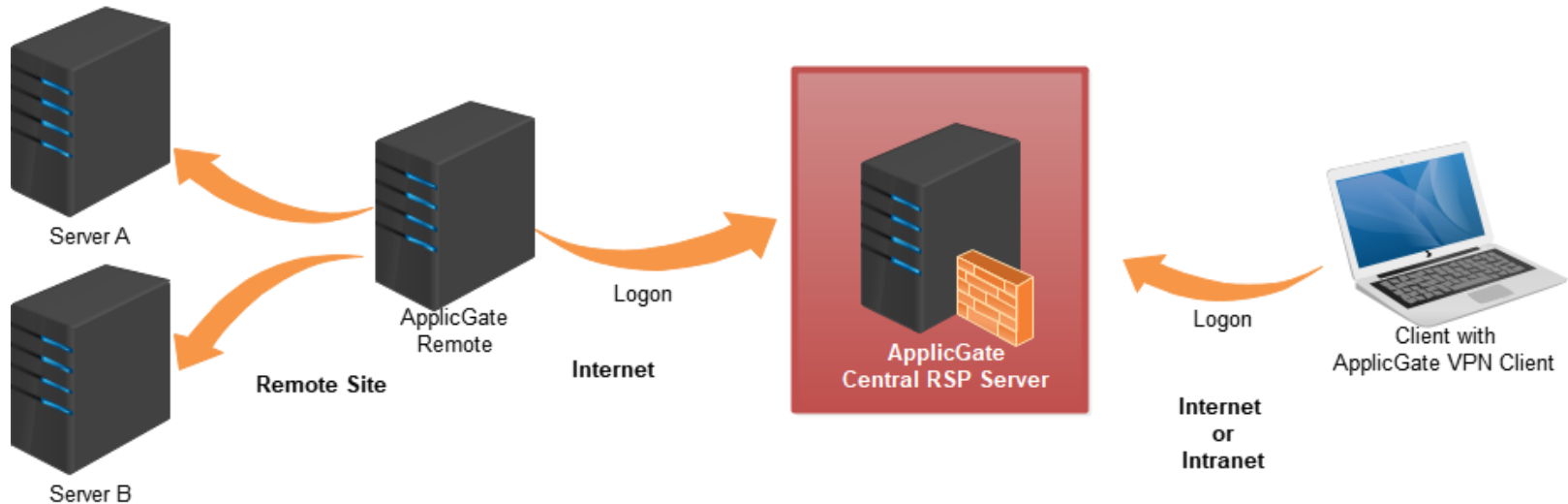
Functions

- Secure authentication via smartcards, software certificates, One-Time-Password (sent via email or SMS), TOTP, se.SAM, FIDO2 or OAuth 2.0
- Support of various TCP protocols such as RDP, CIFS, VNC ...
- Transparent routing
- Integrated logging
- Can be managed and configured by plant operator
- Optional notification by email at session setup/termination

Remote Service Platform - Access to remote Site

Remote Site:

- Only outgoing connections, web proxies are supported
- Simple firewall configuration (only one TCP port must be open)
- Logon of the remote site using certificates
- Logon can be controlled by timers and/or operators
- Operators at the remote can control and monitor access



ApplicGate VPN Client:

- It can be loaded and updated automatically via ClickOnce
- It is operated via a web browser (e.g. Microsoft Edge or integrated ApplicGate WebView)
- Logon via certificate, smartcard, OTP, TOTP (Authenticator), se.SAM, FIDO2 or OAuth 2.0

Remote Service Platform versus standard VPN solution

Topics	Remote Service Platform	Standard VPN Solution
For web sites: Works without client installation	yes	no
Separation of IP address ranges	yes	no
Menu of available connections (user dependent)	yes	no
Display of connection status	yes	no
Integrated shared shortcuts	yes	no
Central management & logging	yes	no
Automatic software update	yes	no

Steps to access remote sites

Logon to RSP

- Start the ApplicGate VPN Client to connect to the central RSP server
- Use soft certificate, smartcard, one-time password (OTP), TOTP, se.SAM, FIDO2 or OAuth 2.0 for authentication.

Get a list of available installations

- List of available connections (dependent on user credentials) and their connection status will be shown

Select Shortcut

- Shortcuts can be http(s) links, files (e.g. .RDP files, .bat files to map a network share) stored locally (generated automatically), on network shares or web sites.

Access remote site

- Click the shortcut and enter the necessary credentials to authenticate at the remote site (e.g. username/password for RDP or share mapping)

Steps to access remote sites

Start the ApplicGate VPN Client:

- First start via ClickOnce using a web browser or via local installation
- Desktop icon:



- List of remote sites:

ApplicGate_VPNclient

(v12.0.9340.35528 started 2025-08-01 10:31:09 on LEITNER5) Local deployed!

Home Configuration ▾ Status ▾ UID_Lists ▾ Logfiles ▾ Test ▾ Tools ▾ Help ▾ Stop & Restart ▾

UID List (all users) last changed Fri, 01 Aug 2025 08:31:09 GMT

UID	UIDname	Responsible	Management Location	Expiration
R100	VM2	reinhold.leitner@applicgate.com		*
S102	Leitner Puchenua	reinhold.leitner@aon.at	Puchenua	*

Number of active entries: 1
 Number of inactive entries: 0
 Number of direct links: 1

ApplicGate_VPNclient

(v12.0.9340.35528 started 2025-08-01 10:31:09 on LEITNER5) Local deployed!

Home Configuration ▾ Status ▾ UID_Lists ▾ Logfiles ▾ Test ▾ Tools ▾ Help ▾ Stop & Restart ▾

Routing Table (UID: [S102](#), UIDname: [Leitner Puchenua](#))

last loaded 2025-08-01 10:31:10, last written 2025-08-01 10:31:10

UID	Shortcut	Comment
S102.1proxy		Forward to Proxy
S102.1s	https://*/	Puchenua DIRLIST E:\
S102.45	http://*/main	AppGw LEITNER5 local
S102.6	http://*/	Fronius
S102.7	http://*/	Ohmpilot
S102.11	http://*/main	AppGw LEITNER4
S102.12	LEITNER4-Share.bat	Network Share
S102/17	Leitner4-PC.rdp	RDP
S102.19	https://*/	Synology
S102.20	share: ApplicGate Leitner4\Reinhold	Network Share
S102.20a	share: homes\Reinhold\Reinhold	Synology
S102.21	https://*/	Raspberry
S102.211	https://*/	Raspberry-REVPR-FWCC
S102.22	cmd.putty -P 2222_pi@127.10.22.14	Raspberry via SSH

- Access remote site via shortcuts

Steps to access remote sites

Full display:

ApplicGate_VPNclient

(v12.0.9340.35528 started 2025-08-01 10:31:09 on LEITNER5) Local deployed!

Home Configuration ▾ Status ▾ UID_Lists ▾ Logfiles ▾ Test ▾ Tools ▾ Help ▾ Stop & Restart ▾

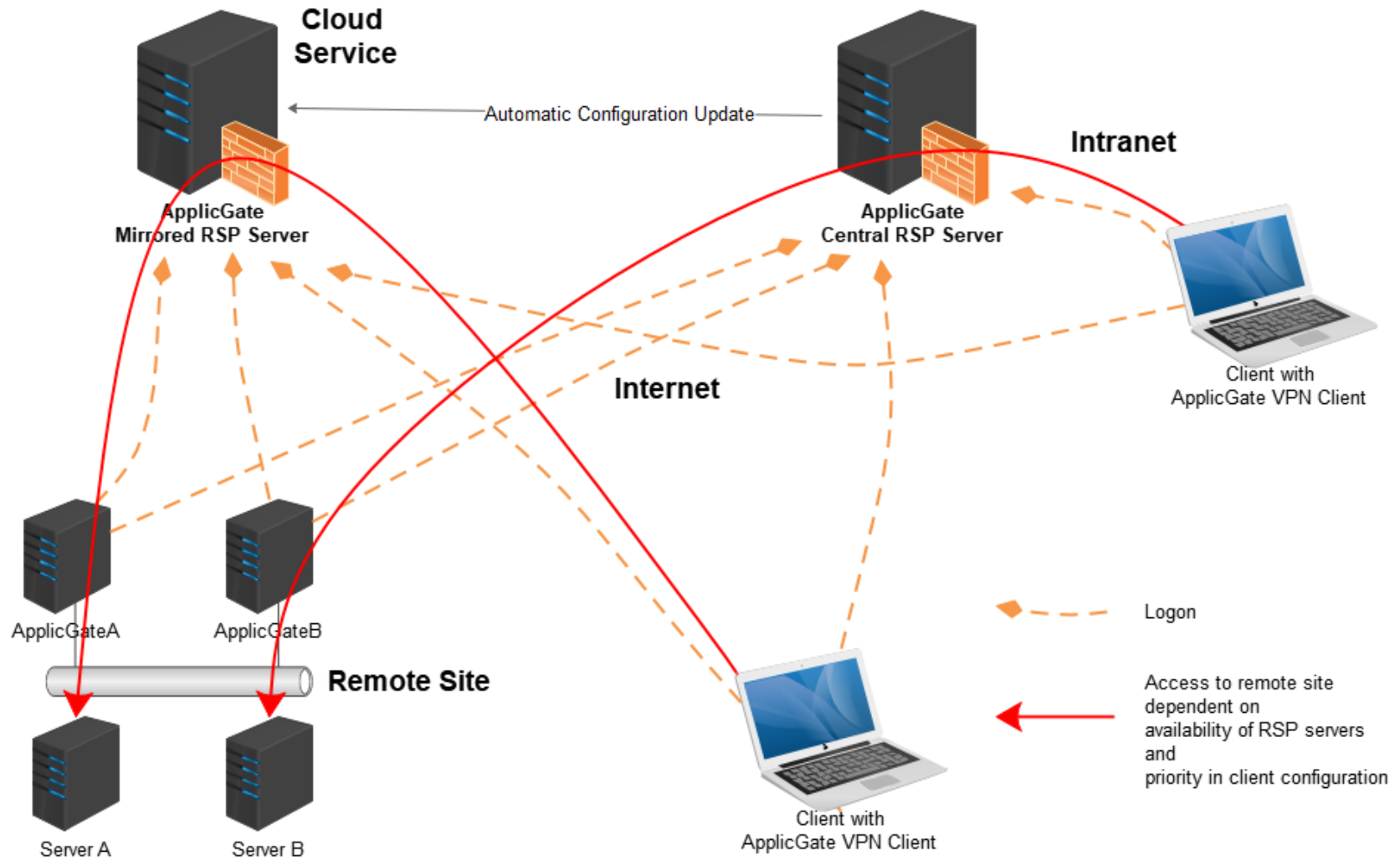
Routing Table (UID: S102, UIDname: Leitner Puchenau) last loaded 2025-08-01 10:31:10, last written 2025-08-01 10:31:10

ID	Listening	Source IP	Gateway IP	Gateway Port	Destination IP	Type	UID	Shortcut	Comment
30048	true	*	127.10.0.5	8888	AGPuchenau.rsp@applicgate.com:R4%LEITNER4	more...	S102.1proxy		Forward to Proxy
30075	true	*	127.10.22.12	877	AGPuchenau.rsp@applicgate.com:R5%LEITNER4 raspberrypi	more...	S102.1s	https://*/	Puchenau DIRLIST E:\
30076	true	*	127.10.22.12	89	AGPuchenau.rsp@applicgate.com:R4%LEITNER5	more...	S102.45	http://*/main	AppGw LEITNER5 local
30077	true	*	127.10.22.12	83	AGPuchenau.rsp@applicgate.com:R4	more...	S102.6	http://*/	Fronius
30078	true	*	127.10.22.12	84	AGPuchenau.rsp@applicgate.com:R4	more...	S102.7	http://*/	Ohmpilot
30079	true	*	127.10.22.13	90	AGPuchenau.rsp@applicgate.com:R1%LEITNER4	more...	S102.11	http://*/main	AppGw LEITNER4
30080	true	*	127.11.22.13	445	AGPuchenau.rsp@applicgate.com:R2%LEITNER4	more...	S102.12	LEITNER4-Share.bat	Network Share
30081	true	*	127.10.22.13	3390d	AGPuchenau.rsp@applicgate.com:R4%LEITNER4	more...	S102/17	Leitner4-PC.rdp	RDP
30082	true	*	127.10.22.14	4999	AGPuchenau.rsp@applicgate.com:R4%LEITNER4 raspberrypi	more...	S102.19	https://*/	Synology
30083	true	*	127.11.22.14	445	AGPuchenau.rsp@applicgate.com:R4%LEITNER4	more...	S102.20	share: ApplicGate_Leitner4\Reinhold	Network Share
30084	true	*	127.11.22.15	445	AGPuchenau.rsp@applicgate.com:R4%LEITNER4 raspberrypi	more...	S102.20a	share: homes\Reinhold NAS1\Reinhold	Synology
30085	true	*	127.10.22.14	5555	AGPuchenau.rsp@applicgate.com:R4%raspberrypi	more...	S102.21	https://*/	Raspberry
30086	true	*	127.10.22.14	5556	AGPuchenau.rsp@applicgate.com:R4%raspberrypi	more...	S102.211	https://*/	Raspberry-REVPR-FWCC
30087	true	*	127.10.22.14	2222	AGPuchenau.rsp@applicgate.com:R4%LEITNER4 raspberrypi	more...	S102.22	cmd.putty -P 2222 pi@127.10.22.14	Raspberry via SSH

Number of routing entries: 14

Remote Access to Customer Site via RSP

Redundant Configuration: Central and Remote Site



Remote Service Platform - FAQs (1)

- **How is the remote (customer) site connected to central RSP?**
ApplicGate at the remote site connects via public Internet to the official IP address of the central RSP installation, any TCP port can be used (usually port 443). Only outgoing connections (from the customers point of view)!
- **Which type of Internet access can be used at the remote site?**
Any Internet access ((A)DSL, fiber, mobile etc.) can be used.
- **Are dynamic IP addresses for Internet access at the remote site allowed?**
Yes, identification of the remote sites at the central Remote Service Platform depends on certificates etc. and not on IP addresses of the sender.
- **Can the connections from ApplicGate be routed via web proxies at the remote site?**
Yes, any number of web proxies at the remote site can be used.
- **Can I reach any computer at the remote site?**
Depending on the restrictions of the remote site you can connect to any computer that is reachable from the ApplicGate at the remote site.
- **Can the customer control access to computers at the remote site?**
Yes, the customer may enable and disable access via a web interface and all connections are logged in a log file on the customer machine at the remote site.

Remote Service Platform - FAQs (2)

- **How does the customer know when somebody connects to computers at the remote site?**

The Remote Service Platform can send mails automatically to the customer when a connection is activated and/or when this connection is terminated. All connections are logged in a file. This log file can also be accessed via the web interface of ApplicGate. The identity and e-mail address of the users are logged.

- **Does the customer have access to the configuration of the ApplicGate at the remote site?**

Yes, all configurations can be controlled via web interface or via configuration files on the computer.

- **How are customer computers accessed by authorized users?**

Users have to logon to the central Remote Service Platform using a certificate (software certificate or smartcard), TOTP, Time-based One-Time-Password (Authenticator), se.SAM, FIDO2 or OAuth 2.0. After successful authentication they can access the remote machines via predefined address/port combination. They will need the application credentials supplied by the customer to connect to a customer machine.

Remote Service Platform - FAQs (3)

- **How can the forwarding by the proxy functionality be restricted by the customer?**
Filters with allowed addresses and ports can be configured at the customer instance.
- **Are there any passwords stored within the Remote Service Platform?**
No, access to the Remote Service Platform is given based on certificates, One-Time-Password, se.SAM crypto processor, FIDO2 or OAuth 2.0.
- **Where are the passwords and login information stored that are needed to logon to customer computers and applications?**
This information is not stored in the Remote Service Platform and can be stored in any store with appropriate protection (e.g. protected network share, KeePass etc.).
- **Is the data encrypted during transmission?**
Yes, between the central Remote Service Platform and the instance at the remote site the data is transmitted via a TLS encrypted channel.

Remote Service Platform - FAQs (4)

- **What is the required bandwidth for the Internet access at the remote site?**
This depends on the requirements especially when uploading data.
Please keep in mind that very often links to the Internet are asymmetric (high download bandwidth, low upload bandwidth). Very important is that the Internet connection is stable and has a low latency.
- **Can a client access the remote (customer) site while not connected to the Intranet but connected to the Internet (e.g. business trip)?**
Yes.
- **Can customers access their own systems via Internet using the Remote Service Platform?**
Yes.
- **What about redundancy and high availability?**
ApplicGate can be configured as hot-standby or multiple central RSP installations can be operated in parallel.

Contact

Reinhold Leitner

ApplicGate Network Security e.U.

Birkenweg 5

4048 Puchenau

Austria

Mobil: +43 (663) 03118601

E-mail: reinhold.leitner@applicgate.com

www.applicgate.com

ApplicGate Network Security excludes any liability whatsoever under or in connection with any provided information, estimates and assumptions. The provided information, estimates and assumptions shall be without prejudice to any possible future offer and/or contract.

Any use of information provided by ApplicGate Network Security to the recipient shall be subject to applicable confidentiality obligations and for the own convenience of and of the sole risk of the recipient.