reinhold.leitner@applicgate.com
www.applicgate.com
2024-06-11

ApplicGate VPN Client

1 Introduction

The goal is to secure access to servers located in the Intranet or any remote sites using **strong authentication** (certificates, TOTP or OAuth 2.0).

The advantages of this solution:

- The VPN client receives a list of computers where the user is authorized for access and an indication if the target computer is online or not.
- For easy access shortcuts can be generated. Several protocols are supported.
- The VPN client can use a web proxy to connect to the Internet.
- All protocols (RDP, CIFS etc.) are tunnelled through encrypted connections.
- Access can be controlled by timers (date, hours, and weekdays).

This document shows some examples how to configure ApplicGate as a VPN client and how to configure the corresponding ApplicGate VPN server.

2 Network Schema

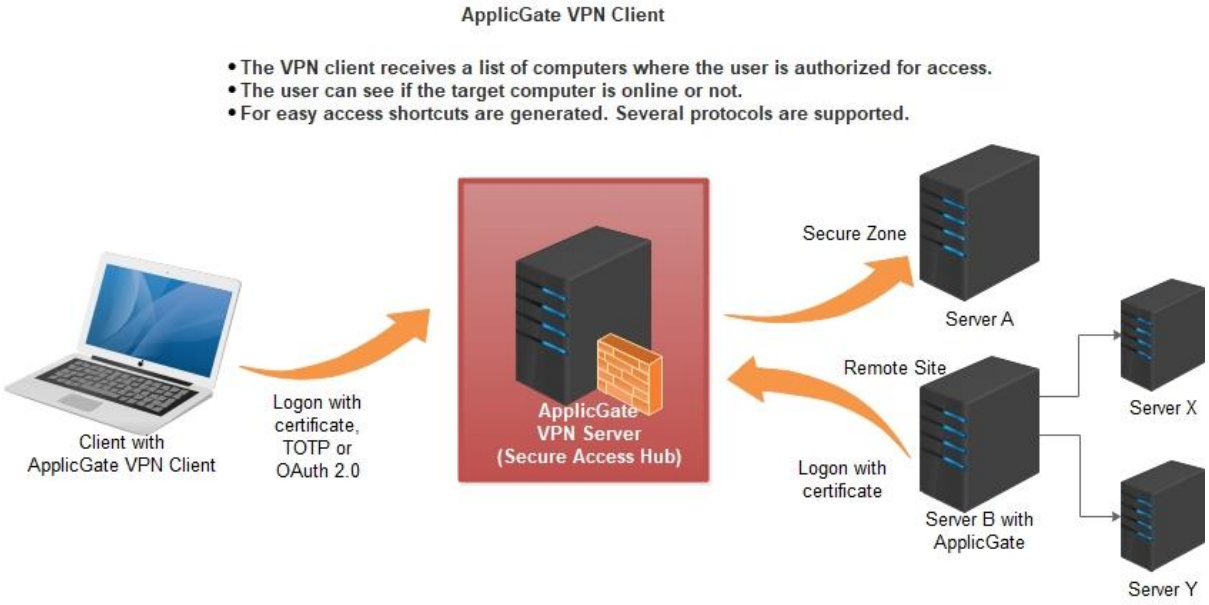


Figure 1

The ApplicGate VPN server acts as a Secure Access hub.
Only authenticated users are allowed to access Secure Access Hub.

Remark:
The “ApplicGate VPN Server” role can be installed at any server usually located in a DMZ.

2.1 Options to access the target server

There are three options how the VPN Server can access the target server:

A) The VPN Server can access the target server directly (Server A in figure 1).
B) The target server (Server B in figure 1) has to logon to the VPN Server. Now the target server accepts connections from the VPN Server.
C) The target servers (Server X and Y in figure 1) are reachable via ApplicGate configured as proxy (Server B in figure 1).

3 Configuration of ApplicGate VPN Server

There are various configuration options available.
In this document the configuration is done manually.
Additionally there is the RSP-Wizard to simplify the configuration: See
https://help.applicgate.com/helpmeRW.htm and
https://download.applicgate.com/download/ApplicGate-RSP-Wizard.pdf .

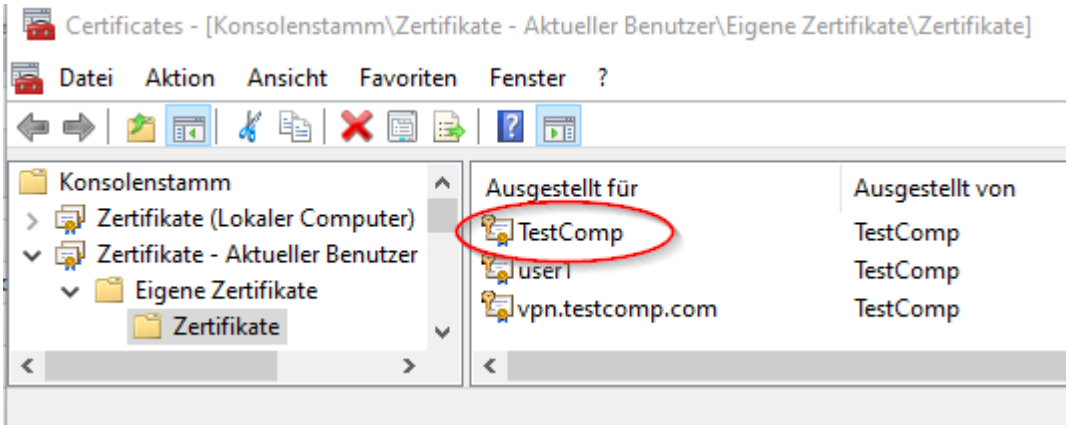
3.1 Prerequisites

- A computer with a public IP address where the ApplicGate VPN server feature can be configured:
  Any Windows or Linux (e.g. Debian or Raspbian) machine
- Windows 10 or 11 for the ApplicGate VPN client
- ApplicGate software, see www.applicgate.com
- Certificates (see also chapter “Certificates for Authentication and Encryption” below).
  As an alternative ApplicGate VPN clients can use TOTP or OAuth 2.0 for authentication.

3.2 Trusted Root

The VPN server must trust the client certificate.
If you have generated the certificates as defined below proceed as follows:

- On your Windows computer export the signing certificate (the CA certificate) using mmc certificates to TestCompCA.crt (without public key, Base64 encoded):



- At the ApplicGate VPN Server define the CA certificate as trusted:
  For Linux e.g. (depends on Linux version):
  sudo cp TestCompCA.crt /usr/local/share/ca-certificates
  sudo update-ca-certificates
  For Windows:
  use mmc with snap-in certificates and
  import the certificate TestCompCA.crt into
  “Certificates (Local Computer), Trusted Root Certification Authorities, Certificates”.

If you have other certificates, you must ensure the trust if not done already (similar procedure as above).

3.3 Configuration Files for Option A

Connections to the target computer (Server A) are forwarded directly.

We need two configuration files for the ApplicGate VPN Server: **routing.csv** and **groups.csv.**

For detailed information see https://help.applicgate.com or the local help in ApplicGate.

3.3.1 Example of Routing Table (routing.csv)

```
SourceIP;GatewayIP;GatewayPort;GatewayIP2  ;DestinationIP;DestinationPort;Expiration;Type                                                    ;UID               ;Comment           ;eMail
*       ;127.0.0.1;98         ;manage      ;             ;  ;* ;TINT:5,LGS,FLG:yes,BPRI:AboveNormal, REFRH,REFRU,LOG:1, GRPUPD,RTUPD ;MGMTloc          ;Mgmt local        ;admin@testcomp.com
*       ;*        ;99         ;manage      ;             ;  ;* ;SSL:vpn.testcomp.com.pfx/vpntest, REFRH,REFRU,LOG:1, GRPUPD,RTUPD, CCR:Mgmt ;MGMT          ;Mgmt              ;
*       ;*        ;441        ;reverselogon;R1|R3|mgmt   ;  ;* ;SSL:vpn.testcomp.com.pfx/vpntest, CCR:*rsp@testcomp.com, ISS:"CN=TestComp"  ;VPNSRV        ;VPN Server Logon  ;
*       ;*        ;442        ;reverselogon;client|mgmt  ;  ;* ;SSL:vpn.testcomp.com.pfx/vpntest, CCR:user*@testcomp.com,ISS:"CN=TestComp"  ;VPNC          ;VPN Client Logon  ;
VPNclients1 ;127.2.1.1 ;3389  ;*           ;10.0.0.20    ;  ;* ;UIDN:"VPN myComp!VPNclients1!!Vienna", LDAC:yes                        ;VPN.1r~ServerA.RDP ;RDP to Server A   ;admin@xyz.com
VPNclients1 ;127.2.1.1 ;445   ;*           ;10.0.0.20    ;* ;* ;LDAC:yes, NOLISTEN                                                      ;VPN.1f~CIFS.bat    ;Fileshare Server A;admin@xyz.com
```

View of the routing entries via ApplicGate management:

Routing Table last loaded 2024-06-10 15:58:07, last written 2024-06-10 15:57:37

ID	Listening	Source IP	Gateway IP	Gateway Port	Gateway IP2	Destination IP	Destination Port	Expiration	Type	UID	Comment	eMail
2	true	*	127.0.0.1	98	manage	*	*	*	TINT:5,LGS,FLG:yes,BPRI:AboveNormal, REFRH,REFRU,LOG:1, GRPUPD,RTUPD	MGMTloc	Mgmt local	admin@testcomp.com
3	true	*	*	99	manage	*	*	*	SSL:vpn.testcomp.com.pfx/vpntest, REFRH,REFRU,LOG:1, GRPUPD,RTUPD, CCR:Mgmt	MGMT	Mgmt	
4	true	*	*	441	reverselogon	R1|R3|mgmt	*	*	SSL:vpn.testcomp.com.pfx/vpntest, CCR:*rsp@testcomp.com, ISS:"CN=TestComp"	VPNSRV	VPN Server Logon	
5	true	*	*	442	reverselogon	client|mgmt	*	*	SSL:vpn.testcomp.com.pfx/vpntest, CCR:user*@testcomp.com,ISS:"CN=TestComp"	VPNC	VPN Client Logon	
6	true	VPNclients1	127.2.1.1	3389	*	10.0.0.20	*	*	UIDN:"VPN myComp!VPNclients1!!Vienna", LDAC:yes	VPN.1r ~ServerA.RDP	RDP to Server A	admin@xyz.com
7	true	VPNclients1	127.2.1.1	445	*	10.0.0.20	*	*	LDAC:yes, NOLISTEN	VPN.1f ~CIFS.bat	Fileshare Server A	admin@xyz.com

Detailed description:

ID 2: The first entry defines the local **manage**ment interface:
Accessible via http://127.0.0.1/98 .
In the Type field the keyword TINT defines the internal timer interval with 5 seconds, LGS enables logging of sessions (one line per session with start time, duration etc.), FLG enables logging to the general log file, BPRI sets the priority of ApplicGate, REFRH defines the refresh rate of the Home window, REFRH defines the refresh rate of the UID list, LOG defines the logging level, GRPUPD and RTUPD allow updates of group.csv and routing.csv via the web interface.

ID 3: The second entry defines the remote **manage**ment interface (optional):
Accessible via all network interfaces via https://vpn.testcomp.com:99 (the DNS name for vpn.testcomp.com must have been defined).
The Type field defines the server certificate via the keyword SSL. Authentication via client certificates is requested by keyword CCR. This keyword refers to the group Mgmt with email addresses where access is granted.

ID 4: Allows logon of servers where the email in the certificate matches *rsp@testcomp.com.
Rules R1 and R3 offered by the remote servers are accepted. This routing entry is used by “Option B” below.

ID 5: The **reverselogon** entry defines how the clients log on to the ApplicGate VPN server:
Accessible via all network interfaces via TCP port 442.
The field DestinationIP defines the supported functions: client (download rules to the client) and mgmt (optional, allows management of the client via the VPN Server).
The Type field defines the server certificate, the keyword CCR requests client certificates (all certificates with email address ending with @testcomp.com are allowed) and the certificate issuer must match as defined in the keyword ISS.

ID 6 and ID7: The last two entries define the rules that are transmitted to the client if the client has the proper authorization:
VPNclients1 is a group with a list of email addresses (e.g. usera@testcomp.com), that are allowed to access these entries.
GatewayIP is a local address (127.x.x.x), DestinationIP and DestinationPort (* means same as GatewayPort) define where to forward the connection request.
Each routing entry should have a unique identification (UID). It consists of a main part separated from a sub part by “.”.
The keyword UIDN defines a long text for all UID entries with same main part (in this case “VPN myComp”, used to generate the UID list), defines the access to this list (in this case the group VPNclients1).

The keyword LDAC:yes enables download of this entry to the clients.
Optionally via the field UID the name of a shortcut may be specified (see next chapter).
Hint: Specify the keyword NOLISTEN in the type field. Then this routing entry does not conflict with existing services on the server (e.g. Server service with port 445 for file sharing, RDP with port 3389).

3.3.2 Example of the Groups Table (groups.csv)

```
GroupName  ;IPranges                                  ;Comment   ;eMail ;Expiration
License    ;* mycomputer mycompany 0KO1b...8UjCsaNTu ;License   ;      ;*
Title      ;ApplicGate VPN Server                     ;          ;      ;*
Mgmt       ;*.mgmt@testcomp.com                       ;Management;      ;*
VPNclients1;usera@testcomp.com                        ;          ;      ;*
```

View of the groups via ApplicGate management:

Groups last loaded 2024-06-11 22:27:04, last written 2024-06-11 22:26:57

ID	Name	Group Data: IP Ranges and Addresses etc.	Comment	eMail	Expiration
2	License	* [redacted]	License		*
3	Title	ApplicGate VPN Server			*
4	Mgmt	*.mgmt@testcomp.com	Management		*
5	VPNclients1	usera@testcomp.com			*

Detailed description:

- **License** defines the license which can be obtained via **www.applicgate.com** .
- **Title** defines the title for the management interface.
- **Mgmt** is used for remote management.
- **VPNclients1** is used for access control as shown above.

3.4 Installation of ApplicGate at the VPN Server

For installation on Windows see: https://help.applicgate.com/helpmeST.htm
For installation on Linux see: https://help.applicgate.com/helpmeSX.htm

Chose the installation option **RSPvpnServer** and adapt the routing table and the groups table via web interface or use an editor as necessary.
Note: In this example there is one additional routing entry (with GatewayPort 999) and one additional group (A_RSP) for configuration of ApplicGate by the RSP-Wizard. We do not need these now.

4 Shortcuts

Shortcut files are generated by the ApplicGate VPN client locally and executed on request.

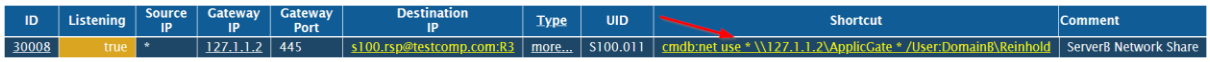
Shortcuts depending on file name and/or type:

- *.RDP … Remote Desktop
- *.VNC … UltraVNC
- *-R.VNC … RealVNC
- *.bat … map a network share via CIFS (SMB)
- *webdav.bat … map a network share via WebDAV

After initial creation these files may be changed:
Username/password and other parameters can be changed and saved to these files.
These shortcut files will not be overwritten except the local address/port is incorrect.

Shortcut commands:

- cmd: ... The command will be executed; the strings %ip% and %port% will be replaced with the actual value. Examples:
  Shortcut to start PuTTY:
  cmd:putty -P %port% %ip%
  Start RDP:
  cmd:mstsc /v:%ip%:%port%
  Example with actual values: cmd:mstsc /v:127.2.2.2:3391
- cmdb: ... The command will be inserted into a temporary .bat file and then the .bat file will be executed. The string %ip% and %port% will be replaced with the actual value.
  At the end of the .bat file the command pause will be inserted. This allows the user to see the result of the command. Example:
  Shortcut to map a network share:
  cmdb:net use * \\%ip%*share* * /User:*domain**user*
  Example with actual values:
  cmdb:net use * \\127.1.1.2\ApplicGate * /User:DomainB\Reinhold



ID	Listening	Source IP	Gateway IP	Gateway Port	Destination IP	Type	UID	Shortcut	Comment
30008	true	*	127.1.1.2	445	s100.rsp@testcomp.com:R3	more...	S100.011	cmdb:net use * \\127.1.1.2\ApplicGate * /User:DomainB\Reinhold	ServerB Network Share

- share:*sharename user* ... The command "NET USE" to map a network drive will be inserted into a temporary .bat file, then the .bat file will be executed.
  The user will be prompted to specify the password of the user.
  Up to two additional arguments for the "NET USE" command may be added.
  As default the argument "/Persistent:no" will be added, it may be overwritten.
  Example (short form of the example above):
  share:ApplicGate DomainB\Reinhold
- file: ... reference to a file
  The file will be loaded into a temporary file, the strings %ip% and %port% within the file content will be replaced by the actual value and the file will be executed.

Examples (Note: The files must have been created manually.):
file:Shortcuts\S102\23.test.bat
file:\\NAS1\Projects\S102\23.test.bat

- http:// or https:// ... links executed by the browser
  The first "*" will be replaced by GatewayIP:GatewayPort
  Example: http://*/abc

5 Configuration of the ApplicGate VPN Client

Supported for Windows, e.g. Windows 10 and 11.

Ensure that the DNS name vpn.testcomp.com can be resolved at the client (via DNS server or local hosts file).

If access to network shares via CIFS (TCP port 445) will be configured:
The Server service must be disabled at the VPN client. Don't forget to reboot after the service has been disabled.

5.1 Install user certificate

Double-click the file usera@testcomp.com.pfx to install the certificate or use any other certificate (in this case authorization must be adapted at the VPN server).

5.2 Installation of the ApplicGate VPN Client

For the following two installation options there are no client licenses necessary.

5.2.1 Local Installation

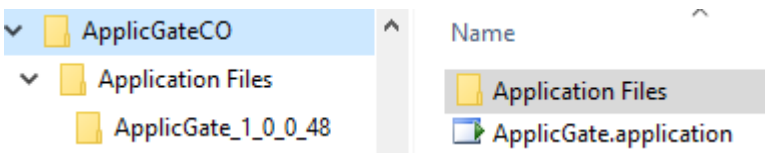
- Create a new directory and store ApplicGate.exe into this directory.
- Start the ApplicGate VPN Client via following command:
  applicgate.exe "/ClickOnce?server=vpn.testcomp.com:442&sslcc=Prompt:*@testcomp.com&title=VPNclient&cifs"
- For definition of parameters see https://help.applicgate.com/helpmeCO.htm

5.2.2 Network Installation via ClickOnce

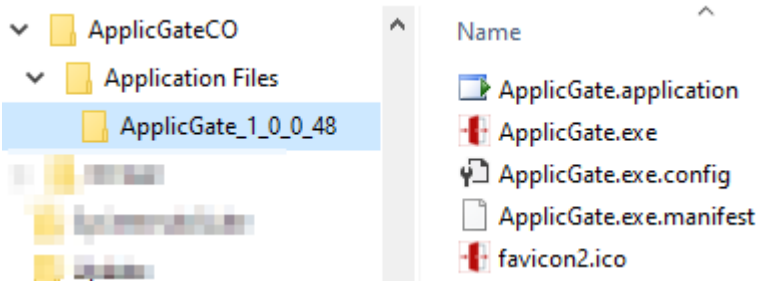
The advantage of this option is the easy installation and update of ApplicGate.
See also https://help.applicgate.com/helpmeCO.htm

ClickOnce is supported by Microsoft Edge. For other browsers add-ins are available.
When using Edge for an initial installation, ClickOnce must be enabled: Enter
edge://flags/#edge-click-once
into the address field of Edge.

Following files must be offered at a web server, e.g. https://www.mycomp.com/ApplicGateCO :



The file ApplicGate.application references to the files stored in ApplicGate_1_0_0_48 or the current version of ApplicGate.



Now installation and start at the client is done via entering following URL into e.g. the Edge browser:
https://www.mycomp.com/ApplicGateCO/ApplicGate.application?server=vpn.testcomp.com:442&sslcc=Prompt:*@testcomp.com&title=VPNclient&cifs

An entry in the start menu will be generated.

5.2.3 Start Parameters for the ApplicGate VPN Client

Required parameter:

- server=*node:port*... IP address or DNS name and port of the ApplicGate VPN server

For authentication one of these three parameters is required:

- sslcc=*sslccparameter* ... certificate selection, same parameter as for keyword SSLCC.
  If totp and oa2 are not specified: default is sslcc=Prompt:*
- totp=[email][!SecurityID] ... use TOTP and specify optional default values, same parameter as for keyword TOTP
- oa2[=provider] ... OAuth 2.0 authentication with the specified provider (optional), same as keyword OA2

Optional parameters:

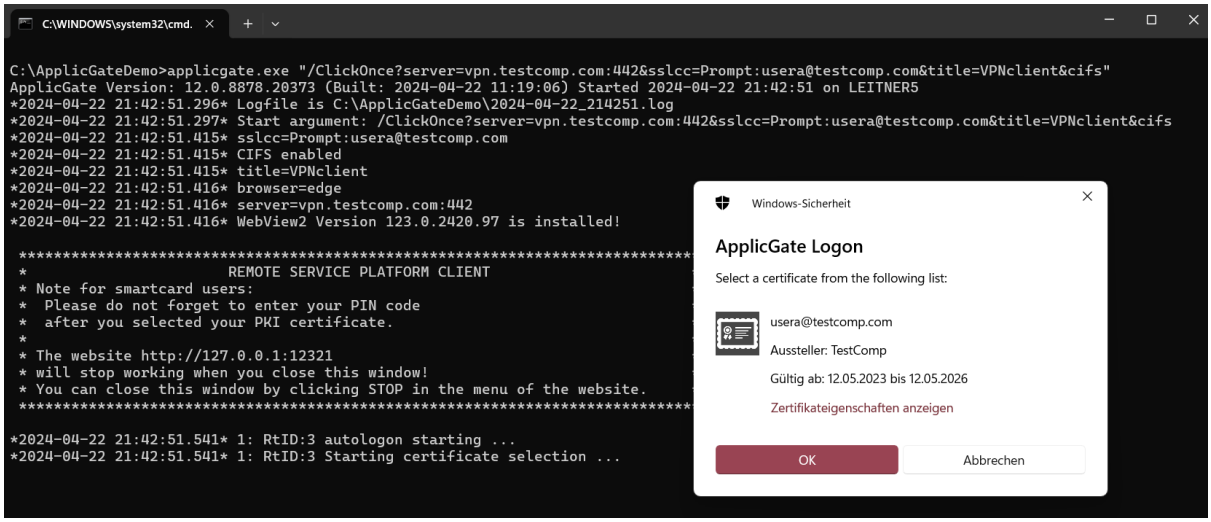
- servercheck[=issuer] ... to check the certificate of the server, same values as parameter issuer in keyword SSLTARGET
- browser=*browsername* ... start web browser: IE, Edge, Firefox or AppliGateWeb View (default is Edge)
- cifs ... same as keyword CIFS: Do not ignore rules with CIFS (IP port 445)
- defcmd=*command* ... default for sslcc is uidall (to see the uid list), default for totp is rouaum (to start the autologon session)
- log=*logvalue* ... one digit log level (0-4), if negativ: log will be shown in start window also (default is 1)
- manage=[http[s]://]ipaddress:port ... address to manage ApplicGate (default is 127.0.0.1:12321). If OAuth 2.0 authentication or https is selected, the ipaddress must be 127.0.0.1
- proxy=*node:port* ... web proxy for connection
- rulenet=*rulenet* ... same as keyword RULENET: Used to construct first part of local IP addresses.
- title=*title* ... Title to display at the management interface

The initial routing table will be constructed using these parameters. All further routing entries will be loaded from the VPN server.

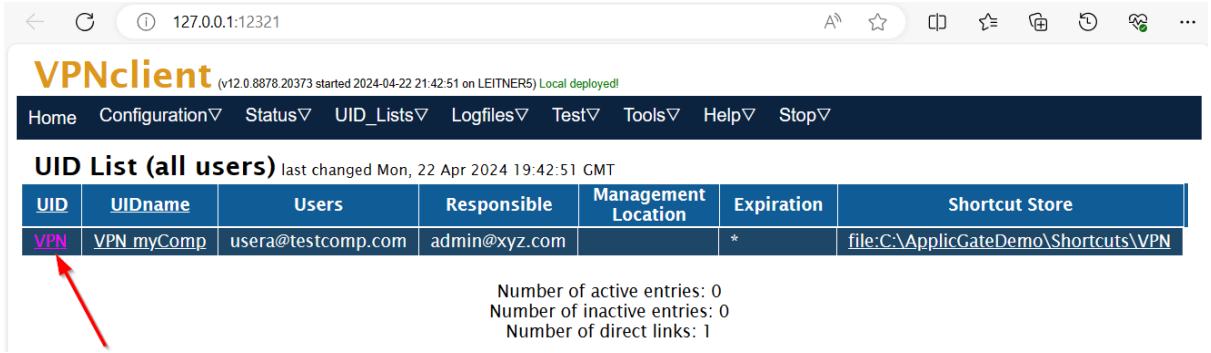
The ApplicGate VPN Client does not have a groups table and there is no license required.

5.3 The ApplicGate VPN Client

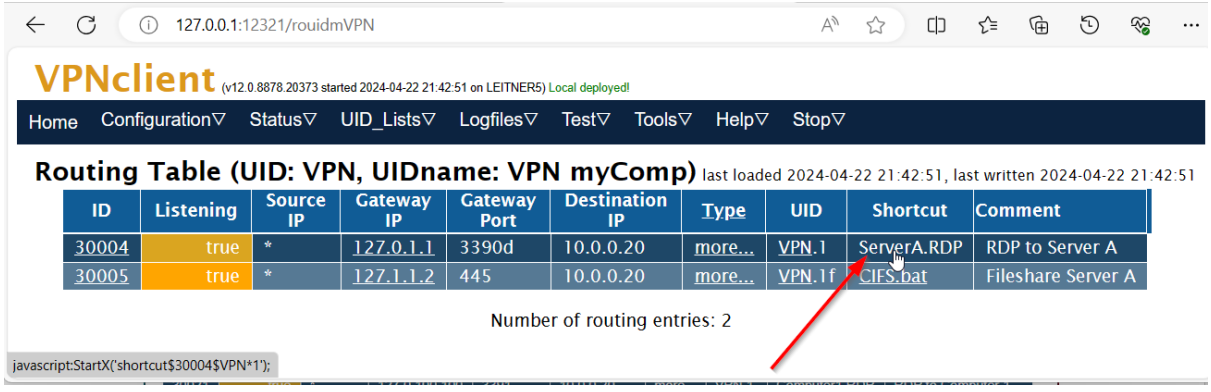
If the ApplicGate VPN client has been started a window like this will show up:



Microsoft Edge will be started, and following window will be shown:



If you click “VPN” you will see all routing entries in detail:



To access Server A via RDP: click the ServerA.RDP.
To map a network share of Server A: click CIFS.bat.

Remark: All shortcuts are generated automatically and are stored locally.

5.4 Stop the ApplicGate VPN Client

Use the Stop command in the Stop menu or terminate the command window.

5.5 ClickOnce Logging

For ClickOnce debugging turn on ClickOnce logging by definition of following registry keys:

To set a custom log file location:
1. Open Regedit.exe.
2. Navigate to the node
HKCU\Software\Classes\Software\Microsoft\Windows\CurrentVersion\Deployment
3. Set the string value LogFilePath to the full path and filename of your preferred custom log location.
This location must be in a directory to which the user has write access. For example create the following folder structure and set LogFilePath to
C:\Users\<username>\Documents\Logs\ClickOnce\installation.log.

To specify verbose log files
1. Open Regedit.exe.
2. Navigate to the node
HKCU\Software\Classes\Software\Microsoft\Windows\CurrentVersion\Deployment.
3. If necessary, create a new string value named LogVerbosityLevel.
4. Set the LogVerbosityLevel value to 1

5.6 Central Policies for VPN Client (only for installations via ClickOnce)

Following ClickOnce parameters can be defined centrally:

- browser
- oa2
- server
- slcc
- title
- servercheck

The text file **ApplicGate.policy** must exist.

This file must be in the ClickOnce download directory (where the file ApplicGate.application and the directory "Application Files" are stored).

At every start via ClickOnce the file ApplicGate.policy will be loaded, store locally and processed.
If the file could not be loaded, a local copy will be used (if there is one).

Comment lines start with # and are not processed.

Example for ApplicGate.policy:

```
# Policy for ClickOnce deployment
server=rsp.mycomp.com:442
browser=applicgatewebview
```

6 Server B logs on to ApplicGate VPN Server (Option B)

In this configuration there is no direct forwarding to the server.

Server B must log on to the ApplicGate VPN server to allow connections from the VPN client.

The VPN client can see the status of the Server B.

6.1 ApplicGate VPN Server

New routing entries have been added:

```
SourceIP   ;GatewayIP;GatewayPort;GatewayIP2  ;DestinationIP;DestinationPort ;Expiration;Type                          ;UID                    ;Comment             ;eMail
S100_Site_B;127.2.1.2;88         ;forward     ;s100.rsp@testcomp.com:R1%ServerB;*;2025-05-01;LISTEN, UIDN:"Site B!S100_Site_B!!Linz" ;S100.010~http://*/home ;ServerB(10.0.0.1) Management;
S100_Site_B;127.2.1.2;445        ;forward     ;s100.rsp@testcomp.com:R3 ;*   ;2025-05-01 ;CONNECT:10.0.0.1:445, NOLISTEN ;S100.011~011.ServerB.bat ;ServerB Network Share;manager@testcomp.com
S100_Site_B;127.2.1.2;3389       ;forward     ;s100.rsp@testcomp.com:R3 ;*   ;2025-05-01 ;CONNECT:10.0.0.1:3389          ;S100.012~012.ServerB.rdp ;ServerB RDP          ;manager@testcomp.com
```

View of the routing entries via ApplicGate management:

Routing Table last loaded 2024-06-10 17:05:04, last written 2024-06-10 17:05:04

ID	Listening	Source IP	Gateway IP	Gateway Port	Gateway IP2	Destination IP	Destination Port	Expiration	Type	UID	Comment	eMail
2	true	*	127.0.0.1	98	manage	*	*	*	TINT:5,LGS,FLG:yes,BPRI:AboveNormal, REFRH,REFRU,LOG:1, GRPUPD,RTUPD	MGMTloc	Mgmt local	admin@testcomp.com
3	true	*	*	99	manage	*	*	*	SSL:vpn.testcomp.com.pfx/vpntest, REFRH,REFRU,LOG:1, GRPUPD,RTUPD, CCR:Mgmt	MGMT	Mgmt	
4	true	*	*	441	reverselogon	R1|R3|mgmt	*	*	SSL:vpn.testcomp.com.pfx/vpntest, CCR:*rsp@testcomp.com, ISS:"CN=TestComp"	VPNSRV	VPN Server Logon	
5	true	*	*	442	reverselogon	client|mgmt	*	*	SSL:vpn.testcomp.com.pfx/vpntest, CCR:user*@testcomp.com,ISS:"CN=TestComp"	VPNC	VPN Client Logon	
6	true	VPNclients1	127.2.1.1	3389	*	10.0.0.20	*	*	UIDN:"VPN myComp!VPNclients1!!Vienna", LDAC:yes	VPN.1r ~ServerA.RDP	RDP to Server A	admin@xyz.com
7	true	VPNclients1	127.2.1.1	445	*	10.0.0.20	*	*	LDAC:yes, NOLISTEN	VPN.1f ~CIFS.bat	Fileshare Server A	admin@xyz.com
8	true	S100_Site_B	127.2.1.2	88	forward	s100.rsp@testcomp.com:R1%ServerB	*	2025-05-01	LISTEN, UIDN:"Site B!S100_Site_B!!Linz"	S100.010 ~http://*/home	ServerB(10.0.0.1) Management	manager@testcomp.com
9	true	S100_Site_B	127.2.1.2	445	forward	s100.rsp@testcomp.com:R3	*	2025-05-01	CONNECT:10.0.0.1:445, NOLISTEN	S100.011 ~011.ServerB.bat	ServerB Network Share	manager@testcomp.com
10	true	S100_Site_B	127.2.1.2	3389	forward	s100.rsp@testcomp.com:R3	*	2025-05-01	CONNECT:10.0.0.1:3389	S100.012 ~012.ServerB.rdp	ServerB RDP	manager@testcomp.com

ID 4: Allow logon of servers where the email in the certificate matches *rsp@testcomp.com. Rules R1 and R3 offered by the servers are accepted.

ID 8: Forward the connection from the client to the target computer using rule R1 (configured for remote management).

ID 9: Forward access to network share using rule R3 (with CONNECT command for the remote proxy)

ID 10: Forward access for RDP using rule R3 (with CONNECT command for the remote proxy)

6.2 Server B

6.2.1 Example of Routing Table (routing.csv)

```
SourceIP ;GatewayIP ;GatewayPort;GatewayIP2;DestinationIP;DestinationPort;Expiration;Type                                                                ;UID;Comment       ;eMail
*        ;127.0.0.1 ;98         ;manage    ;*             ;*             ;*         ;RTUPD,GRPUPD, LGS, BPRI:AboveNormal, FLG:true,TINT:10   ;MGL;Manage local  ;
autologon ;R1|R3|mgmt ;*        ;*         ;vpn.testcomp.com;441         ;*         ;UPDATE, SSLTARGET:vpn.testcomp.com!!s100.rsp@testcomp.com.pfx/s100rsp, RETRY:20s,TTL:325s ;AL ;Autologon ;
incoming ;R1        ;*         ;manage    ;*             ;*             ;*         ;                                                              ;MGR;Manage remote ;
incoming ;R3        ;*         ;*         ;*             ;*             ;*         ;PRX                                                           ;PRX;Incoming Proxy;
```

View of the routing entries via ApplicGate management on ServerB:

Routing Table last loaded 2024-06-10 16:49:29, last written 2024-06-10 16:49:22

ID	Listening	Source IP	Gateway IP	Gateway Port	Gateway IP2	Destination IP	Destination Port	Expiration	Type	UID	Comment
2	true	*	127.0.0.1	98	manage	*	*	*	RTUPD,GRPUPD, LGS, BPRI:AboveNormal, FLC:true,TINT:10	MGL	Manage local
3	true	autologon	R1|R3|mgmt	*	*	vpn.testcomp.com	441	*	UPDATE, SSLTARGET:vpn.testcomp.com!!s100.rsp@testcomp.com.pfx/s100rsp, RETRY:20s, TTL:325s	AL	Autologon
4	true	incoming	R1	*	manage	*	*	*	*	MGR	Manage remote
5	true	incoming	R3	*	*	*	*	*	PRX	PRX	Incoming Proxy

ID 2: Local Management

ID3: Via the autologon entry Server B logs on to the VPN Server and identifies itself using a certificate (email: s100.rsp@testcomp.com)

RETRY … interval in seconds to retry connections in case of error

TTL … Time To Live in seconds: Sends keepalive messages about every 30 seconds (if actual TTL is below 3 minutes)

ID 4: Remote management of ApplicGate at Server B via rule R1

ID 5: Proxy access via rule R3

Note: Rules R1 and R3 must correspond with the entries at the VPN server.

6.2.2 Example of Groups Table (groups.csv)

```
GroupName;IPranges                                ;Comment;eMail ;Expiration
License  ;* ServerB My_Company-My_Name K6IKh7….rS;License;
Title    ; Server B                               ;       ;
```

6.2.3 Installation of ApplicGate

For installation on Windows see: https://help.applicgate.com/helpmeST.htm

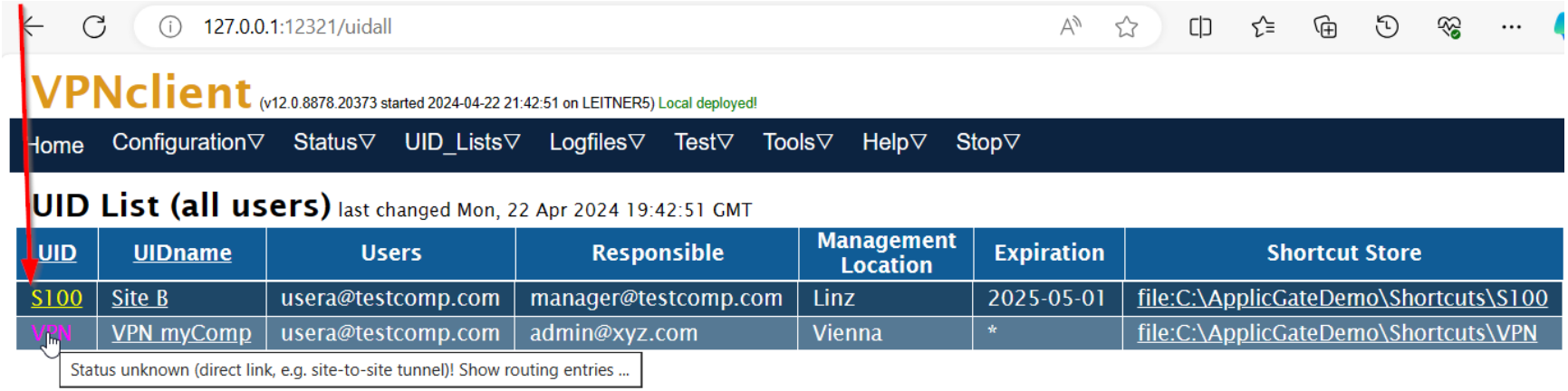
For installation on Linux see: https://help.applicgate.com/helpmeSX.htm

Chose the installation option **RSPremote** and adapt the routing table and the groups table via web interface or use an editor as necessary.

6.3 VPN Client

The advantage is now: The UID colour shows the status of the target computer:

- Magenta … Status unknown (direct link, e.g. site-to-site tunnel)!
- Yellow … All links are active!
- Orange … Some links are inactive! … only for redundant configuration when more than one server is using the same certificate
- Red … No links are active!



The colour of Destination IP and Shortcut shows the status of the target computer:

- Yellow … ready
- Red … inactive

VPNclient (v12.0.8926.34035 started 2024-06-10 19:08:01 on LEITNER5) Local deployed!

Home | Configuration▽ | Status▽ | UID_Lists▽ | Logfiles▽ | Test▽ | Tools▽ | Help▽ | Stop▽

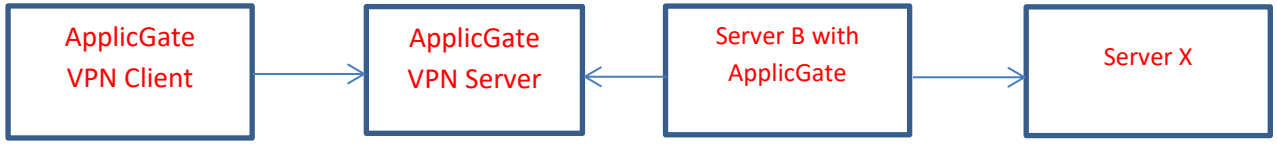
Routing Table (UID: S100, UIDname: Site B) last loaded 2024-06-10 19:08:01, last written 2024-06-10 19:08:01

ID	Listening	Source IP	Gateway IP	Gateway Port	Destination IP	Type	UID	Shortcut	Comment
30008	true	*	127.0.1.2	88	s100.rsp@testcomp.com:R1%ServerB	more...	S100.010	http://*/home	ServerB(10.0.0.1) Management
30009	true	*	127.1.1.2	445	s100.rsp@testcomp.com:R3	more...	S100.011	011.ServerB.bat	ServerB Network Share
30010	true	*	127.0.1.2	3390d	s100.rsp@testcomp.com:R3	more...	S100.012	012.ServerB.rdp	ServerB RDP

7 Connection via remote Proxy (Option C)

Server B must log on to the ApplicGate VPN server.

Server B forwards connections from the VPN client to Server X.



7.1 ApplicGate VPN Server

New routing entries have been added:

```
SourceIP    ;GatewayIP;GatewayPort;GatewayIP2  ;DestinationIP;DestinationPort ;Expiration ;Type                  ;UID                              ;Comment              ;eMail
S100_Site_B ;127.2.1.3 ;445       ;forward     ;s100.rsp@testcomp.com:R3 ;*   ;2025-05-01 ;CONNECT:10.0.0.20:445, NOLISTEN ;S100.021~021.ServerX.bat ;ServerX Network Share ;manager@testcomp.com
S100_Site_B ;127.2.1.3 ;3389      ;forward     ;s100.rsp@testcomp.com:R3 ;*   ;2025-05-01 ;CONNECT:10.0.0.20:3389 ;S100.022~022.ServerX.rdp       ;ServerX RDP          ;manager@testcomp.com
```

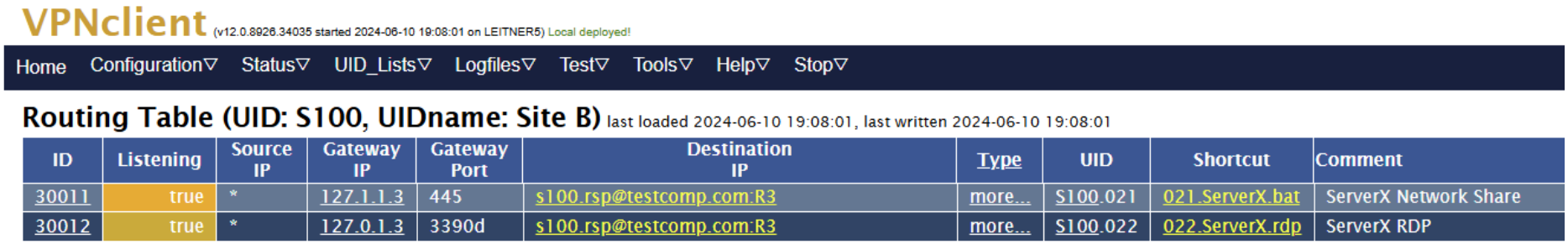
Connections are forwarded to target Server X (IP address 10.0.0.20).

View of the new routing entries via ApplicGate management:

11	true	S100_Site_B	127.2.1.3	445	forward	s100.rsp@testcomp.com:R3	*	2025-05-01	CONNECT:10.0.0.20:445, NOLISTEN	S100.021 ~021.ServerX.bat	ServerX Network Share	manager@testcomp.com
12	true	S100_Site_B	127.2.1.3	3389	forward	s100.rsp@testcomp.com:R3	*	2025-05-01	CONNECT:10.0.0.20:3389	S100.022 ~022.ServerX.rdp	ServerX RDP	manager@testcomp.com

7.2 VPN Client

View of the new routing entries at the VPN client.



8 Certificates for Authentication and Encryption

Any software certificate or smartcard is supported. Certificates can be obtained from various certificate authorities (CAs) or you can generate certificates of your own using e.g. OpenSSL or PowerShell scripts. See also https://help.applicgate.com/helpmeCE.htm .

8.1 Example to Generate Certificates using the PowerShell

- On Windows 11 Professional or Windows Server create a new directory.

8.1.1 Generate Server Certificate

- Download the PowerShell Script from https://help.applicgate.com/helpmePS.htm to this directory with name e.g. GenerateServerCertificateWithCA.ps1.
- Execute this script with PowerShell:
  The first time you will be prompted to enter the Subject and the Organization to generate a signing certificate (the CA certificate).
  Then enter the name of the server and the domain.
  To export the certificate you must enter a password.

Example:

```
PS C:\certs> Set-ExecutionPolicy Unrestricted -Scope Process
PS C:\certs> .\GenerateServerCertificateWithCA.ps1
************************************************************
*            Generate server certificate                   *
*                                                          *
* Example:                                                 *
*   Input:                                                 *
*     Servername:  www                                     *
*     Domain:      test.com                                *
*   Generates a certificate for server www.test.com        *
*                                                          *
* Hint:                                                    *
*  Servername may be                                       *
*       *  to generate a wildcard certificate             *
*       .  no servername, use domain only                  *
*                                                          *
*     If the signing certificate could not be found:       *
*       A new signing certificate will be created.         *
*                                                          *
*     ApplicGate Network Security (C) October 2023         *
************************************************************
Try to read saved hash of signing certificate from file CAsavedHash.txt ...
Saved hash of CA cannot be found or certificate not found. Generate new CA certificate?[Y/N]:Y
Generating CA certificate in certificate store CurrentUser ...
Enter Subject: TestComp
Enter Organization: Test Company

Exporting  TestComp.cer  ...
    Directory: C:\certs
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/23/2024   4:27 PM           1319 TestComp.cer
Following certificate will be used for signing:
FriendlyName              : TestComp
NotAfter                  : 4/23/2039 4:27:47 PM
NotBefore                 : 4/23/2024 4:17:48 PM
SerialNumber              : 2CF960D2BB65F2B84AD83A4CD9260BDC
Thumbprint                : 7500E4FD8874D50F8701C783723B38836112C5F9
Issuer                    : CN=TestComp, O=Test Company
```

```
Subject                 : CN=TestComp, O=Test Company

Please enter following data to generate the server certificate:
Servername (* for wildcard, . if no servername, no input for exit): vpn
Domain: testcomp.com
Generating certificate for vpn.testcomp.com in certificate store CurrentUser\My ...

Following certificate has been generated:
NotAfter                : 4/23/2027 4:29:44 PM
NotBefore               : 4/23/2024 4:19:43 PM
SerialNumber            : 5D730976C8B790BE4EE1A91049F56F53
Thumbprint              : 8437CBFAC57E37DC3C14C52E90342EE22567B0CF
Issuer                  : CN=TestComp, O=Test Company
Subject                 : CN=vpn.testcomp.com
DnsNameList             : {vpn.testcomp.com}

Export server certificate? [Y/N]: y
Enter password for .pfx file: vpntest
Exporting  vpn.testcomp.com.pfx  ...
-a----         4/23/2024   4:30 PM           2966 vpn.testcomp.com.pfx
Exporting  vpn.testcomp.com.cer  ...
-a----         4/23/2024   4:30 PM           1090 vpn.testcomp.com.cer
Enter Return to exit:
```

- Note: The file CAsavedHash.txt contains the hash of the signing certificate so that it can be used later.

8.1.2 Generate Client Certificate

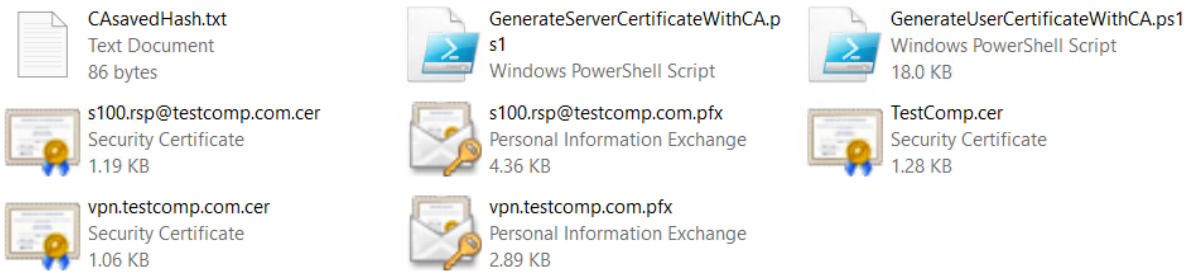
- Download the PowerShell Script from https://help.applicgate.com/helpmePC.htm to this directory with name _GenerateUserCertificateWithCA.ps1
- Execute this script with PowerShell:
  Then enter the name of the user and the organization (domain).
  To export the certificate you have to enter a password.

```
PS C:\certs> .\GenerateUserCertificateWithCA.ps1
*********************************************************
*             Generate user certificates                *
*                                                       *
*    If the signing certificate could not be found:     *
*      A new signing certificate will be created.       *
*                                                       *
*     ApplicGate Network Security (C) October 2023      *
*********************************************************
Try to read saved hash of signing certificate from file CAsavedHash.txt ...
Following certificate will be used for signing:
   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My
Thumbprint                                Subject
----------                                -------
7500E4FD8874D50F8701C783723B38836112C5F9  CN=TestComp, O=Test Company

Please enter following data to generate the user certificate:
Username: s100.rsp
Domain: testcomp.com
Generating certificate for E=s100.rsp@testcomp.com,CN=s100.rsp@testcomp.com,O=testcomp.com in
certificate store CurrentUser\My ...
TextExtension 2.5.29.17={text}Email=s100.rsp@testcomp.com&UPN=s100.rsp@testcomp.com

Following certificate has been generated:
29C7815E0839FEB0897C338892731B3213539DF1  E=s100.rsp@testcomp.com, CN=s100.rsp@testcomp.com,
O=testcomp.com
Export user certificate? [Y/N]: y
Enter password for .pfx file: s100rsp
Exporting  s100.rsp@testcomp.com.pfx  ...
```

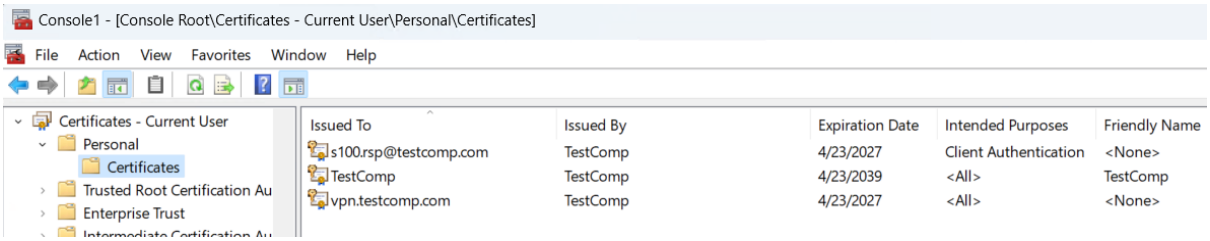
```
LastWriteTime : 4/23/2024 4:53:58 PM
Length        : 4470
Name          : s100.rsp@testcomp.com.pfx

Exporting  s100.rsp@testcomp.com.cer  ...

LastWriteTime : 4/23/2024 4:53:58 PM
Length        : 1223
Name          : s100.rsp@testcomp.com.cer

Enter Return to exit:
```

8.1.3 Generated Files

Content of directory:



Certificates in Microsoft certificate store (seen via mmc with Certificates snap-in):



9 Table of Contents