

ActiveGraf Technical Whitepaper

IT checklist for ActiveGraf Installation

This document includes advanced technical information. If you are not sure how to accomplish the below-described steps, ask for the help of computer support professional or contact your IT department!



Installation

Installation

During the installation process ActiveGraf Installer installs the necessary system components and settings required for the smooth operation of ActiveGraf.

Please use the below checklist to ensure error free installation.

IT desktop support

1. Make sure to turn off all virus protection software for the duration of the ActiveGraf installation. Virus protection software can block some actions initiated by the ActiveGraf installer resulting in a miss-configured ActiveGraf installation.

2. Verify that the user account used for the installation is having sufficient authorization (local admin) to modify the Windows host file. ActiveGraf installer inserts an entry to the windows hosts file located here: C:\Windows\System32\drivers\etc

The following entry allows ActiveGraf to communicate to the localhost-based server component (will be added by the ActiveGraf Installer):

- 127.0.0.1 activegraf.localhost

3. Verify that the user account used for the installation is having sufficient authorization (local admin) to run cmd.exe with elevated rights. The following command will be run by ActiveGraf Installer:

```
CheckNetIsolation LoopbackExempt -a -n="microsoft.win32webviewhost_cw5n1h2txyewy"
```

Some Windows editions block the communication with Localhost based servers, therefore this block needs to be released. Office Add-ins use Microsoft Edge Web View Control, so the communication between this component and the ActiveGraf Server must be allowed.

4. Verify, if Internet Options / Protected Mode is enabled for the Restricted Site Zone. This is typically enabled by default. If it is disabled, an error will occur when you try to launch ActiveGraf add-in. Steps to enable Protected Mode:

- Open Internet Explorer
- Click Tools
- Click Internet Options
- Click Security tab
- Select Internet Sites zone

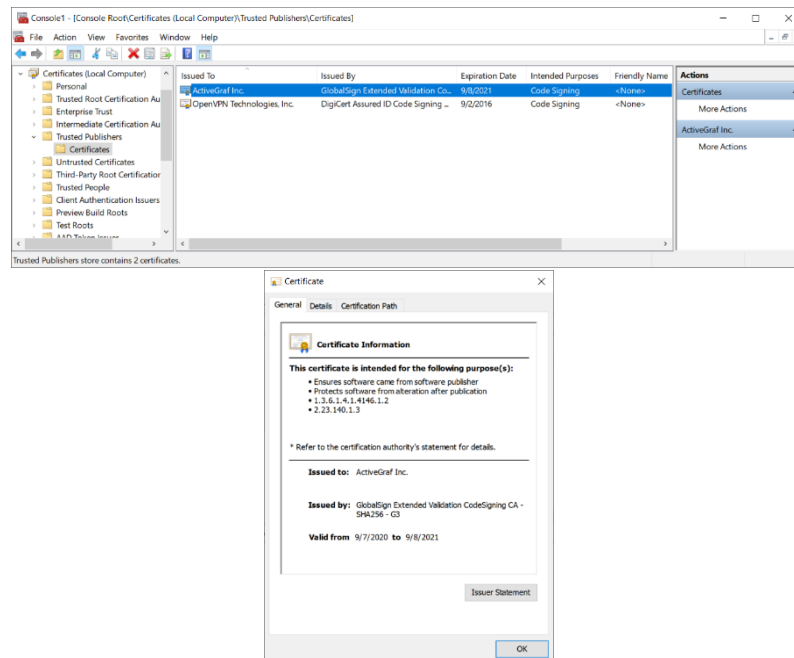


- Select Enable Protected Mode
- Click OK
- Restart Internet Explorer and all Office applications

5. Verify that the user account used for the installation is having sufficient authorization (local admin) to install and configure MS Loopback adapter. This is required to ensure smooth operation, even when there is no internet connection. All ActiveGraf client-server communication is routed via this adapter.

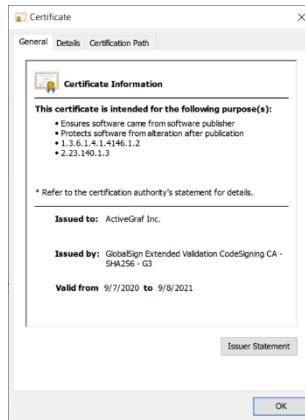
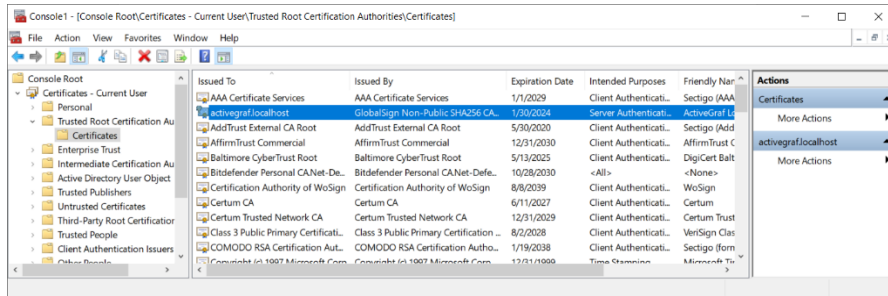
6. Verify that the user account used for the installation is having sufficient authorization (local admin) to install an Extended Validation Code Signing Certificate issued by GlobalSign. The ActiveGraf code and installer are signed with this certificate, ensuring, that the installation file is not tempered and/or no virus infected. The location of the certificate is:

7.



8. Verify that the user account used for the installation is having sufficient authorization (local admin) to install an SSL certificate issued by GlobalSign. The communication between the ActiveGraf server component and the add-in components is secured by this SSL certificate. This certificate is required for the proper operation of the system, without it the https communication between the system components will not work. The location of the certificate is:





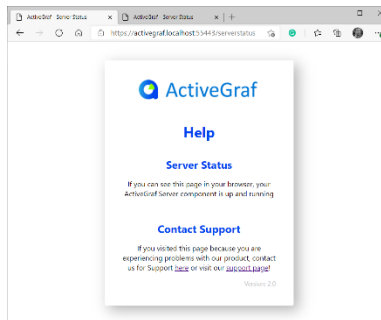
Network Support / Network Security

9. Verify that the following ports are open in the firewall configuration: ActiveGraf uses the following ports to communicate with the Localhost ActiveGraf Server Component:

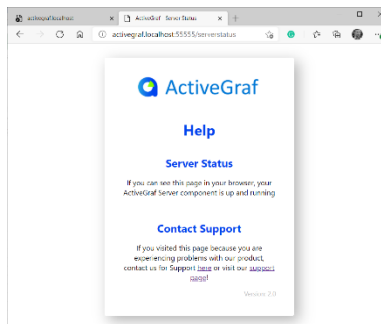
- 55443 (https)
- 55555 (http)

The above ports need to be opened towards localhost for the proper communication. For testing the connection to the localhost server, the following URLs can be used. Both should display the ActiveGraf Server Status page. If they work, the communication between the client and server-side should also work properly.

- <https://activegraf.localhost:55443/serverstatus>



- <http://activegraf.localhost:55555/serverstatus>



10. Verify that the following ports are open in the firewall towards the Cryptlex licensing engine web API:

- 54.147.158.222
- 54.147.163.93
- 54.144.124.187
- 54.144.46.201

Alternatively, you can also whitelist Cryptlex web API URL: <https://api.cryptlex.com:443>



The ActiveGraf Licensing engine uses internet connection to validity of the ActiveGraf subscription. The licensing engine must be made available in from the computer running ActiveGraf, so the validation can take pace.

11. Verify that the VPN settings (if used) allow VPN split tunneling and no restrictions in place blocking the communication towards the localhost based ActiveGraf server component.



Appendix 1 - VPN client configuration options

- Cisco VPN Client and AnyConnect Client
<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/70847-local-lan-pix-asa.html>
<https://answers.uillinois.edu/illinois/page.php?id=81643>
- FortiClient
<https://www.youtube.com/watch?v=BpexigfsD34#t=589>
- NordVPN Teams
<https://support.nordvpn.com/General-info/1596155872/Split-tunneling-What-it-is-and-how-you-can-use-it.htm>
- Perimeter 81 Enterprise VPN
<https://support.perimeter81.com/docs/split-tunneling>
- OpenVpn
<https://openvpn.net/cloud-docs/split-tunnel/>
- SOPHOS VPN
https://support.sophos.com/support/s/article/KB-000034338?language=en_US
- Pfsense VPN
<https://www.lawrencsystems.com/split-tunnel-routing-with-openvpn-and-pfsense/>

