



ZF Net Remote 3.1 Installation Instructions – External Users



For Partners / Externals

Doc.Version 3.1.00

2024-09-01



Table of contents

1.	Introduction	4
1.1.	Possible installation versions	4
1.2.	Installation files	4
1.2.1.	Software versions	4
1.3.	Hardware requirements for 64 bit operating systems	5
1.4.	Software installation (overview)	5
1.5.	Note	5
1.6.	Installation note for virtualized systems	5
1.7.	Disclaimer	6
2.	Ivanti Secure Access Client	7
2.1.	Installation Ivanti Secure Access Client and Installer Service	7
2.1.1.	Ivanti Secure Access Client with the ZF dialing profiles (classic UI mode)	9
2.1.2.	Completion of the installation	9
2.2.	Uninstalling Ivanti / Pulse Secure	10
3.	Multi Factor Authentication (MFA)	11
3.1.	MS Authenticator registration	12
4.	Installation Certificates	14
4.1.	Installation certificates	15
5.	Additional information	17
5.1.	Update from Version 3.01 to 3.1.x	17
5.1.1.	"PingID " - uninstall	17
5.1.2.	Uninstall Registry	17
6.	ZF HelpDesk (IT Hotline)	18

Introduction

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!
Printed Copies are for information only and not subject of a change service!



1. Introduction

This document describes the installation and setup of the standard parameters for ZF Net Remote (ZFNr) clients. Operation, expanded configuration, and troubleshooting are explained in the current operating instructions. Operation instruction is to find at:

<https://web-ras.zf.com/zfnr3/manuals/clients/>

1.1. Possible installation versions

The software clients are compatible with systems:

- Windows 11 64bit
- Windows 10 32/64bit

1.2. Installation files

The software is the same for all ZF domains.

You can download the respective current version of the software from the https server:

<https://web-ras.zf.com/zfnr3/software/externusers/>

Save the ZIP file in a local folder and **unpack** all files to this folder.

Comment:

These instructions and the screenshots were created using several Windows systems.

1.2.1. Software versions

64 bit operating systems

- Pulse Secure ver. 9.1r15.x (eg. 9.1r15.4-b17585)
- Ivanti Secure Access Client ver. 22.7 (eg. 22.7r2-b29103 , 22.7r3-b30227)
or newest version.



1.3. Hardware requirements for 64 bit operating systems

- Minimum 4GB RAM (with Windows 10, Windows 11)
- Minimum 1 GHz CPU
- Minimum 4 GB available hard drive space

1.4. Software installation (overview)

- **Deleting any old software versions**

Uninstall Pulse Secure / Ivanti

section 2.2

- **Installing the software**

Install Ivanti Secure Access Client via Batch- File

section 2.1

1.5. Note

Important:

The software must be installed "as administrator"!

Uninstall other VPN clients and old program versions prior to the installation.

The computer must be restarted after the installation.

1.6. Installation note for virtualized systems

Please follow these instructions if you clone your guest-system or ZF Net Remote is installed into a virtual environment.

General:

Unzip the ZFNR software package in a local folder of the virtual machine.

Cloning guest systems:

Pulse Secure :

1. On cloned images, all have the same GUID.
2. Reinstall Pulse Secure thereafter at each cloned guest.

Note: If the reinstallation was not performed, the cloned systems interrupt mutually if application ZFNR simultaneously is running.



1.7. Disclaimer

ZF Friedrichshafen AG enables the download of the WIN10 32/64 bit, Windows 11 64 bit compatible software suite from your Web server. The "ZF Net Remote" software (after referred to as ZFNR) made available here has been tested and functioned faultlessly with the specified Windows operating systems. A complete back-up of your computer is mandatory before installation of the ZFNR software. In addition, it must be ensured that other VPN software has been uninstalled – a reboot is required. ZF Friedrichshafen AG and Deutsche TELEKOM AG are not liable for malfunctions or consequences that result from the installation of this software. If problems arise in connection with the installation, ZF Friedrichshafen AG and TELEKOM are not obliged to provide reimbursement or support.

Introduction

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!
Printed Copies are for information only and not subject of a change service!



2. Ivanti Secure Access Client

VPN client for dialing into the ZFNR 3.1.x system:

Software and setup files

- 64 bit systems: Pulse Secure ver. 9.1r15.x (eg. 9.1r15.4-b17585), or Ivanti Secure Access Client ver. 22.7 (eg. 22.7r2-b29103 , 22.7r3-b30227) or newest version.
- ZFNR_3_01_EXT.pulsepreconfig
- PulseSecureInstallerService.msi
- Cert folder
- ZFNR3-VPN_External64.bat

Important!

It is crucial that you save the files from *.zip package to your local folder, **because** the batch files expect to find the software in the same directory.

2.1. Installation Ivanti Secure Access Client and Installer Service

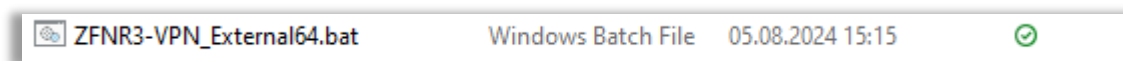
Note:

- The installation of the Ivanti / Pulse Secure and Installer Service is executed in admin context!
- Uninstall any existing software versions first (section [2.2](#)).

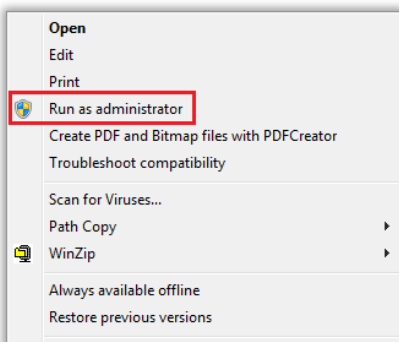
Start installation of the Ivanti and Pulse Secure Installer Service by the same .bat file:

Win11/Win10 64 bit operating systems: file "**ZFNR3-VPN_External64.bat**"

Select the batch file by clicking the right mouse button:



Click on "Run as administrator":



Ivanti Secure Access Client

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!
Printed Copies are for information only and not subject of a change service!



Script will run instalaltion process and necessary components:

```

C:\WINDOWS\system32\cmd.exe

C:\Users\serwis\Downloads\ZFN3-Suite_External_test_Ivanti\ZFN3-Suite_External>REM ENG The package was created for inst
all Pulse Secure 3.1 for External Users and Partners ZF

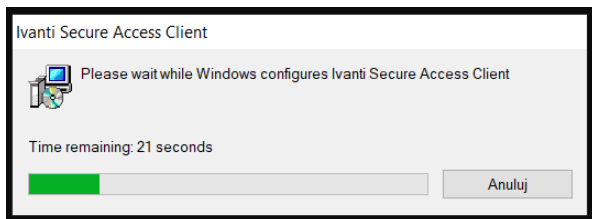
C:\Users\serwis\Downloads\ZFN3-Suite_External_test_Ivanti\ZFN3-Suite_External>REM 08 August 2024 FIII53 GK

C:\Users\serwis\Downloads\ZFN3-Suite_External_test_Ivanti\ZFN3-Suite_External>msiexec /i C:\Users\serwis\DOWNLO~1\ZFN3-
3--1\ZFN3--1\PulseSecureInstallerService.msi

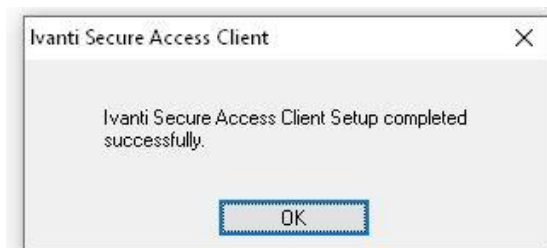
C:\Users\serwis\Downloads\ZFN3-Suite_External_test_Ivanti\ZFN3-Suite_External>REM PulseSecureInstallerService ver 9.1.
25505.0

C:\Users\serwis\Downloads\ZFN3-Suite_External_test_Ivanti\ZFN3-Suite_External>msiexec /i C:\Users\serwis\DOWNLO~1\ZFN3-
3--1\ZFN3--1\ps-pulse-win-22.7r3-b30227-64bit-installer.msi CONFIGFILE=C:\Users\serwis\DOWNLO~1\ZFN3--1\ZFN3--1\ZFN3-
3_01_EXT.pulsepreconfig BRANDINGFILE=C:\Users\serwis\DOWNLO~1\ZFN3--1\ZFN3--1\PulseWin3.1.PulseBranding /qb+
  
```

Currently instalaltion using silence module and a lot of installation screens was hidden.



Installing Pulse Secure is finished when fallowing information will appear and all background messages can be closed.



NOTE:

During the installation, the Ethernet connection is temporarily disrupted due to the installation and the incorporation of a virtual network adapter, in order to integrate the virtual network adapter!!!

Ivanti Secure Access Client

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!
Printed Copies are for information only and not subject of a change service!



2.1.1. Ivanti Secure Access Client with the ZF dialing profiles (classic UI mode)



2.1.2. Completion of the installation

**The computer must be rebooted once after completion of the installation (mandatory).
After the reboot, the installation is completed.**

After the installation, you can check all necessary components are installed.
Please open Control Panel, select Programs, next Programs and Features. All Ivanti /Pulse Secure components you can compare with the list below:

	Ivanti Secure Access Client 22.7	Ivanti, Inc.	01/10/2024		22.7.30227
	Pulse Secure Installer Service	Ivanti, Inc.	01/10/2024	8,37 MB	9.1.25505
	Pulse Application Launcher	Ivanti, Inc.	01/10/2024	25,7 MB	22.7.30227

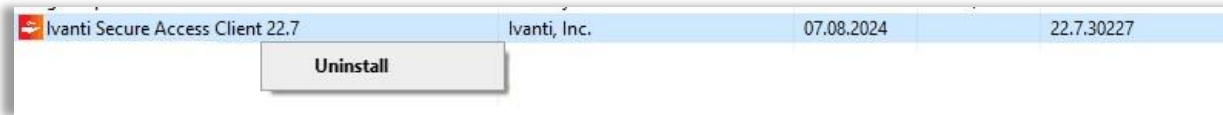
Ivanti Secure Access Client

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!
Printed Copies are for information only and not subject of a change service!



2.2. Uninstalling Ivanti / Pulse Secure

You require administrator rights to uninstall the "Pulse Secure" software. Open Control Panel and select all the Ivanti Secure Access / Pulse Secure clients separately by right-clicking the mouse button. After that, click in "Uninstall" as screen below:



Uninstall old components via system control before a software update or new installation. After uninstalling, an operating system reboot is recommended.

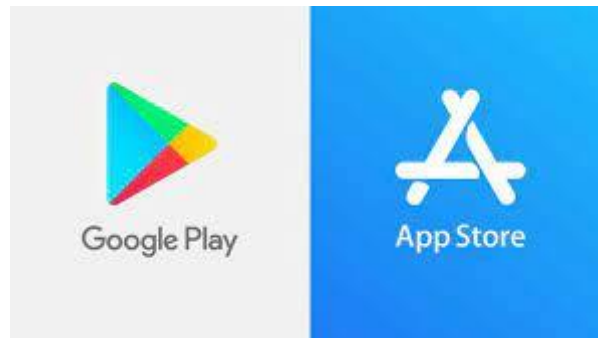


3. Multi Factor Authentication (MFA)

Multifactor Authentication (MFA) is becoming the standard at ZF. All External users should use MS Authenticator App as an authenticator for VPN connections.

Following Microsoft Authenticator (MFA) Registration Instructions for iOS and Android devices install and setup Microsoft Authenticator as your primary authentication method.

To use MFA please open Google Play Store for android device or App store for IOS device:



and install the **Microsoft Authenticator** app on your mobile device.



Important:

As login use ZF communication mail (ZF account) eg. name.surname.external@zf.com

More information about this application you can find in Microsoft support webpage:

<https://support.microsoft.com/en-us/account-billing/download-and-install-the-microsoft-authenticator-app-351498fc-850a-45da-b7b6-27e523b8702a>

Watch this training video :

<https://www.youtube.com/watch?v=k0oiKQK3LjQ>

ZF employees can find more information in corporate KBA article :

[KBA00024238 - How to register for Azure Multi-Factor Authentication](#)

Smart@work – HowTo:

English: [How to register for Azure Multi-Factor Authentication](#)

Deutsch: [Wie registriere ich mich für Azure Multi-Factor Authentication](#)

Multi Factor Authentication (MFA)

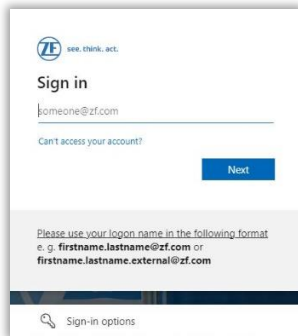
Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!

Printed Copies are for information only and not subject of a change service!



3.1. MS Authenticator registration

Open <https://aka.ms/mfasetup> in your browser

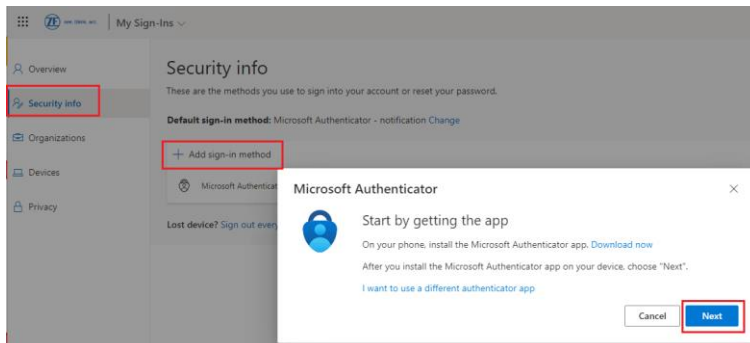


By default the MS EntraID Multi-Factor Authentication is asking you to setup Microsoft Authenticator as your primary authentication method.

Hint: If you cannot install the app on your phone / tablet please select "I want to set up a different method" and choose "Phone" from drop-down menu and "Confirm". Otherwise proceed with the setup of the Microsoft Authenticator App.

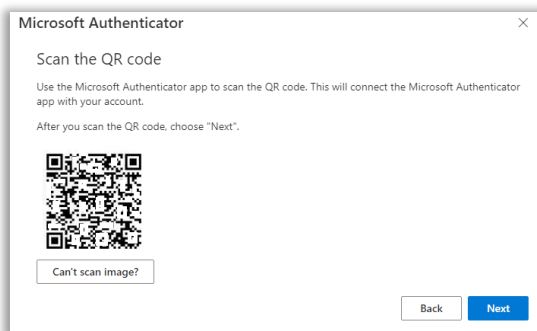
If you are not already registered, the following registration page will be shown to set up Microsoft Authenticator App.

In case you already registered with Azure MFA the Security Info Page loads, and you click on "+ Add Method" to register a new authentication method.



Then accept next screen concerning set up your account and enter "Next" button.

You will get the QR code to use in next step.



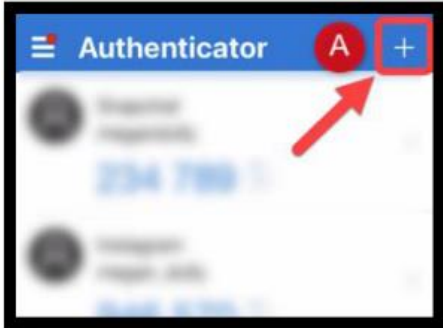
2

Multi Factor Authentication (MFA)

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!
Printed Copies are for information only and not subject of a change service!

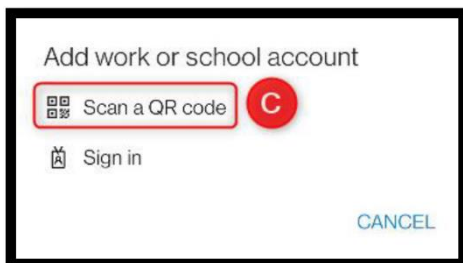
Open your AS Authenticator App add new Authenticator :

A) Tap on the “+”



B) Tap on **Work or School account**

C) Tap **Scan a QR code**



Your phone camera will activate.

D) Tap **Scan a QR code**

Point your mobile device camera (within the Microsoft Authenticator app) to your PC screen to scan the QR code.

Note:

If you are requested to enter a pin code, enter the same one used to unlock your screen.

E) A code will appear on the Authenticator app on your smartphone

F) Insert in this field the code generated by your Authenticator app.

G) Click sign In.

Multi Factor Authentication (MFA)

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!

Printed Copies are for information only and not subject of a change service!



4. Installation Certificates

For activation and SSL VPN connection establishment, the ZF Net Remote client requires the ZF certificates on the Windows client system. If certificate error messages appear, they must be reinstalled. ZF internal certificates are needed by various ZF applications.

In the Windows System you can check installed certificates by select Run from the Start menu, and then enter certmgr. msc.

Correct implementation of certificates is following:

"Trusted master certification bodies" :

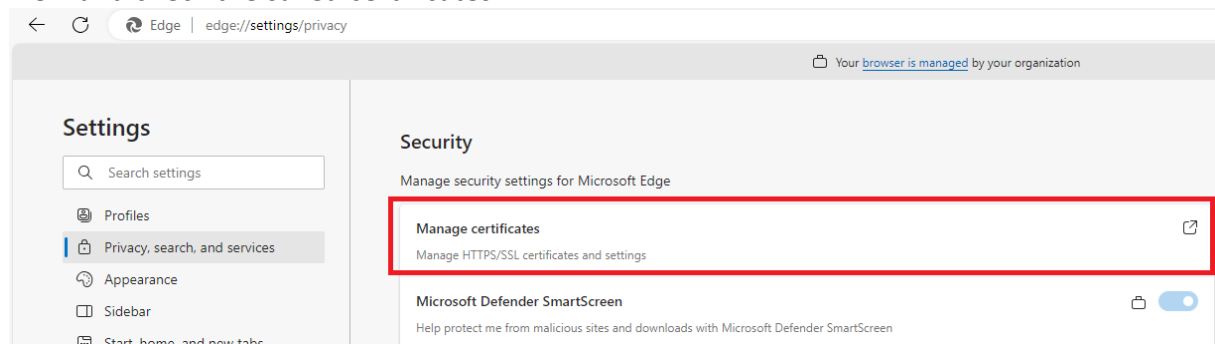
- zfglobalrootca.crt
- rootcaCert.crt
- TrustedRoot.crt
- DigiCertCA.crt
- zfrootca.cer

"Intermediate certification bodies"

- DigiCert SHA2 High Assurance Server CA
- zfintermediateca01.cer
- zfissuingca0101.cer
- zfissuingca0103.cer
- caCert.crt
- ZF SecMail CA 02.cer
- ZF Securemail CA 01.cer
- zfcloudca01.cer
- zfintermediateca02.cer
- zfissuingca0201.cer

You can find the certificates in local folder **cert** and install / reinstall them if required as follows in next point.

To check installed certificates you can use also the EDGE browser. Open browser and go to the tab [Settings]– [Privacy, search and services]– [Security]– [Manage certificates], extend view and check the saved certificates :



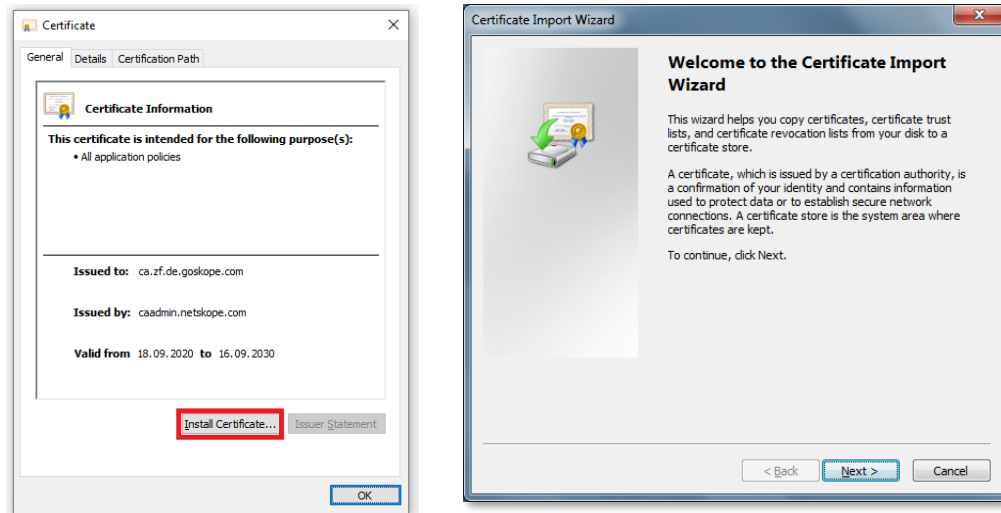
Installation Certificates

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!

Printed Copies are for information only and not subject of a change service!

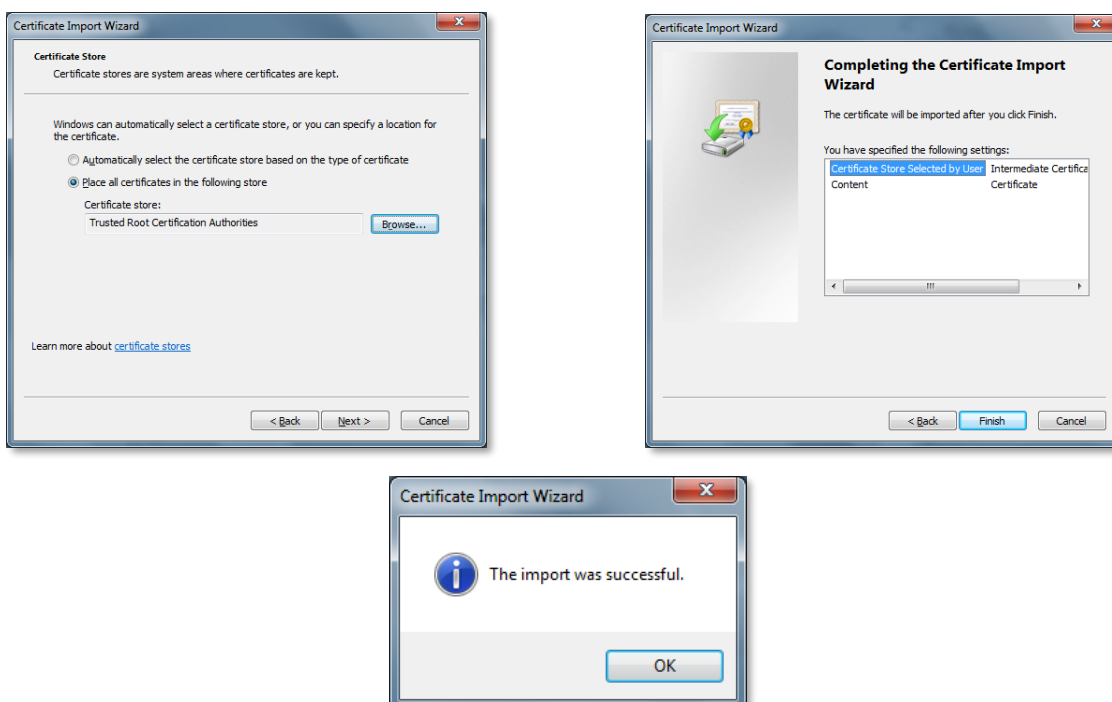
4.1. Installation certificates

The installation procedure starts after you click on the “Install certificate...” button:



Important! Save the following certificates to the certificate memory:
"Trusted Root Certification Authorities"

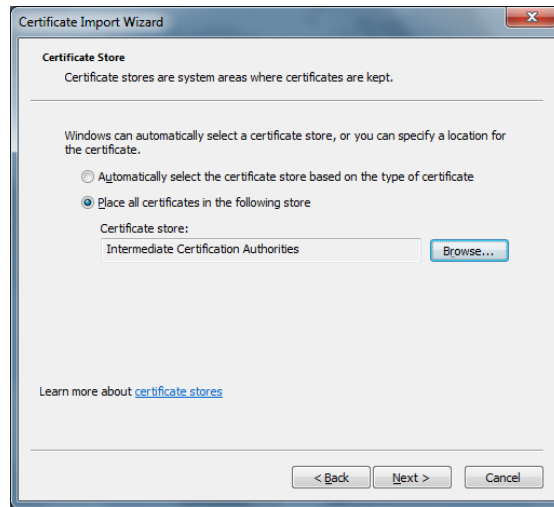
- zfglobalrootca.crt
- rootcaCert.crt
- TrustedRoot.crt
- DigiCertCA.crt
- zfrootca.cer



Installation Certificates

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!
Printed Copies are for information only and not subject of a change service!

Important ! Rest of the certificates add to the certificate memory:
"Intermediate Certification Authorities"



Installation Certificates

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!
Printed Copies are for information only and not subject of a change service!



5. Additional information

5.1. Update from Version 3.01 to 3.1.x

In a lot of cases uninstalling last version will done automatically and manually uninstallation will not necessary.

Only in case of trouble we recommend uninstalling the entire software and only then installing the new software after reboot.

5.1.1. "PingID " - uninstall

If you have installed an old solution, the "RSA SecurID" software or "PingID" app, you can uninstall this software as it will no longer be used by the ZF VPN client.

"RSA SecurID" uninstall via system control – programs and features. After uninstalling, a restart of the operating system is necessary.

You need administrator rights to uninstall the "RSA SecurID" software.

"PingID" you can remove directly from your mobile phone.

5.1.2. Uninstall Registry

!!! This Section is only required for uninstalling the registry !!!

32bit delete key: If exist the key you should delete, if not no action is required

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\RSA\Software Token]

"CtkipURL"="https://rsa1.int.gca-protect.de:7004/ctkip/services/CtkipService"

Name	Type	Data
(Default)	REG_SZ	(value not set)
CtkipURL	REG_SZ	https://rsa1.int.gca-protect.de:7004/ctkip/services/CtkipService

64bit delete key: If exist the key you should delete, if not no action is required

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\RSA\Software Token]

"CtkipURL"="https://rsa1.int.gca-protect.de:7004/ctkip/services/CtkipService"

Name	Type	Data
(Default)	REG_SZ	(value not set)
CtkipURL	REG_SZ	https://rsa1.int.gca-protect.de:7004/ctkip/services/CtkipService

Additional information

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!

Printed Copies are for information only and not subject of a change service!



6. ZF HelpDesk (IT Hotline)

To contact ZF HelpDesk call 3600 (from outside: site number + extension 3600)

The IT Global Service Desk is available in multiple language via phone.

English	24 hours a day, 7 days a week
German	Mon – Fri, 7am to 7pm CET
Spanish	Mon – Fri, 7am to 7pm CDT
GSD Chat (English only)	24 hours a day, 7 days a week

ZF HelpDesk (IT Hotline)

Ausgedruckte Exemplare dienen nur zur Information und unterliegen nicht dem Änderungsdienst!
Printed Copies are for information only and not subject of a change service!