

Add on

Contents

1	Module – Fundamental principles	3
1.1	General	3
2	OpenScape Web Collaboration	4
2.1	Introduction	4
2.2	Hardware and Software Requirements	5
2.3	Installation of the FastViewer Application Package	6
2.4	Checking the Registry (valid 04/2012)	14
2.5	Configuring the Web Collaboration Server	15
2.5.1	Preparing the Web Collaboration Server for the Native Windows Client (FastClient.exe)	18
2.5.2	Services Controlling	21
2.5.3	Checking the Installation of the Web Conference Server	24
2.5.4	Installing the Web Collaboration Web Client	25
2.5.4.1	Supported features	25
2.5.4.2	Installing the required program	25
3	OpenScape Web Collaboration - Exercise	36
3.1	Exercise	36
4	OpenStage Gate View	41
4.1	Overview of Functions	42
4.2	Installation	42
4.2.1	Prerequisites	42
4.2.2	Installation in Three Steps	43

5	Setting up a VPN configuration	44
5.1	Procedure	44
5.1.1	DSL configuration	46
5.1.1.1	Configure the WAN port of OpenScape Office	46
6	VPN Exercise - Site to Site via “PSK”	49
6.1	Site to Site networking of the OSO	49
6.1.1	Configuration - System 5	50
6.1.2	Configuration of System 6	54
6.1.3	Expert-Mode: VPN specification Tunnel - Rules	55
6.1.4	Maintenance	59
7	Teleworkers	60
7.1	Teleworker Exercise	62
7.1.1	Configuration NCP Client - Example Teleworker 5	66
7.1.2	Configuration of Windows VPN Client - Example Teleworker 6	69
8	VPN Exercise - Public Key Infrastructure (PKI) //draft//	74
8.1	Tunnel setup with digital signatures	76
8.1.1	Maintenance	82
8.1.2	Configuration of NCP Client - “Certificates” - Example Teleworker 5 //draft//	83
8.1.3	Configuration Windows VPN Client - “Certificate” - Example Teleworker 6//draft//	85

1 Module – Fundamental principles

1.1 General

This examples and exercises are optional - hence, they have no relevance for certification.

Please use the following entries as necessary for your particular location...

- "Classroom" infrastructure or...
- "Flying Classroom" infrastructure

Content overview:

- Gateview - in brief...
- VPN Scenarios
 - Based on „Pre-Shared-Key“ (PSK)
 - Based on certificates

TRAINKIT_A._Manin_24-07-12

2 OpenScape Web Collaboration

2.1 Introduction

OpenScape Web Collaboration is a web conferencing solution that, owing to its scalability, high security and reliability, enables comprehensive multi-media collaboration. A web conference is usually supplemented by a voice conference.

OpenScape Web Collaboration is based on the **FastViewer** product.

If allowed by the user, web conferences enable **mirroring the desktop**. Web conference participants all over the world can thus see the same desktop on their screens, which facilitates communication. **Documents** and the **entire desktop** can also be shared for editing. Additional features such as **Chat** and **Whiteboard** improve discussing and illustrating issues. Also **Video** functionality (webcam) is supported with FastViewer. In case of web conferences it is irrelevant where the web conference participants are situated. This ensures a high degree of flexibility and saves expenses for long journeys, accommodation etc. Since all session data is transmitted encrypted (256-bit AES encryption), sensitive data can be transmitted as well.

TRAINKIT_A._Manin_24-01-2012

2.2 Hardware and Software Requirements

For details please check the OpenScape Web Collaboration Installation Guide.

OpenScape Office supports the „Embedded“ variant. This edition supports only a restricted number of features - e.g. Audio is not supported by the Web Collaboration Server and must be carried out by the OpenScape Office system.

In particular the following should be considered for the „Embedded“ variant:



*The **CLA and CLM** must be installed and Web Collaboration Embedded license must be active! (April 2012)*



Use the myPortal Conference Module to establish a web collaboration.

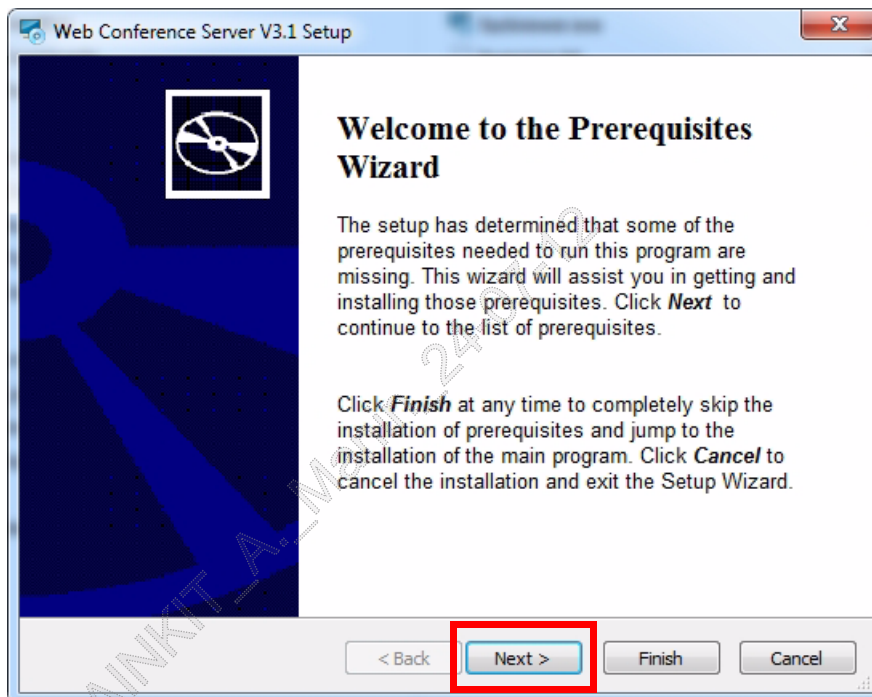
TRAINKIT_A._Manin_24-07-12

2.3 Installation of the FastViewer Application Package

Execute the following setup steps for the installation of the FastViewer Server:

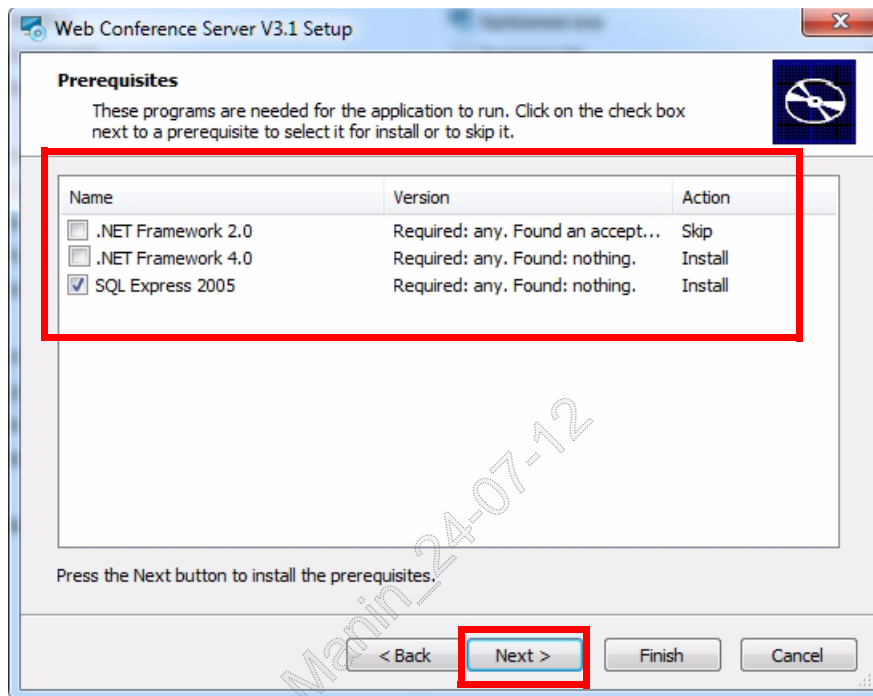
Setup preparations

1. Extract the **FastViewer-<version>.zip** file on the Web Collaboration server computer. You find this file on the OpenScape UC Application DVD1 or Patch in the folder **contrib**.
2. Execute the **setup.exe** file.

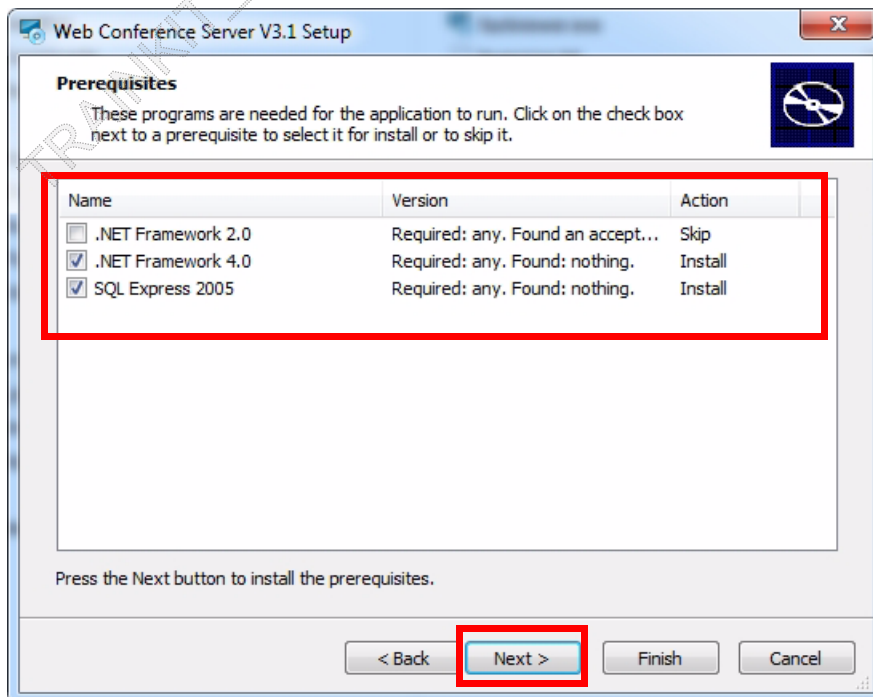


3. FastViewer needs a **SQL Database** and **.Net Framework 4.0** (needs **.Net Framework 2.0**). The components will be installed during the FastViewer installation process, if they are not found on the Web Collaboration Server.

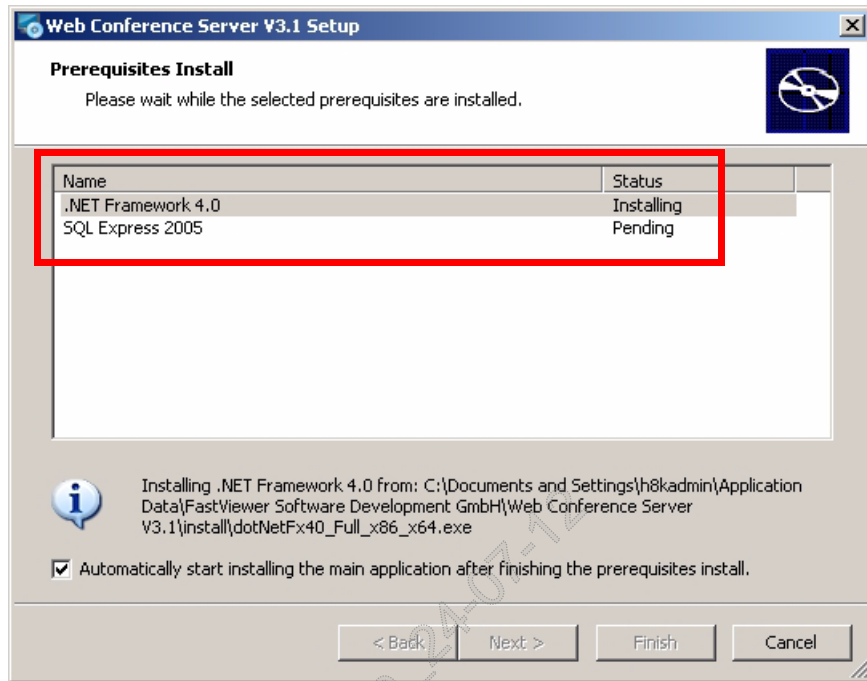
a) **.Net Framework** already installed:



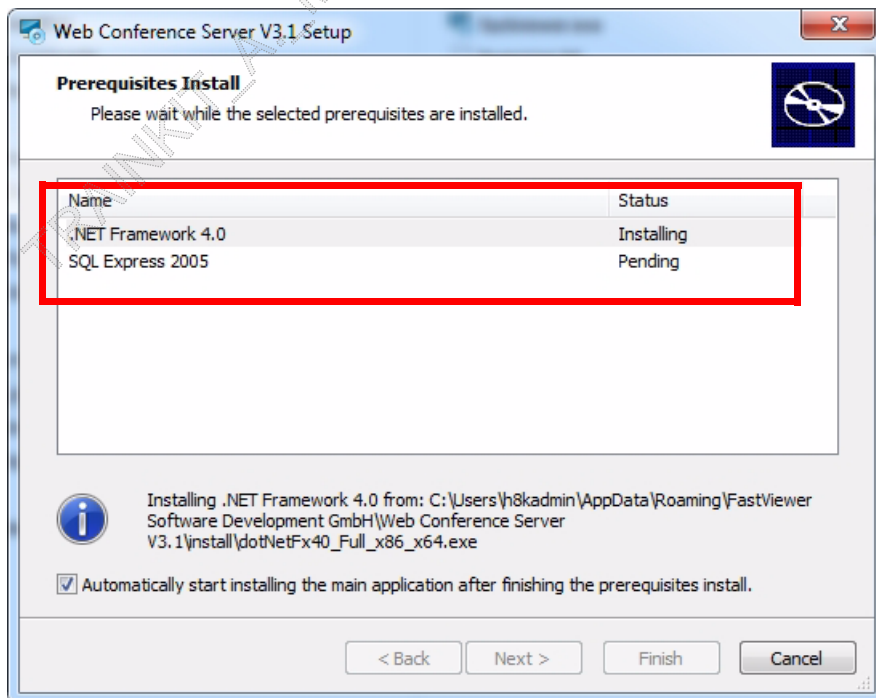
b) **.Net Framework 4.0** and **SQL Database** not installed:



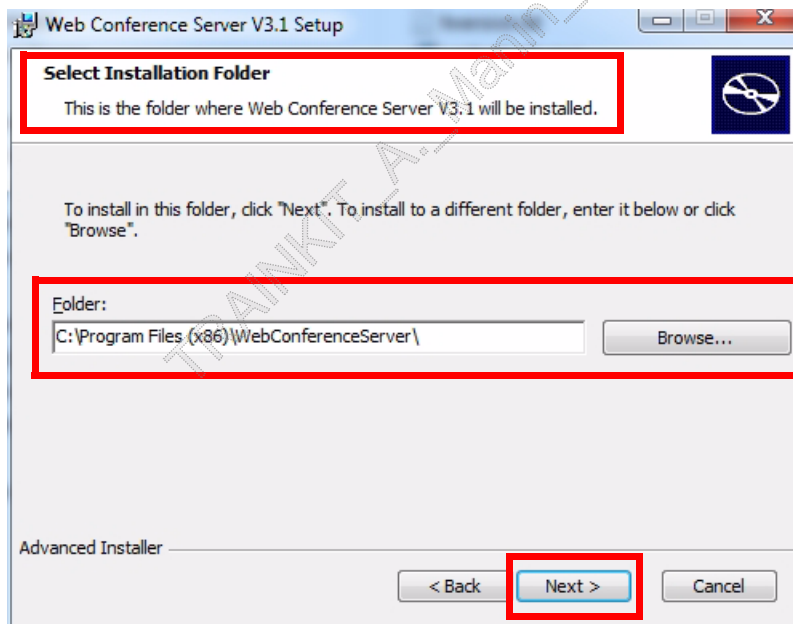
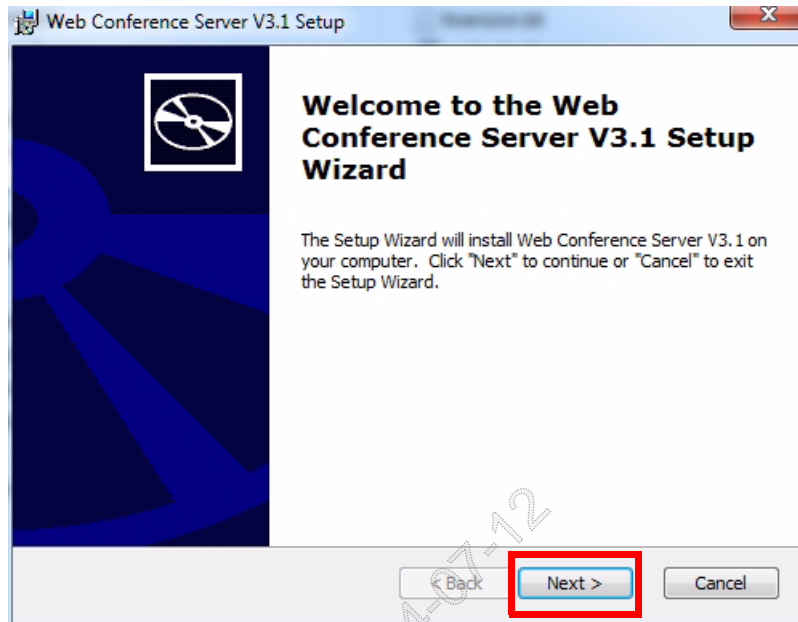
4. The installation steps for **.Net Framework 2.0** and **4.0** will be skipped, if they are already installed.



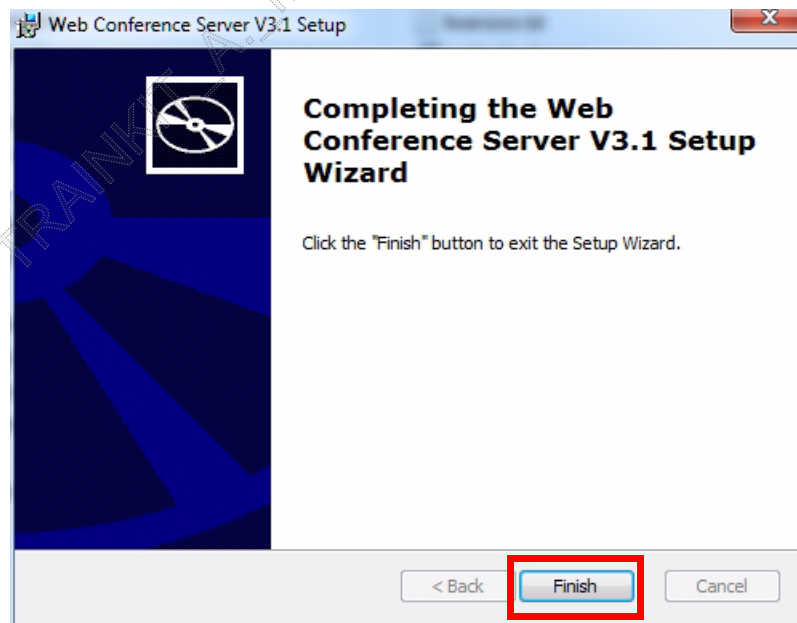
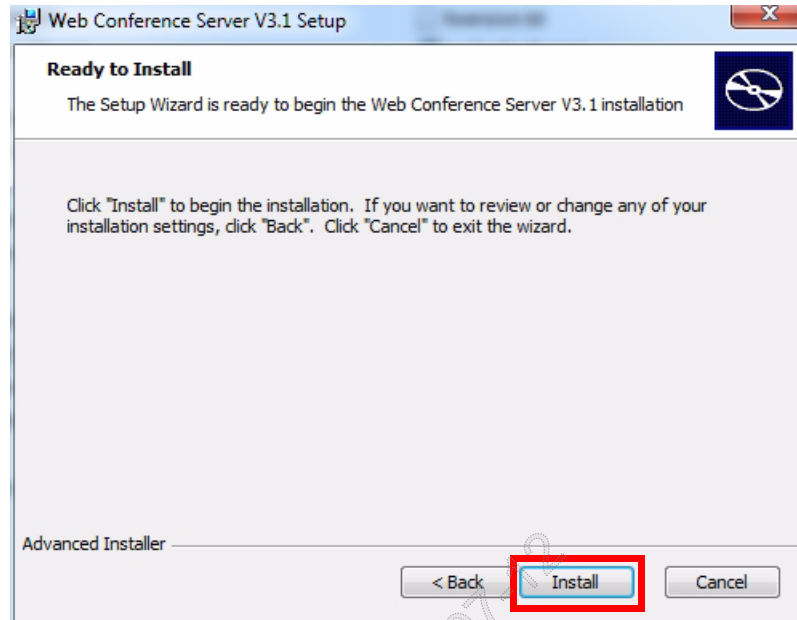
5. The installation of the **SQL Database** is started automatically, if not already installed.



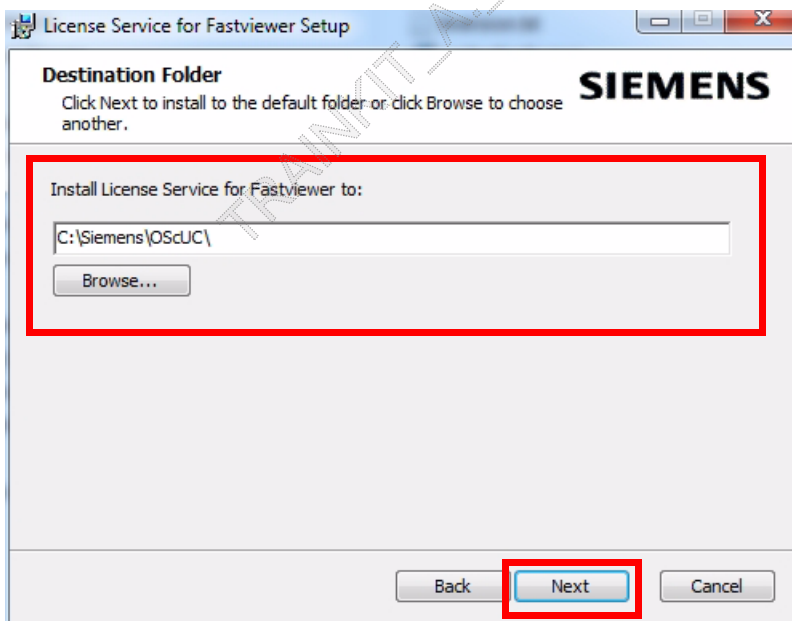
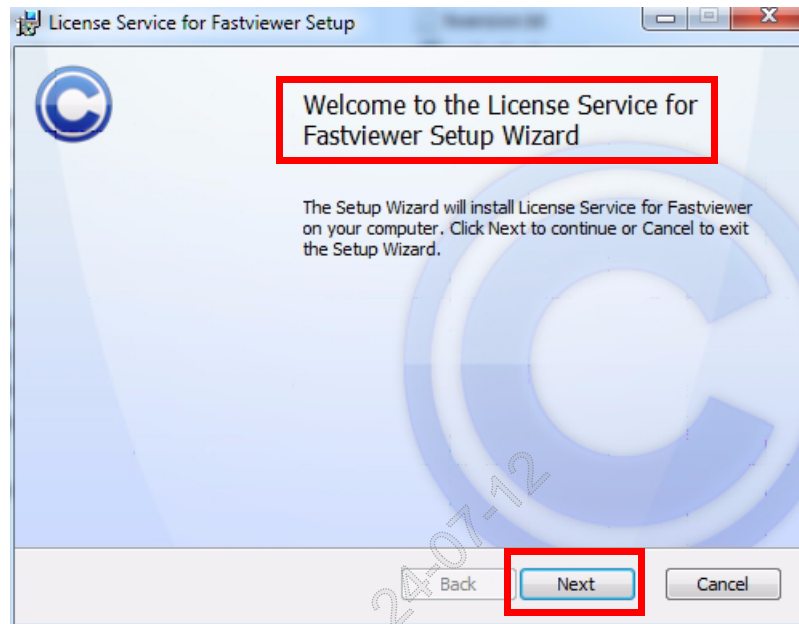
6. After the **SQL Database** installation has finished, the '**Conference Server Setup Wizard**' is started.



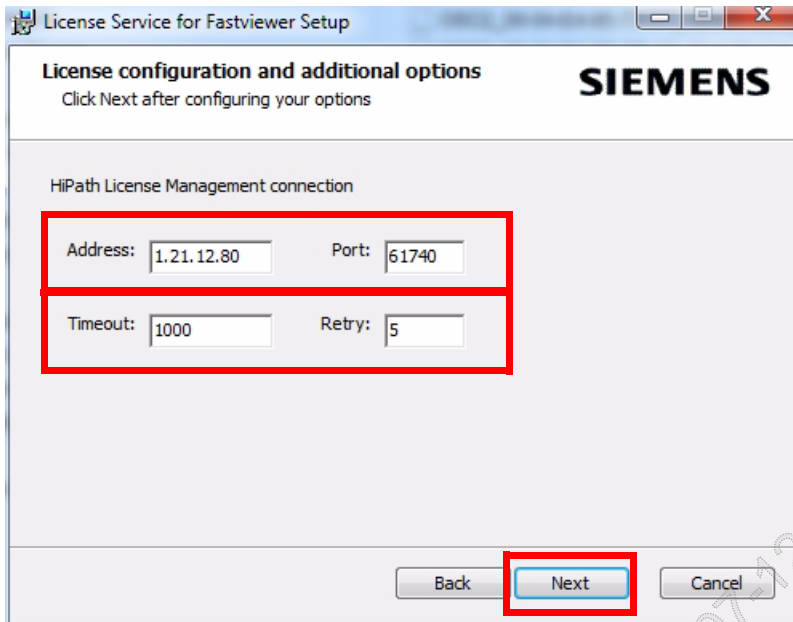
Accept or select the '**Installation Folder**'.



7. After the **Conference Server** installation has finished, the '**License Service for Fastviewer Setup Wizard**' is started. The CLA must be installed and the Web Collaboration Embedded license must be active!

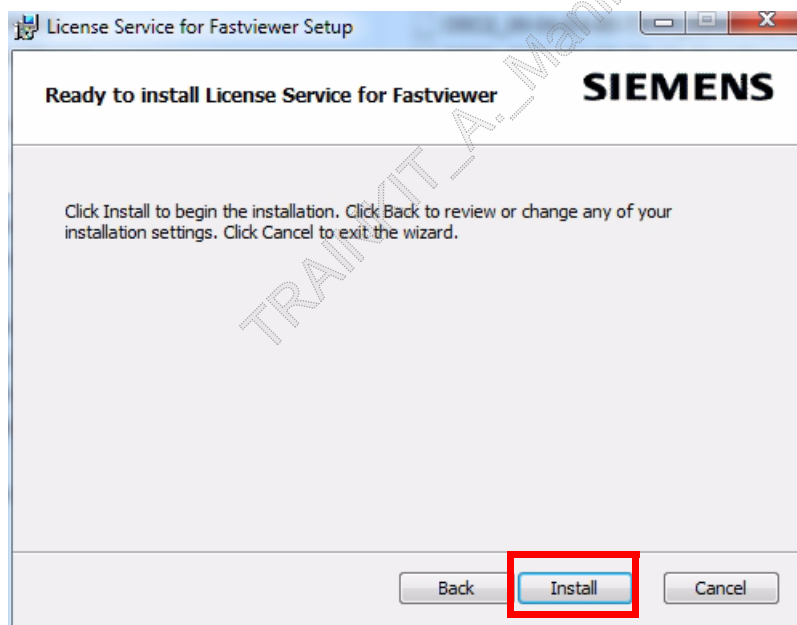


Accept or select the
'**Installation Folder**'.



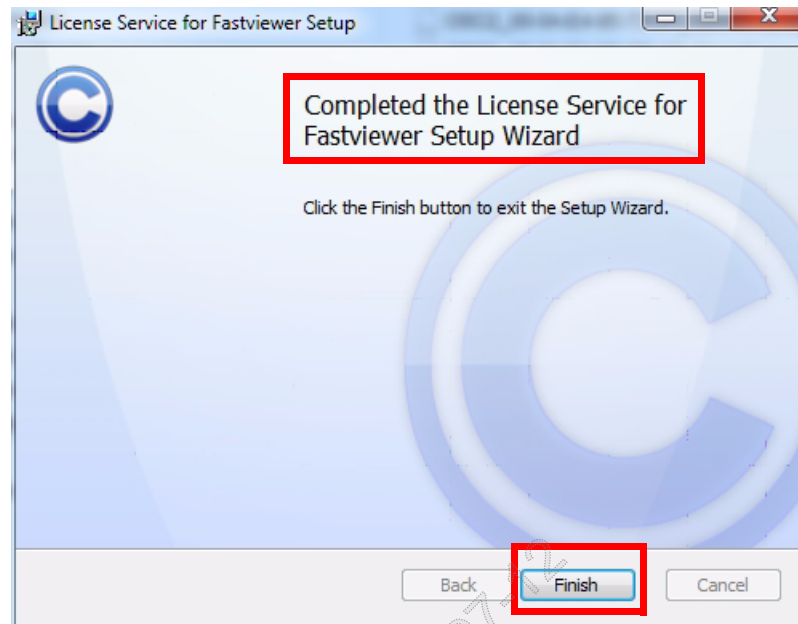
The screenshot shows the 'License configuration and additional options' window. It features a 'SIEMENS' logo at the top right. Below the title bar, the text 'Click Next after configuring your options' is displayed. The main area is titled 'HiPath License Management connection'. It contains four input fields: 'Address' (1.21.12.80), 'Port' (61740), 'Timeout' (1000), and 'Retry' (5). These fields are grouped into two rows. At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red rectangle.

Enter the **IP Address** and **Port** of the computer that hosts the Customer License Agent (CLA). The **Timeout** field specifies the intervals in milliseconds in which the attempt is made to connect to the computer that hosts the Customer License Agent. From the **Retry** field you can gather how often this attempt is repeated. Change the defaults if required.



The screenshot shows the 'Ready to install License Service for Fastviewer' window. It features a 'SIEMENS' logo at the top right. Below the title bar, the text 'Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.' is displayed. At the bottom, there are three buttons: 'Back', 'Install', and 'Cancel'. The 'Install' button is highlighted with a red rectangle.

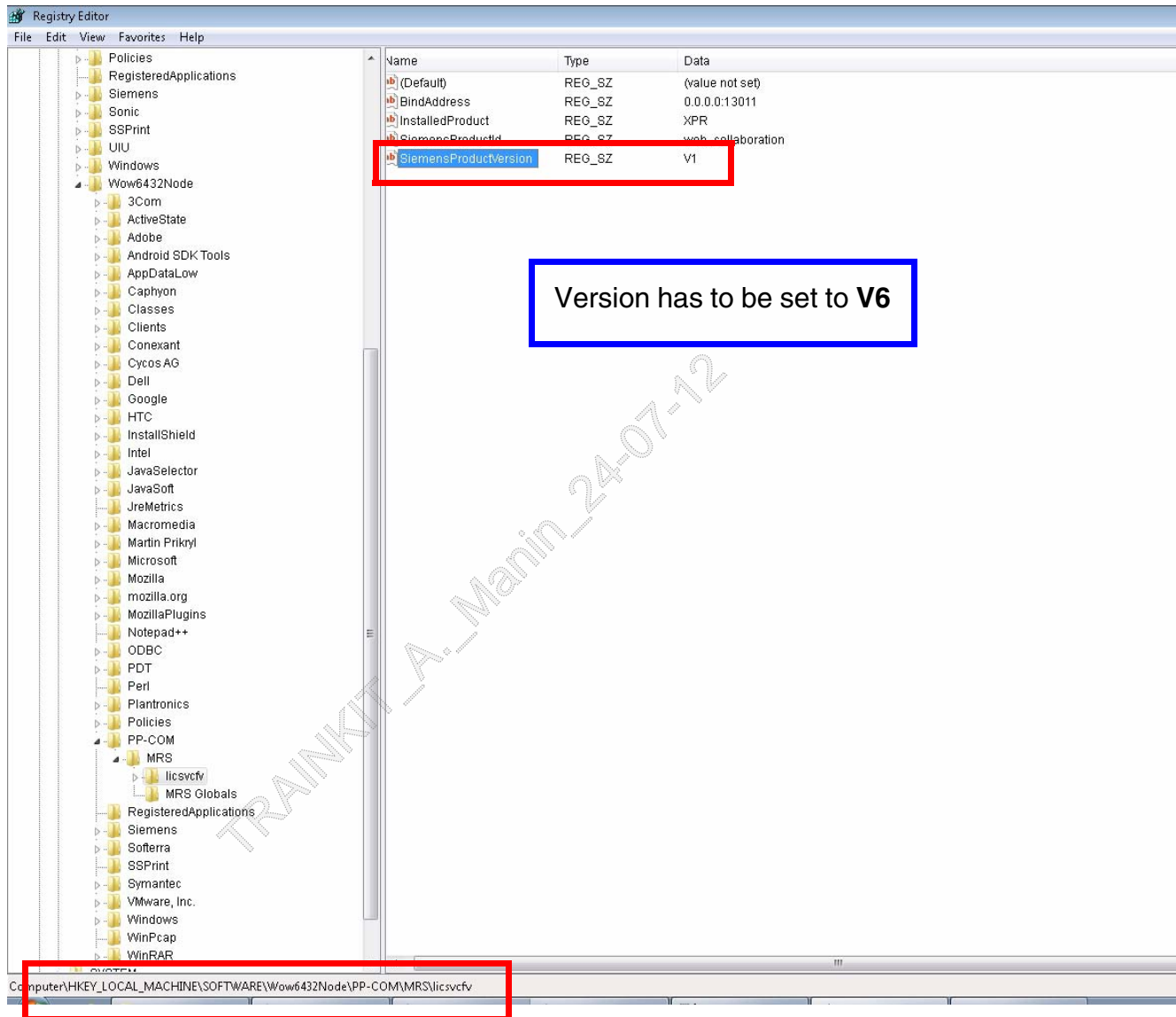
Start the installation of the License Service with the set installation data.



2.4 Checking the Registry (valid 04/2012)

Start the “regedit” and check the Fastviewer version in the following path:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\licsvcfv



2.5 Configuring the Web Collaboration Server

Open the `settings.ini` file in the installation folder of the Web Collaboration Server in an editor. The path is by default:

```
c:\Program Files\WebConferenceServer or
c:\Program Files (x86)\WebConferenceServer
```

1. Look for the lines with the value `Change2YourServer` in the `settings.ini` file:

```
ExternalAddress=Change2YourServer
```

Replace the string `Change2YourServer` with the external, fully qualified domain name (FQDN) of the Web Collaboration Server.



The external FQDN is the full outside name of the Web Collaboration server computer. The internal FQDN is the full name of this computer as seen from the internal corporate network. If only one single FQDN is available, use it.

2. In the `settings.ini` file, log levels for log groups can be configured, too. Search this file for the following section:

```
[Logging]
; The setting value is the limit at which a log message is logged.
; 0=Info, 1=Uncritical, 2=Warning, 3=Important, 4=Critical, 5=Disabled
;All=0 ; this overwrites all others, if less

;Connection=2
;PacketManager=2
;DatabaseManager=2
;General=2
;License=2
;MessageProtocol=2
;SessionManager=2
;XmlProtocol=2
;Log file path
;LogFilePath="tunnelserver.log"
;MaxLogFileSizeMB=512
```

0	= Information
1	= Uncritical messages
2	= Warning
3	= Important errors
4	= Critical errors
5	= Logging deactivation for this log group

There are the following log groups:

- **General**
- **License**
- **Connection**
- **PacketManager**
- **DatabaseManager**
- **MessageProtocol**
- **SessionManager**
- **XMLProtocol**
- **All**

For each log group you can enter a value that is independent from the values of other log groups. If the value of log group **All** is not **5**, it applies for all log groups. The values that may have been entered for other log groups are ignored.

3. In the **settings.ini** file, you can also configure the session manager. Search this file for the following section:

```
[SessionManager]
ClientURLBase=http://Change2YourServer/client/fastclient_i_%1.exe
;WebclientURLBase=http://Change2YourServer/joinclient.aspx?inv=%1
; You can use SingleURL=true only if the webclient is installed,
then all XMLRPC answers are with the webclient URL.
SingleURL=false
```

- a) Replace the string **Change2YourServer** in value **ClientURLBase** with the external, fully qualified domain name (FQDN) of the Web Collaboration Server.



The external FQDN is the full outside name of the Web Collaboration server computer. The internal FQDN is the full name of this computer as seen from the internal corporate network. If only one single FQDN is available, use it.

This URL is selected if the native **Windows Client (FastClient.exe)** is used for the Web Conferences.

- b) If you use the **Web Collaboration Web Client (Java based)**, you need to remove the semicolon (;) that precedes **WebclientURLBase**.

Replace the string **Change2YourServer** in value **WebclientURLBase** with the external, fully qualified domain name (FQDN) of the Web Collaboration Server.

If you want to use a client different from the native Windows client (FastClient.exe), you need to set **SingleURL** to value **true** and you need to install the Web Collaboration Web Client (???see [Section 1.4.3, “Installing the Web Collaboration Web Client”](#)).

Later when you click on the globe icon in the OpenScape WebClient, the **settings.ini** file of the **Web Collaboration Web Client** determines which client is started.

If **SingleURL** is not set to value **true** or the Web Collaboration Web Client is not installed, always the native Windows client (FastClient.exe) will be started when the globe icon in the OpenScape WebClient will be clicked.



When the **ini** file is modified the **Service „WebConference Server“** has to be restarted or stopped and started (???see page 22).

2.5.1 Preparing the Web Collaboration Server for the Native Windows Client (FastClient.exe)

- Open the following Web page in a browser:
<http://openscape.fastviewer.com>
 - 'number range' and 'servername' configuration

fastviewer client customization [View/Subscribe to Changelog](#)

Please add the customer server(s) to the following list and click "Download FastClient" afterwards! When communicating via https, the server name must be entered with https://

number range: 10000 - 99999

servername: 1.69.11.10

Download FastClient V 3.20.0009

[Login](#) in order to enable advanced functions!

Usage-Hints:

- Insert at least 1 server to the list
- The listed server names must be unique
- Each line reflects one Web Conference server
- The range of numbers has to be the same as defined in the server's settings.ini
- The range of numbers has to be unique in the list
- Don't mix external and internal FQDN's
- Internal FQDN's will only work inside of the customer Network
- If an external FQDN is defined, it must be reachable from inside AND outside of the customer Network

Server-Installation for more than 1 server

- All servers have to use the same Database
- Normally this is the Database from the first server

- Leave the values in the 'number range' fields unchanged.
- Enter the external FQDN in the 'servername' field and click on the  icon.



Use the external FQDN you used in ???step 3 on page 17.

fastviewer client customization [View/Subscribe to Changelog](#)

Please add the customer server(s) to the following list and click "Download FastClient" afterwards! When communicating via https, the server name must be entered with https://

10000-99999:1.69.11.10

number range: 10000 - 99999

servername:

Download FastClient V 3.20.0009

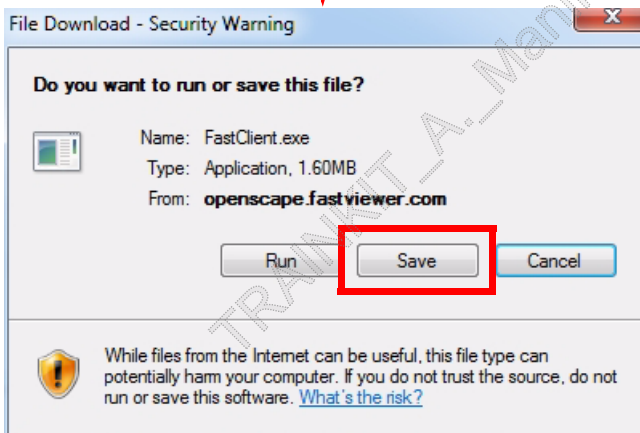
[Login](#) in order to enable advanced functions!

Usage-Hints:

- Insert at least 1 server to the list
- The listed server names must be unique
- Each line reflects one Web Conference server
- The range of numbers has to be the same as defined in the server's settings.ini
- The range of numbers has to be unique in the list
- Don't mix external and internal FQDN's
- Internal FQDN's will only work inside of the customer Network
- If an external FQDN is defined, it must be reachable from inside AND outside of the customer Network

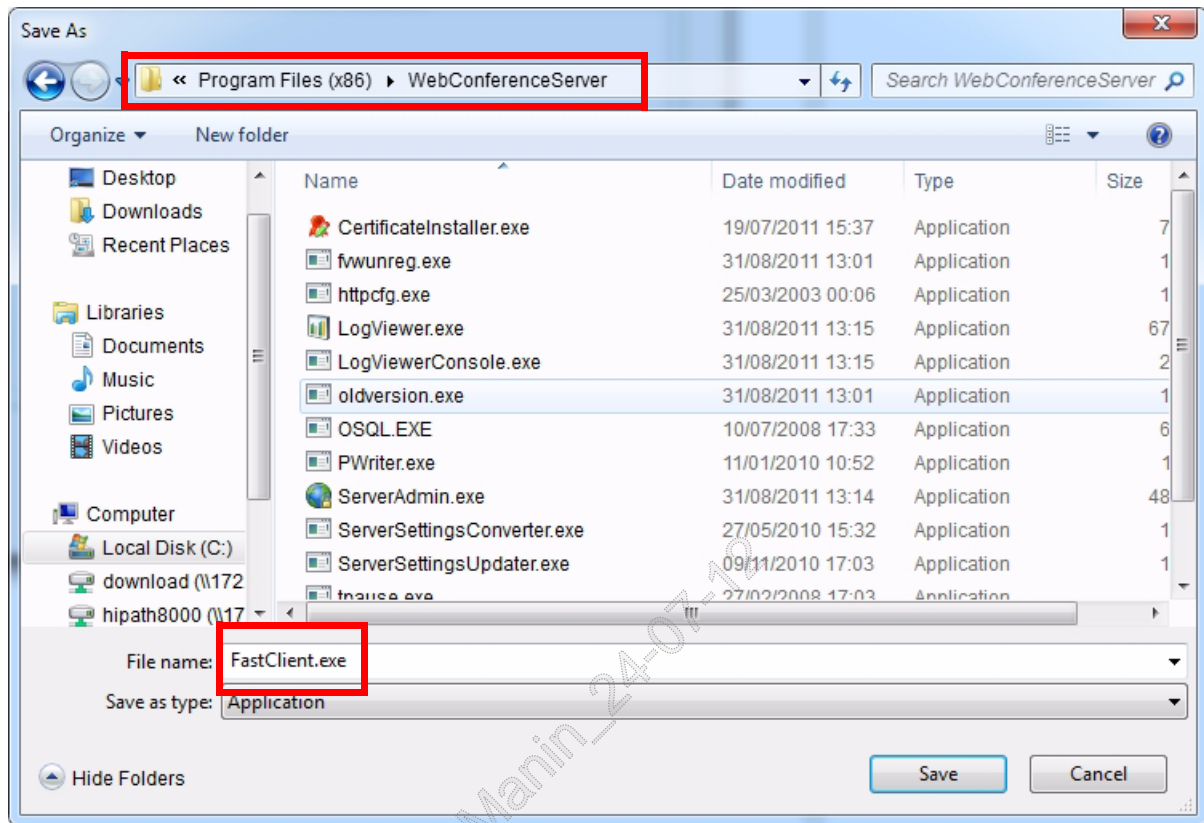
Server-Installation for more than 1 server

- All servers have to use the same Database
- Normally this is the Database from the first server



Save the downloaded file to the setup folder of the Web Collaboration Server. This is the following folder by default:

c:\Program Files\
WebConferenceServer
or
c:\Program Files (x86)\
WebConferenceServer



2.5.2 Services Controlling

Open the Windows '**Control Panel**' by selecting

Start --> Settings --> Control Panel --> Administrative Tools --> Services

Rightclick the **Web Conference Server** entry and select the **Start** option.

If the "**Startup Type**" is not set to "**Automatic**" rightclick the **Web Conference Server** entry and select the **Properties** option. Verify that value **Automatic** is selected in the **Startup type** field.



Services are only started if the CLA is installed and the Web Collaboration Embedded license is active!

Name	Description	Status	Startup Type	Log On As
VMware USB Arbitration Service		Started	Automatic	Local Syst...
Volume Shadow Copy	Manages a...		Manual	Local Syst...
Web Conference Server	openscape ...		Automatic	Local Syst...
Web Management Service	The Web M...		Manual	Local Servi...
WebClient	Enables Wi...		Manual	Local Servi...
Windows Audio	Manages a...	Started	Automatic	Local Servi...
Windows Audio Endpoint	Manages a...	Started	Automatic	Local Syst...
Windows Backup	Provides Wi...		Manual	Local Syst...
Windows Biometric Service	The Windo...		Manual	Local Syst...
Windows CardSpace	Securely en...		Manual	Local Syst...
Windows Color System	The WcsPlu...		Manual	Local Servi...
Windows Connect Now -	WCNCSVC ...		Manual	Local Servi...
Windows Defender	Protection a...	Started	Automatic (D...	Local Syst...
Windows Driver Foundati	Manages u...	Started	Automatic	Local Syst...
Windows Error Reporting	Allows error...		Manual	Local Syst...
Windows Event Collector	This service...		Manual	Network S...
Windows Event Log	This service...	Started	Automatic	Local Servi...
Windows Firewall	Windows Fi...	Started	Automatic	Local Servi...
Windows Font Cache Service	Optimizes p...	Started	Automatic (D...	Local Servi...
Windows Image Acquisition (WIA)	Provides im...		Manual	Local Servi...
Windows Installer	Adds, modif...		Manual	Local Syst...
Windows Management Instrumentation	Provides a c...	Started	Automatic	Local Syst...

Name	Description	Status	Startup Type	Log On As
VMware USB Arbitration Service		Started	Automatic	Local Syst...
Volume Shadow Copy	Manages a...		Manual	Local Syst...
Web Conference Server	openscape ...		Automatic	Local Syst...
Web Management Service	The Web M...		Manual	Local Servi...
WebClient	Enables Wi...		Manual	Local Servi...
Windows Audio	Manages a...	Started	Automatic	Local Servi...
Windows Audio Endpoint	Manages a...	Started	Automatic	Local Syst...
Windows Backup	Provides Wi...		Manual	Local Syst...
Windows Biometric Service	The Windo...		Manual	Local Syst...
Windows CardSpace	Securely en...		Manual	Local Syst...
Windows Color System	The WcsPlu...		Manual	Local Servi...
Windows Connect Now -	WCNCSVC ...		Manual	Local Servi...
Windows Defender	Protection a...	Started	Automatic (D...	Local Syst...
Windows Driver Foundati	Manages u...	Started	Automatic	Local Syst...
Windows Error Reporting	Allows error...		Manual	Local Syst...
Windows Event Collector	This service...		Manual	Network S...
Windows Event Log	This service...	Started	Automatic	Local Servi...
Windows Firewall	Windows Fi...	Started	Automatic	Local Servi...
Windows Font Cache Service	Optimizes p...	Started	Automatic (D...	Local Servi...
Windows Image Acquisition (WIA)	Provides im...		Manual	Local Servi...
Windows Installer	Adds, modif...		Manual	Local Syst...
Windows Management Instrumentation	Provides a c...	Started	Automatic	Local Syst...

Web Conference Server Properties (Local Computer)

General Log On Recovery Dependencies

Service name: Web Conference Server

Display name: Web Conference Server

Description: openscape Server for Webcollaboration

Path to executable:
"C:\Program Files (x86)\WebConferenceServer\TunnelService.exe"

Startup type: Automatic
Automatic (Delayed Start)
Manual
Disabled

Service status: Stopped

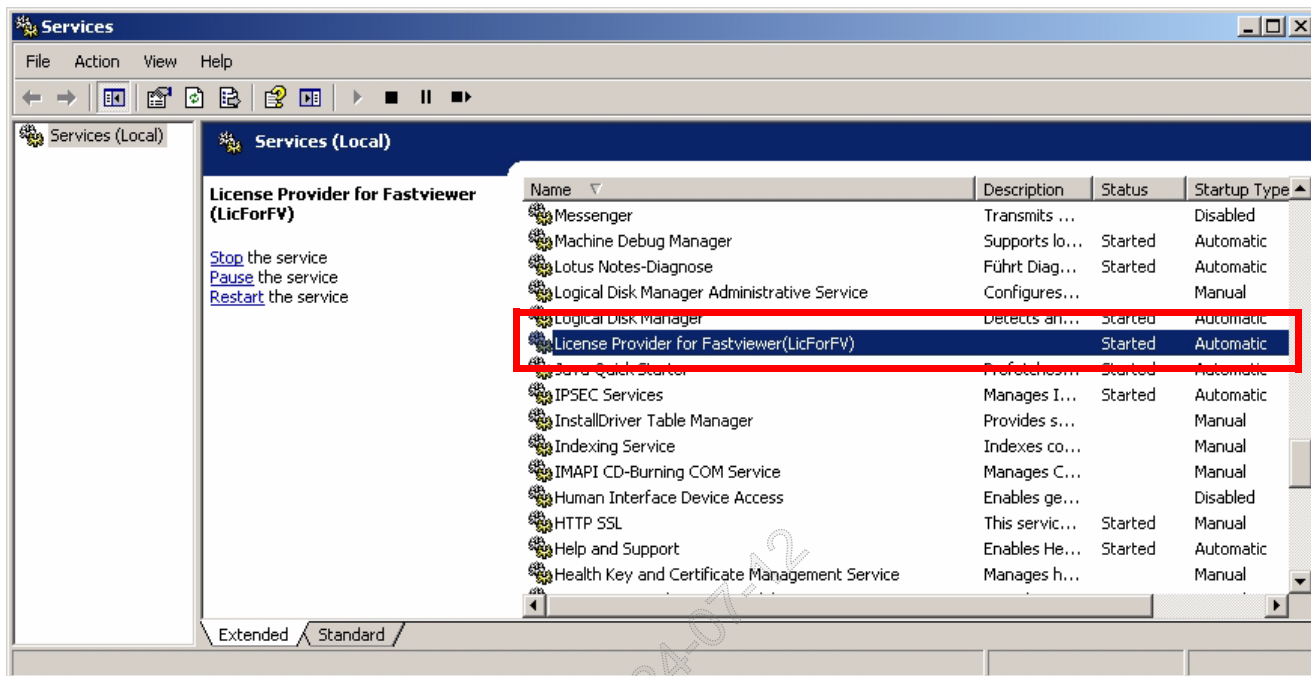
Start Stop Pause Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK Cancel Apply

- Check another two '**Services**', which are necessary for the FastViewer integration:

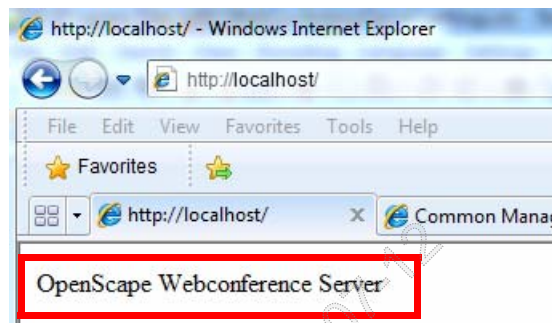


Name	Description	Status	Startup Type	Log On As
Remote Procedure Call (RPC) Locator	In Windows ...		Manual	Network S...
Remote Registry	Enables re...		Manual	Local Servi...
Routing and Remote Access	Offers routin...		Disabled	Local Syst...
RPC Endpoint Mapper	Resolves R...	Started	Automatic	Network S...
Secondary Logon	Enables sta...		Manual	Local Syst...
Secure Socket Tunneling Protocol Service	Provides su...		Manual	Local Servi...
Security Accounts Manager	The startup ...	Started	Automatic	Local Syst...
Security Center	The WSCSV...	Started	Automatic (D...	Local Servi...
Server	Supports fil...	Started	Automatic	Local Syst...
Shell Hardware Detection	Provides no...	Started	Automatic	Local Syst...
Simple TCP/IP Services	Supports th...	Started	Automatic	Local Servi...
Smart Card	Manages ac...		Manual	Local Servi...
Smart Card Removal Policy	Allows the s...		Manual	Local Syst...
SNMP Service	Enables Si...	Started	Automatic	Local Syst...
SNMP Trap	Receives tr...		Manual	Local Servi...
Software Protection	Enables the...		Automatic (D...	Network S...
SQL Server (FASTVIEWER)	Provides st...	Started	Automatic	Network S...
SQL Server Active Directory Helper	Enables int...		Disabled	Network S...
SQL Server Browser	Provides S...	Started	Automatic	Network S...
SQL Server VSS Writer	Provides th...	Started	Automatic	Local Syst...
SSDP Discovery	Discovers n...	Started	Manual	Local Servi...

2.5.3 Checking the Installation of the Web Conference Server

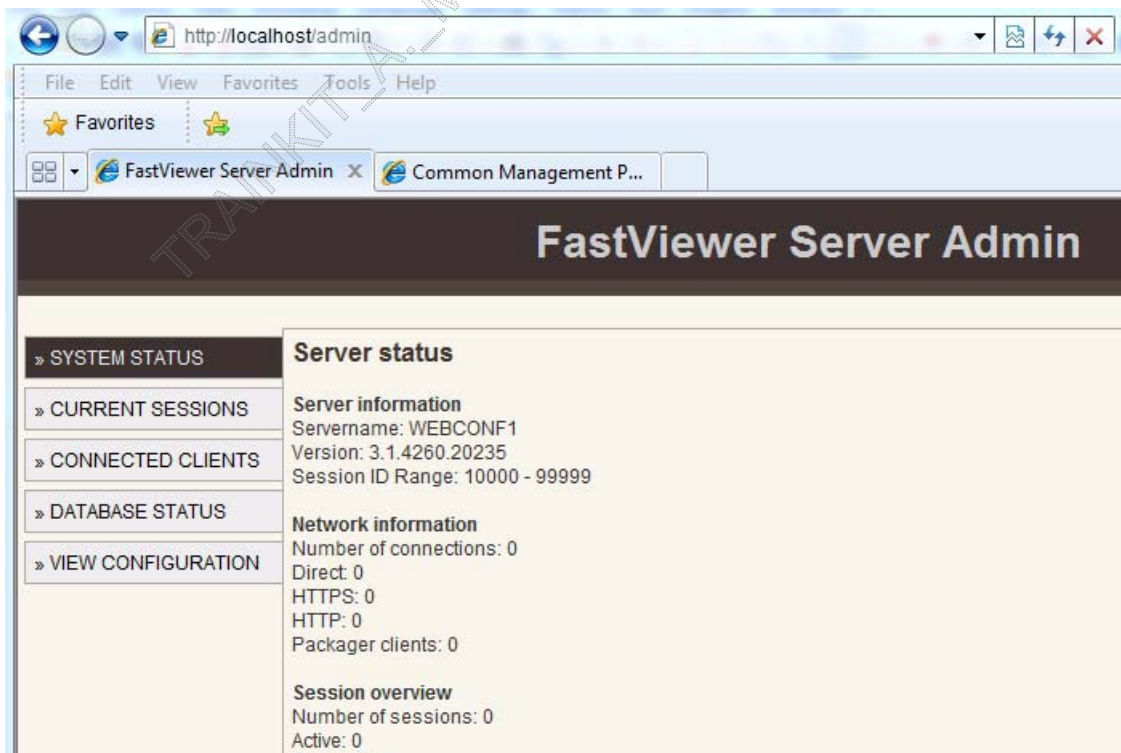
Open the address <http://localhost> or <http://localhost:81> in the internet explorer on the Web Collaboration Server computer. These two steps to check the installation of the Web Conference Server are only available when **no IIS** is installed. When IIS is installed the same Listener port for HTTP is used by the Web Conference Server and the IIS (see [step 5 on page 35](#)).

The website shows the following:



or enter

<http://localhost/admin> or <http://localhost:81/admin>



2.5.4 Installing the Web Collaboration Web Client

The Web Collaboration Web Client 3.1.x is a JavaScript client running on all web browsers supporting JavaScript. Except for the writing of instant messages, it is a passive client in a web conference. It can monitor a web conference, but not interfere in the web conference in an active way. The client does not support e. g. desktop sharing. The client recognizes automatically the platform on which it should run and selects then the corresponding file to be executed.

2.5.4.1 Supported features

- List of web conference participants
- Showing the web conference
- Showing videos
- Reading and writing instant messages

2.5.4.2 Installing the required program



The Web Collaboration Web Client is installed on the computer on which the Web Collaboration server has been installed.

- The operating system that are supported for the Web Collaboration Server are supported for the Web Collaboration Web Client as well.
- ASP.Net
- IIS
- .NET Framework 3.5



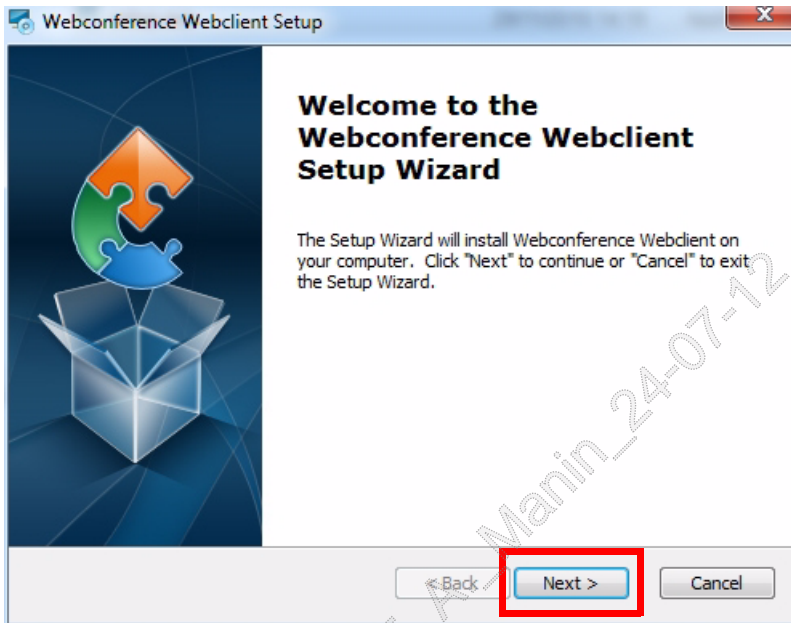
IMPORTANT:

This version must be installed and no higher version must be installed. Several versions may be installed in parallel on the same computer, e. g. .NET Framework 4.0, which is used for the Web Collaboration server.

- Running Web Collaboration server computer
(see [Section 2.5.2, “Services Controlling”](#))

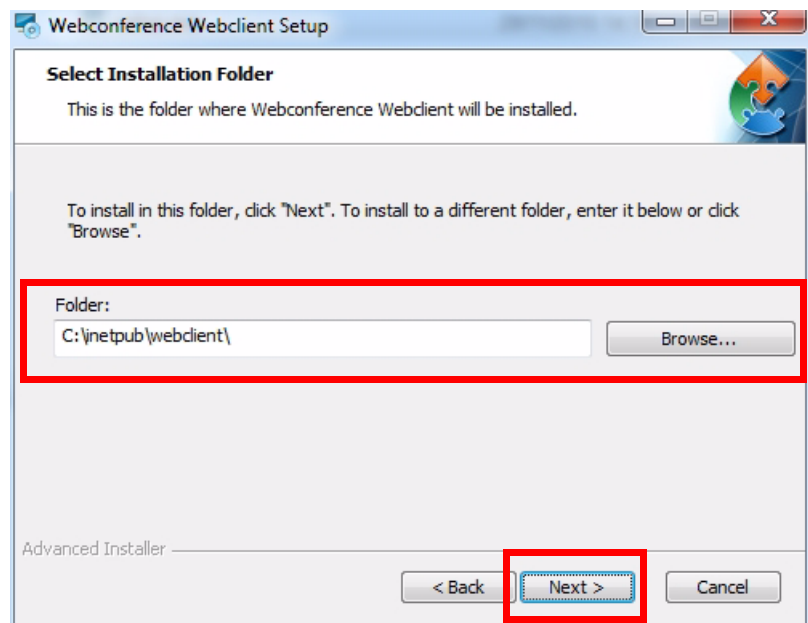
For the installation of the Web Collaboration Web Client requirements, execute the following steps:

1. Decompress the following file on the OpenScope UC Application setup DVD or Patch:
contrib/FastViewerWebClient-<version>.zip
2. Start the **setup.exe** file you will find in the ZIP file.

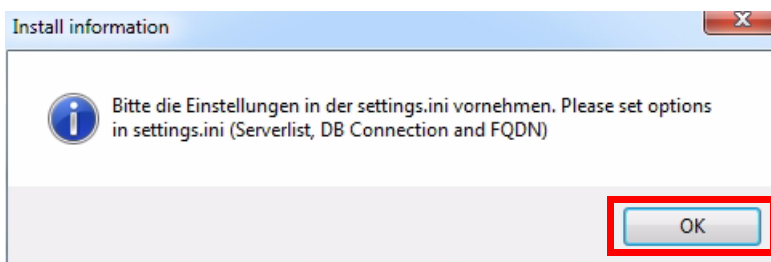
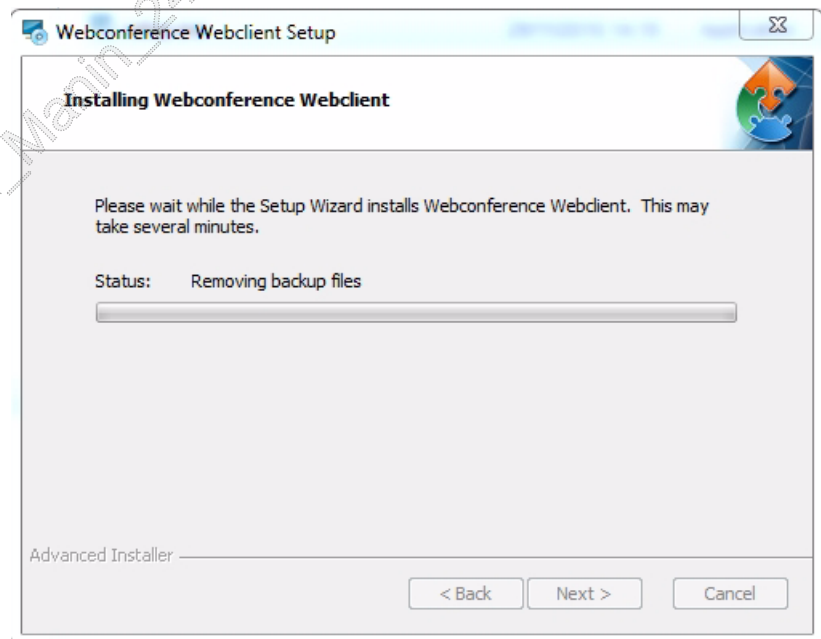
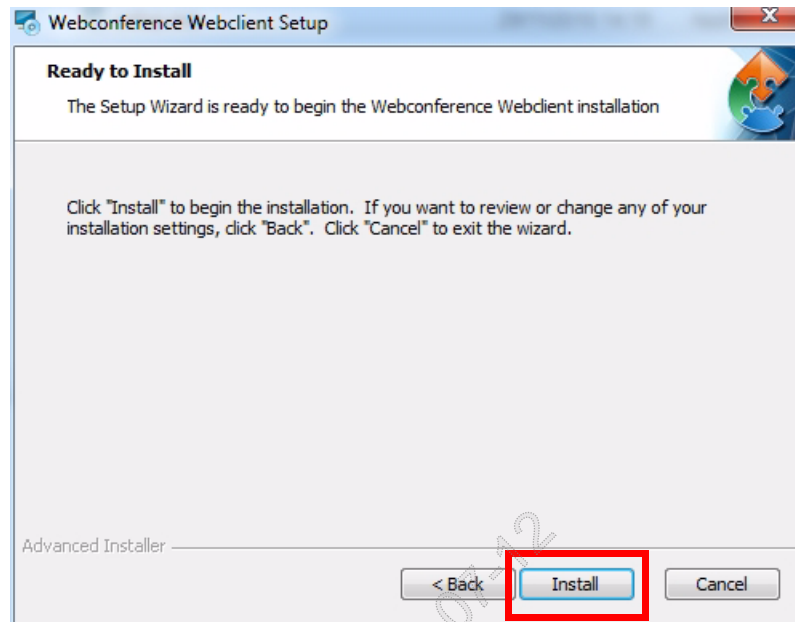


Accept or select the installation folder.

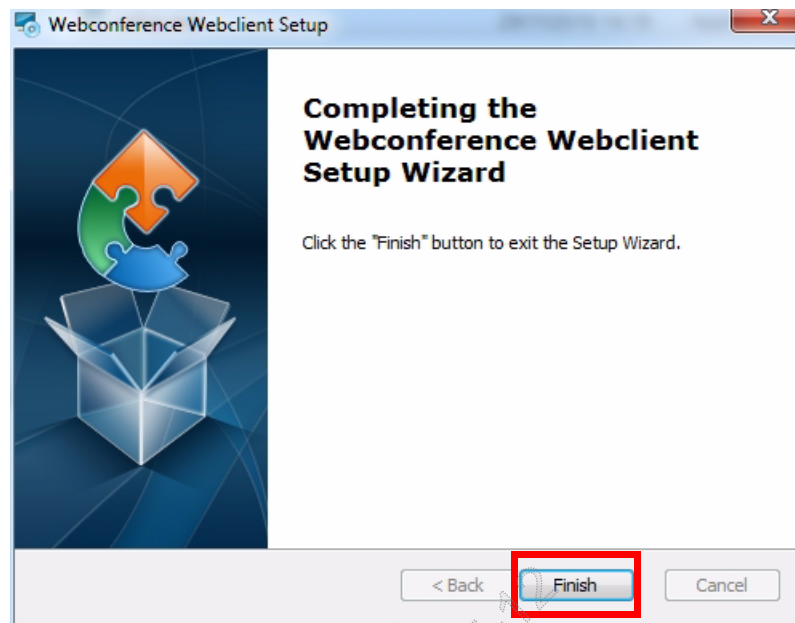
If .NET Framework 3.5 SP1 is not installed the Setup Wizard will install it. Therefore refer the Service Manual “*Installation and Upgrade Guide*”



3. Start the installation.



The settings of the parameters mentioned here is described in detail in **step 4**.



4. Open the **settings.ini** file in the setup directory. By default, it is located in the directory **C:\inetpub\webclient**.

Without comments and blank lines, it looks like this:

```
[Settings fastviewer V 3.x WebClient]
Serverlist=
ServerListURLs=
DBConnectionString=""
EnableLogging=0
OEMVersion=1
FQDN="change2your.server.com"
SysLogServerIp=
SysLogPort=514
ClientForWindows=1
ClientForMAC=1
ClientForIPhone=3
ClientForMobile=1
ClientForUnknown=1
PathToPresavedFiles="C:\Programme\WebConferenceServer\clients"
DomainForPathToPresavedFiles=""
UsernameForPathToPresavedFiles=""
PasswordForPathToPresavedFiles=""
[Settings END]
```

To make Web Collaboration server properties known to the Web Collaboration Web Client, you can enter these specifications yourself in the settings.ini file or enter the HTTP address of a file on a web server containing these specifications.

For the first option, perform substep a, for the second option, perform substep b. Thus, the use of the `Serverlist` parameter and the `ServerlistURLs` parameter is not possible at the same time.

- a) Set the value of the `Serverlist` parameter to the value entered in ???[section 1.4.1 on page 19](#). Use the format of the following example:

Example:

```
Serverlist=10000-99999:change.yourserver.com
```

Leave the value of `ServerlistURLs` empty.

- b) Set the value of the `ServerlistURLs` parameter. This value indicates the HTTP address of a file on a webserver containing the Web Collaboration server specifications which can be downloaded by the Web Collaboration Web Client. The webserver must not necessarily be the IIS of the Web Collaboration server computer.

Example:

```
ServerListURLs=http://change.yourserver.com/list.txt
```

Leave the value of the `Serverlist` parameter empty.

- c) Set the value of the `DBConnectionString` parameter to the same string value used in the settings.ini file in the installation folder on the Web Collaboration server computer (???see [section 1.4 on page 16](#)). By default, this folder is `C:\Program Files (x86)\WebConferenceServer`. This parameter is used to create the database connection.

Example:

```
DBConnectionString="Data Source=(local)\fastviewer;Initial  
Catalog=fastviewer;Persist Security Info=True;User ID=sa;  
Password=topsecret"
```

- d) Use EnableLogging to set whether the Information tab should be displayed and events should be logged.

Example:

EnableLogging=0

- e) OEMVersion indicates whether this Web Collaboration web client is an OEM version. If the value is 1, no logo is displayed.

Example:

OEMVersion=1

- f) Set the value of the FQDN parameter to the external fully qualified domain name (FQDN) of the computer on which the Web Collaboration Web Client is installed.

Example:

FQDN="change2your.server.com"

If FQDN is empty, the value "[host name].fastviewer.com" is used.



The external FQDN is the full outside name of the computer. The internal FQDN is the full name of this computer as seen from the internal corporate network. If only one single FQDN is available, use it.

- g) If log messages should be sent according to the syslog standard, enter under SysLogServerIp the IP address of the syslog server and under SysLogPort the port. By default, port 514 is used.

syslog, 514: UDP

Example:

SysLogServerIp=123.123.123.123

SysLogPort=514

- h) The Web Collaboration Web Client detects automatically the operating system on which it is running. Depending on the operating system, there are different clients to be started. The following table shows with which operating system detected which parameter in the `settings.ini` file must be set to which value.

Operating system detected	Parameter	Value
Windows	ClientForWindows	0 ¹ or 1 or 2
Macintosh	ClientForMAC	1
iOS (e. g. iPhone, iPad or iPod)	ClientForiPhone	3 or 1
Operating system of a mobile device ² except iPhone, iPad or iPod	ClientForMobile	1
None of the above mentioned operating systems	ClientForUnknown	1

Table 77 Parameter to determine the Web Collaboration Web Client

1 Note the instructions in substep i.

2 The Windows Mobile operating system is detected as a mobile operating system, and not as a Windows operating system.

The following table shows which client is used due to a value.

Value	Meaning
0	Native Windows client (fastviewer.exe)
1	JavaScript Web Client
2	Flash Client
3	Native iPhone client, iPad client or iPod client

Example:

ClientForWindows=1

ClientForMAC=1

ClientForiPhone=3

ClientForMobile=1

ClientForUnknown=1

- i) If in step **h)** you use the value **0**, you must set the **PathToPresavedFiles** parameter to the UNC path or the local path of the **fastclient.exe** file. This is the file downloaded **on page 20** and copied to the Web Collaboration server computer.

Example:

```
PathToPresavedFiles="C:\Program Files (x86)\WebConferenceServer\"
```

If a domain, a user name and a password is required to access this file, you must set the following parameters to the appropriate values:

```
DomainForPathToPresavedFiles=" "
```

```
UsernameForPathToPresavedFiles=" "
```

```
PasswordForPathToPresavedFiles=" "
```

5. If you install the Web Collaboration Web Client on the Web Collaboration server computer, you must use different host headers for the Web Collaboration server and the Web Collaboration Web Client. The Web Collaboration server and the IIS use the same HTTP listener on the same Windows computer. Edit the **listener...** entries in the **[HTTPListenURLs]** section in the **settings.ini** file on the Web Collaboration server computer. Save the file after you have performed the modifications and reboot the Web Collaboration server service (service name: **Web conference server**). You need not reboot the Web Collaboration server computer.

```
settings.ini
```

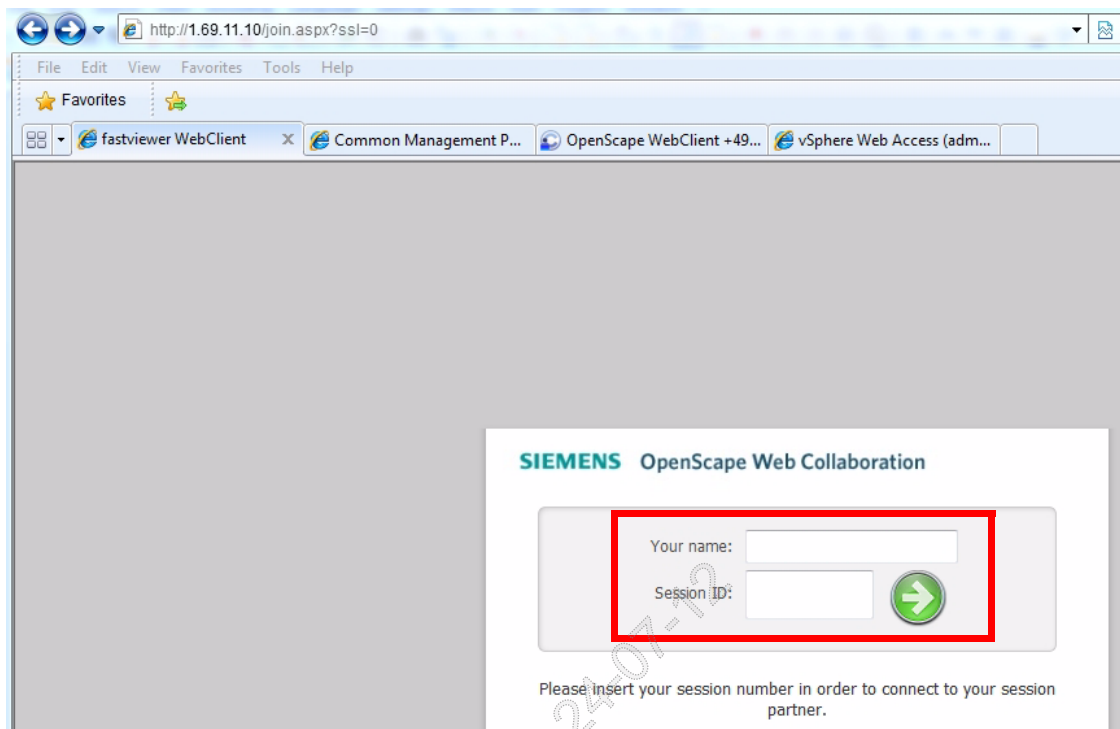
Example:

```
listen1="http://*:81"
```

6. To check the installation, proceed as follows:

- a) Open a browser.
- b) Enter the external FQDN in the browser address field.

On the page displayed, enter the name of a conference participant and a Session ID.



- c) Start a Web Collaboration session in the conference mode and enter the session PIN on the website. You will see the moderator's desktop.

7. In the `settings.ini` file of the **Web Conference Server**, you can also configure the session manager. Search this file for the following section:

```
[SessionManager]
ClientURLBase=http://Change2YourServer/client/fastclient_i_%1.exe
;WebclientURLBase=http://Change2YourServer/joinclient.aspx?inv=%1
; You can use SingleURL=true only if the webclient is installed,
then all XMLRPC answers are with the webclient URL.
SingleURL=false
```

If you use the **Web Collaboration Web Client (Java based)**, you need to remove the semicolon (;) that precedes `WebclientURLBase`.

Replace the string `Change2YourServer` in value `WebclientURLBase` with the external, fully qualified domain name (FQDN) of the Web Collaboration Server.

If you want to use a client different from the native Windows client (FastClient.exe), you need to set **SingleURL** to value **true** and you need to install the Web Collaboration Web Client (see Section 1.4.3, “Installing the Web Collaboration Web Client”).

Later when you click on the globe icon in the OpenScope WebClient, the **settings.ini** file of the **Web Collaboration Web Client** determines which client is started.

If **SingleURL** is not set to value **true** or the Web Collaboration Web Client is not installed, always the **native Windows Client** (FastClient.exe) will be started when the globe icon in the OpenScope WebClient will be clicked.



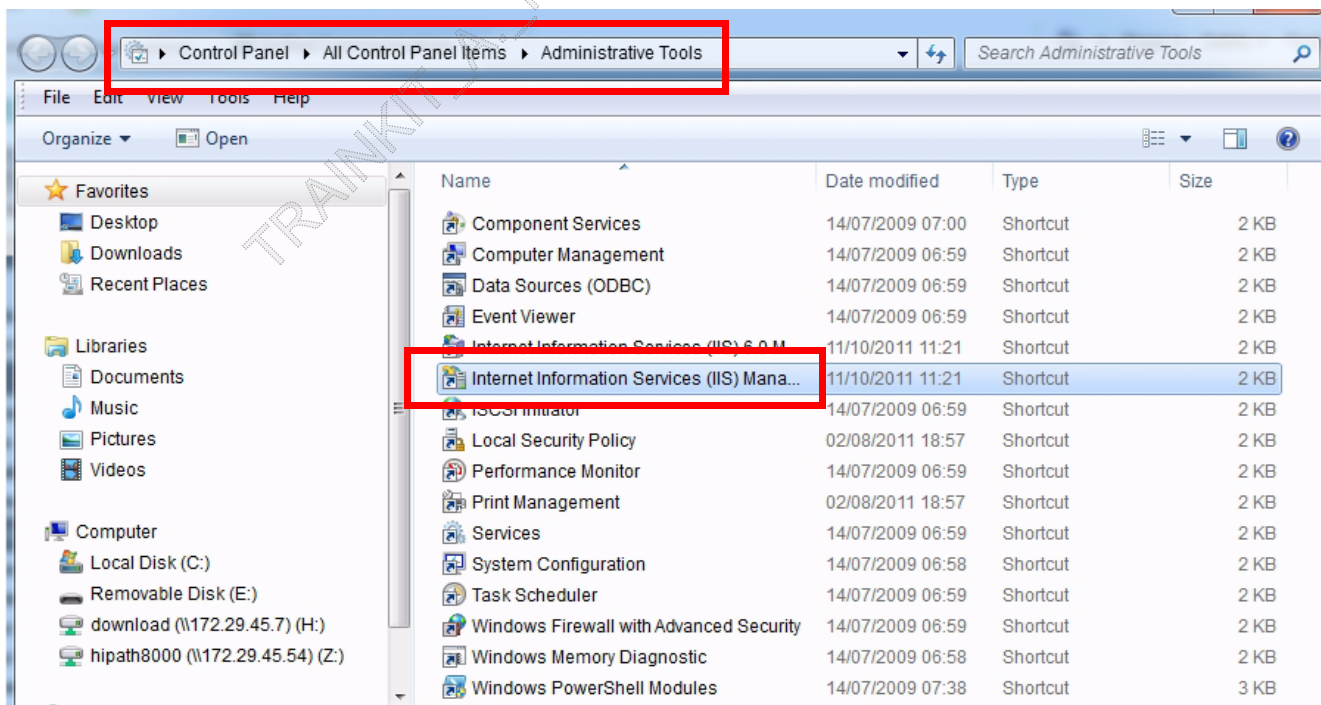
When the **ini** file is modified, the **Service „WebConference Server“** has to be restarted or stopped and started (???see page 23).

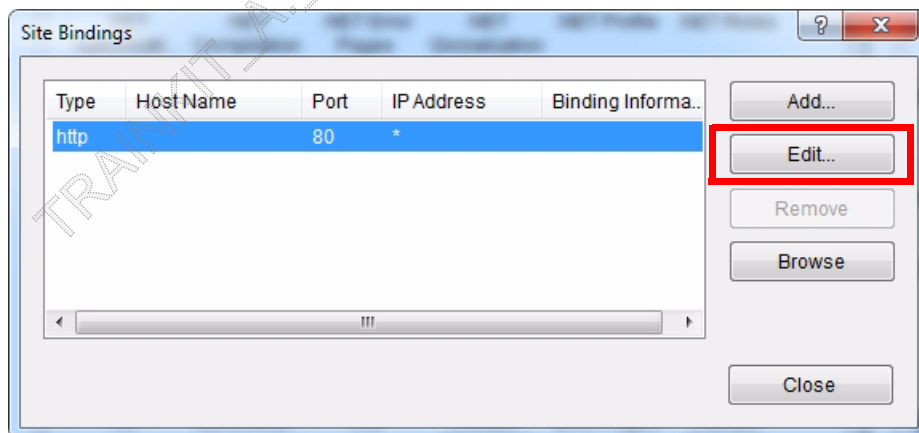
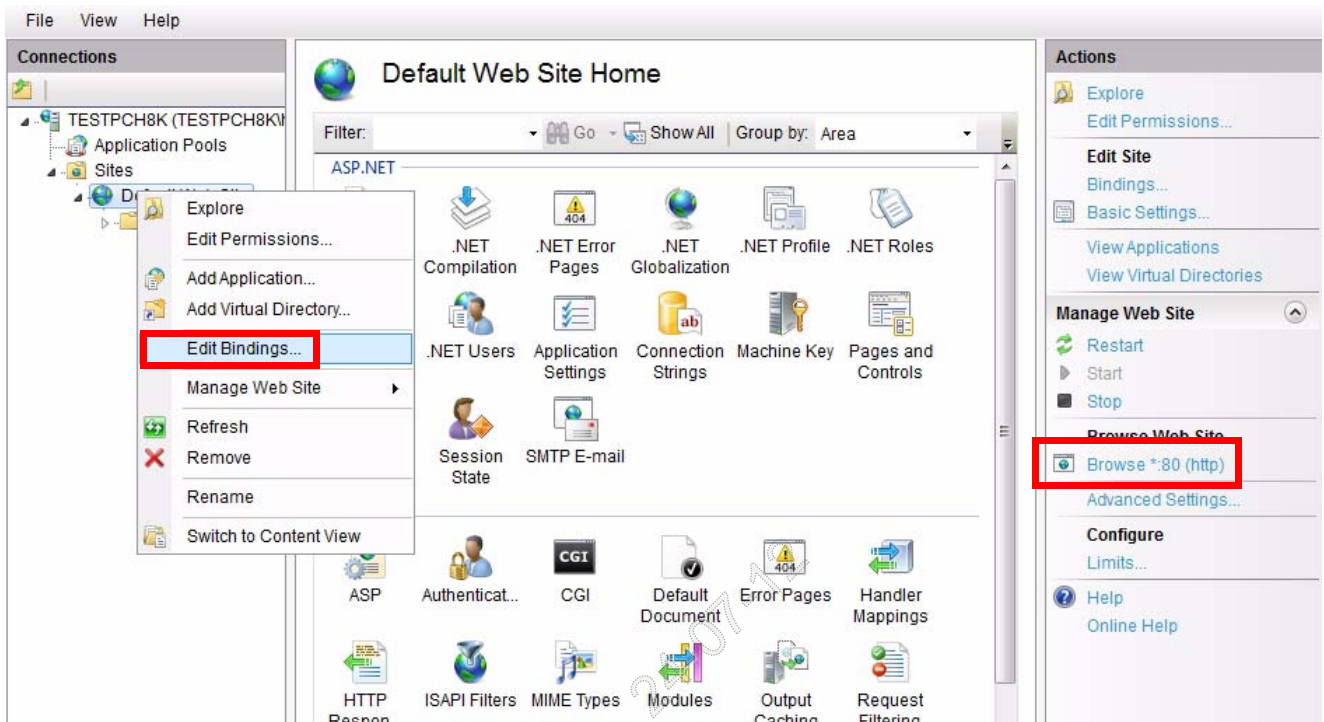
8. Port Problem



The IIS is using in standard **Port 80** which is also used by the **Web Collaboration Web Client**.

Using the **Control Panel** and the **Administrative Tools** and select the **IIS Manager**





3 OpenScape Web Collaboration - Exercise

3.1 Exercise

Starting point:

- OpenScape Office user including an Email address are configured.
- My Portal is installed.

Aim:

An OpenScape Office conference should be carried out with web collaboration.

Invitation Email should be delivered in advance.

Optional:

- Automatically start the phone conference with web collaboration.

or...

- during an established phone conference.

Please adapt the following settings according your infrastructure.

Setup meet-me conference(advanced mode)

Occurs 20/03/2012 from 14:10:00 to 15:10:00

Choose between the different conference types (MeetMe, Permanent and Open)
Activate and/or deactivate the different functions.
These selections will be your new default settings for all new conferences.

Conference Type: Meet Me Conference (No Password)

Conference Language: English (United Kingdom)

☒ This conference is an active conference

☐ This conference requires the conference controller to be present

☐ Force participant to enter "*" (star) to enter the conference

☒ Automatically start phone conference with web collaboration.

☐ Automatically record this conference.

☒ Automatically send email invitation to conference participants

Notes

Basic Save Apply Cancel

Optional: either start with the voice conference or... during a voice conference is established...

Setup meet-me conference(simple mode)

Occurs 20/03/2012 from 14:10:00 to 15:10:00

Please add the conference name, date and start/end times then click on the add participant button to search and add participants

Conference Name: richards web collaboration

Start Date: 20-Mar-2012

Start Time: 14:10:00

End Time: 15:10:00

☐ Recurring Conference

Conference DID: +49897970077430

Add Participant

Participants: bianca, richi, hans h3k

Advanced Save Apply Cancel

My Conferences Conferences I belong to

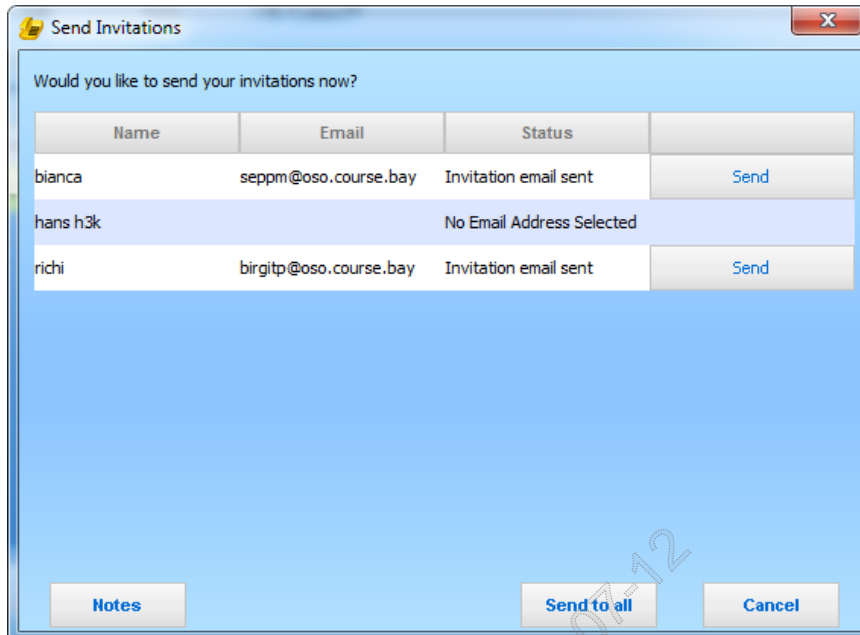
Conference Name	Next Recurrence
richards web collaboration	Tuesday, 20. March 2012 14:10:00

richards web collaboration
Tuesday, 20. March 2012 14:10:00

Start Conference

Send Invitations

New Edit Remove View Close



Email example for web collaboration link...

richi has invited you to join the richards web collaboration conference.

This conference is scheduled to run at 14:10 on Tuesday
, 20th March 2012 for 60 minutes.

The conference system will call you on
7100.

Alternatively, you can dial +49897970077430 between 14:10 and 1
5:10 and enter your conference ID.

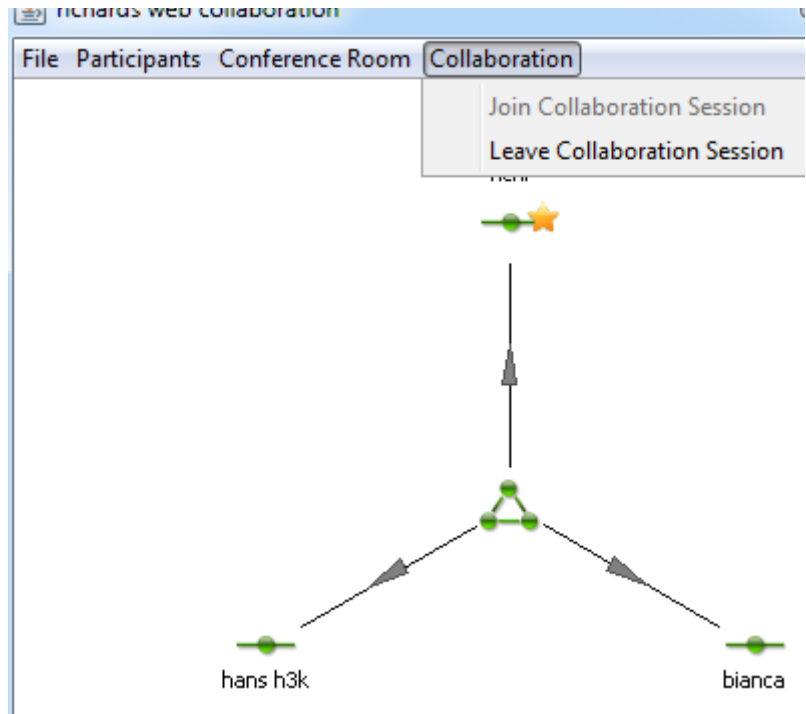
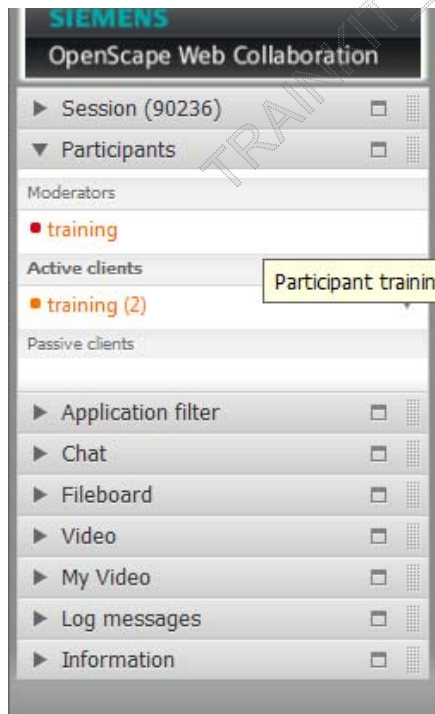
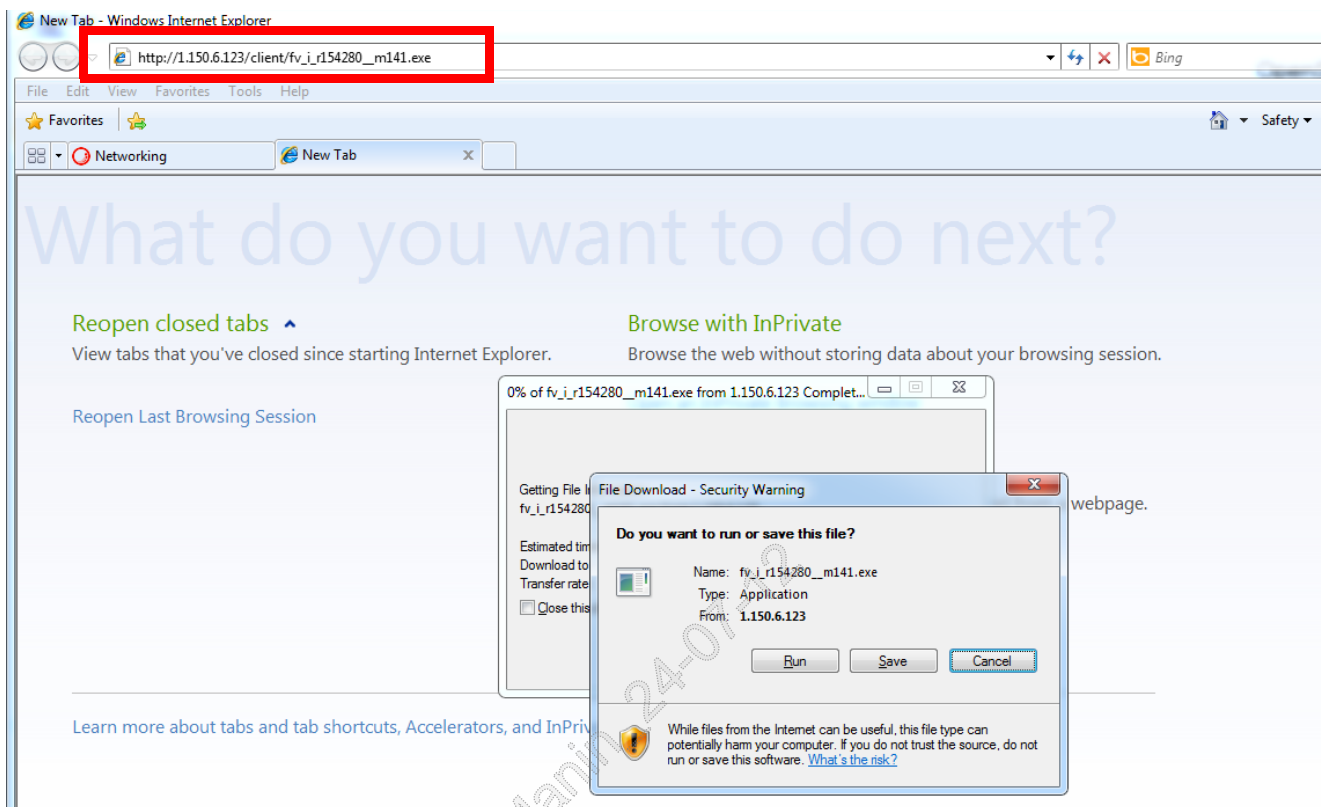
Your conference ID for this conferenc
e is 1

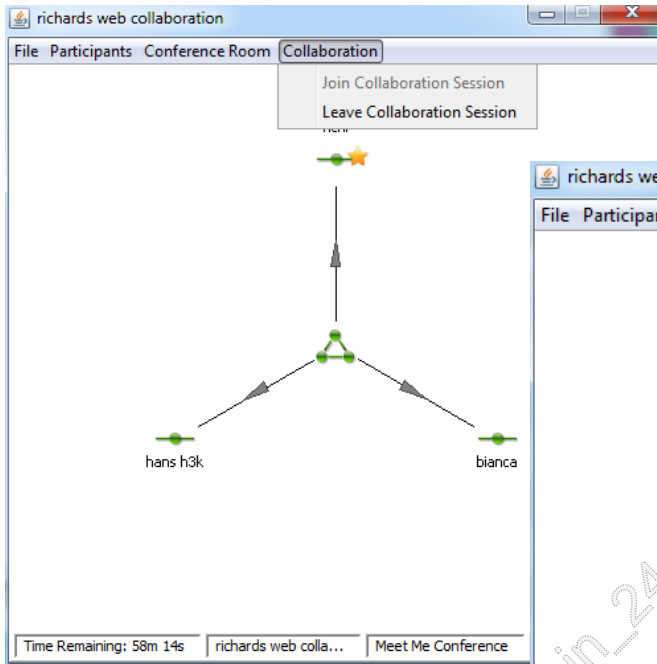
Your Collaboration URL is http://1.150.6.123/client/fv_i_r154280_m141.exe

Please do not disclose any information found within this email
.

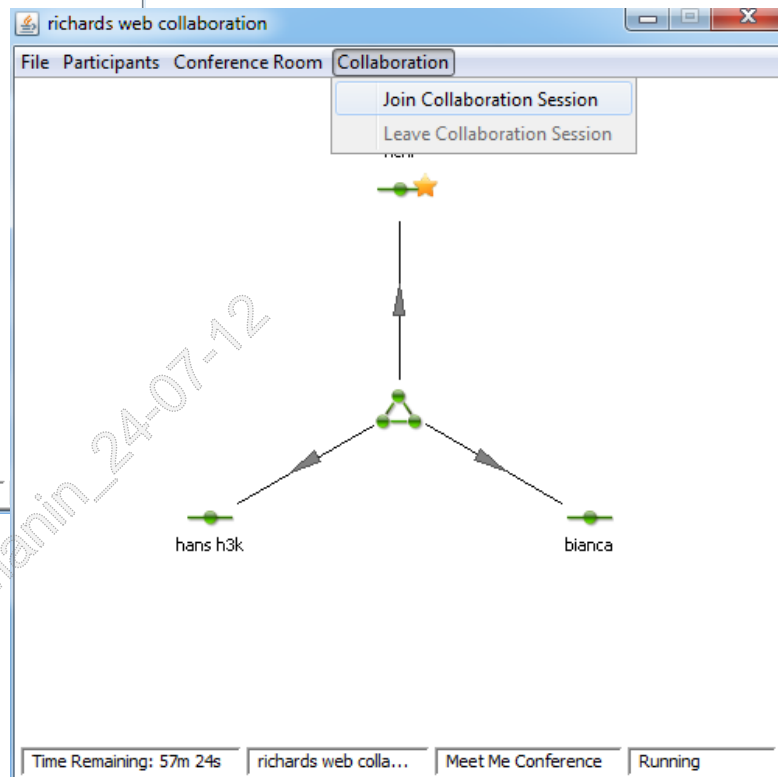
Regards,

OpenScape Office





Automatically started with the voice conference...



start web collaboration, if not automatically started...

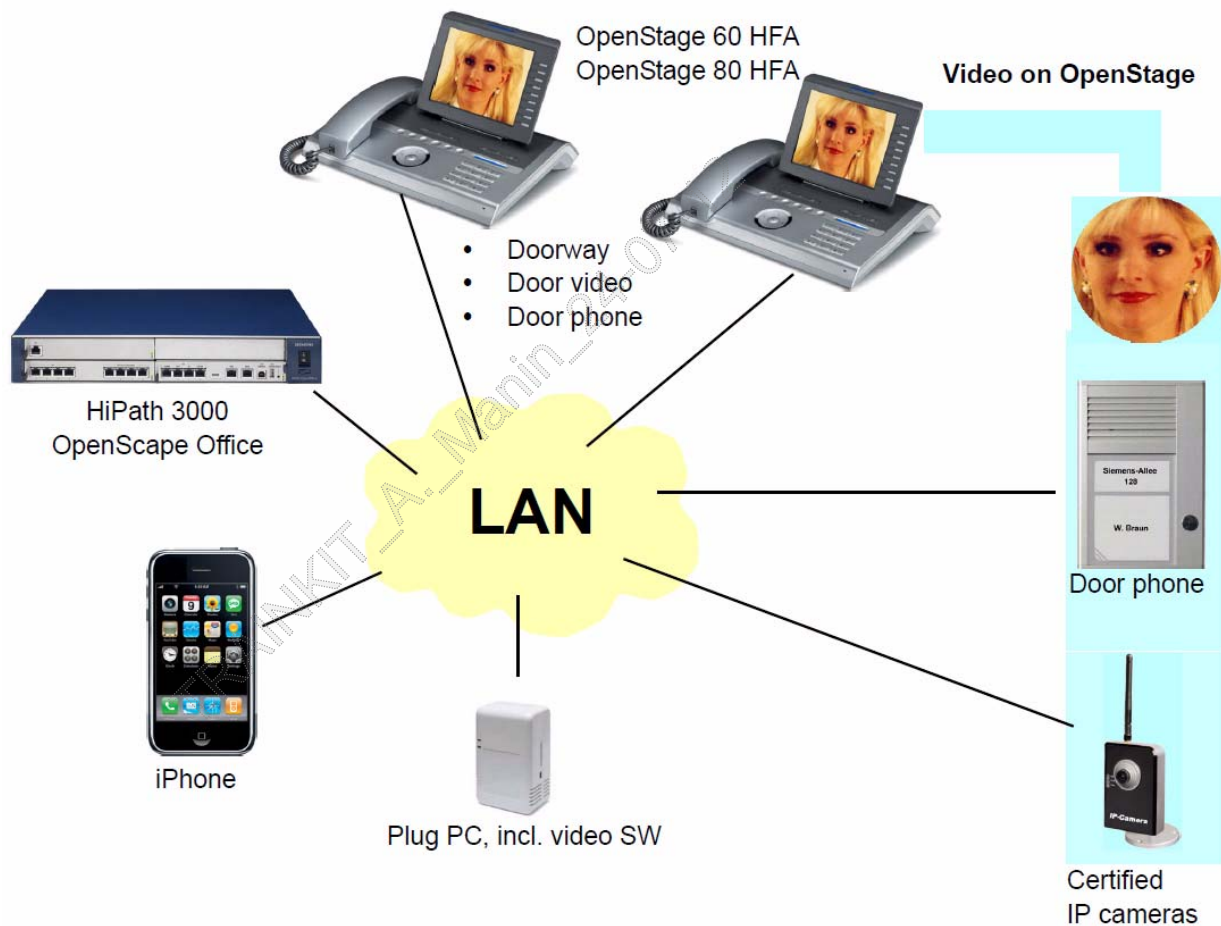


Assuming, the conference has been activated with web collaboration support and the myPortal Client has been opened, the web collaboration will start automatically.

4 OpenStage Gate View

OpenStage Gate View combines video surveillance with the communication system. An external Plug PC is used for streaming video signal to OpenStage phones. Maximal 2 phones can be streamed by one camera.

The following example shows a typical deployment scenario, where the video camera is used as an extension to an existing door phone.



4.1 Overview of Functions

Enables the combination of voice, video and the door-opening function via a single device.

Overview:

- OpenStage 60/80 HFA (max. 2 phones per camera)
- The iPhone connection enables video to be displayed on the move
- Modular in structure and integrated with previously made investments for infrastructure or installed equipment
- Administration via WBM
- Low maintenance overhead

4.2 Installation

The following gives you an overview of the installation process.

4.2.1 Prerequisites

- Delivery package
 - PlugPC Server
- Available devices
 - IP phone
 - OpenStage 60/80 HFA with SW version V2 R0.48.0 or later
- PC for configuration
- IP camera > see list of certified cameras at wiki.siemens-enterprise.com or Administration Manual „OpenStage Gate View“.

4.2.2 Installation in Three Steps

- Step 1: Plug PC Server
- Step 2: IP Camera
- Step 3: IP Phone (e.g., OpenStage 60 HFA)



For details, please refer to the Administration Manual - „Installation“.

TRAINKIT_A._Manin_24-07-12

5 Setting up a VPN configuration

Prerequisites:

The DSL connections are enabled and login information is available to you.

A DynDNS account is set up for each OpenScape Office system and the login information are available to you.

For VPN a DynDNS account is also required per Microsoft XP Client software.

Licenses:

The basic OpenScape Office package contains the licenses IPsec and LWCA among others.

The teleworker software NCP Client, including licenses, is available to you.

The teleworker Microsoft XP Client software for VPN is available to you.

Details in the respective chapters!



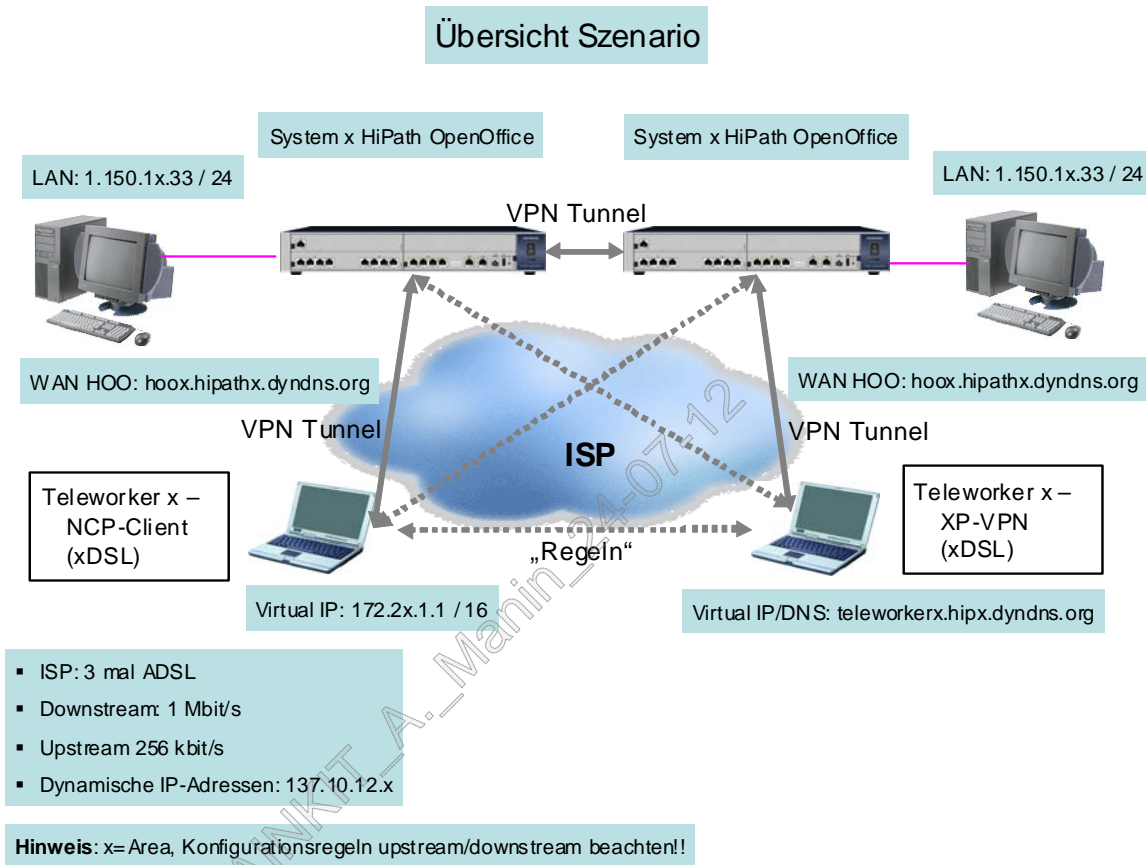
A maximum of 50 teleworker workstations can be connected via VPN per OpenScape Office system.

5.1 Procedure

- DSL configuration with variable IP addresses and “DynDNS”.
Explanation: DynDNS is an additional service for assigning dynamic IP address host names (FQDN). Despite a changing IP address at the WAN port, connectivity by the “Full Qualified Domain Name” is thus possible.
- Central configuration should be prepared. The configuration created should be imported on the respective VPN peers.
- VPN capability should be activated on the two systems.
- The first configuration example shows the tunnel setup via Pre-Shared Key.
- Internet access should be set up for the enterprise network.
- Startup of NCP client and/or Microsoft Standard Client (teleworkers) and the associated tunnel and rules in accordance with the following guidelines:
 - Communication of the VPN client with the OpenScape Office target system provided for that purpose
 - Enable communication between the VPN clients.
 - Provide Internet access for the VPN client.

- **Add-on Expert Level:** A LightWeight CA should be activated, relevant peer certificates and a CRL list are generated. X.509- and PKCS#12 certificates should be exported and imported.

Overview of infrastructure:



As soon as VoIP is also deployed over a combined VPN and Internet gateway, one-sided interference with the voice data can occur. The reason is that the downstream Internet traffic (Internet -> OpenScape Office) cannot be influenced by the OpenScape Office. If, therefore, VoIP packages and data packages are routed at the same time from the Internet in the direction of OpenScape Office and the downstream transmission rate of the DSL line for the incoming data is not sufficient, package losses in the ISP can occur. If the ISP supports QoS, these package losses can be avoided for prioritized data (e.g. voice).



Note:

“Inbound” (downstream) bandwidth control in the OpenScape Office allows prioritized handling of VoIP packages inside the OpenScape Office.

The bandwidth available in each case for VoIP and data from OpenScape Office in the direction of the Internet (upstream) can be configured. As a result, only the Internet downstream constitutes an incalculable interference factor that cannot be influenced.



Carry out a “backup” before beginning work!

Never activate IPsec before all rules required for trouble-free operation have been established. The rules act like firewall entries and can limit access to the module. If it ever happens that IPsec is activated prematurely and you no longer have access to the system as a result, you can reset the system with “Reload”.

5.1.1 DSL configuration

5.1.1.1 Configure the WAN port of OpenScape Office.

Details for authentication will be provided by your lecturer.

WAN: DSL connection type PPPoE

IP Parameters

Partner IP address of the PPP connection:	1.0.0.2
Local IP address of the PPP connection:	1.0.0.1
Max. data packet length (Bytes):	1492
IP address negotiation:	<Default>

General PPP parameters

Default router:	Yes
Internet access with DNS request:	Yes
Name of the Internet Service Provider:	Name of ISP
PPP standard header:	Yes
IP header compression:	No
Send LCP Echo demand:	Yes

Automatically connect PPP: Yes

Automatically reconnect PPP: Yes

Short-Hold

Short-Hold mode: No

Short-Hold time (s): No input

Authentication

PPP authentication: Yes

PPP user name: As assigned by the ISP

PAP authentication mode: PAP client

PAP password: As assigned by the ISP

CHAP authentication mode: Not used

CHAP password: No input

Data compression

STAC data compression: No

MPPC data compression: No

Address translation

NAT: Yes

Address mapping: No

QoS parameters of the interface

Bandwidth of the connection (kbit/s): 256 (as agreed by the ISP)

Bandwidth control for voice connections: Yes, inbound and outgoing

Bandwidth for voice/fax connections (%): 80

QoS capabilities: Identical

Notes on the fields:

The presettings for “**Partner IP address of the PPP connection**” and “**Local IP address of the PPP connection**” should not be changed, even if “**IP address negotiation**” is set to “Request new IP address”. These entries are necessary so that the PPPoE interface can be set up if no IP address is available yet for the PPPoE interface.

“Default router: Yes” means that the entire IP data traffic is routed in external IP subnetworks (e.g. Internet). **“Default Routing via: DSL”** is then shown in the menu item **“Explorer > Routing > IP Routing > (right mouse key) Default Router”**. The specification of the IP address **“1.0.0.1”** of the default router has no relevance here.

A prioritization for Voice over IP is set by activating **“Bandwidth control for voice connections”**. Only as many calls are allowed as bandwidth is available. The selection of **“inbound and outgoing”** is recommended in order to always give priority to VoIP packages from the perspective of HiPath.

The correct value for the upstream speed of the Internet connection must be specified in **“Bandwidth of connections (kbit/s)”** for this.

The specification in **“Bandwidth for voice/fax connections (%)”** specifies the restriction of what percentage of the bandwidth may actually be used for Voice over IP.

9. **Configure “Automatic Control of Disconnect (ACD)”** (automatic control of the connection cleardown) so that the disconnection of the DSL PPPoE connection is not carried out by the Internet Service provider (i.e. every 24 hours) at an unfavorable point in time. A time of 3 o'clock in the morning (hour = 3, minute = 0, second = 0) is selected for the disconnect and reconnect in our example:
See also **“Change ACD”** in the Administration Manual.

ACD configuration

Connection time: (only display of the connection time)

Force reconnect at: 3:00

Now click on **“Apply”**.

6 VPN Exercise - Site to Site via “PSK”

Starting point:

The OSO and the teleworkers are connected with the Internet Service Provider (ISP). First “Site to Site” startup of the OSO systems should be carried out. In addition, the teleworkers should be subsequently connected. DynDNS Accounts are already preconfigured and are available for following Dynamic Hosts - Scenario APT Munich:

- hoox.hipx.dyndns.org - x=1 to 6
- teleworkerx.hipx.dyndns.org - x=1 to 6

Your lecturer will provide the password for the DynDNS login.

Aim:

- Site to Site networking of the systems (OSO).
- Central configuration -> Advantage: All systems and teleworkers are configured on one system. The "roll-out" of the configuration for the VPN peers is then carried out. Required tunnels and rules are automatically created.

6.1 Site to Site networking of the OSO

This exercise requires teamwork! Create the central configuration - make an inventory of the systems. Two systems/areas work together and are split up as follows:

- System 1 -> for System 2
- System 3 -> for System 4
- System 5 -> for System 6

6.1.1 Configuration - System 5

Please adapt to your own infrastructure!

Configure the necessary settings in the VPN wizard. Example for System 5 - APT Germany.

Tip: Check settings in expert mode!

Setup > Wizards > Network / Internet > VPN Configuration > Configure VPN.

1. Dyn. DNS configuration if not yet carried out

IP-Adress-Zuordnung

Dyn. DNS

Benutzername:

Passwort:

Passwort wiederholen:

Hostname:

Domainname: ▼

2. Test DynDNS access

DynDNS-Zugang tester

3. If the test passed successful proceed with „OK“.

4. Add system(s) -> System 5 and System 6

System 5

Konfiguration und Zuordnung der Teleworker für System 5

System

Daten des eigenen Systems verwenden: ☒

aktiviert: ☒

System Name:

Adresstyp:

globale IP-Adresse/DNS-Name (WAN):

lokale IP-Adresse (LAN):

lokale Subnetzmaske (LAN):

Kommentar:

Teleworker

	Name	virtuelle IP Adresse	Kommentar
Hinzufügen	Neuer Eintrag		

Hilfe Abbrechen Zurück OK & Weiter Daten löschen

System6

System Selection					
	System name	global IP-Address/DNS-Name (WAN)	Address Type	Comment	active
Add	New Entry				
Edit	System 5	hoo5.hip5.dyndns.org	DNS Name	local System	✓

System 6

Konfiguration eines neuen Systems und Zuordnung der Teleworker

System

Daten des eigenen Systems verwenden: ☐

aktiviert: ☒

System Name: System 6

Adresstyp: DNS-Name

globale IP-Adresse/DNS-Name (WAN): hoo6.hip6.dyndns.org

lokale IP-Adresse (LAN): 1.150.16.33

lokale Subnetzmaske (LAN): 255.255.255.0

Kommentar: target system

Overview:

System auswählen					
	System Name	globale IP-Adresse/DNS-Name (WAN)	Adresstyp	Kommentar	Status
Hinzufügen	Neuer Eintrag				
Bearbeiten	System 5	hoo5.hip5.dyndns.org	DNS-Name	local System	●
Bearbeiten	System 6	hoo6.hip6.dyndns.org	DNS-Name	target system	●

5. Security settings for connections -> "PreShared Secret" - sufficiently long and sufficiently secure in accordance with the guideline!

Security setup for connections					
from	to	PreShared Secret	Repetition of the PreShared Secret	Comment	active
System 5	System 6	Event	✓

Explanation: The negotiation of the security settings for the tunnel setup always takes place between the tunnel end points. To enable the setup of the VPN tunnel, the tunnel end points always use the same "PSK"!

6. Export the topology data. Use a sufficiently long and secure password!

VPN Status Information

VPN is switched off ☐

System name	Local LAN/Teleworker Name	IP Address/DNS Name	active
System 5		hoo5.hip5.dyndns.org	—
	System 5-LAN	1.150.15.33	—
System 6		hoo6.hip6.dyndns.org	—
	System 6-LAN	1.150.16.33	—

24-07-12

Help Abort Back OK & Next **Export/Import** Configuration of VPN VPNOn

Explanation: The encrypted configuration data are provided with a checksum (CRC). The purpose is to be able to detect a defective configuration file.

Please keep the key secure! It will be required for importing the topology data.

Note: The centrally generated topology data must be made available to the respective VPN peers!

6.1.2 Configuration of System 6

Please adapt to your own infrastructure!

Configuration of the other peers (2 + X). Use the previous example in order to derive the approach!

1. Check/configure the Internet access.
2. Activate the DynDNS function.
3. Import the previously backed up topology data (*.zip file - document layout: xml but **encrypted!**)
4. **Activate "VPN" in all systems.**
5. To check the routing function over the setup tunnel, you can start *ping* and/or *tracerroute* on the IP address of the counterpart station. Make sure you use the correct gateway!
Also check access to the Internet: <http://kb.iandc.training.com>
(APT Germany - Please adapt to your own infrastructure!)

TRAINKIT_A._Manin_24-07-2012

6.1.3 Expert-Mode: VPN specification Tunnel - Rules

Check the automatically generated tunnel and rules in Expert Mode.

Tunnel - Functionality:

The screenshot displays the Siemens VPN configuration interface. On the left is a tree view of the configuration hierarchy, including 'Sicherheit', 'VPN', 'Tunnel', and 'Regeln'. The 'Aktive Tunnel' configuration is selected. The main panel shows the 'Tunneldaten anzeigen' tab, which is divided into 'Allgemein' and 'Security' sections. The 'Allgemein' section displays the tunnel name 'System 5--System 6' and the endpoints for both local and remote tunnels. The 'Security' section shows the proposed security protocol (ESP), encryption algorithms (AES, DES, 3DES), hash algorithms (MD5, SHA1), and session key handling. The 'Zugehörige Regeln' section lists the associated send and receive rules.

Aktive Tunnel	
Tunneldaten anzeigen	
<input checked="" type="radio"/> Tunneldaten	<input type="radio"/> Schlüsseltauschdaten
Allgemein	
Name des Tunnels: System 5--System 6	
Endpunkttyp des lokalen Tunnel: DNS-Name	
Endpunktadresse des lokalen Tunnel: hoo5.hip5.dyndns.org	
Endpunkttyp des Remote Tunnel: DNS-Name	
Endpunktadresse des Remote Tunnel: hoo6.hip6.dyndns.org	
Security	
Vorgeschlagenes Sicherheitsprotokoll: ESP	
Vorgeschlagene Verschlüsselungsalgorithmen: AES, DES, 3DES	
Vorgeschlagene Hash-Algorithmen: MD5, SHA1	
Session-Key-Handhabung: Automatisch, mit dem IKE-Protokoll	
Vorgeschlagene Lebensdauer der Session-Keys: 10 Min.	
Vorgeschlagene Lebensdauer der Schlüsseltausch-Session: 10 Min.	
Vorgeschlagene Datenvolumen der Session-Keys: unbegrenzt	
Zugehörige Regeln	
Zugehörige Senderegeln: - 2000 - 2001 -	
Zugehörige Empfangsregeln: - 2002 - 2003 -	

Explanation Tunnel data: The "method of operation" of the IP Security Protocol (IPSec) is defined here. Authentication is carried out by the "PSK" procedure. For additional information, see IPSec architecture.

Notes on the fields:

- End point address of the local tunnel contains the DynDNS name of the own WAN interface.
- End point address of the remote tunnels contains the DynDNS name of the WAN interface of the counterpart station.
- Preset encryption and hash algorithms. DES is only still listed for reasons of compatibility and should no longer be used as encryption algorithm.
- "PFS": PFS is used in the public key infrastructure. Any later derived compromised keys of "suspects" are inoperative.
Only Expert: With PFS, additional key exchange material must be included in order to negotiate Phase 2 of a hunt group. Phase 2 proceeds in so-called "Quick Mode".
- Select pre-shared keys (PSK) as the authentication procedure for VPN peers. A sufficiently long and secure password for the pre-shared key must be selected! Note these data. The same password must also be entered in the tunnel in the counterpart system.
- Diffie-Hellman Groups
Explanation: Define the length of the public key.

Rules - Functional Operation, e.g. "2000":

Basically (Host: 0.0.0.0) packages are sent to the WAN interface (hoo6.hip6.dyndns.org) over the tunnel (system5--system6) (PASS_OUTGOING) here.

Prerequisite: Successful authentication via "PSK".

Regel anzeigen	
Priorität:	2000
Dienst:	Beliebiger Dienst
Aktion für die Regel:	PASS_OUTGOING
Verschlüsselung erforderlich:	Ja
Regel-Status:	Aktiviert
Quelladresse	
Typ:	Host
IP-Adresse:	0.0.0.0
Zieladresse	
Typ:	DNS-Name
DNS-Name:	hoo6.hip6.dyndns.org
Tunnel für die Verschlüsselung	
Tunnel auf der Empfangsseite:	Keine Tunnelzuordnung
Tunnel auf der Sendeseite:	system 5--system 6

- **Priority:** The highest priority is 1 and the lowest 65000. In this case the priority 2000 is assigned. The rules for the source and target address are worked through according to their priority, i.e. if a matching rule to the target is found, an exit is made.
- **Service:** Any Service - Pull-down menu: A service-specific restriction can be configured here.
- **Action For the Rule:** Pass_Outgoing - seen from the perspective of the OSO are packages in the outgoing direction.
- **Encryption required:** Data between the two subnetworks should naturally be encrypted. The encryption procedure was defined beforehand in the tunnel configuration.
- **Tunnel on the receiver side:** No tunnel is assigned. The entry is required for the counter rule.

- *Tunnel on the transmitter side:* The assignment of the previously defined tunnel is made here with the name "system 5--system 6". The assignment of the tunnel for the rule can be read as follows: "I, the source address Host 0.0.0.0 want to send data to the target address hoo6.hip6.dyndns.org. I send the data in the tunnel with the name 'system5--system6'.

Regel anzeigen	
Priorität:	2003
Dienst:	Beliebiger Dienst
Aktion für die Regel:	PASS_INCOMING
Verschlüsselung erforderlich:	Ja
Regel-Status:	Aktiviert
Quelladresse	
Typ:	Host
IP-Adresse:	0.0.0.0
Zieladresse	
Typ:	DNS-Name
DNS-Name:	hoo5.hip5.dyndns.org
Tunnel für die Verschlüsselung	
Tunnel auf der Empfangsseite:	system 5--system 6
Tunnel auf der Sendeseite:	Keine Tunnelzuordnung

Explanation:

Basically (Host: 0.0.0.0) packages from the tunnel to the WAN interface (hoo5.hip5.dyndns.org) are accepted here (PASS_INCOMING).

Prerequisite: Successful authentication via "PSK".

Note: The IPSec architecture is very complex and requires further know-how. A brief overview of individual components/functions is shown below:

- No "NAT" for tunnel packages is carried out from the perspective of the OSO.
- UDP Port 500 (ISAKMP/IKE) for the first connect is the "well known port".

- Form a unidirectional Security Association (SA) based on "ISAKMP" for Phase 1
- Internet Key Exchange (IKE) Protocol

Explanation: *IKE* describes the key administration and the key exchange procedure as a whole and adopts parts of various other protocols at the same time. The key exchange material is used, among other things, for forming an SA. The *ISAKMP* protocol essentially describes the format of the key exchange messages. The actual key exchange material is exchanged via IKE specification.

- Encapsulation security payload (*ESP*) in tunnel mode

Explanation: High security claim through full authentication/encryption (exception: router-relevant data) in *ESP* and additional "Outer IP Header" in tunnel mode.

- Encryption and hash algorithms - e.g. RSA and SHA1.
- Perfect Forward Secrecy (*PFS*) for use in PSK and Public Key Infrastructures

Explanation Greater security through additional key exchange material!!

Expert only: Normally all required keys originate from the one Diffie-Hellman "Basis key" that was negotiated at the beginning of IKE Phase 1. For the use of PFS an own Diffie-Hellman key exchange is carried out in IKE Phase 2. This means that the 4 keys for the IPsec SAs originate from an own Diffie-Hellman "Basis key" and no longer from the Diffie-Hellman-"Basis key" from IKE Phase 1. Thus the keys of the two IPsec SAs are independent of the keys of the IKE SA. Also, on each rekeying of the IPsec SAs, a new Diffie-Hellman key exchange is always carried out so that also consecutive keys for the IPsec SAs are independent of one another.

This brings increased security: After compromising a Diffie-Hellman "Basis key" many less keys are compromised than without the use of PFS.

6.1.4 Maintenance

- For diagnostic purposes, use the preconfigured trace profile "VPN".
- Detail traces via XTracer and/or TCP dump.

Attention: XTracer should only be used temporarily for diagnostic purposes. Don't forget deactivation!

7 Teleworkers

The OSO system gives the option of connecting up to 50 teleworkers. For teleworker setup in the HOO, a distinction is made fundamentally between:

- Setup via Assistant > “VPN Configuration” - through “Smart Trained Technician”
 - Variant 1: Internet access with fixed IP address - recommended!!
 - Variant 2: Internet access with variable IP address - DynDNS is required!!
 - Assignment of the teleworkers to the respective system - e.g. Teleworker 5 to System 5
 - Configuration for “Authentication”
 - Virtual IP or DynDNS name
 - PreSharedKey - later: Digital Signatures

Conclusion: Configuration via wizard allows simple implementation of teleworkers based on the authentication procedure of “PreSharedKey” (abbreviated as PSK). Additional functions such as a Public Key Infrastructure (abbreviated as PKI) with X.509-based certificates are not possible (e.g. Certificate Revocation List).

Recommendation: A PKI infrastructure is to be used to cater for increased requirements on security and configuration. OSO Expert Mode provides the option of creating and administering a complete PKI infrastructure. Setup of a “Digital Signature”-based environment only in “Expert Level”.

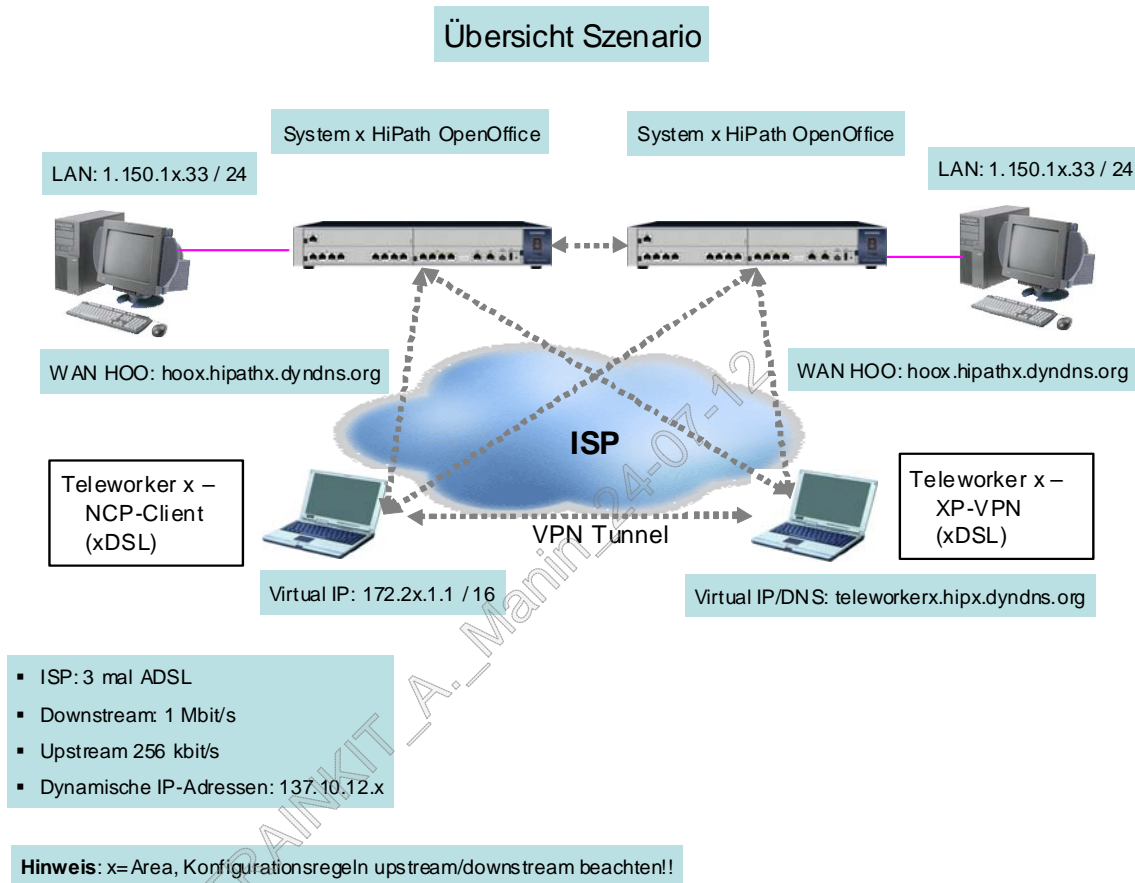


Note:

Additional knowledge on the construction and administration of security structures in the enterprise is required. More advanced courses are therefore recommended, e.g. Siemens APT HG15IPSECS.

Starting point:

The OSO and the teleworkers are connected with the Internet (ISP). As VPN client the solution of "NCP Client" and "Windows VPN Client" should be used.



Aim:

- Startup of the teleworkers
- Global connectivity (meshed VPN peers).
- Central configuration -> Advantage: All systems and teleworkers are configured on a system. The "roll-out" of the configuration for the VPN peers is then carried out. Required tunnels and rules are automatically created.
- Import of the topology data at the VPN Client

7.1 Teleworker Exercise

This exercise requires teamwork! Creating the central configuration - two systems/areas work together and are partitioned as follows:

- System 1 - for System 2 and teleworkers
- System 3 - for System 3 and teleworkers
- System 5 - for System 6 and teleworkers

Configure the necessary settings in the VPN wizard. Example for System 5 and 6 incl. Teleworker 5 and Teleworker 6 - APT Germany.

Tip: Check settings in expert mode!

Setup > Wizards > Network / Internet > VPN Configuration > Configure VPN.

1. Dyn. DNS configuration if not yet carried out
2. Test DynDNS access
3. Add teleworkers -> System 5 and System 6

Note: Windows VPN Client requires DynDNS authentication! See Startup of Windows VPN Client.

Add Teleworker 5 to System 5

Konfiguration und Zuordnung der Teleworker für System 5

System

Daten des eigenen Systems verwenden: ☒

aktiviert: ☒

System Name:

Adresstyp:

globale IP-Adresse/DNS-Name (WAN):

lokale IP-Adresse (LAN):

lokale Subnetzmaske (LAN):

Kommentar:

Teleworker

Name	virtuelle IP Adresse	Kommentar
Neuer Eintrag		

Hinzufügen

Hilfe Abbrechen Zurück OK & Weiter Daten löschen

Konfiguration des Teleworker Teleworker sys 5

Name:

Adresstyp:

virtuelle IP Adresse/DNS-Name:

System:

Kommentar:

aktiviert: ☒

Add Teleworker 6 to System 6

Konfiguration und Zuordnung der Teleworker für System 6

System

Daten des eigenen Systems verwenden: ☐

aktiviert: ☒

System Name:

Adresstyp:

globale IP-Adresse/DNS-Name (WAN):

lokale IP-Adresse (LAN):

lokale Subnetzmaske (LAN):

Kommentar:

Teleworker

	Name	virtuelle IP Adresse	Kommentar
Hinzufügen	Neuer Eintrag		

Caution: Microsoft VPN Client only with DynDNS!!

Konfiguration des Teleworker teleworker 6

Name:

Adresstyp:




virtuelle IP Adresse/DNS-Name:

System:

Kommentar:

aktiviert: ☒

4. Security settings for connections for System 5 and 6 to teleworkers -> "PreShared Secret" - sufficiently long and sufficiently secure in accordance with the guideline!

Sicherheitseinstellungen für Verbindungen					
	von	nach	Sicherheitseinstellung	Kommentar	Status
Bearbeiten	System 5	System 6	vorhanden	optional	
Bearbeiten	System 5	Teleworker	vorhanden	info:psk	
Bearbeiten	System 6	Teleworker	vorhanden	info: psk	

Note: Use different "PSK" for each tunnel!

5. On System 5: Export the topology data from "Teleworker" and "System".

VPN Status-Informationen

● VPN ist eingeschaltet

System Name	Lokales LAN/Teleworker Name	IP-Adresse/DNS-Name	Status
system 5		hoo5.hip5.dyndns.org	●
	system 5-LAN	1.150.15.33	●
	teleworker 5	172.25.1.1	●
system 6		hoo6.hip6.dyndns.org	●
	system 6-LAN	1.150.16.33	●
	teleworker 6	teleworker6.hip6.dyndns.org	●

Hilfe Abbrechen Zurück **OK & Weiter** **Export/Import** VPN konfigurieren VPN ausschalten

Exportieren und Importieren von VPN Konfigurationsdaten

Exportieren der Teleworker-Daten vom System

Schlüssel: Schlüssel wiederholen: Export

Exportieren der Topologie-Daten vom System

Schlüssel: Schlüssel wiederholen: Export

6. The centrally generated topology data (from System 5) must be made available to respective VPN peers and teleworkers!
7. Import the topology data on System 6 in order to enable communication to Teleworker 6 (Windows VPN).

Note: Topology data of the teleworkers can be used for the simplified startup of the NCP Client and Windows VPN Client. Refer to the "readme" for details.

7.1.1 Configuration NCP Client - Example Teleworker 5

Starting point:

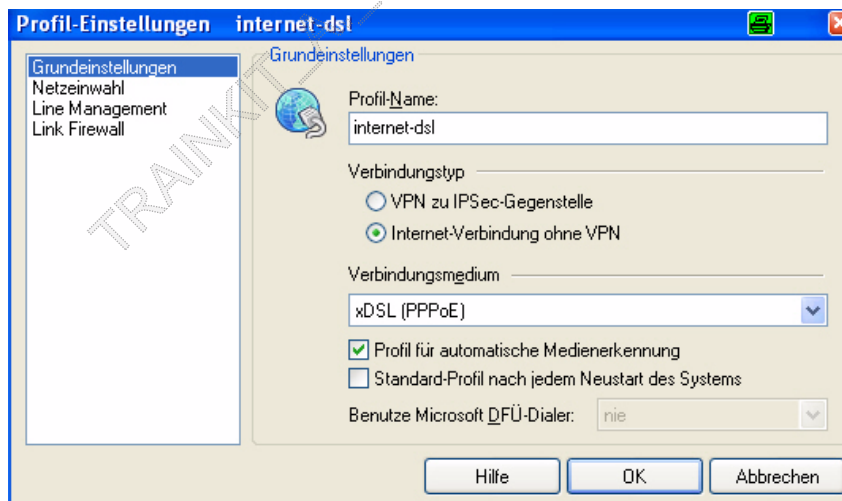
The license-based NCP client software is available. Internet access is available on the client computer - e.g. PPPoE directly from the xDSL modem. Topology data are available.

Aim:

Startup of the NCP Client. The previously generated topology data should be used.

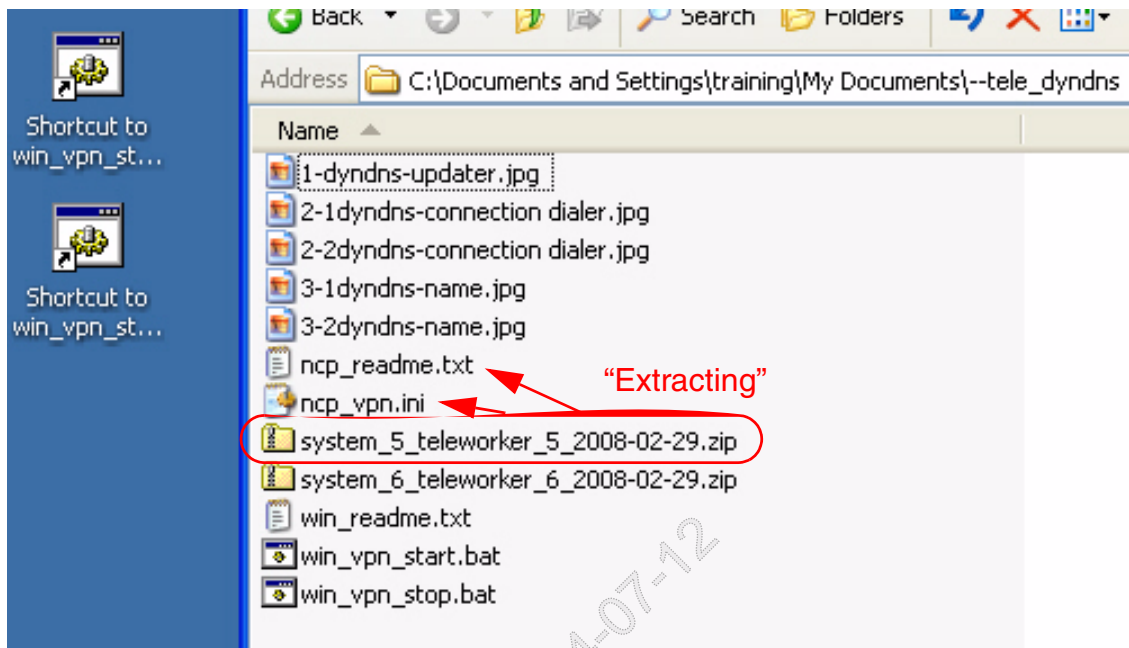
Startup:

1. Install the NCP client software. Use APT Munich "APT-PC" of the respective area!
2. Start the installation with "*.exe" > Default setup incl. compatibility test.
3. Restart computer.
4. NCP Secure Entry Client:
5. Configure a new profile for the Internet connection (without VPN)
6. Dial the connecting medium - e.g. xDSL (PPPoE) incl. network dial-in. APT Munich: Ask your lecturer.



7. Profile should be the default for automatic media detection.
8. If necessary: Configure Inactivity Timeout to "Always On" (max. 65356 sec.)!

9. Extract the previously exported topology data for system5_teleworker_5.



10. Import the previously generated topology data.

NCP Secure Entry Client

Verbindung Konfiguration Log Fenster Hilfe

Profil: internet-dsl

Profil-Einstellungen
Firewall-Einstellungen
WLAN-Einstellungen

Amt
Zertifikate
Verbindungssteuerung
EAP-Optionen
Logon Optionen
Konfigurations-Sperren
Profil importieren
Hotspot

Verbindungsart: xDSL

Statistik:
Daten (Tx) in Byte: 331
Daten (Rx) in Byte: 0,000
Durchsatz (kB/s): 0,000

Software ist nicht aktiviert (noch 30 Tage gültig)

Profil Import Assistant

Importdatei wählen
Aus welcher Datei soll die Konfiguration gelesen werden?

Bitte wählen Sie die Importdatei, aus der die neuen Profile eingelesen werden sollen. Die Importdatei muss mit dem vollständigen Pfad angegeben werden.

Dateiname:
C:\Dokumente und Einstellungen\training\Eigene Dateien\ncp_vpn.ini

Profil Import Assistant

Profile wählen
Welche Profile sollen importiert werden?

Die unten aufgeführte Liste beinhaltet alle Profile der Importdatei. Bereits existierende Profile werden durch den Import überschrieben.
Bitte markieren Sie die zu importierenden Profile der Liste.

Name	Status
HOOOME	Überschreiben

Profil Import Assistant

Profile importieren
Die Profile werden importiert.

Die ausgewählten Profile werden importiert und zu den aktuellen Profil-Einstellungen hinzugefügt.

PARAMETER "Name"	= HOOOME
PARAMETER "ConnMedia"	= automatische Medienerkennung
PARAMETER "Timeout"	= 0
PARAMETER "PriVoIP"	= ein
PARAMETER "Gateway"	= hoo5.hip5.dyndns.org
PARAMETER "IkeLTSec"	= 000:00:08:00
PARAMETER "IPSecLTSec"	= 000:00:07:00
PARAMETER "PFS"	= DH-Gruppe 2 (1024 Bit)
PARAMETER "IkeIdStr"	= 172.25.1.1
PARAMETER "Secret"	= #####

Fertigstellen

11. Test connection setup incl. logbook. System 5 and System 6 should be accessible.

Maintenance tip: Use the "XTracer" tool for the extended trace diagnostics!

Attention: XTracer should only be used temporarily for diagnostic purposes. Don't forget de-activation!

7.1.2 Configuration of Windows VPN Client - Example Teleworker 6

Starting point:

The import of the previously generated topology data has been carried out on the respective system (please adapt to your own area!). The support tools for Windows service pack 2 are available to you on the teleworker PC. Licensing for the VPN client is not necessary. Internet access is available on the client computer - e.g. PPPoE on the xDSL modem. Topology data are available. The dynamic host: teleworker6.hip6.dyndns.org" is created, the login information for the DynDNS access is available to you.

Aim:

Startup of the DynDNS function on the client PC - DynDNS Updater. Startup of the Windows VPN Client. The previously generated topology data should be used.



Note:

The helper tool "DynDNS Updater" can differ in function and view because of newer versions!

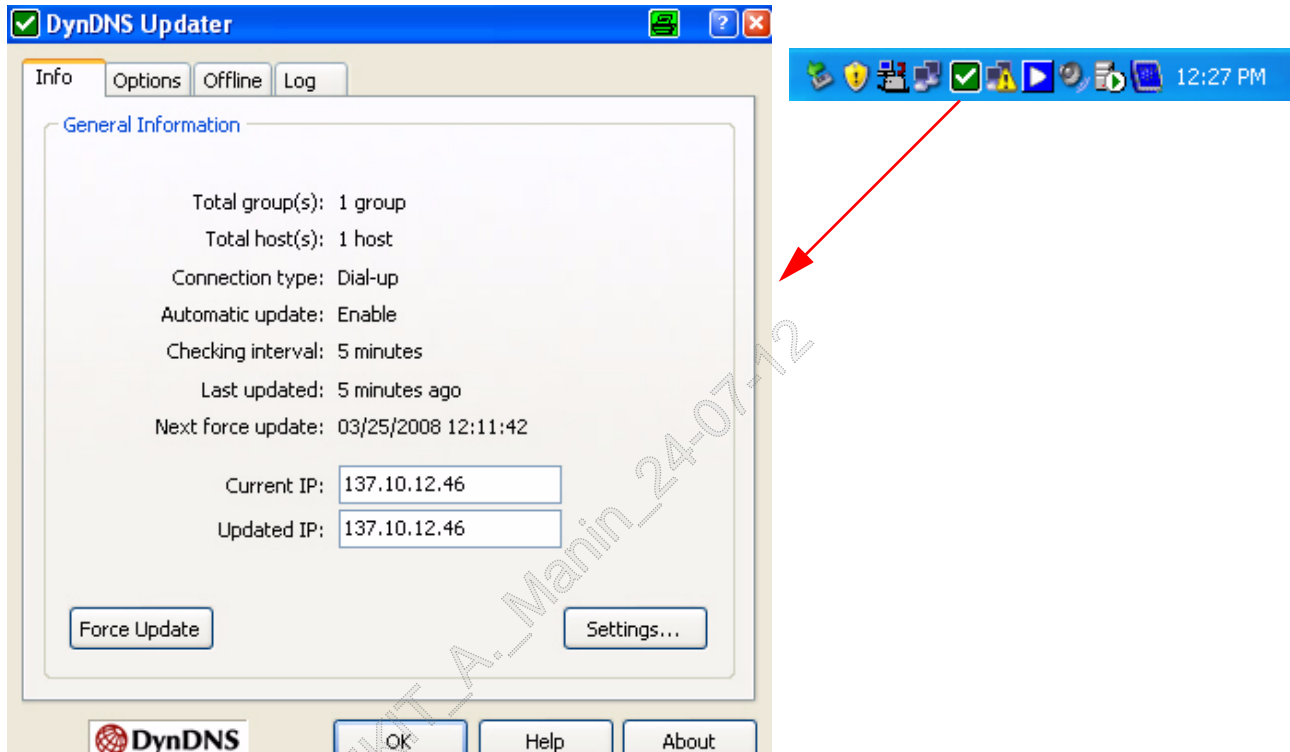


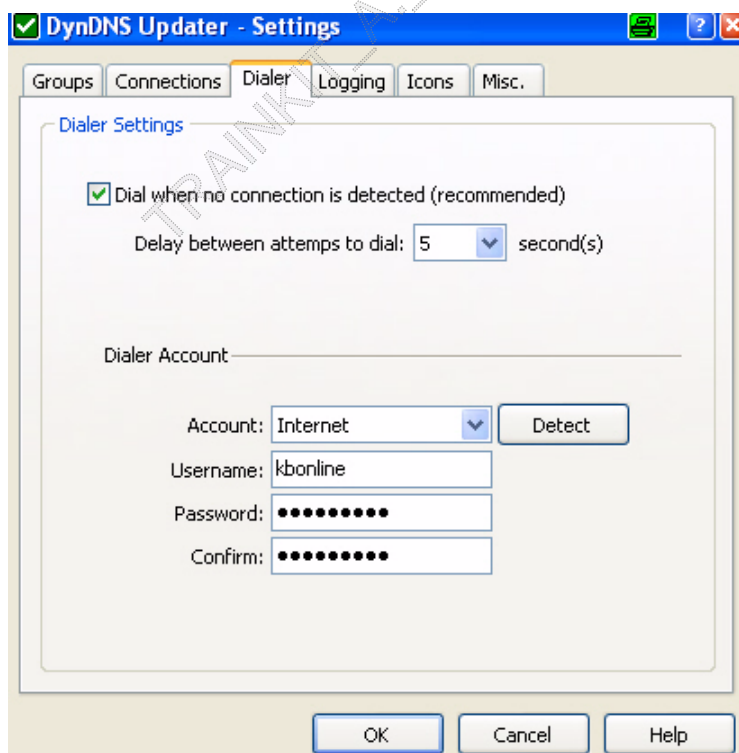
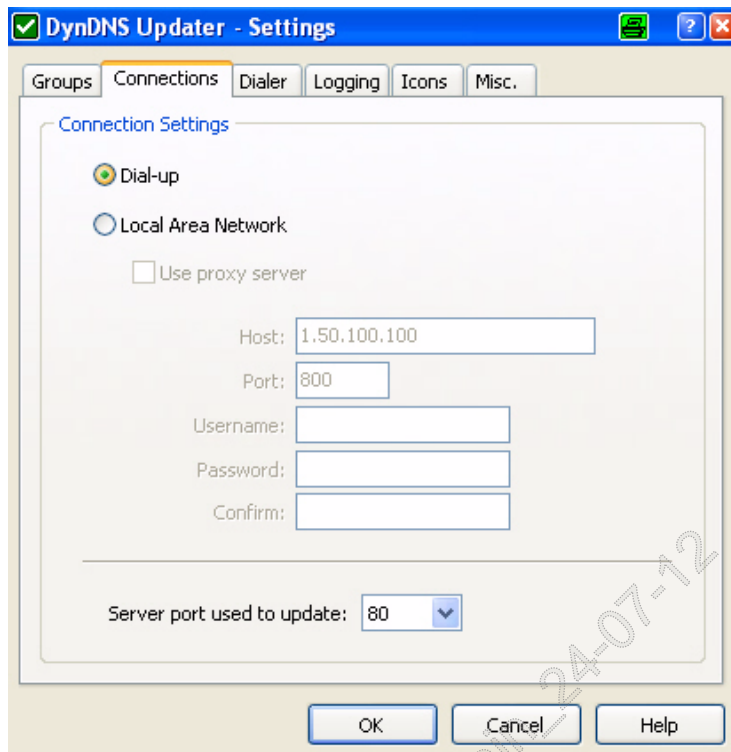
*Windows XP ServicePack 2 VPN client is currently only configurable via "DynDNS".
"Virtual IP address" is not currently supported.*

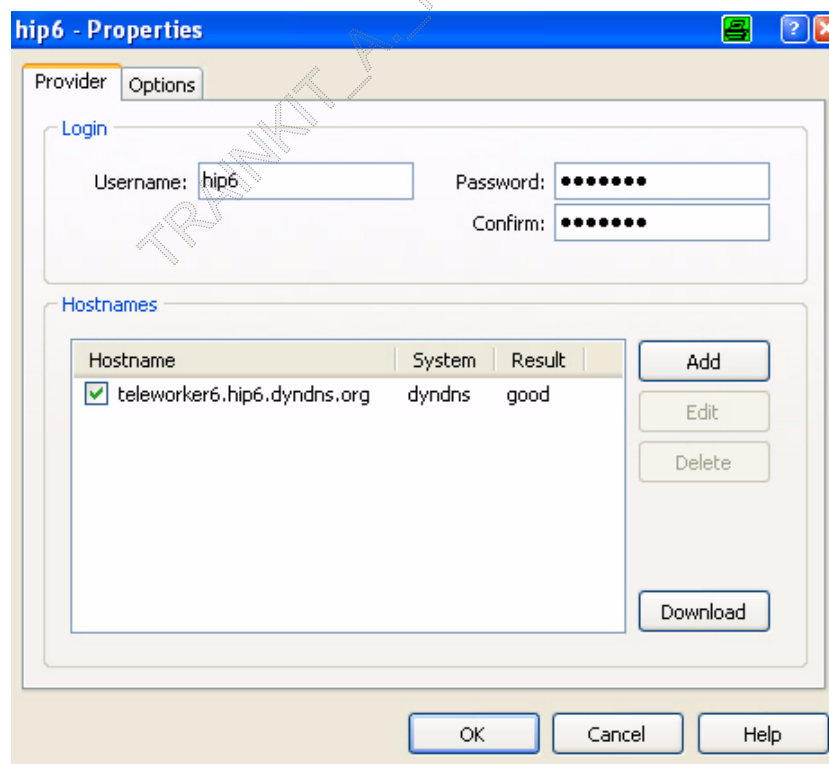
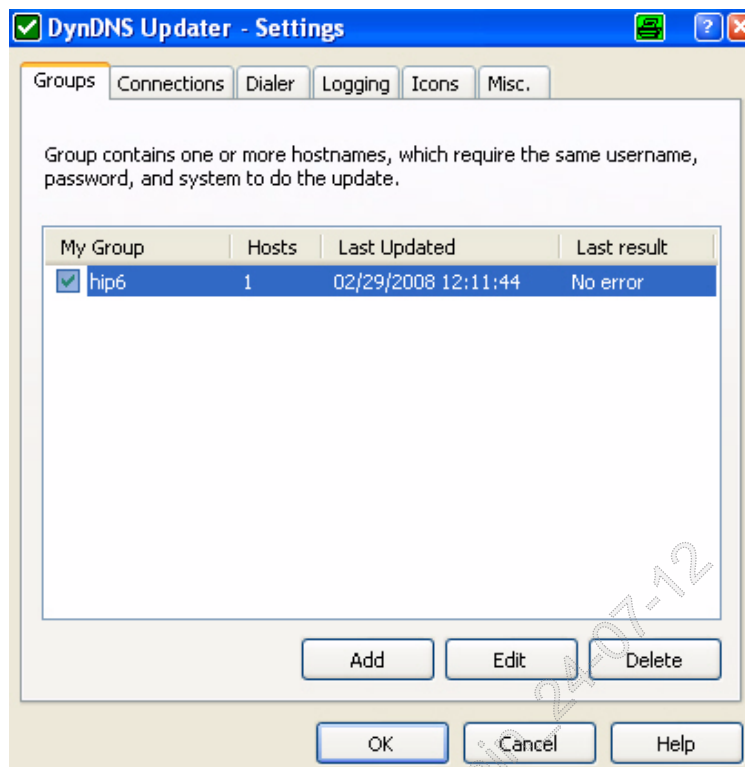
Startup:

1. Download of the "DynDNS Updater" software - available on the Internet, details at www.dyndns.org - APT Munich: Fileserver.

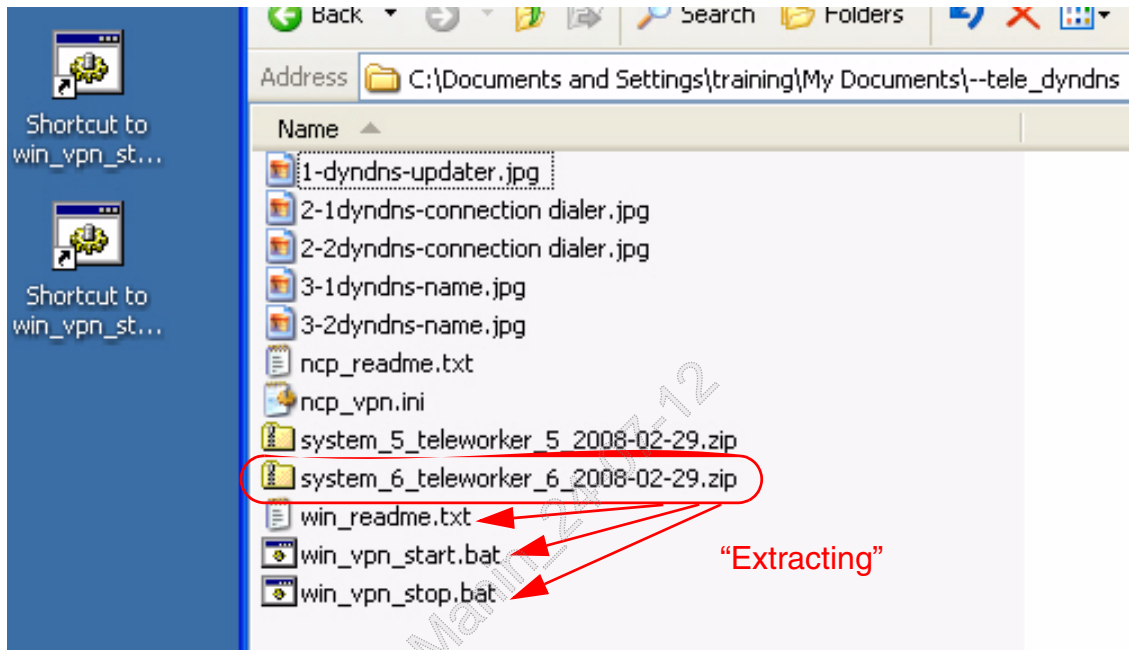
Note: The example shows the configuration after installation:







2. Install the current support tools for Windows on the client PC. Select "complete" as the set-up mode.
3. Restart computer.
4. Extract the previously exported topology data for system6_teleworker_6.



Refer to the information in the "readme".

5. Create shortcuts for the *.bat files - for convenient start/stop.
 6. Test connection setup: To activate the tunnel, start the executable file: win_vpn_start.bat
- Test the connection to the target system via "ping" and/or "tracerroute".

Maintenance tip: Use the "XTracer" tool for the extended trace diagnostics!

Attention: XTracer should only be used temporarily for diagnostic purposes. Don't forget de-activation!

Finished!!

8 VPN Exercise - Public Key Infrastructure (PKI) // draft//

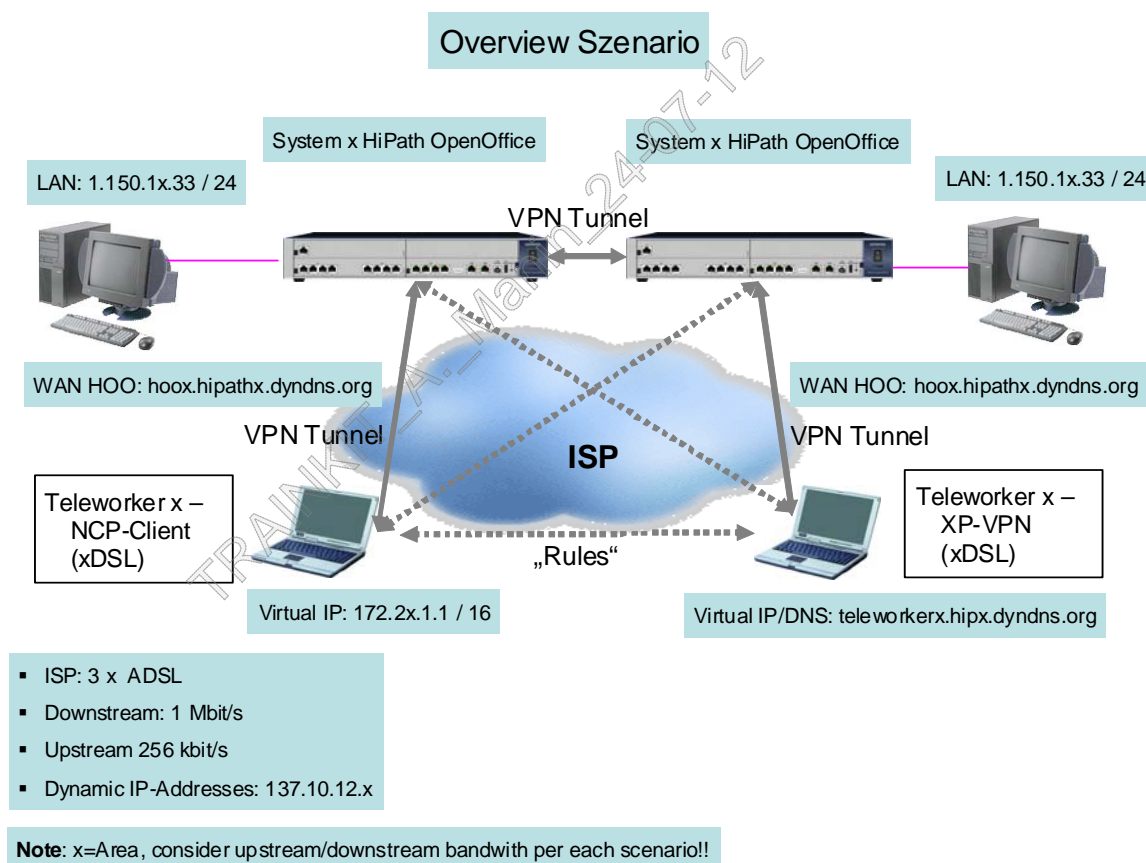
A “trustable” environment based on X.509v3 certificates is to be created in the following.

Starting point:

A functioning authentication that uses “PSK” is to be changed to “Digital Signatures”. The configuration can only be carried out in “Expert Mode”.

Advantage: Existing “rules” can be adapted and do not have to be completely recreated.

Overview of components



Procedure:

- Creation of a “Root CA” including “Trusted” certificates, “Peer” certificates, and Certificate Revocation List (CRL).
Note: The “Root CA” creates the necessary certificates and Certificate Revocation Lists for all VPN peers!
- Import the necessary certificates on the peers involved.
- Configuration of the tunnel.
- Assignment of the rules.

TRAINKIT_A._Manin_24-07-12

8.1 Tunnel setup with digital signatures

Assumption: System 5 should constitute the “Root CA” in the following example. Please adapt to your own infrastructure!

1. Generate a self-signed LightWeight CA certificate via the WBM administration of the HOO System 5:
Expert Mode - Telephony Server > Security > VPN > Lightweight CA > Generate CA Certificate” (see also Administration Manual “Generate CA Certificate”).

The certificate should contain the following data:

Name of the certificate:	IPsec LW CA
Serial number of the certificate:	1
Signature algorithm type:	sha1RSA
Certificate validity:	10 years
Length of the public key:	1536 bits
Country (C):	DE
Organization (O):	Siemens
Organizational unit (OU):	APT
Common Name (CN):	LWCA
Alternate applicant name:	Space for further information (alternative)
CRL distribution point	<info>

Notes on the fields:

- Assign an unambiguous name to the certificate. This makes identification considerably easier later.
- If the customer wants to configure teleworkers with VPN clients, please note that the VPN client supports the signature algorithm used in the system - RSA or DSA!
- Serial number: You can assign 1 as the serial number. Unambiguousness is ensured because this certificate is the first of this type.
Note: There is no correlation between an SSL CA and a LightWeight CA. The same thing applies to the server or peer certificates.
- The certificate validity cannot be subsequently extended!

2. Note the fingerprint of the created certificates.
3. Export the previously created, self-signed LightWeight CA as X.509 certificate:
Security > VPN > Lightweight CA > Desired Certificate > Export Certificate [X.509] - “Load” (see also Administration Manual “Export Certificate [X.509]”).

Save the certificate on a data carrier in the dialog that appears.

4. Now import the previously exported LightWeight CA certificate as Trusted CA Certificate in all HOOs of your network:
 Security > VPN > Certificate Administration > Trusted CA Certificate > Configured Certificates > Import Trusted CA Certificate [X.509] (see also Administration Manual: "Import Trusted CA Certificate [X.509]").
 Assign a meaningful name to the certificate, e.g. Trusted LWCA.

 During the import compare the fingerprint with the fingerprint noted in Step 2! Only if both fingerprints are identical, the certificate is trustable.
5. Generate an empty certificate revocation list:
 Security > VPN > Lightweight CA > Desired Certificate > "Generate Certificate Revocation List (CRL)" (see also Administration Manual "Generate Certificate Revocation List (CRL)").

Note: Example of empty CRL.

A practical validity period of a revocation list depends on the security requirements of the customer as it is probable that issued certificates must be entered in the revocation list (e.g. if access to the system is to be refused to a suspicious or terminated employee). High security - with a validity period of the revocation list of a few days means that a new revocation list must be generated, stored and imported into the HOO systems before the validity expires. The validity period in the example is 1 **year**.

Save the Certificate Revocation List on a data carrier.

6. Import the Certificate Revocation List in the Trusted CA certificate of all HOOs in your network:

Security > VPN > Certificate Administration > Trusted CA Certificates > Configured Certificates > Desired Certificate > Import Certificate Revocation List (CRL)
(see also Administration Manual “Import Certificate Revocation List (CRL)”).

Configured Certificates

Display Certificate Delete Certificate Display CRL **Import CRL**

Certificate Name: LWCA-Trusted
 Certificate Type: Self-Signed CA Certificate
 Serial Number of Certificate: 1
 Serial Number of Certificate (hex): 01
 Type of Signature Algorithm: sha1RSA
 Start Time of Validity Period (GMT): Wednesday, 03/19/2008 00:00:00
 End Time of Validity Period (GMT): Monday, 03/19/2018 00:00:00
 CRL Distribution Point: info - System 5

Issued by CA

Country (C): DE
 Organization (O): Siemens
 Organization Unit (OU): APT
 Common Name (CN): LWCA

Subject Name

Country (C): DE
 Organization (O): Siemens
 Organization Unit (OU): APT
 Common Name (CN): LWCA

This Certificate Revocation List can be displayed at any time. If, for instance, a certificate is to be defined as blocked for a teleworker, a new Certificate Revocation List must be created by the LightWeight CA that then contains this expired peer certificate. Then the new certificate list must be imported again in all trusted CA certificates.



Caution:

By definition a Certificate Revocation List (CRL) is not replaced before expiry of their validity. There would in fact be 2 valid CRLs then in circulation. This means that theoretically a “man-in-the-middle” attack could also be carried out after exchange of the certificates. Effective protection is offered by the relatively short validity (e.g. few days) of the CRL, but consequently also requires more frequent replacement of the CRL. Alternatively, the OSO can be incorporated in PKIs. LDAP access allows the system to call up the CRL from an external CA (PKI). The final deletion of the old CRL takes place only after a reset of the system. However the removal of the CRL from external components (theoretic attack scenario) is not ensured by this.

7. Generate a PKCS#12 peer certificate for all HOO and teleworkers in your network:



Note:

Each VPN peer requires a peer certificate for authentication! The teleworker certificates - in our example Teleworker 5 and Teleworker 6 - are created beforehand and activated during teleworker startup.

Security > VPN > Lightweight CA > Desired Certificate > Generate CA signed peer certificate [PKCS#12]

(see also Administration Manual “Generate CA signed peer certificate [PKCS#12]”).

The certificate should contain the following data:

Password:	Should be sufficiently long and secure
Serial number:	Always unique and greater than 1
Certificate validity:	e.g. 5 years
CRL distribution point:	Info element. Enter the URL of the HOO that issued this certificate. So at any time it is apparent from the certificate which Root CA issued the peer certificate.
Length of the public key:	1536 bits
Applicant:	Enter an unambiguous name, e.g. "HOOsys5" or "Teleworker5". The name of the applicant (CN) must be different from the CN of the applicant.

Export format (*.p12). Select a memory location on a data carrier for the certificate.

8. Note the fingerprint of the created certificates.
9. Import the PKCS#12 Peer Certificate previously generated and saved for each HOO in the relevant HOO system of your network:

Security > VPN > Certificate Administration > Peer Certificates > Import Peer Certificate [PKCS#12]

(see also Administration Manual “Import Peer Certificate [PKCS#12]”).

10. Set up a tunnel to the counterpart system:
You should use the already configured tunnel (orange) as a template - see Exercise “PSK”. Only the configuration of the “key exchange data” is different.
In our example System 5 must be configured in the following tunnel.

- Old: system 5 -- system 6 -> New: system 5 *PKI* -- system 6 *PKI*
- Old: system 5 -- Teleworker -> New: system 5 *PKI* -- Teleworker *PKI*

Configuration example for tunnel: system5 PKI -- system 6 PKI

Security > VPN > Tunnel > Configured Tunnel > Add Tunnel

Name of the tunnel:	system5 PKI--system6 PKI
End point type of the local tunnel	DNS name
End point address of the local tunnel	hoo5.hip5.dyndns.org
End point type of the remote tunnel:	DNS name
End point address of the remote tunnel:	hoo6.hip6.dyndns.org
Session key operation:	Automatic, with the IKE protocol
Recommended encryption algorithms:	AES and DES and 3DES
Recommended hash algorithms:	MD5 and SHA1

Recommended lifetime of the session keys:	8 hours (default)
Recommended lifetime of the key exchange session:	8 hours (default)
Recommended data volume of the session keys:	Unlimited (default)

Select the option “key exchange data” and set the key exchange parameters for this newly set-up tunnel:

Session key operation:	Automatic, with the IKE protocol
Recommended Diffie-Hellman groups:	DH group 2, DH group 5
Activate 'Perfect Forward Secrecy':	Yes
Authentication procedure for the VPN peers:	Digital Signatures
List of CA certificates:	LWCA

11. “Digital Signatures” are used as the authentication procedure for the VPN peers. And then the trusted CA certificate must be selected from the list of the CA certificates:

Configured Tunnels

Display General Tunnel Data | Display Rules for all Tunnels | **Add Tunnel**

Tunnel Data | **Key Exchange Data**

Name of the Tunnel: system 5--system6

Type of the Local Tunnel Endpoint: DNS Name

Local Tunnel Endpoint Address: hoo5.hip6.dyndns.org

Type of the Remote Tunnel Endpoint: DNS Name

Remote Tunnel Endpoint Address: hoo6.hip6.dyndns.org

Session Key Handling: Automatically, using IKE protocol

Suggested Encryption Algorithms

AES ☒ DES ☒ 3DES ☒

Suggested Hash Algorithms

MD5 ☒ SHA1 ☒

Suggested Lifetime of the Session Keys: 8 hours 0 min. 0 sec.

Suggested Lifetime of the Key Exchange Session: 8 hours 0 min. 0 sec.

Suggested Data Volume of the Session Keys: Gigabyte Megabyte Kilobyte unlimited ☒

Key Exchange Data

Activate Perfect Forward Secrecy: ☒

VPN Peer Authentication Method: **Digital signatures**

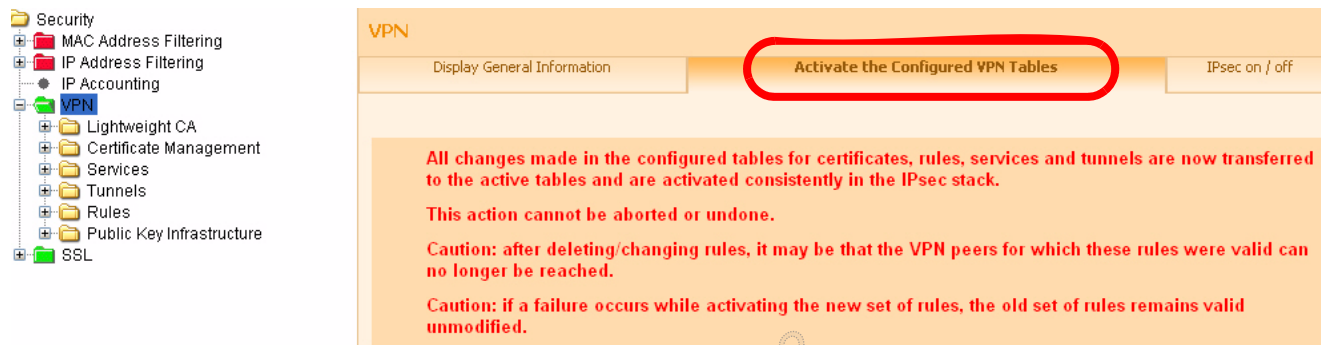
List of CA Certificates

LWCA-Trusted ☒

Suggested Diffie-Hellman Groups

DH Group 1 ☐ DH Group 2 ☒ DH Group 5 ☒

12. Now the existing tunnel rules need to be assigned to the new tunnels. The order of priority of the rules should be retained.
13. Delete the old tunnel.
14. Activate the rules and tunnel.



15. Check the function with a ping to the partner system. Please note that some configuration steps must still be carried out in the same way on the other systems in your network.

8.1.1 Maintenance

- For diagnostic purposes, use the preconfigured trace profile "VPN".
- Detail traces via XTracer and/or TCP dump.
- Create Backup.
- Customer presentation: security relevant configuration - e.g. USB-stick with created certificates and passphrases - should be delivered by „Eye-to-Eye“ principle.

8.1.2 Configuration of NCP Client - "Certificates" - Example Teleworker 5 //draft//

Starting point:

The installation of the Windows NCP client has been carried out. The authentication via "PSK" was operative and has been changed - Example System 5 - to "Digital Signatures" on the target system.

Prerequisite:

The following certificates are available:

- Peer-teleworker certificate (*.p12)
- *Optional:* CRL list (*.crl)
- Trusted LWCA (*.crt)

Startup:

The necessary configuration is shown in the example.

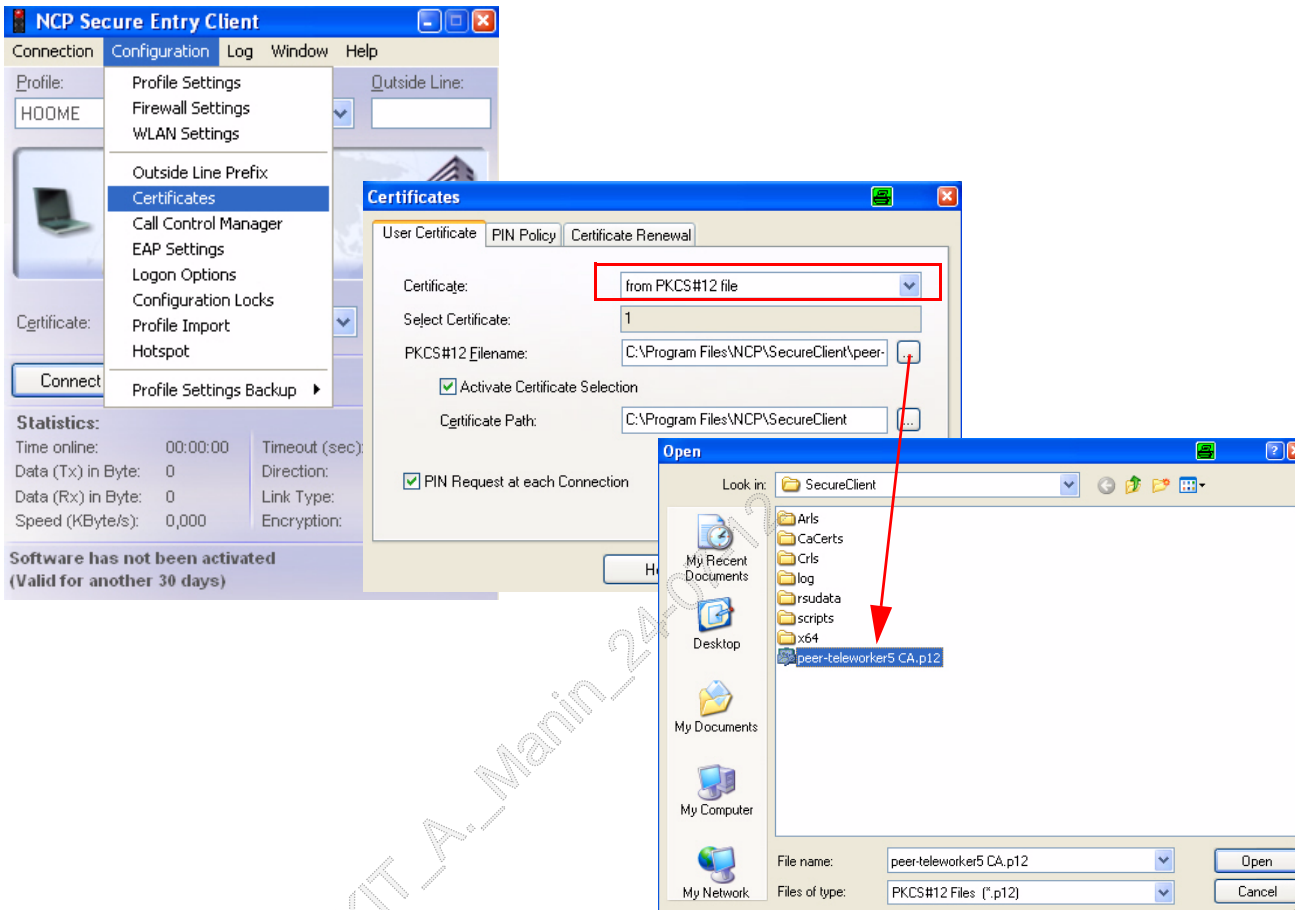
1. Copy the Trusted Certificate under the NCP client installation path <drive>:\<Installationpath>\NCP\SecureClient\CaCerts*.crt
2. Copy the Peer-Teleworker Certificate under the NCP client installation path <drive>:\<Installationpath>\NCP\SecureClient\CaCerts*.crt
3. *Optional:* Copy the Certificate Revocation List under the NCP client installation path <drive>:\<Installationpath>\NCP\SecureClient\Crls*.crl



Note:

Maintenance of the Certificate Revocation List in the client is not required as the VPN gateway - i.e. the HOO - keeps revocation lists and revokes certificates if necessary.

4. Add a Peer-Teleworker Certificate.



5. Check the function with a ping to the partner system.
6. Test the call setup to the target system. For details, start the “Logbook”.

8.1.3 Configuration Windows VPN Client - "Certificate" - Example Teleworker 6//draft//

Starting point:

The installation of the Windows VPN client has been carried out. The authentication via "PSK" was operative and has been changed - Example System 6 - to "Digital Signatures" on the target system.

Prerequisite:

The following certificates are available:

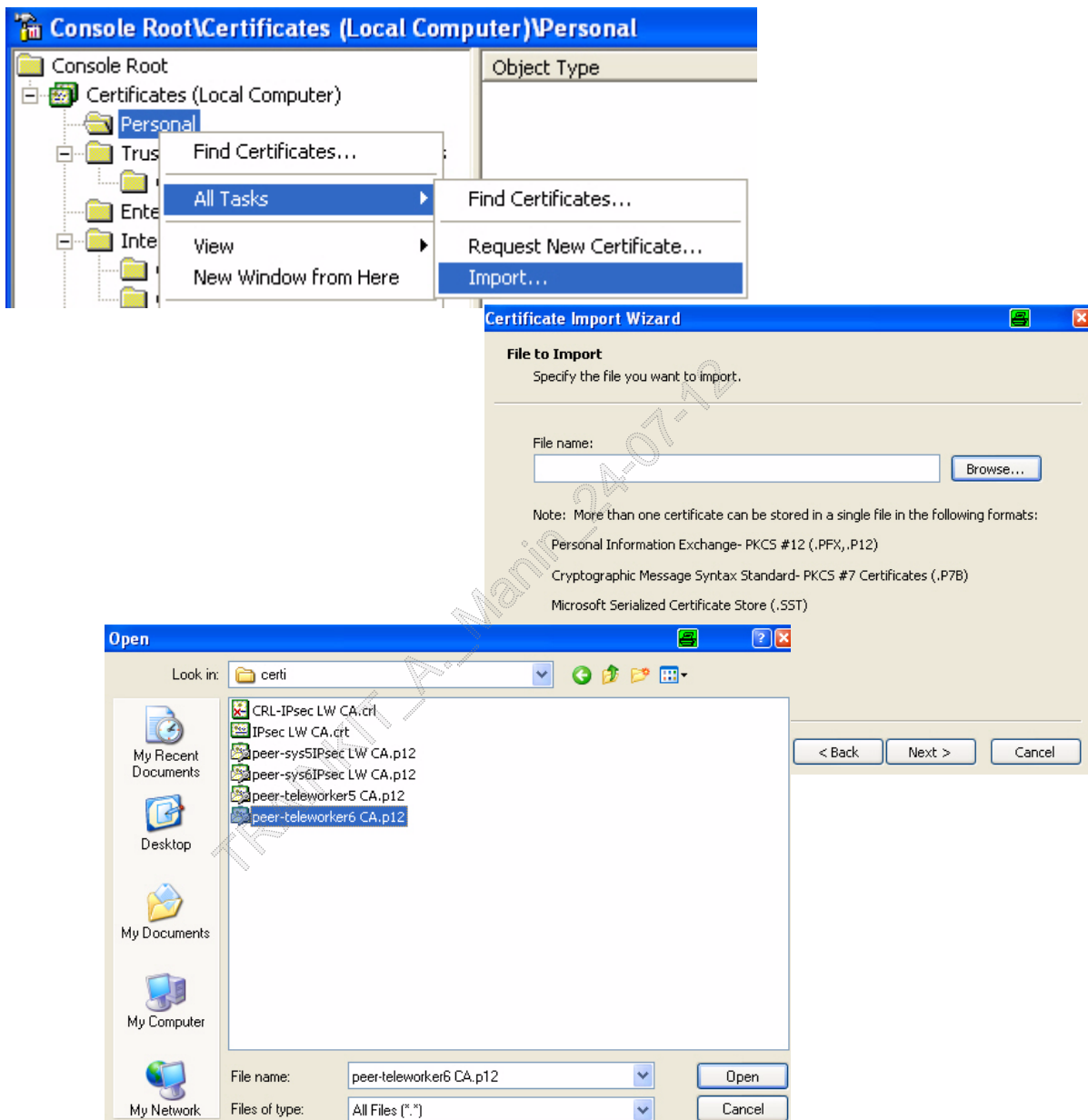
- Peer-Teleworker Certificate (*.p12)
- *Optional:* CRL list (*.crl)
- Trusted LWCA (*.crt)

TRAINKIT_A._Manin_24-07-12

Startup:

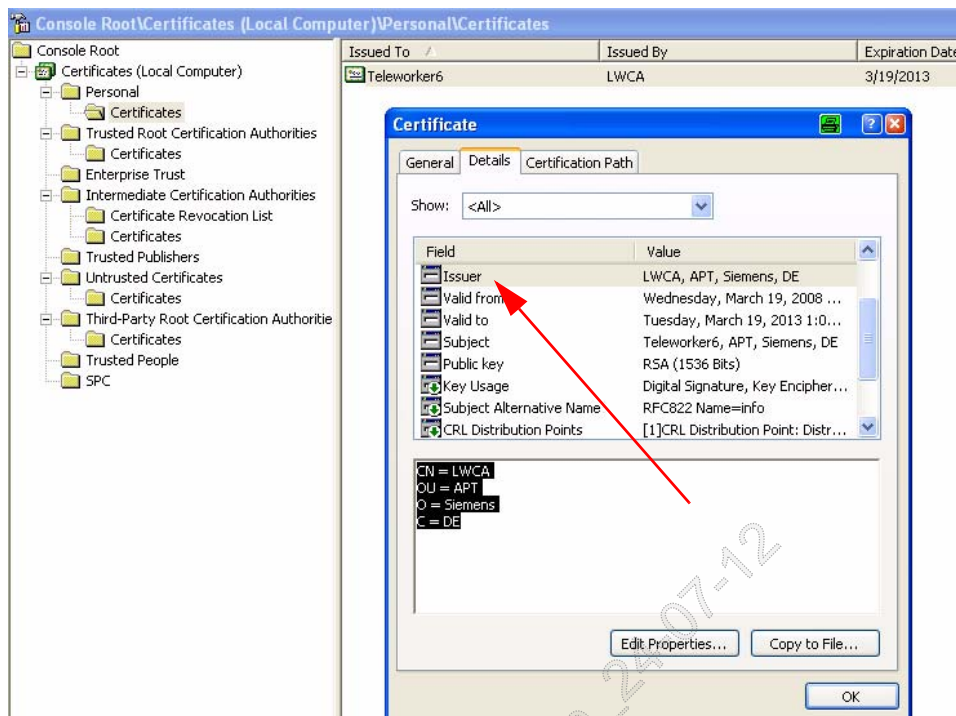
The necessary configuration is shown in the example.

1. Open a Management Console (MMC) > Import the Peer-Teleworker Certificate:



You still need the “Private” key for installation of the certificate!.

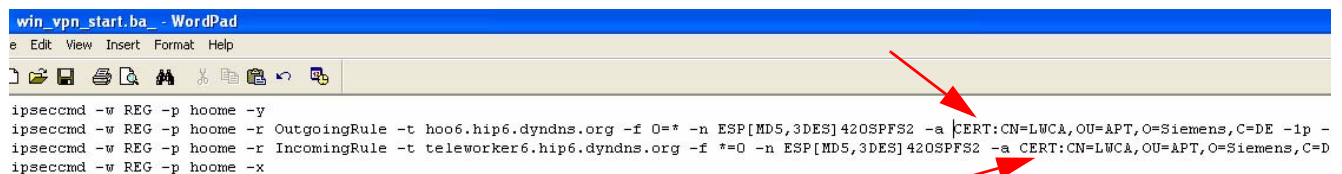
The “issuer” of the certificate with the unambiguous name is important here - term: “Distinguish Name” - abbrev.: “dn”.



2. Import the Trusted LWCA Certificate



3. Change the VPN start file from the "PSK" procedure to "CERT".



4. Check the function with a ping to the partner system.