

XP Unlimited software

Contents

XP Unlimited software.....	1
Introduction to the SSL Gateway.....	2
Specifications.....	3
Objective.....	3
Configuration example 1: Stand Alone XPU Server.....	4
Configuration example 2: XPU Farm with 3 servers and 2 internet connections.....	5
Maintenance.....	6
Step 1: Generate a Server Certificate and Key pair.....	6
Step 2: Enable the SSL Gateway.....	8
Step 3: Generate one or more Client Certificates- and Key pairs.....	9
Step 4: Generate a Client Build.....	10
Install the Client Setup Build.....	11
Vista: User Access Control (UAC).....	11
xpuWin32client.exe.....	12
Details of the Client Setup Build.....	13
Operate.....	15
SSL Gateway and the Farm.....	15
Unknown other Certificates and Keys.....	16
Viewing Active SSL Connections.....	17
Failed connections logging.....	18
Changelog.....	19
All contents copyrighted by IPConsult BV.....	20
Portions copyrighted by others.....	20

Introduction to the SSL Gateway

Specifications

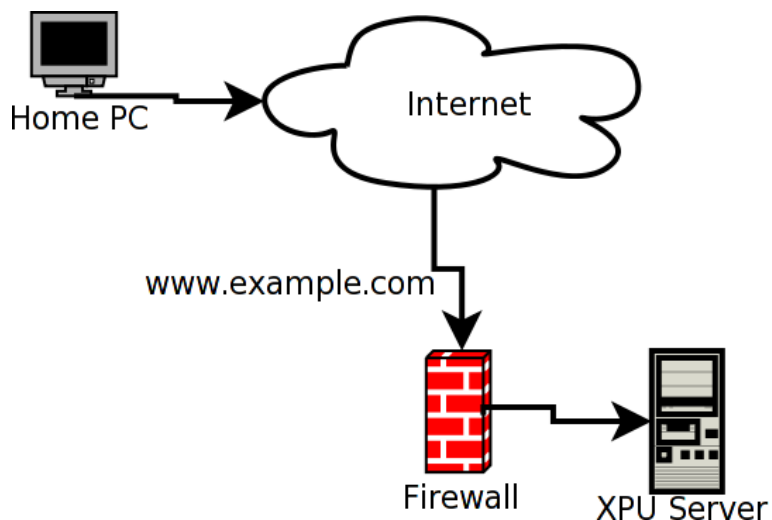
- The certificates generated by the SSL Gateway are based on RSA, 2048 bits.
- Both the client and the server do verify each other certificate.
- The SSL Gateway can be used in a XPU Farm.

Objective

The objective of the SSL Gateway is to deliver a secure Desktop session between any location in the world and a XPU-Server. The term “secure” implies:

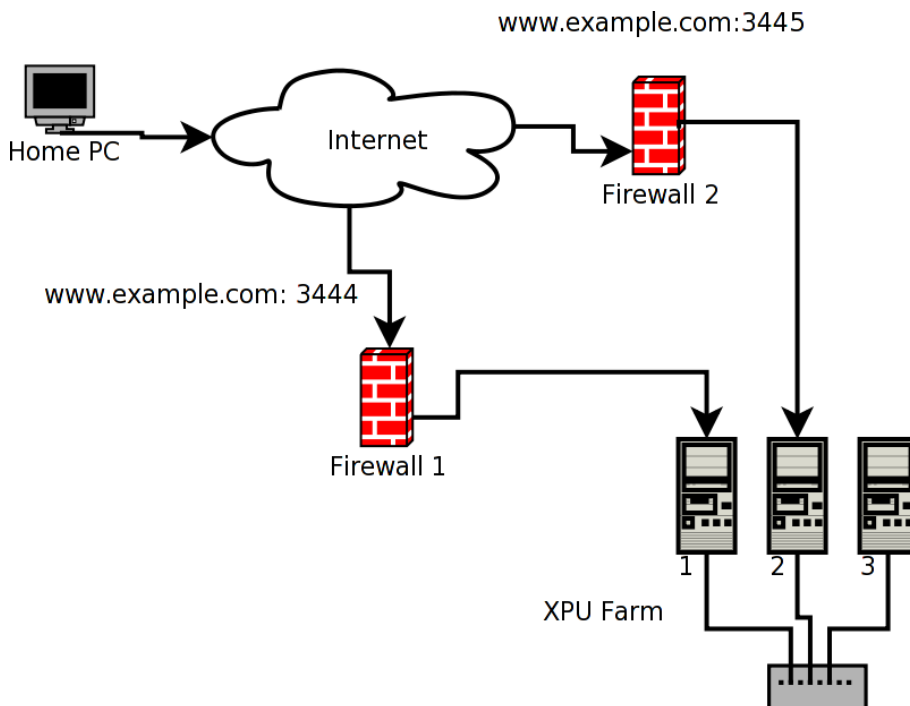
- Strong SSL encryption is used in order to avoid “listening” on the connection. The RDP-protocol in itself is already encrypted, but a SSL encryption beneath the RDP connection, using strong certificates, will do a better job.
- Identification of both the client and the server. The SSL Gateway gives an Administrator the possibility to deliver specific Client Builds with an included certificate, which can only connect to 1 or more XPU Servers. Also, the Administrator can “withdraw” a Client certificate, such that the client can not connect any more.

Configuration example 1: Stand Alone XPU Server



- The company has a connection with the internet. This connection is reachable by the domain name `www.example.com`
- The client using the home PC connects using `www.example.com:3443`.
- The Firewall does forward incoming connections for port 3443 to the XPU Server.
- The XPU Server is running the SSL Gateway on port 3443.
- It is a stand-alone XPU Server; there is no XPU Farm.

Configuration example 2: XPU Farm with 3 servers and 2 internet connections



- The company has 2 connections with the internet.
 - When a client tries to connect to `www.example.com:3444`, the connection goes through the first firewall.
 - When a client connects using `www.example.com:3445`, the connection goes through the second firewall.
- The client at the Home PC can use either `www.example.com:3444` or `www.example.com:3445`
 - By offering client 2 connection addresses, and having 2 connections with the internet, the company can offer the client redundancy for the connection to the XPU Farm
- The first firewall forwards port 3444 to the SSL Gateway on XPU Server 1
- The second firewall forwards port 3445 to the SSL Gateway on XPU Server 2
- The SSL Gateways on both XPU Server 1 and 2 will handle the correct forwarding to the appropriate XPU Server in the Farm, based on the Load Balancing Parameters.
- XPU Server 3 does not run the SSL Gateway

Maintenance

Step 1: Generate a Server Certificate and Key pair

Server Settings

Enable SSL Gateway SSL Gateway is not running

Enter the Port Number of this Server for the SSL connections.

...no info...

Generate Server When you generate a new Server Certificate and Key pair, the current Server Certificate and Key will be deleted.

Delete Server

When you click on Apply, current active SSL Connections will be disconnected.

Apply

After a fresh installation of XPUnlimited, the server does not have any certificate. Enable the “Generate Server” button, and you can generate a Server Certificate- Key pair.

- The Certificate- and Key pair is valid for 10 years
- The Certificate contains the (netbios) name of the server

Current Server Key and Certificate:

Valid from: 2009-01-28 21:17:46

Valid until: 2019-01-26 21:17:46

Key: D:\Program Files\XPUnlimited\certs\xpuServer_JEWEL.key

Certificate: D:\Program Files\XPUnlimited\certs\xpuServer_JEWEL.crt

Generate Server When you generate a new Server Certificate and Key pair, the current Server Certificate and Key will be deleted.

Delete Server

Using the Delete Server button you can delete the current Server Certificate- and Key pair.

Important:


The Server Certificate (not the Key) will be made available to the Client. If you Delete the current Server Certificate- and Key pair, and generate a new pair, you will need to distribute a Client Setup Build to all your clients in order to supply them with the new Server Certificate.

After deleting the current Server Certificate- and Key pair, it is not possible any more for any Client who has the current Server Certificate, to establish a connection with the Server.

Therefore, be careful with deleting the current Server Certificate- and Key pair. Use it only deliberately when you **do not want** that Clients who knows the current Server Certificate are able to establish a connection with the Server.


Step 2: Enable the SSL Gateway


Server Settings | Client Certificates and Keys | Other Certificates and Keys | Connections

Enable SSL Gateway  SSL Gateway is running


Enter the Port Number of this Server for the SSL connections.

Current Server Key and Certificate:
Valid from: 2009-01-28 21:17:46
Valid until: 2019-01-26 21:17:46
Key: D:\Program Files\XPU\certs\xpuServer_JEWEL.key
Certificate: D:\Program Files\XPU\certs\xpuServer_JEWEL.crt

 Generate Server When you generate a new Server Certificate and Key pair, the current Server Certificate and Key will be deleted.

 Delete Server

When you click on Apply, current active SSL Connections will be disconnected.

 Apply

Enable the SSL Gateway using the upper checkbox, and click on the Apply button. The “running or not running” status of the SSL Gateway will be shown.

Enabling the SSL Gateway does also enable the next tabpages.

Step 3: Generate one or more Client Certificates- and Key pairs

Client Name	Serial	Valid After (UTC)	Valid Until (UTC)
JEWEL_andre	361FE0A4D6C	2009-01-27 16:18:37	2019-01-25 16:18:37
JEWEL_rene	514E312EDFA	2009-01-27 16:18:21	2019-01-25 16:18:21
JEWEL_sales	4395F6040E6C	2009-01-27 16:21:17	2019-01-25 16:21:17

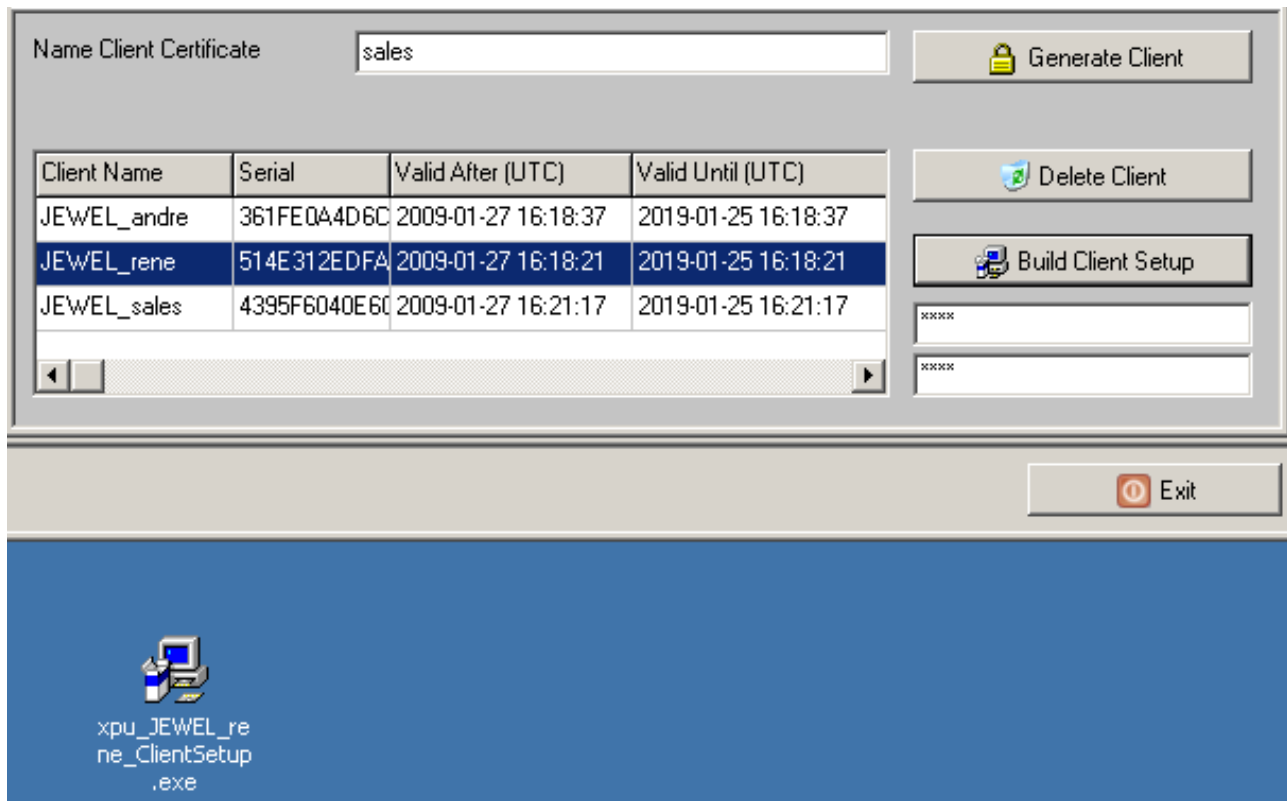
Enter a name for the client.

- The name is at least 4 positions.

You can generate a separate Certificate- and Key pair for each individual. You can also choose to generate a “functional user” Certificate- and Key pair, like 1 pair for Sales-employees.

Using the Delete Client button, a Certificate- and Key pair of the selected user will be deleted. Any user that has this Certificate- and Key pair, will not be able any more to establish a connection with the Server.

Step 4: Generate a Client Build



- Select a Client Certificate- and Key pair.
- Enter, optional, a password. The user for who the Client Setup Build is intended, will need to enter this password when installing the Client Setup Build.
- Click on the button “Build Client Setup”.

On the desktop of the Administrator an EXE-file will be created which is the complete Client Setup Build for the selected user.

- Distribute the Client Setup Build to the intended user.

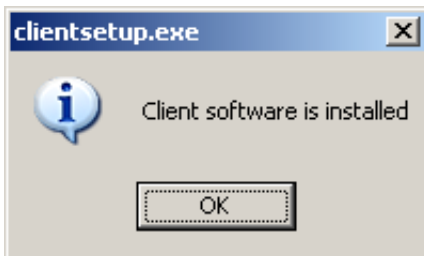
Install the Client Setup Build

- Distribute the Client Setup Build -Exe to the intended user.

The only thing the user has todo is double-click on the Executable.

- The Client Setup Build -Exe requires Administrator rights on the Client PC in order to install.

A successfully installation ends with the following message:



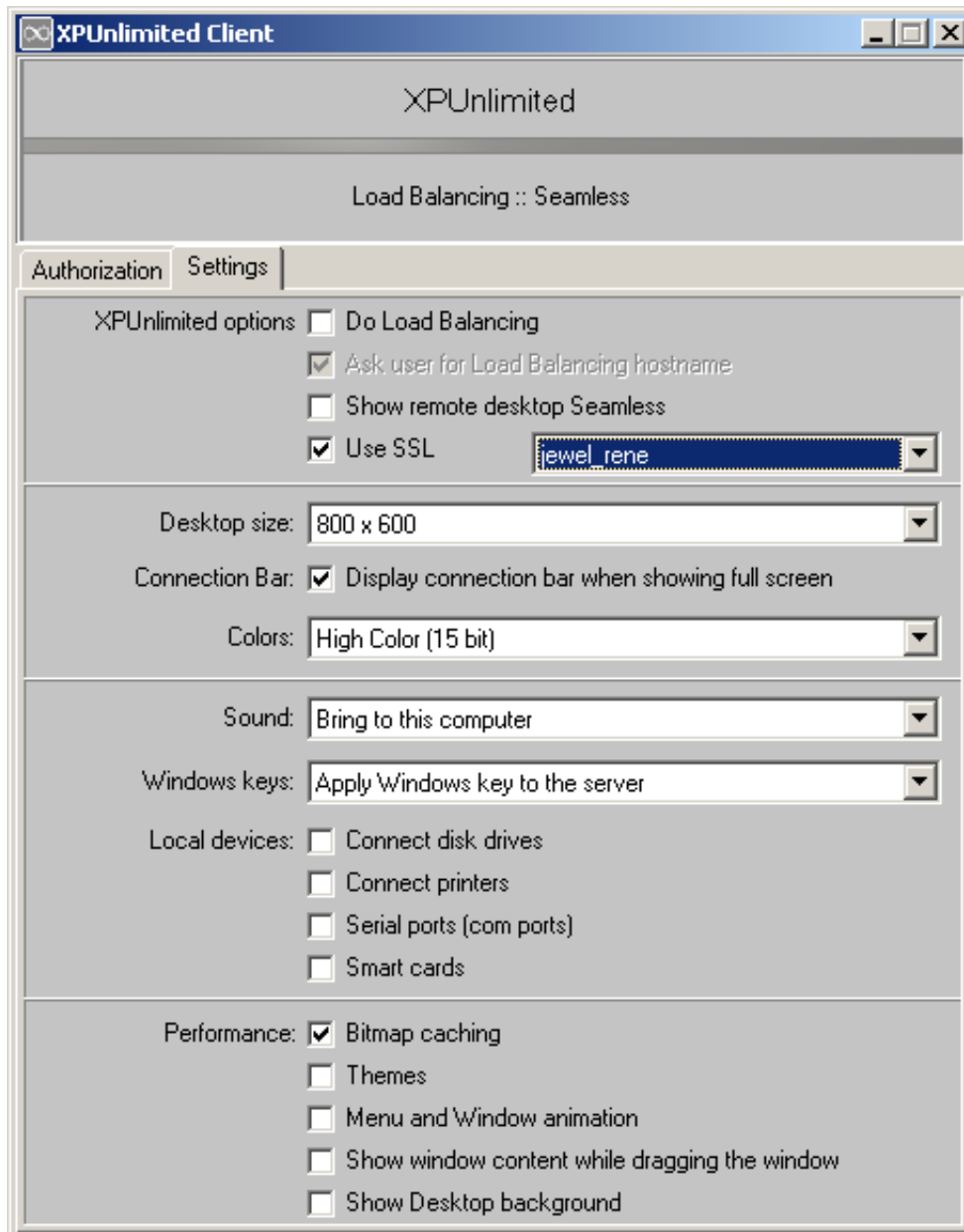
- In the Start Menu of the PC, an entry is placed
- Using Add / Remove software the Client Setup Build can be un-installed from the PC.

Vista: User Access Control (UAC)

The certificates are installed such that every user on a Vista PC can “read” the certificates. Users can not add or delete certificates.

xpuWin32client.exe

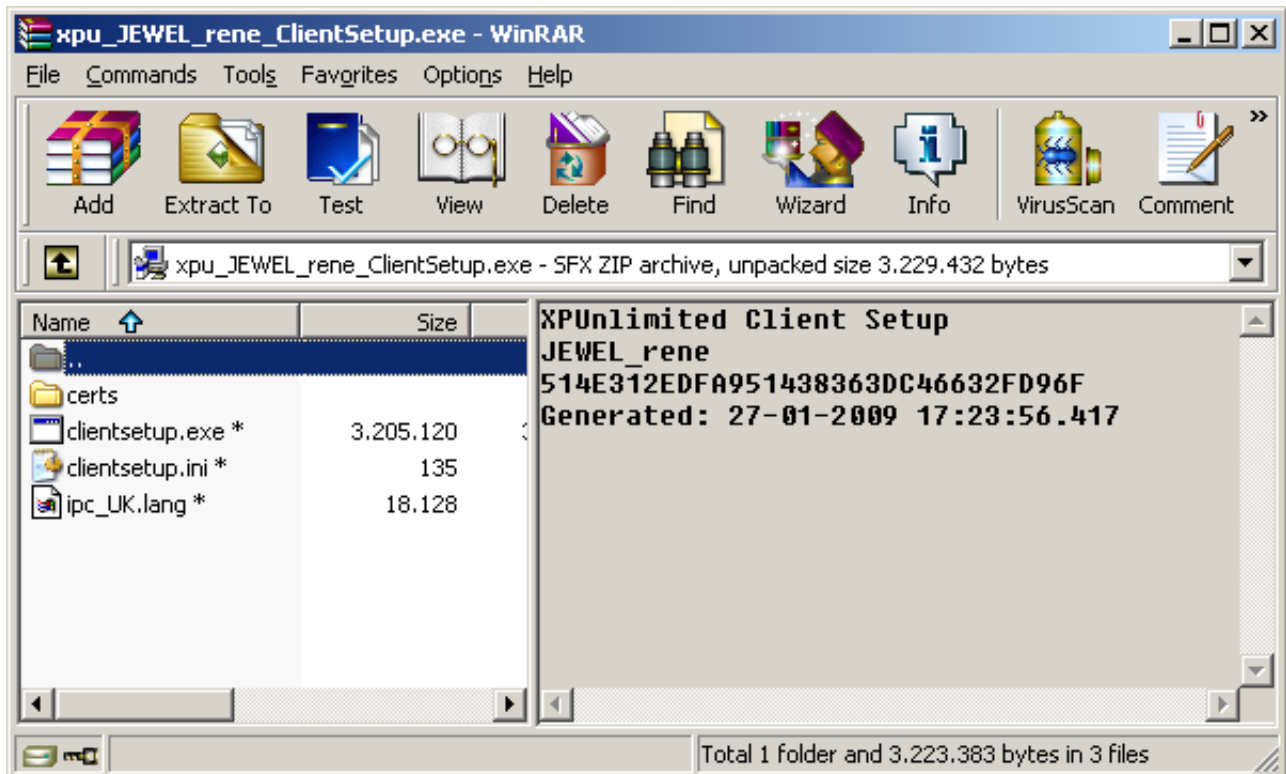
The client program xpuWin32client has an extra option for the SSL connection:



Select the “Use SSL” checkbox, and select the Certificate. Usually a Client Setup Build contains only 1 Certificate- and Key pair, so there is not much to choose....

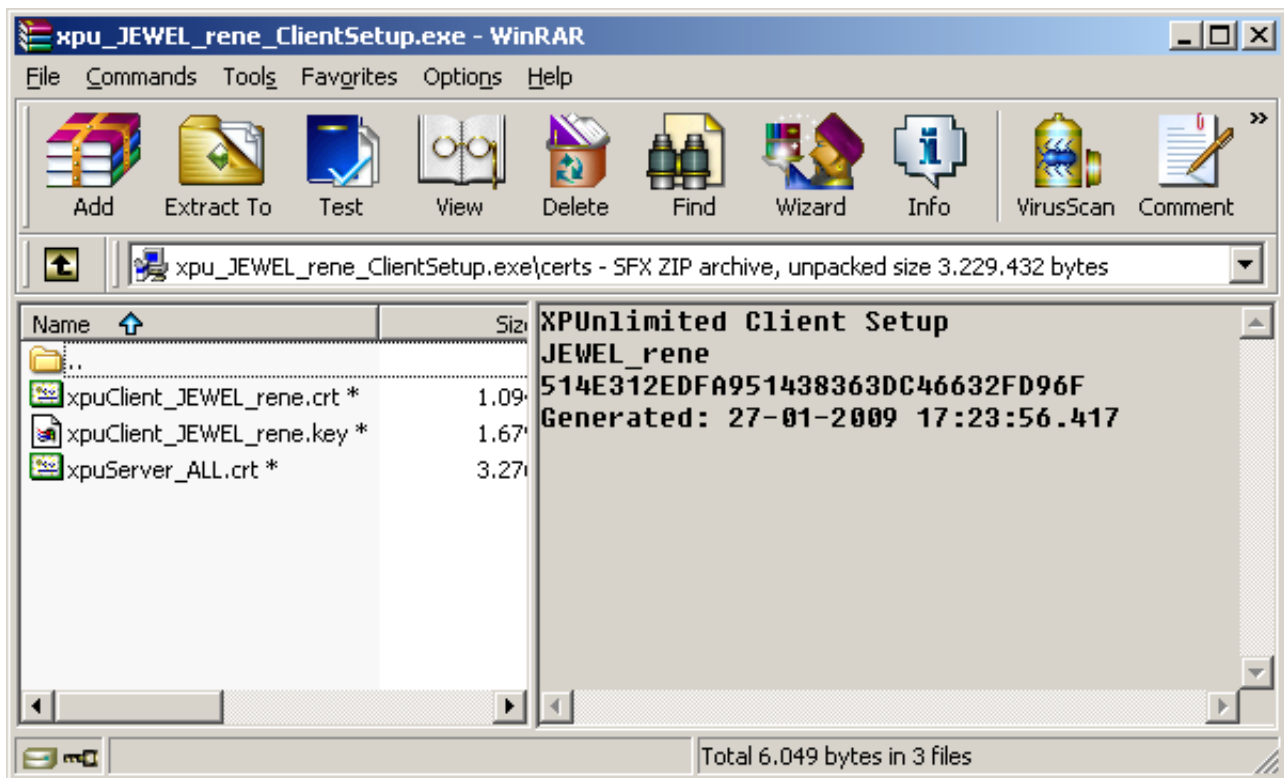
Details of the Client Setup Build

The details of the Client Setup Build are revealed when you open it with, for example WinRAR:



- Client Setup Build will, when double-clicked by the user, run the program ClientSetup.exe.
- The included language is the same as installed on the XPUnlimited server.
- The * behind the filenames do indicate that there is a password protection on each file. It is the password the Administrator did enter with the previous step.

The folder certs contains the Certificates- and Keys:



- Only the Certificate- and Key pair of the intended user is included.
- The file xpuServer_All.crt contains all Server Certificates. In case of a XPUnlimited Farm, there will be a Server Certificate for each Server in the Farm.

Important:

The user must be instructed that he / she is careful with the *.key file. If this key file gets in somebodies else hands, it is possible that somebody else impersonates the intended user while doing a SSL connection.

If this is happening, the Administrator should delete the Client Certificate- and Key pair as shown in Step 3, using the button Delete Client.

Operate

SSL Gateway and the Farm

When the Server is part of a XPU Farm, the Servers in the Farm will inform each other about the Certificates:

The screenshot shows a management window with several tabs: Application, Translate, Auto Logon, Domain / Workgroup, Load Balancing, SSL Gateway, and Web Server. The 'SSL Gateway' tab is active, and within it, the 'Other Certificates and Keys' sub-tab is selected. This sub-tab contains two sections:

- Other Server Certificates and Keys:** A table listing certificates for other servers in the farm. It includes a 'Delete Server and Clients' button.

Server Name	Serial	Valid After (UTC)	Valid Until (UTC)
JEWEL	4F6F08D279DDB84FA9924FBA920AA7DB	2009-02-11 22:21:19	2019-02-09 22:21:19
XPUTEST1	B2209F4B50FD463B0C36E077BDD664F7	2009-02-18 10:55:38	2019-02-16 10:55:38
- Other Client Certificates and Keys:** A table listing certificates for other clients in the farm. It includes a 'Delete Client' button.

Client Name	Serial	Valid After (UTC)	Valid Until (UTC)
JEWEL_andre	08AD2D8CEF8C117884D824C0BD18407D	2009-02-11 22:21:34	2019-02-09 22:21:34
JEWEL_rene	E819CD2E29D12567B00F8E2A361214C0	2009-02-11 22:23:10	2019-02-09 22:23:10
XPUTEST1_sandra	E3B82FD19D9DEB5266D7CB40FE68497C	2009-02-18 10:55:57	2019-02-16 10:55:57

Unknown other Certificates and Keys

If a server in the Farm is down, or a server is permanently removed, the other servers do not “know” any more the Certificates and Keys. This is shown:

The screenshot shows the 'Other Server Certificates and Keys' section with the following data:

Server Name	Serial	Valid After (UTC)	Valid Until (UTC)
!AMD64	6B10C8B4C0FCD7A060BCDC84630410AB	2009-02-25 16:30:50	2019-02-23 16:30:50
!RBR-PC	B3B1102041CA7F889AD10BB3E58318CF	2009-02-22 19:31:15	2019-02-20 19:31:15
WIN-H3C1E66V8FI	543595065BEABD31A11AA3407318EF85	2009-02-27 18:24:33	2019-02-25 18:24:33
XPUTEST1	B2209F4B50FD463B0C36E077BDD664F7	2009-02-18 10:55:38	2019-02-16 10:55:38
!XPUTEST2	C065C557A0169CEA8CB6344A8B545A3F	2009-03-01 19:42:58	2019-02-27 19:42:58

The 'Other Client Certificates and Keys' section shows the following data:

Client Name	Serial	Valid After (UTC)	Valid Until (UTC)
WIN-H3C1E66V8FI_rene	EA9623D095E84CAF747BAD6F166426D0	2009-03-01 19:20:47	2019-02-27 19:20:47
WIN-H3C1E66V8FI_sales	C6454EA5483EBEB1BCD907A268E7E32C	2009-03-01 19:20:55	2019-02-27 19:20:55
XPUTEST1_sandra	E3B82FD19D9DEB5266D7CB40FE68497C	2009-02-18 10:55:57	2019-02-16 10:55:57
!XPUTEST2_charlie	0912BEDDFE48DBE1A93E2C273219730E	2009-03-01 19:43:43	2019-02-27 19:43:43
!XPUTEST2_williams	EF42EA94F111922D5D011719447C8177	2009-03-01 19:43:20	2019-02-27 19:43:20

- Servers AMD64, RBR-PC and XPUTEST2 are not available in the Farm. Those servers are offline and not available.
- The Administrator did generate 2 Client Certificates on Server XPUTEST2, called charlie and williams. Both Client Certificates are distributed among the Farm.

Using the Delete-buttons, the Administrator can delete those unknown Certificates.

Please note: when you accidentally deletes the Certificates and Keys of a server which is only temporarily down, it is not a big problem. When this temporarily down server is back in the Farm, it will automatically distribute its Certificates and Keys among the Farm.

Viewing Active SSL Connections

Active connections can be viewed with the following tabpage:

Settings Certificates and Keys Other Certificates and Keys Connections				
<input type="checkbox"/> Disconnect				
Certificate	Client	Server	User	Time connected
JEWEL_sales 4395f6040e6cec5e0cedae951497183	DEVELOP 192.168.200.130	XPUTEST1 192.168.200.241	/ domain003	28-01-2009 09:23:22 00:01:37
JEWEL_rene 514e312edfa951438363dc46632fd96	CLIENT1 192.168.200.231	XPUTEST2 192.168.200.242	TESTXP.INTERN/ domain001	28-01-2009 09:24:36 00:00:23
JEWEL_rene 514e312edfa951438363dc46632fd96	CLIENT2 192.168.200.232	JEWEL 192.168.200.162	TESTXP.INTERN/ domain002	28-01-2009 09:24:48 00:00:11

- The example shows that 2 different PC's which are both using the same SSL Client Certificate. Apparently the Client Setup Build containing the certificate JEWEL_rene is installed on 2 PC's.
- The XPU Server in the example above is part of a XPU Farm. Based on the load balancing parameters the SSL Gateway has forwarded each session to the appropriate server in the XPU Farm.
- Names like DEVELOP, CLIENT1, XPUTEST1, etc, in the example above, are the PC or Server (netbios) names.

Failed connections logging

In the folder \windows\temp a logging file is created which contains logging about failed SSL connections. For example, when a Client Certificate- and Key-pair is deleted, and an user is still attempting to connect to the XPU Server(s) using this Certificate- and Key-pair, it will logged.

Changelog

4 march 2009	Updated the manual <ul style="list-style-type: none">• Information about the certificates and User Access Control (UAC)
1 march 2009	Introduced a button for deleting “unknown” certificates and keys
4 february 2009	Bugfix <ul style="list-style-type: none">• A crash of the XPUTserver could happen on multi core cpu's
27 january 2009	First release SSL Gateway

All contents copyrighted by IPConsult BV

IPConsult BV
Tiel, The Netherlands
4 march 2009

Portions copyrighted by others

The SSL Gateway is based on, and inspired by the Indy TCP/IP components. See
www.indyproject.org
for more information.

The SSL Gateway is using OpenSSL libraries. See
www.openssl.org
for more information.