Thinstuff TSX Gateway
User Manual

Version 1.0.1

www.**thinstuff**.com

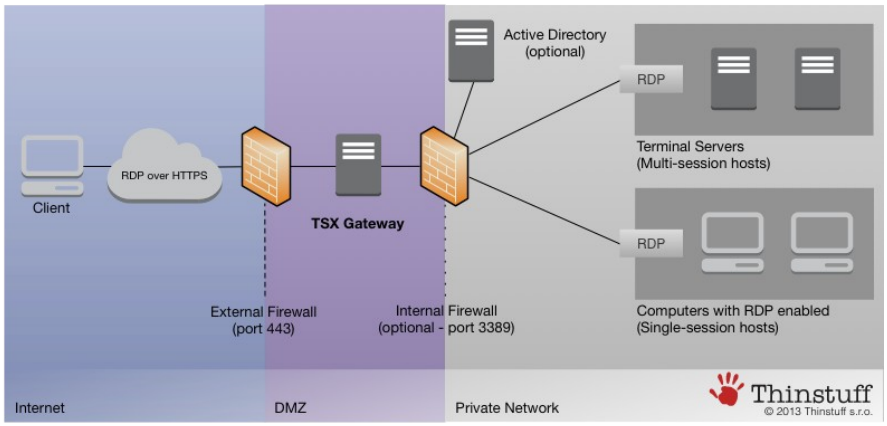
Table of contents

1 Introduction

1.1 General description

TSX Gateway is a highly secure RDP-VPN solution which encapsulates the standard Remote Desktop Protocol (RDP) over HTTPs to establish a secure and encrypted connection between remote users in the internet and your local network resources on which your productive applications are running.

Using TSX Gateway you can connect to internal resources that are hosted behind the firewall.



Network resources can be any RDP enabled hosts, such as:

Multi-session hosts

- Thinstuff XP/VS Server
- Microsoft Remote Desktop Session Host (RDSH/Terminal Server)

Single Session Hosts

- Thinstuff Remote Desktop Virtualization Host (RDVH)
- Thinstuff Remote Desktop Host (RDH)
- Microsoft Remote Desktop Virtualization Host (RDVH)

TSX Gateway is not only a proxy but has to be seen as Terminal Service VPN:

- Secure Connection - RDP over HTTPS Proxy using SSL/TLS encryption and standard HTTPs port 443.
- User Authentication: TSX Gateway allows to set up different rules for authorized remote users to connect remotely.
- Access to authorized network resources: Only specified users can use TSX Gateway to access the specified resources in the network.

TSX Gateway combined with RDP file signing and server authentication secures internet access from mobile workers.

2 Requirements

TSX Gateway is only available with XP/VS Server Professional.
Further information regarding our terminal server software XP/VS Terminal Server you will find on our website[1].

2.1 Server

2.1.1 Supported operating systems:

TSX Gateway supports all **x86** (32 Bit) and **x64** (64 Bit) versions of the following server-side operating systems:

- Windows XP (Service Pack 3)
- Windows Vista
- Windows 7 (Starter, Home Basic, Home Premium, Professional / Service Pack 1)
- Windows 8 (Standard, Professional, Enterprise)
- Windows Server 2003 (also SBS)
- Windows Server 2008
- Windows Server 2008 R2 (also SBS)
- Windows Server 2012

2.2 Client

The client computer has to run Remote Desktop Protocol (RDP) 6.0 or better.

We also offer our free own RDP-client "TSX Connection" which is part of the TSX RemoteApp installation package. You can use it independently from TS RemoteApp and it offers additional functions compared to Microsoft's RDP Client.

Further information you will find in our FAQ Site : TSX Connection[2]

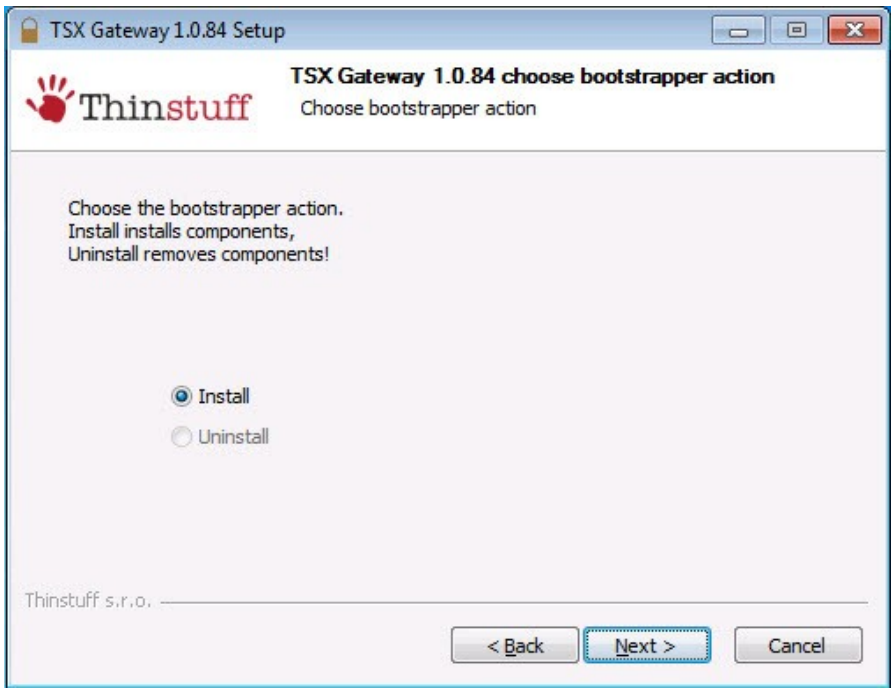
[1] http://www.thinstuff.com/products/xpvs-server/
[2] http://www.thinstuff.com/faq/index.php?solution_id=1088

3 Software installation and maintenance

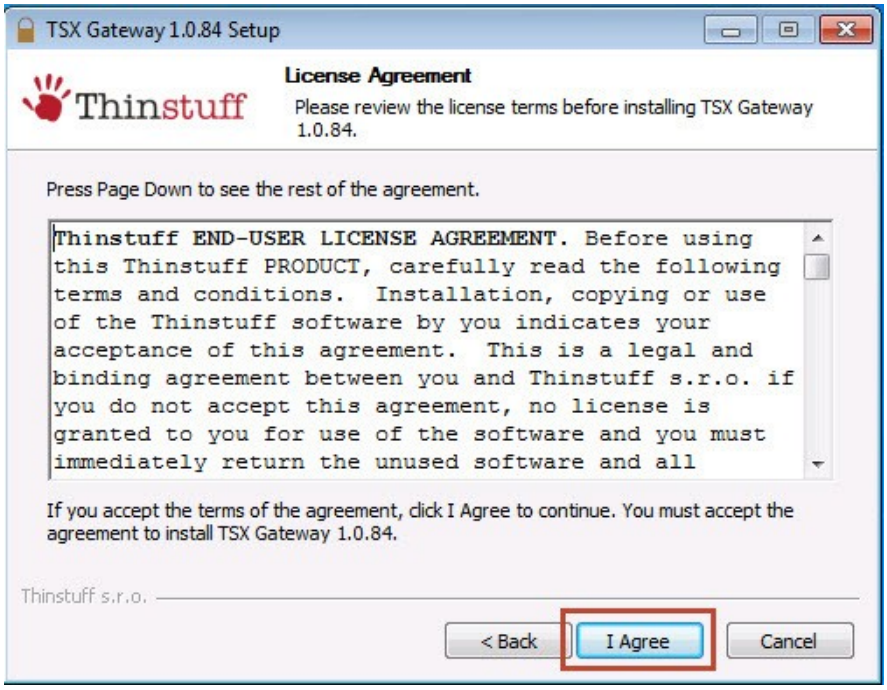
3.1 Installing

1. Download the TSX Gateway installer from here: http://www.thinstuff.com/releases/ThinstuffTsxGateway-latest.exe and run the installation
2. Welcome Dialogue - Select "Next"

Now select "Install" to proceed

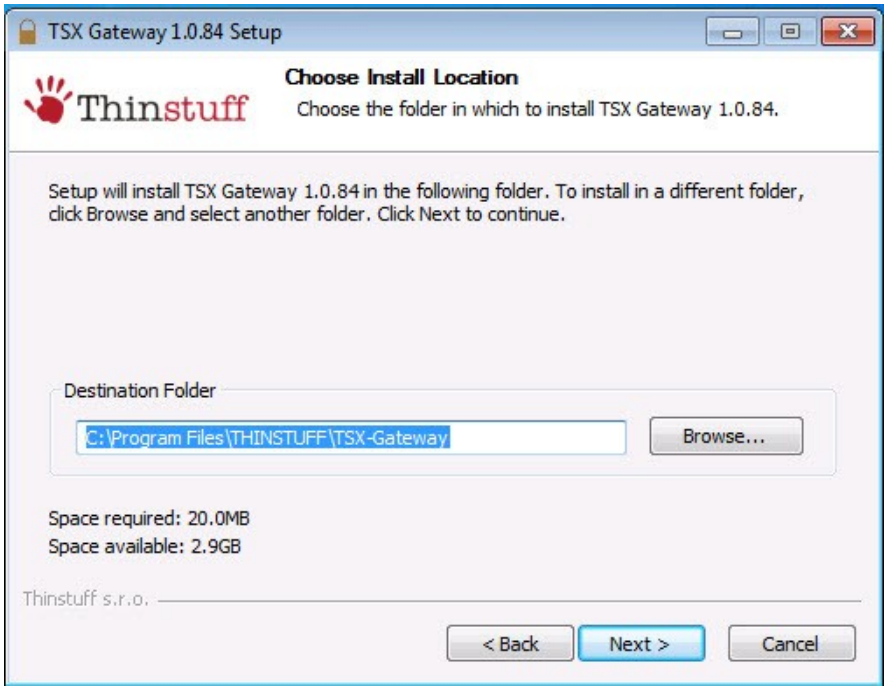


3. To proceed with installation you have to agree to the "End-user License Agreement" and the press "Next".



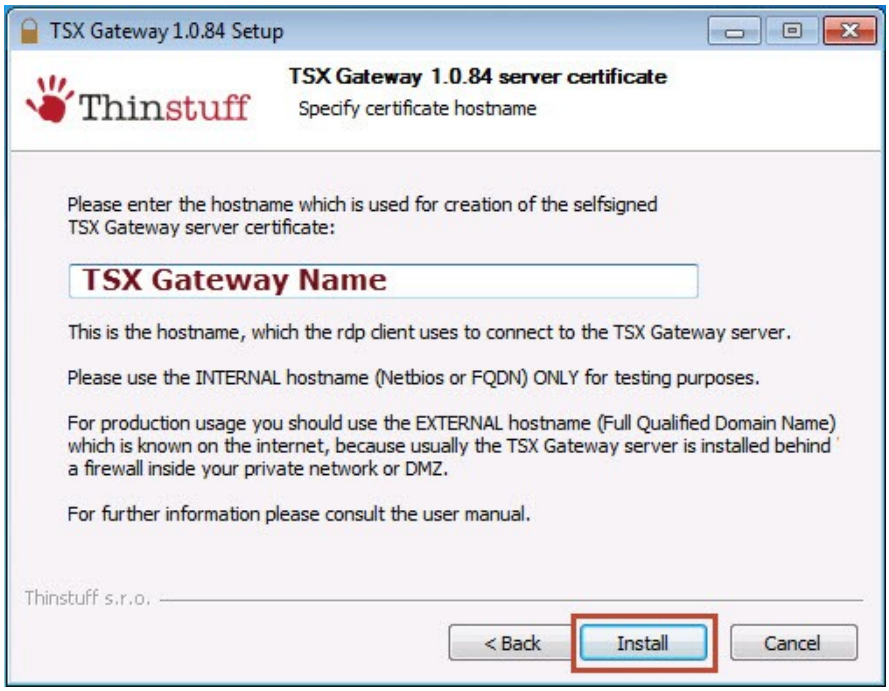
4. Choose Install Location

Per default TSX Gateway will be installed in "C:\Program Files\Thinstuff\TSX-Gateway". If you want to change install location select "*Browse*…"



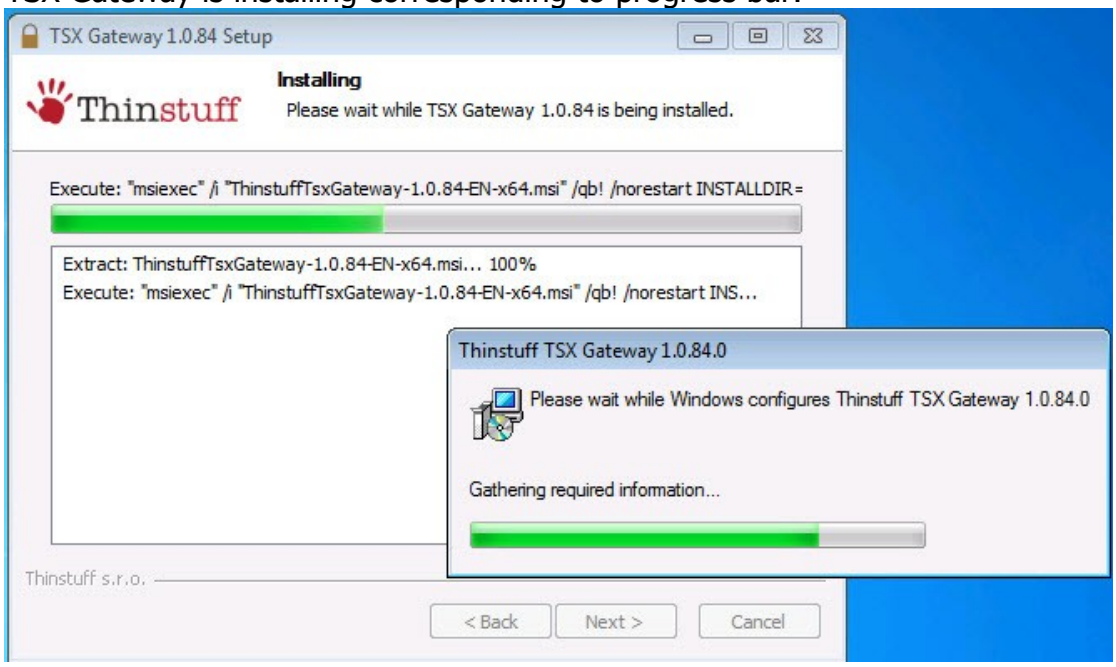
click "*Next*"

5. TSX Gateway x.x.xx server certificate
Enter now the "*Hostname*". The CN (Certificate Name) must match the DNS name that the client uses to connect to the TSX Gateway Server. You have to use internal hostname (NetBIOS) only for testing purposes!



Click "*Install*" to start the installation

6. TSX Gateway is installing corresponding to progress bar.



7. The installation is finished. Now you have to reboot the computer to use TSX Gateway

Now TSX Gateway is successfully installed, reboot is not required.

3.2 Update

You can update TSX Gateway any time.
The latest software is always available on our website[3]
- press green "Download" button.

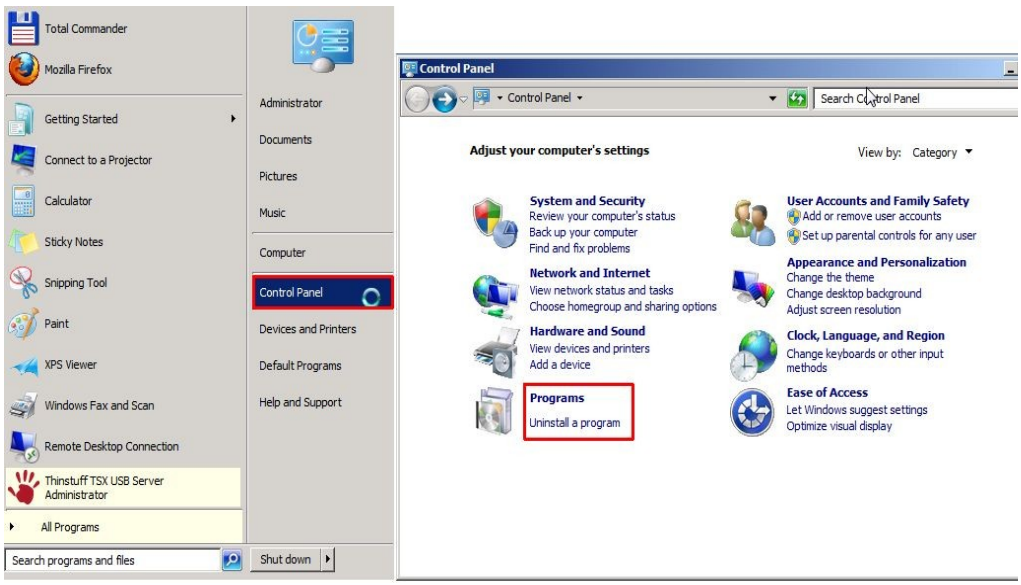
Or you can download the latest version here:
http://www.thinstuff.com/releases/ThinstuffTsxGateway.exe

To update the software, you only need to run the installation and restart the computer.
During this process the old version will be un-installed automatically.
Your settings and licenses will be kept during that procedure.

3.3 Un-Installing

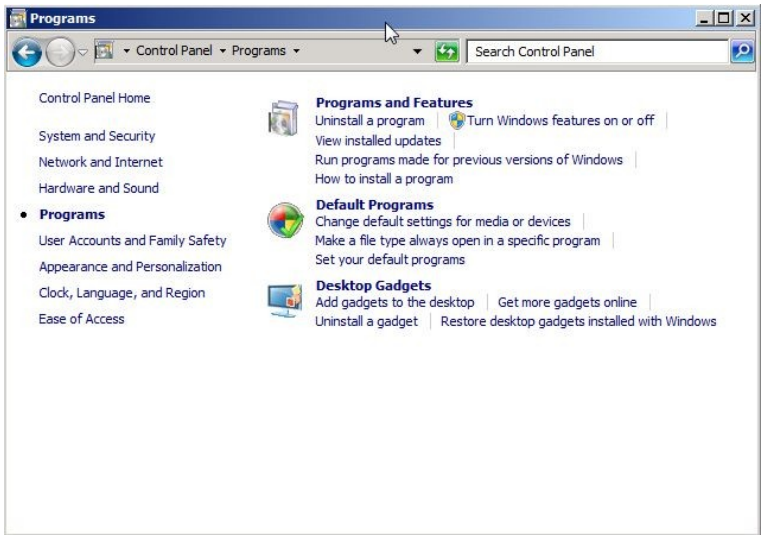
If you want to uninstall TSX Gateway, do the following:

1. Click on the Start-Button, open the "Control Panel" and click "Programs"

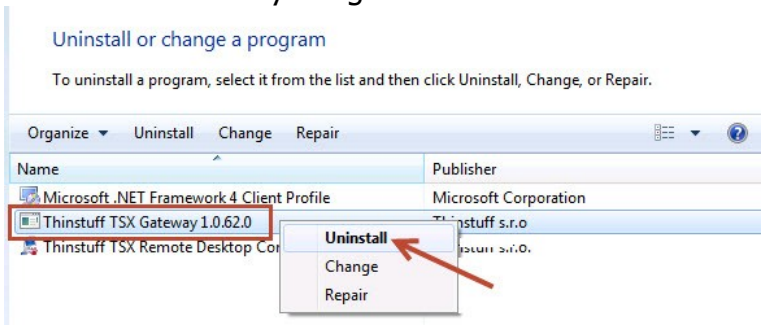


[3] http://www.thinstuff.com/products/tsx-gateway

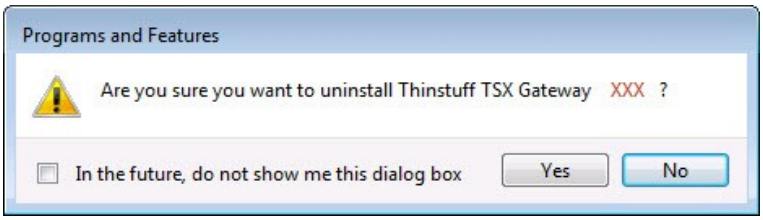
2. Now click on "Uninstall a program" in the menu "Programs and Features"



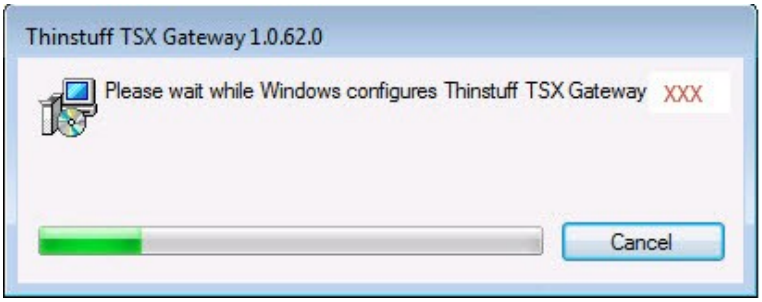
3. Select TSX Gateway - right mouse click – select "Uninstall"



4. To start the un-installing process click "Yes" in the following dialogue box.



5. Software will be un-installed corresponding to process bar



Un-Installation completed, no reboot required.

4 Licensing

4.1 General

TSX Gateway is always licensed per server, no matter if that server is a physical computer or a virtual machine.

TSX Gateway license is only available for free with Professional XP/VS Terminal Server license (with your invoice you will get license code for XPVS Server and for TSX Gateway).

But of course you can purchase the software at any time directly in our webshop[4].

There are principally 2 different types of TSX Gateway licenses:

a) Demo licenses which are only valid for 14 days after installation

b) Full licenses

TSX Gateway licenses (except demo licenses) are one-off-payment and will never expire.

By activating a TSX Gateway license is bounded to the hardware of the machine and tied to a Thinstuff Account.

You can only activate those licenses, which are available in your "Thinstuff Account"!

If you have to switch the license to a different hardware you have to send an email to "support@thinstuff.com" with license ID and reason and we will release the license for reactivation (for free).

4.2 Trial period

In the first 14 days after installation, TSX Gateway can be used freely for non-commercial purpose test. When trial period has expired, the demo license is loosing its validity.

That means – as soon as 14-days trial-period has expired, it is not longer possible to open a remote-connection to your "Host" Computer, using the Gateway service. To continue the usage of "TSX Gateway" you need to import a valid purchased "TSX Gateway license" or install XP/VS Server Professional.

4.3 Registration

As registered user you have several possibilities in your "Thinstuff Account":

- to manage and activate licenses
- to create once a 14-days trial license

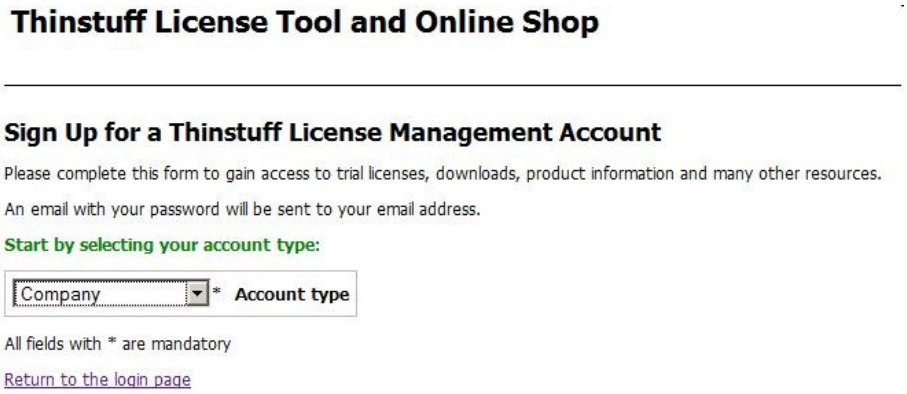
[4] https://www.thinstuff.com/licensing/

To register, please proceed with the following:

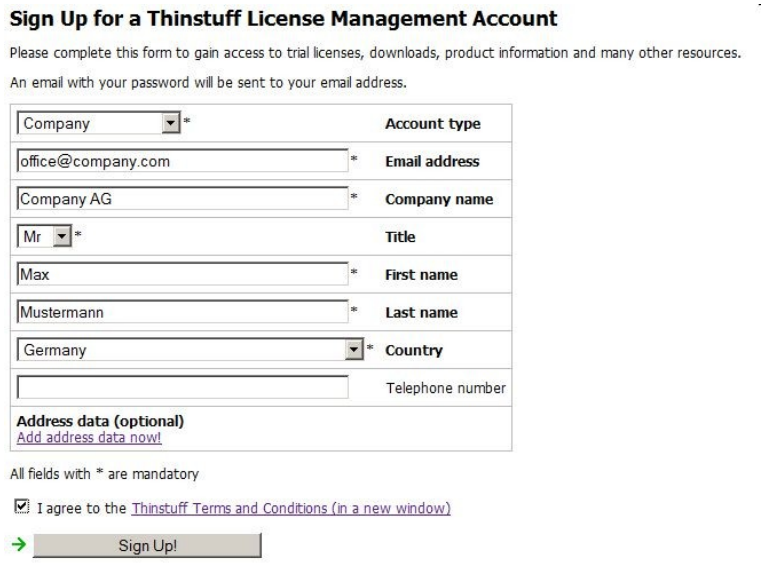
1. Open your web browser and enter the following address: https://www.thinstuff.com/licensing/index.php?action=login

2. Now click on "Create new account":

3. Select whether you want to register as "company" or as "private person". As a precaution you may change this selection in the next step. You will be redirected automatically to the next registration step.



4. To create a valid "Thinstuff Account" please fill the mandatory fields, marked with "*" and confirm with "Sign Up".



5. Now you have successfully created your "Thinstuff Account", and within a short time you will receive an email with your password.

6. Now you can sign in your "Thinstuff Account" with your user-name and password.

4.4 Licenses

If you purchase as end-customer directly in our web-shop the license will be created and ready for activation as soon as payment succeeded.

As payment method we accept credit card (Visa, MasterCard), PayPal or bank transfer (for bank account detail please contact sales@thinstuff.com)

4.5 Activation

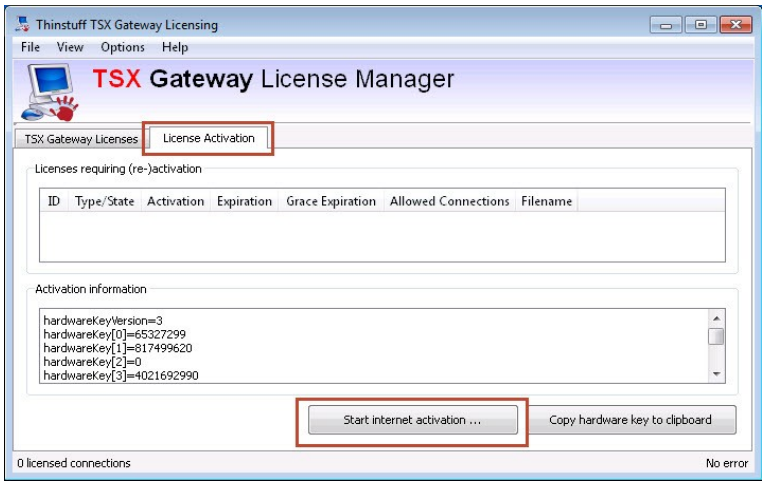
4.5.1 General

The license for TSX Gateway is available for free in each purchased, valid license of XP/VS Server Professional or you purchase the license for TSX Gateway directly in our webshop[5]

4.5.2 Online Activation

1. Start activation

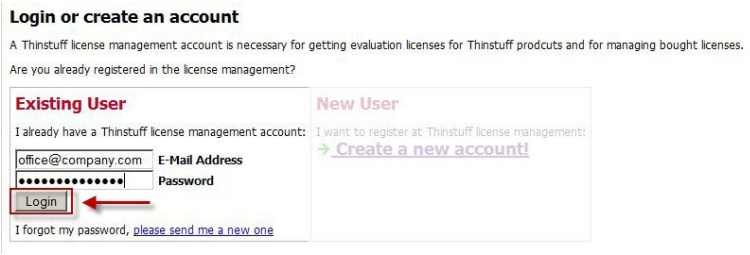
   fig.1 Open the "*TSX Gateway License Manager*" on the your server machine and switch to tab "License Activation" and then click "Start internet activation" button bottom right.



2. *Log into your Thinstuff account*
   Further information concerning registration you will find in chapter 4.3 Registration.

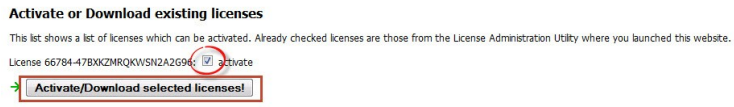
   fig.1 Your web browser will be opened and you have to login with your user name and your password.

[5] https://www.thinstuff.com/licensing/



3a. *If you have bought a license directly in our web-shop*

fig.1 You have to select "activate" next to your license. After that click on "Activate/download selected license"



Now the hardware information of your server will be transferred encrypted to the web server, which creates your license file. Proceed here: 4. Download activated license

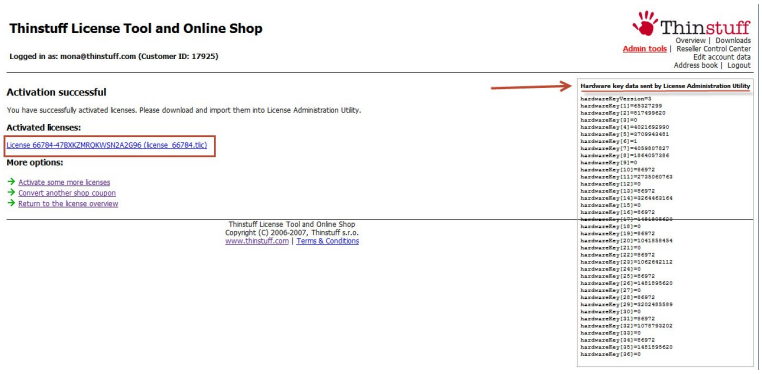
3b. *(Optional) You want to buy now*

fig.1 bottom left you will find the second possibility to get a TSX Gateway license – click the link "Buy Thinstuff products"

And you will be redirected automatically to Thinstuff product page for TSX Gateway. Here you can select your favourite license and proceed with payment.
As soon as payment succeeded the license will be available in your Thinstuff account, ready for activation – Chapter 4.5.2 Online Activation

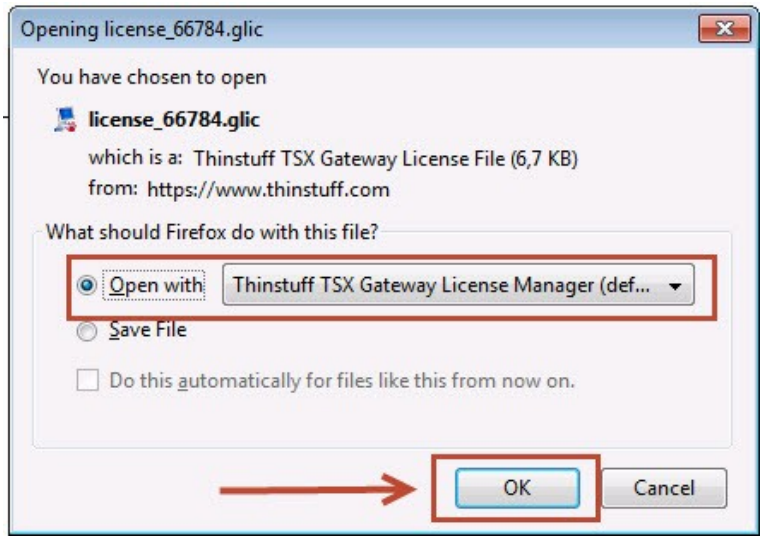
4. *Download activated license*

fig.1 As mentioned above (3a) the hardware information is sent to the webserver and the license file will be created. As soon as this process is done a link for downloading the license will is offered. Click now on this link to download the newly activated license below the item "Activated licenses".



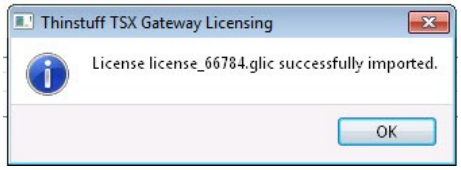
5. *Import the license*

fig.1 In the following dialogue please select „Open with: TSX Gateway License Manager..” and the license will be imported automatically

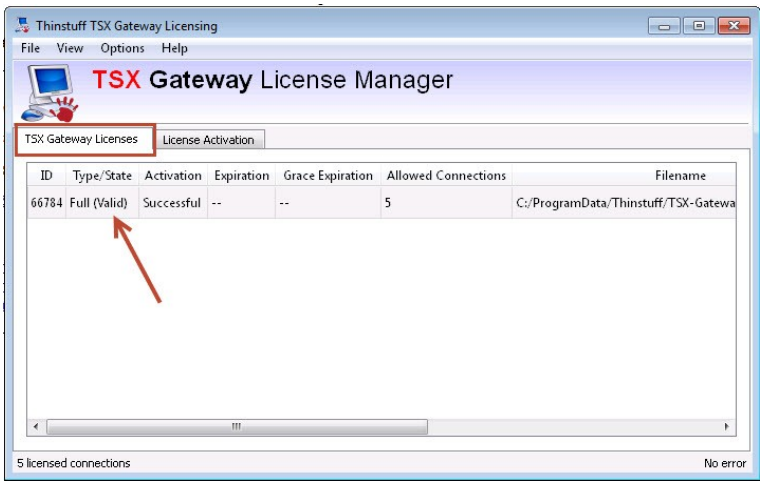


6. *Activation completed*

fig.1 You will get the confirmation that your license is imported successfully



And now the license is shown up as Full (Valid) in TSX Gateway License-Manager – tab "TSX Gateway Licenses"

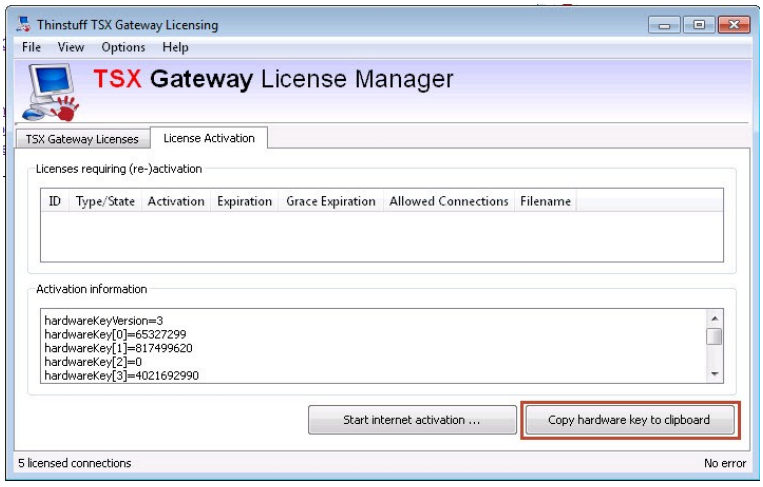


4.5.3 Offline Activation

You also have the possibility of an offline-activation by copying the activation information from your computer without internet access to one with internet access.

1. *On your computer without internet access, where you have installed TSX Gateway*

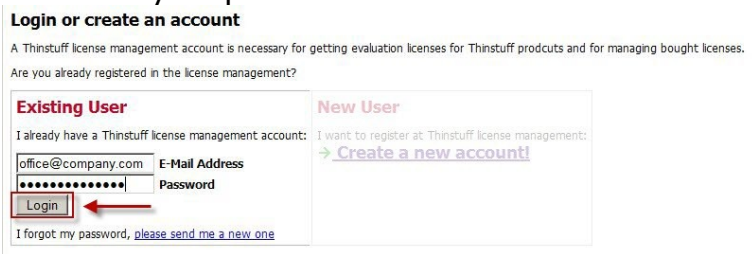
   fig. 1 Open the TSX Gateway License Manager and click on tab "License Activation" and bottom right "Copy hardware Key to clipboard" button.



2. *Paste the text into a text editor* (e.g. Notepad), save it locally (e.g. xxx-hwkey.txt) and copy this text file to your computer with internet access.

3. *On your computer with internet access*:

   fig. 1 Log into your "Thinstuff Account". Further information concerning registration you will find in chapter 4.3 Registration
   Your web browser will be opened and you have to login with your user name and your password.



4. *If you have bought a license directly in our webshop*

fig. 1 Switch into your account to "Overview" and click on "Activate" next to your favoured license.

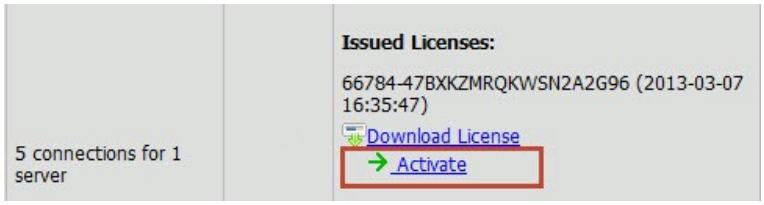


fig. 2 Please select your text file, which you have created previously based on the activation-information.

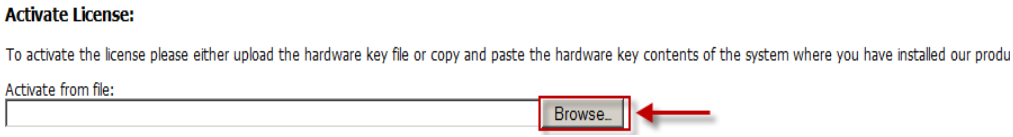
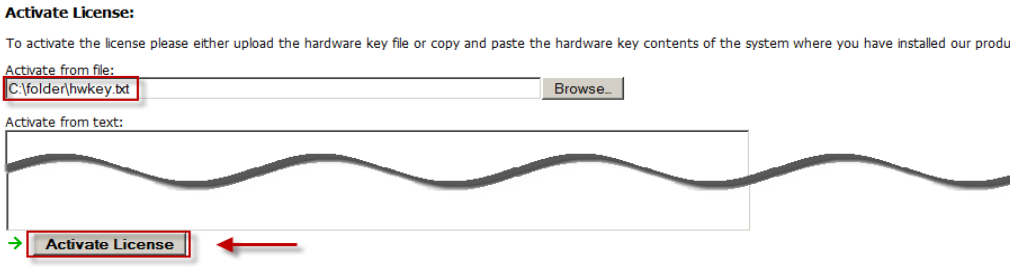


fig. 3 Now click on „Activate license".



5. *Download activated license*

fig. 1 Click now on the newly activated license below the item "License file to download an re-import".

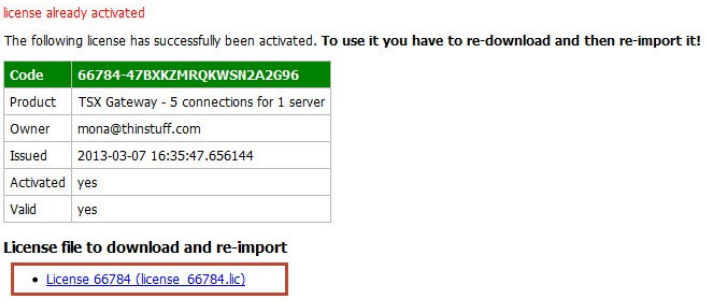
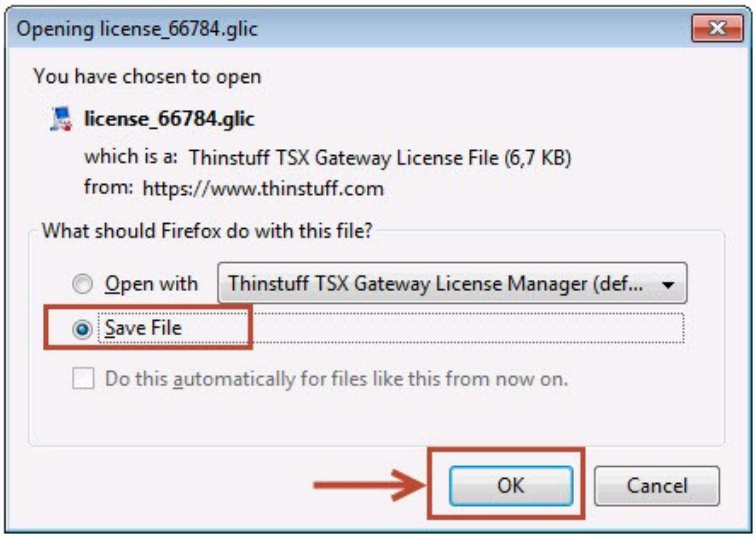


fig. 2 In the following dialogue please select „Save" to save the license file.



6. *Copy the license file* (license_XXXXX.glic) on that computer, where you have installed TSX Gateway

7. *Import the license*

fig. 1 Open the TSX Gateway License Manager select in menu bar "File" and in drop-down menu "Import license from file"

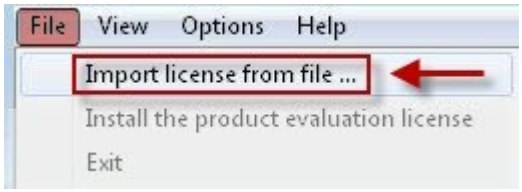
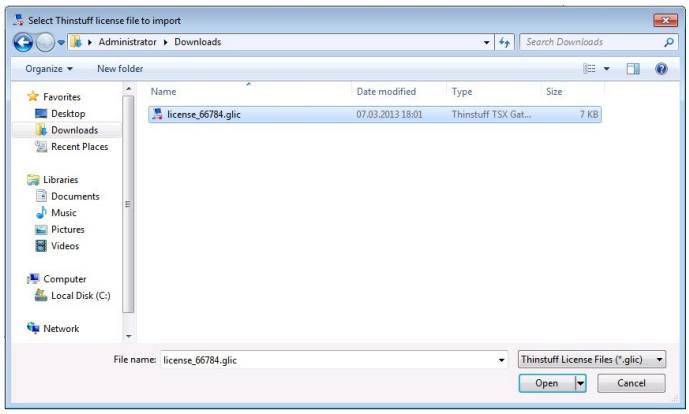
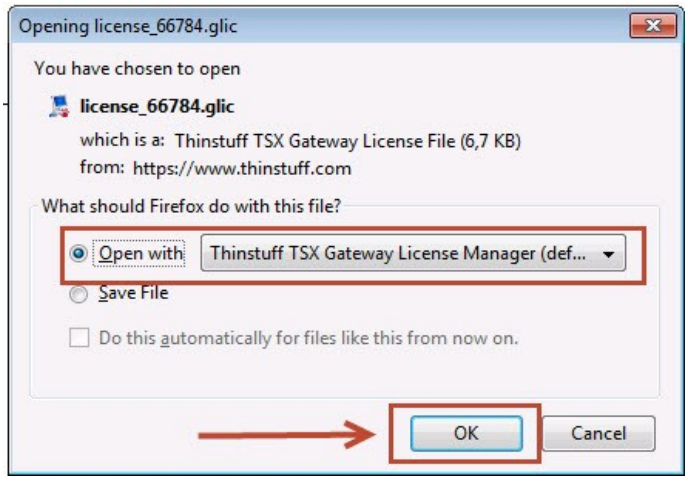


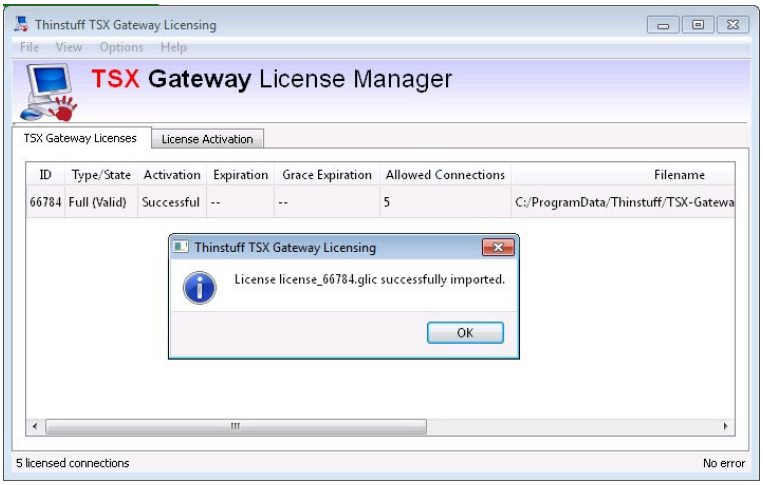
fig 2 Now select your license file (.glic) and click on „Open".





8. *Activation completed*

fig.1 As shown in the window, the license appears now as valid in your TSX Gateway License Manager.



4.6 Licensing on virtual machines

On virtual machines the TSX Gateway license is always bound to the MAC address of the primary Windows network interface.

In following cases this can lead to problems with TSX Gateway licensing:

A) If you on e.g. VMWARE try to move or copy a virtual machine and select "create new identifier" a new MAC address is created.

B) Also changing the order of the network interfaces in Windows (if. e.g. another network interface is added - e.g. a VPN connection ...) causes the MAC address of the primary Windows network interface to change.

C) Some visualization solutions (e.g. HyperV, Xen, etc.) will create a new MAC-address for every new Guest OS.

In all of this cases the TSX Gateway license becomes invalid (invalid hardware key)
To avoid this, please make sure that the MAC address of the primary Windows network interface does not change on virtual machines.

In case B) you can fix your problem by recreating the initial order of the Windows network interfaces.

In case C) can be avoided by assigning a static MAC-address.

If you use a visualization platform (e.g. VMWare, HyperV, Xen, etc.), please assign a static MAC-Address to your Virtual Guest Computers before you install TSX RemoteApp server.

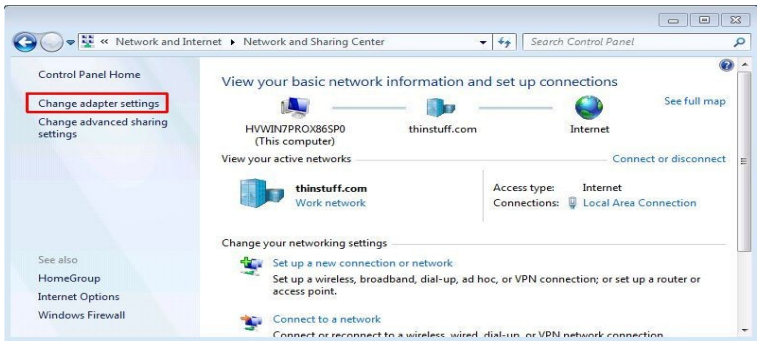
4.6.1 Change of the Primary Network Interface

Please follow the steps below to change your network adapter:

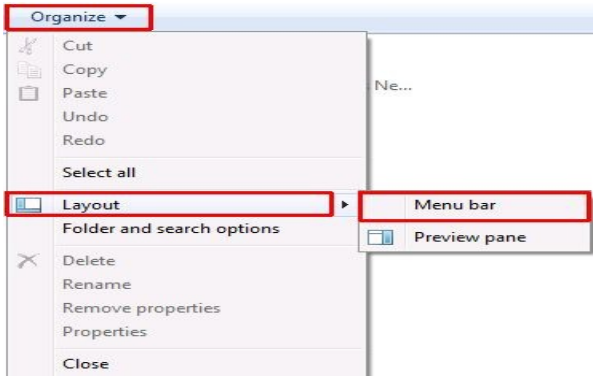
1. Go to "Start" and open "Control Panel"

2. Open in the preference window "**Network and Internet**" and click to **"Network and Sharing Center"**

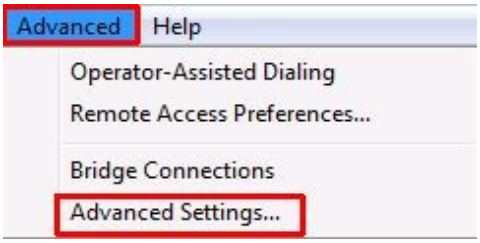
3. There you will find "**Change Adapter Settings**" next to the point that you open.



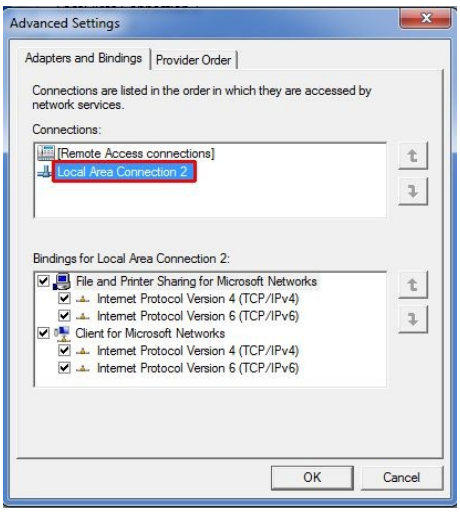
4. By default the menu bar is hidden, but it can be shown by "**Organize → Layout → Menu bar**"

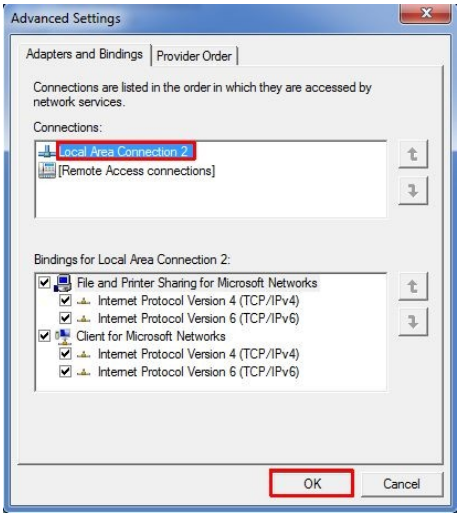


5. Now please open the "Advanced Settings", click to Advanced → Advanced Settings.



6. To change the priority of a network adapter, please select the favoured adapter from and move with the arrow key on the right. Subsequent click OK.





4.7 Reactivation

TSX Gateway license is bounded by activation to the hardware of the respective computer. If the hardware has changed significantly on your system (replacement of motherboard, any component or of the entire computer), in the TSX Gateway License Manager on your machine will be displayed the error message "Invalid hardware key".

For virtual machines, this case occurs, when the MAC-address of the primary Windows network interfaces has changed.

In such a case please contact your trader or send us an email: *support@thinstuff.com*.

IMPORTANT! Please enter in the email with your customer number, license number, and the reason for the reactivation.

After approval of reactivation by Thinstuff your license can be reactivated (see 4.5 Activation).

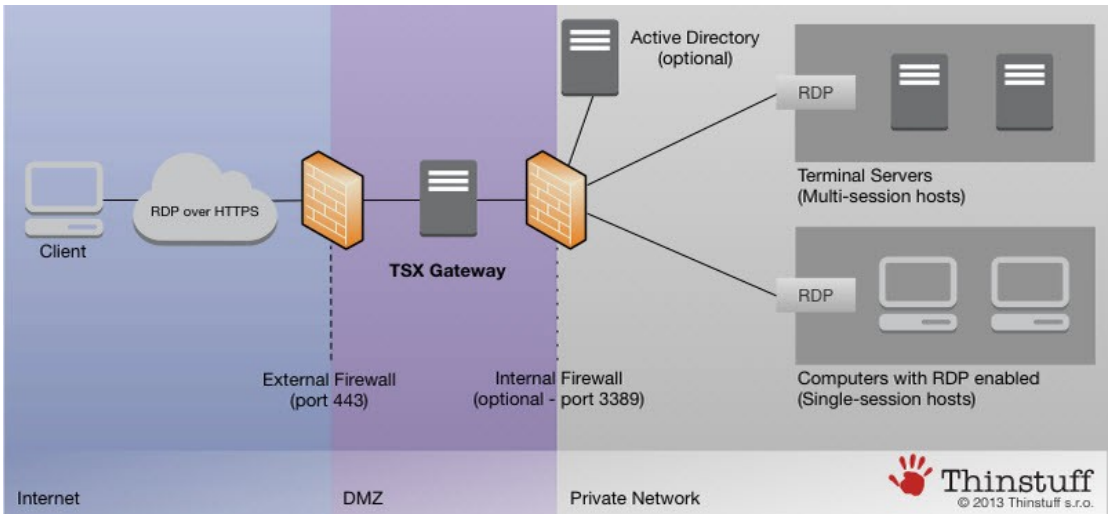
5 Usage

5.1 Technical Explanation

TSX Gateway is not only a proxy but has to be seen as Terminal Server VPN.

Remote users are using the internet connection to establish an encrypted, secure connection to the network. Once established the users are able to perform a remote session to the terminal server using RDP through HTTPs (encrypted version of HTTP uses port 443 based on a certificate).

Using TSX Gateway you can connect to internal resources that are hosted behind the firewall.



1. The user initiates the connection to the private network using an RDP file
2. An SSL tunnel is established between the client and the TSX Gateway server using an SSL certificate. Before the connection is established the server must authenticate and authorize the user according to the Connection Authorization Policy (CAPs) configured in TSX Gateway.
3. When authentication/ authorization has succeeded the client requests a connection to the terminal server (internal resource).
4. The server verifies the name of the terminal server against the name configured in the Resource Authorization Policies (RAPs) configured in TSX Gateway.
5. If the name matches the TSX Gateway server authorizes the request and establishes the secure tunnel through TSX Gateway over HTTPs between the client and the terminal server.

6. From this point any packets the client sends will be forwarded from the TSX Gateway to the resource and vice-versa (now TSX Gateway is acting as proxy).
7. To establish the remote session the Windows Authentication is required (enter credentials).
8. After successful authentication the encrypted RDP packets are sent from the client to the Gateway server over port 443, the server forwards these packages to terminal server using port 3389.

5.1.1 How To Do – Checklist

1. Install TSX Gateway (3 Software installation and maintenance)
2. Use demo license or activate purchased license-ID (4.5 Activation)
3. Open TSX Gateway Management Console, login as Administrator
4. Create/ Import /Download certificate server-side (5.2 Certificates (Server-Side))
5. Install certificate client-side (5.3 Certificates (Client-Side))
6. Configure CAPs and RAPs (5.4 Authorization Policies)
7. Configure RDP-File for remote-connection

5.2 Certificates (Server-Side)

To establish a secure VPN connection between the TSX Gateway and the client private key and public key are required to encrypt the connection.
These keys are included in certificates.

You can obtain a certificate in several ways:

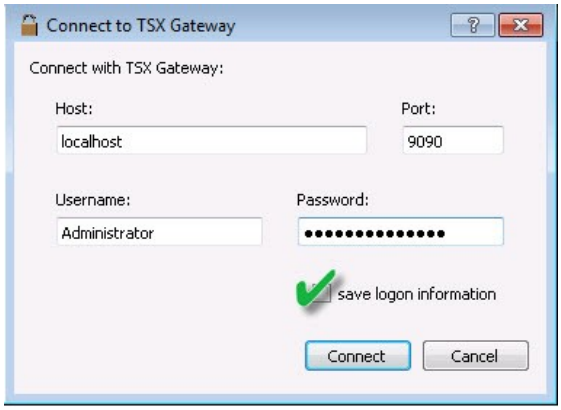
- 5.2.1 Create self-signed certificate
  Either when you install TSX Gateway or
  Create and download certificate in the TSX Gateway Management Console
- 5.2.2 Upload an existing certificate in the .PEM format
- 5.2.3 Create Certificate in Microsoft Certification Authority .PFX format
- Purchase certificate from one of the known certification authority (CA)

Please note !!!
For testing and evaluation purposes we recommended that you use a self-signed certificate.

5.2.1 Create a self-signed certificate

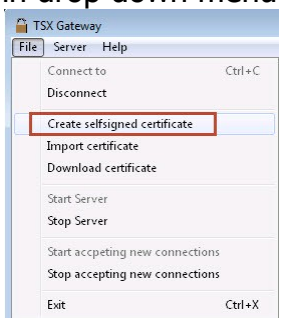
This chapter describes how to use the TSX Gateway Management Console in order to create a self-signed certificate.

1. To open "*TSX Gateway Manager"* login with a local Windows Administrator account.

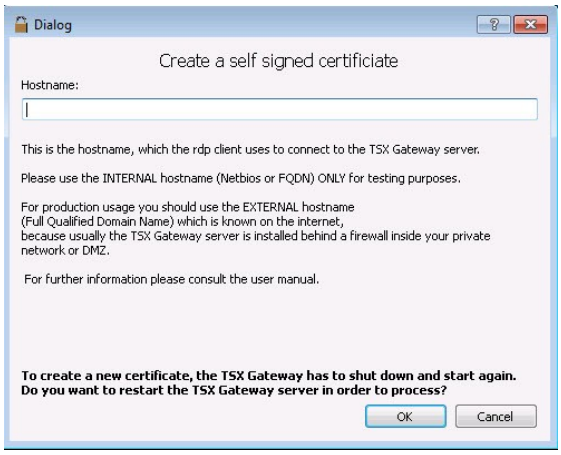


You have the possibility to save the credentials (not recommended)

2. Click „File" in the menu bar and choose "*Create self signed certificate*" in drop down menu list.



3. Enter now the "*Hostname*". The CN (Certificate Name) must match the DNS name that the client uses to connect to the TSX Gateway Server. You have to use internal hostname (NetBIOS) only for testing purposes!

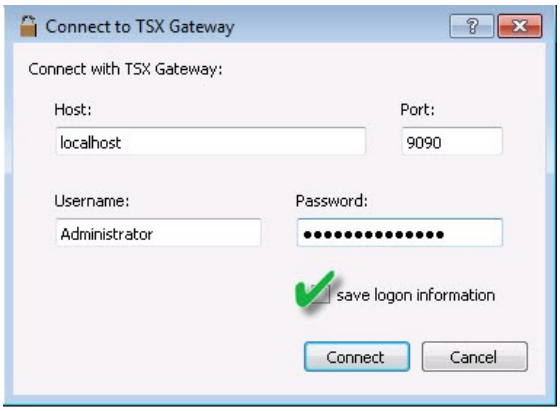


Click "OK" to confirm

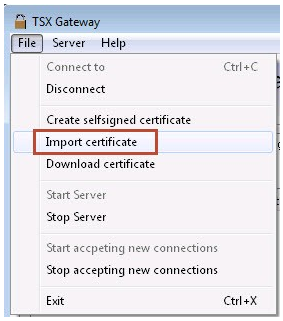
4. A new self-signed certificate is now installed. It can be found in the installation path of the TSX Gateway Server.

5.2.2 Upload Certificate (PEM or PFX)

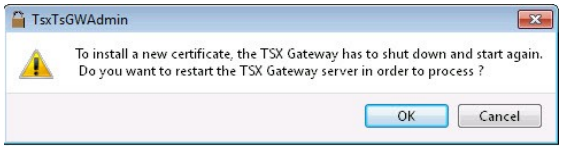
1. To open "T*SX Gateway Manager"* login with a local Windows Administrator account



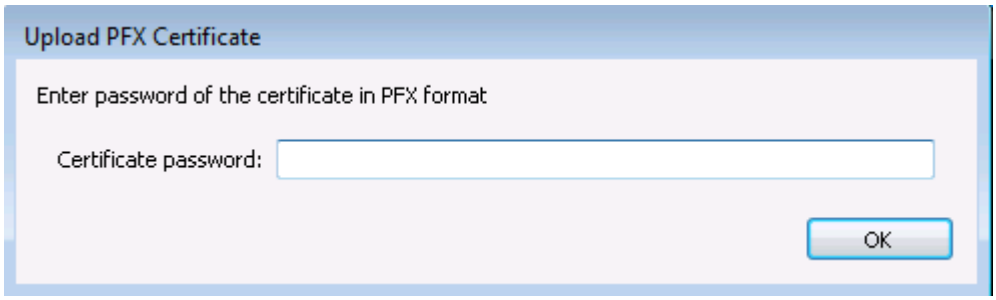
2. Click „*File*" in the menu bar and choose "*Import certificate*" in drop down menu list.



3. To install/upload a new certificate please click on „*Import certificate*" and approve the upcoming notification by clicking on „*OK*".



4. Now select your existing certificate by navigating to the enclosing folder in which the certificate has been saved. The certificate has to be in the "*.pem" or "*.pfx" format.
5. Upload your certificate by clicking on „*Open*".
6. If you use certificate in pfx-format the pfx file password is required



7. Approve the notification dialogue by clicking on „*OK*". The Certificate has now been uploaded and installed.

5.2.3 Create certificate in Microsoft Certification Authority

You will find in our FAQ[6] a pdf-file how to create a certificate, install and import into TSX Gateway.

This procedure presupposes a technical know-how and according environment. Please understand that this information is not part of the TSX Gateway User Manual.

5.3 Certificates (Client-Side)

This chapter describes how to install the certificate (chapter 5.2.1 Create a self-signed certificate or 5.2.3 Create certificate in Microsoft Certification Authority) on the client computer.

This certificate has to be installed on the client computer because it contains the public key for encrypting/decrypting.

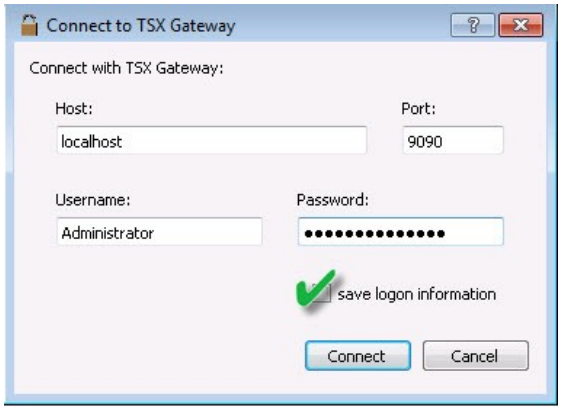
To establish the SSL session with the server the client needs to validate the server's certificate. Therefore the clients must have the CA certificate installed in its "Trusted Root Certificate Store".

You can obtain a certificate for the client computer by following steps below.

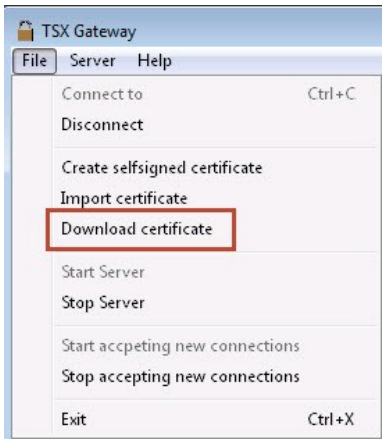
[6] http://www.thinstuff.com/faq/index.php?

5.3.1 Download Client Certificate

1. To open *TSX Gateway Manager* login with an Administrator account



2. Click „*File*" in the menu bar and choose "*Download certificate*" in drop down menu list.



3. Please select the path where TSX Gateway should save the client certificate. The certificate will be saved in the .crt format.

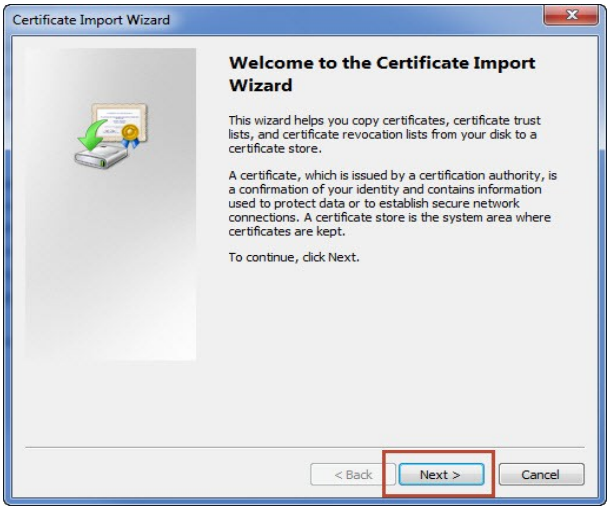
4. Now import this certificate into your client's certificate store.
5.3.2 Install Downloaded Client Certificate

5.3.2 Install Downloaded Client Certificate

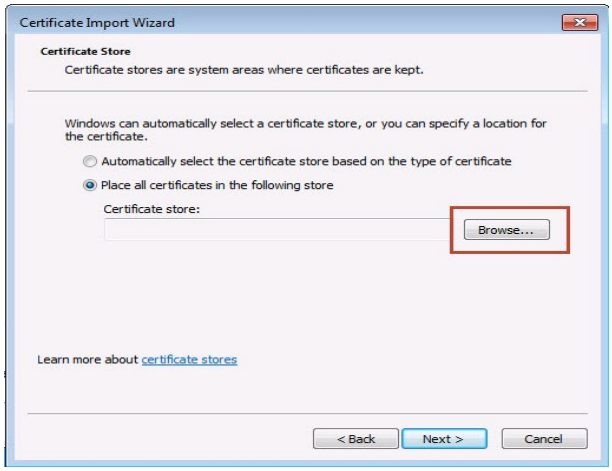
To import a client certificate by using the Certificate Import Wizard please follow these steps:

1. Double click your client certificate and click on „*Install Certificate...*"

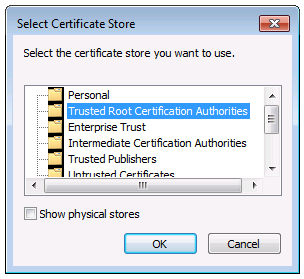
2. The Certificate Import Wizard will now open. Please click on „*Next*".



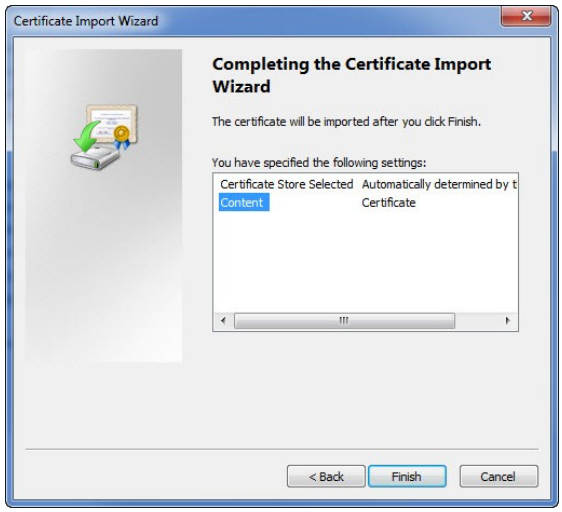
3. Select „*Place all certificates in the following store*" and click "*Browse...*"



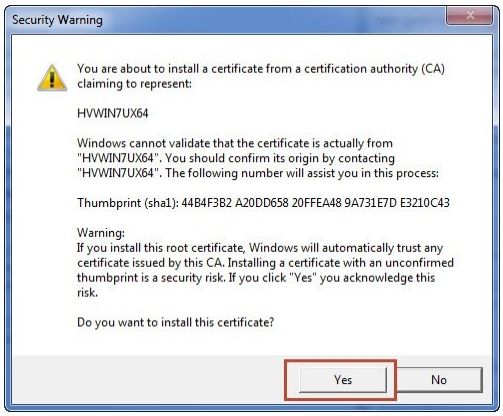
Select "*Trusted Root Certification Authorities*" and confirm with "*OK*"



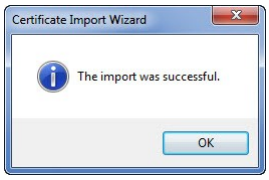
4. To complete the import process click on „*Finish*".



5. Confirm the upcoming security dialogue with „*Yes*".



6. The import was now successful.

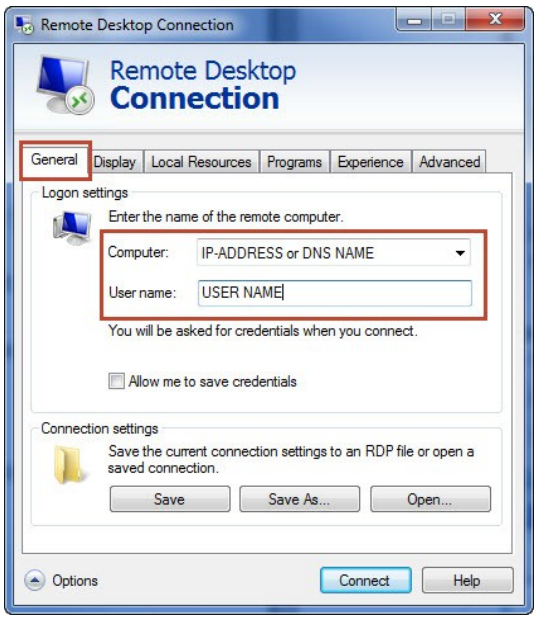


Now you can start your remote session

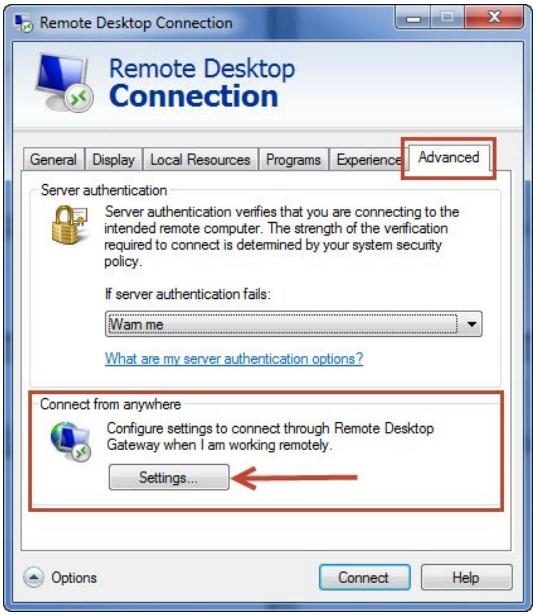
→ see chapter 5.3.3 Configure remote-session with TSX Gateway setting

5.3.3 Configure remote-session with TSX Gateway setting

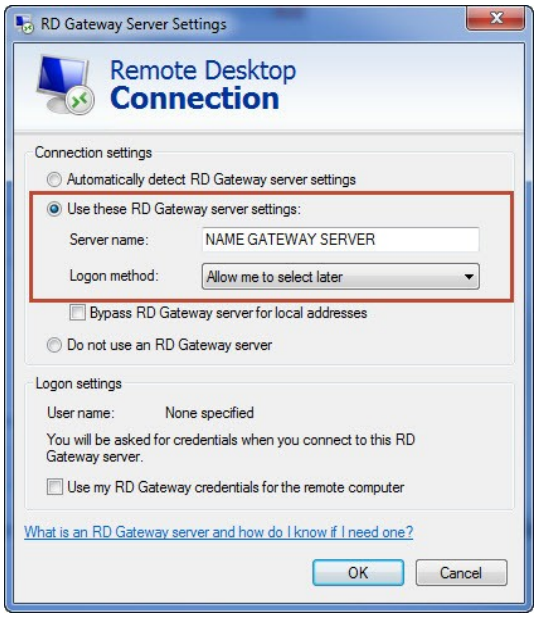
1. Open your Remote Desktop Connection (mstsc.exe)
2. Enter the name of the remote computer in tab "*General*"



3. Navigate to tab "*Advanced*" and click on "*Settings*" under the "*Connect from anywhere" section*



4. Enter the server settings of your TSX Gateway Server and click on "*OK*".



Please note !!!
Enter now the "Hostname" of your server running *TSX Gateway* . The entered name must match the DNS name you have entered when creating the certificate server-side.
You may use internal hostname (NetBIOS) but only for testing purposes!

Additional options

"*Bypass TD Gateway server for local addresses*" can be checked if you force authentication only for external incoming connections.
Not recommended for testing!

"*Automatically detect RD Gateway server settings*"
This option requires according environment (not part of this manual)

"*Use my RD Gateway credentials for the remote computer*"
Only enable this option if user logon credentials are the same to login to the Terminal Server.

5. Now click on "Connect" to start the remote-session.

5.4 Authorization Policies

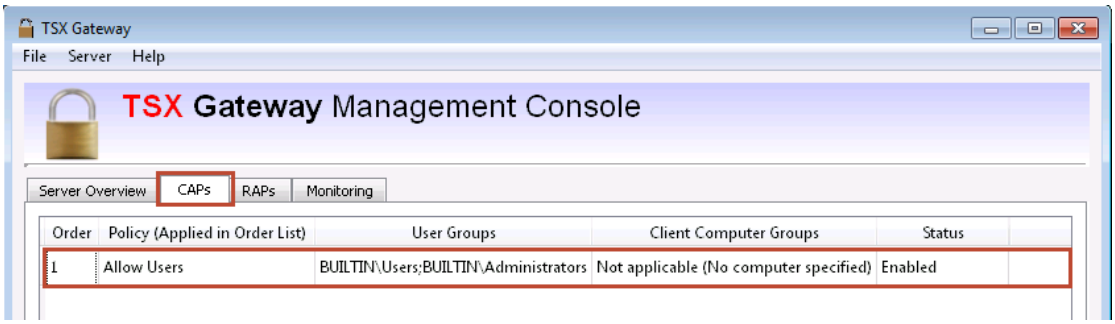
This chapter describes how TSX Gateway uses Authorization Policies to control remote user access and remote connections to internal network resources beyond the gateway.

CAPs and RAPs allow to granularly grant network access based on needing for the clients and at the same time securing the network.
TSX Gateway communicates with Active Directory, it pulls its users or user groups from the central location. Without this ability you have to set up local users or user groups to configure the Authorization Policies.

5.4.1 Connection Authorization Policies (CAPs)

CAPs allow the administrator to specify connection criteria that must been met to connect to the TSX Gateway server. If the first criteria is not met, TSX Gateway will evaluate the second policy, etc. until one TSX CAP fits. If none of these settings is met the remote access is denied.

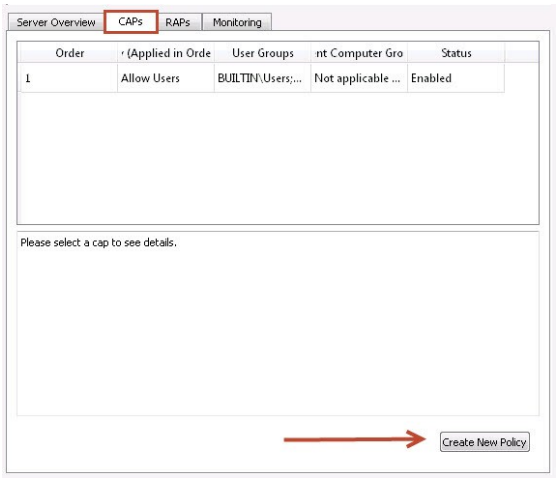
Open the "*TSX Management Console*" and login with Administrator Account. Switch to tab "***CAPs***".



Per default one policy is already preconfigured to allow all users to access the internal network.

5.4.1.1 Create a CAP

In tab "CAPs" you will find bottom right possibility to "*Create New Policy*"

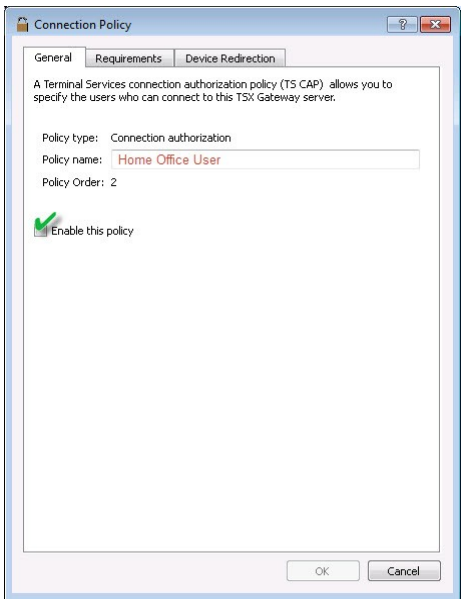


Connection Authorization Policies are divided into 3 sections:

- General
- Requirements
- Device redirection

1. Tab "***General***"

   Specify the name of the new policy– in our example "Home Office Users"
   You can also enable/disable the policy.

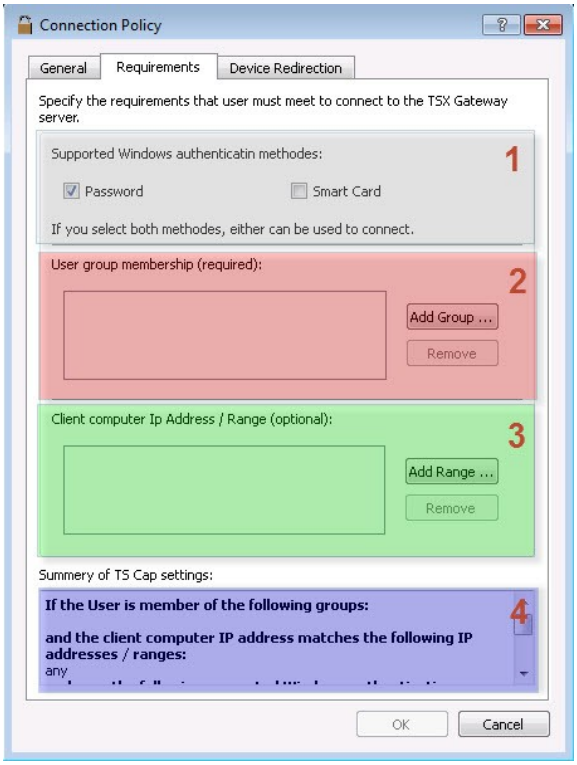


2. Tab "***Requirements***"

- *Authentication Method*
  In the first part please enable "*Password*" for Windows Authentication. "Smart Card" authentication is currently not supported.

- *User group membership* (required)
  Add those users or user groups who are allowed to use internal resources
  To specify a user group (which members can connect to the TSX Gateway) please click on "*Add Group*".

- *Client computer IP addresses*
  Specify the client's computer IP address/range in order to allow/restrict the access to TSX Gateway for specific IP address.



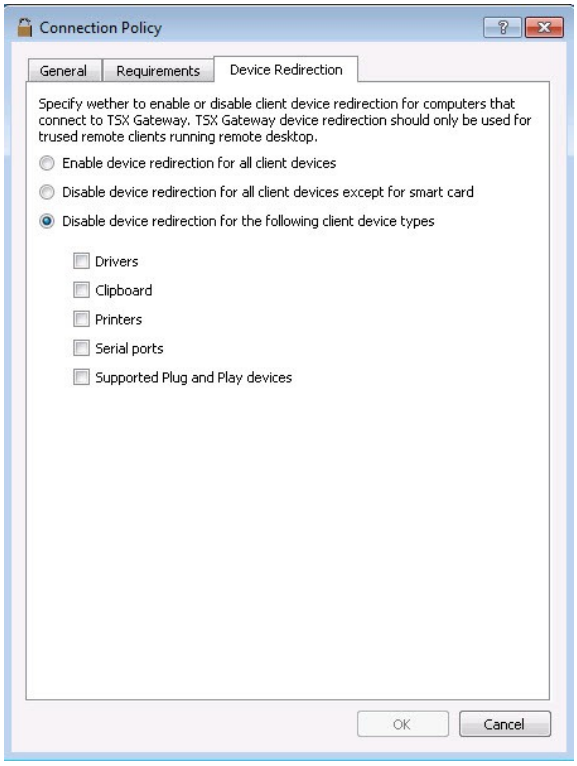
In fourth part you will find the summary of configured "*Requirements*"

3. Tab „***Device Redirection***"

Enable or disable client device redirection for computers that connect to TSX Gateway.

You can choose between the following settings:

- Enable device redirection for all client devices
- Disable device redirection for all client devices except for smart-card
- Disable device redirection for specific client device types (select separately Drives, Clipboard, Printers, Serial Ports and Supported Plug and Play devices)



As soon as configuration for the policy is done, move back to tab "*General*" and click on „*OK*" to enable the new policy.

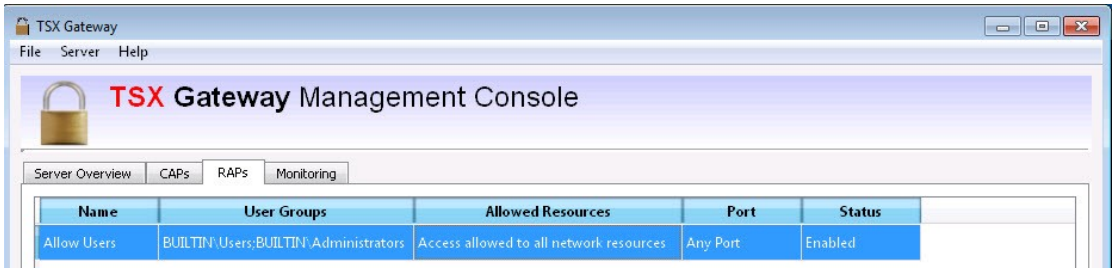
5.4.2 Resource Authorization Policies (RAPs)

RAPs allow you to specify the internal network resources (computers) that remote users can connect through TXS Gateway Server.

Example:

> *You might specify that external employees (members of group "External") may only connect to terminal server 1, while internal employees (group "Internal") might access terminal server 2.*

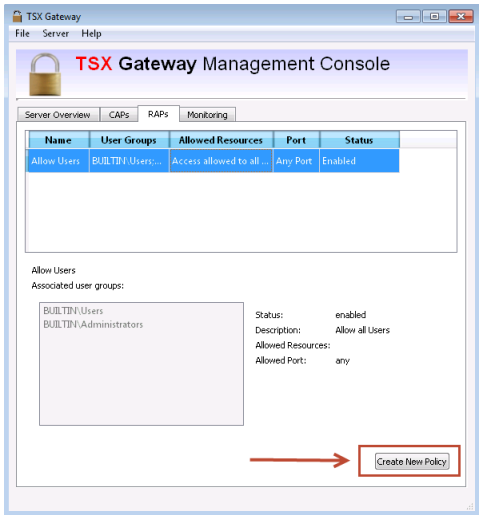
Open the TSX Manager Console and login with a local Windows Administrator Account.
Switch to tab "***RAPs***".



Per default one policy is already preconfigured to allow all users to access the all internal network, all ports allowed.

5.4.2.1 Create a RAP

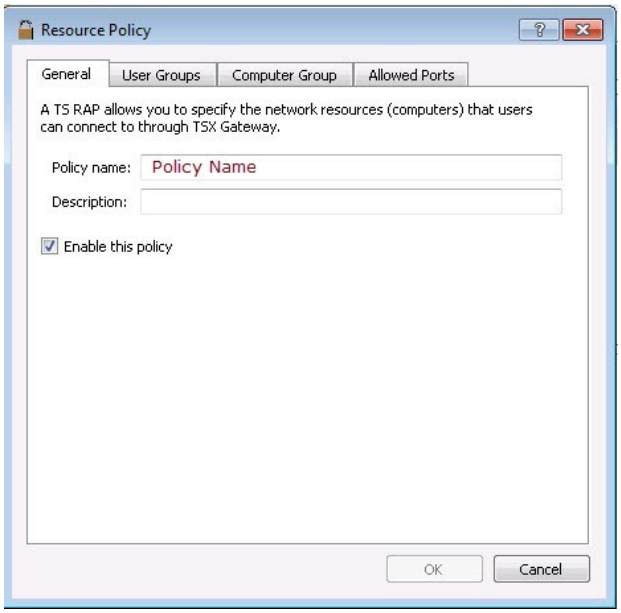
In tab "*RAPs*" you will find bottom right possibility to "*Create New Policy*"



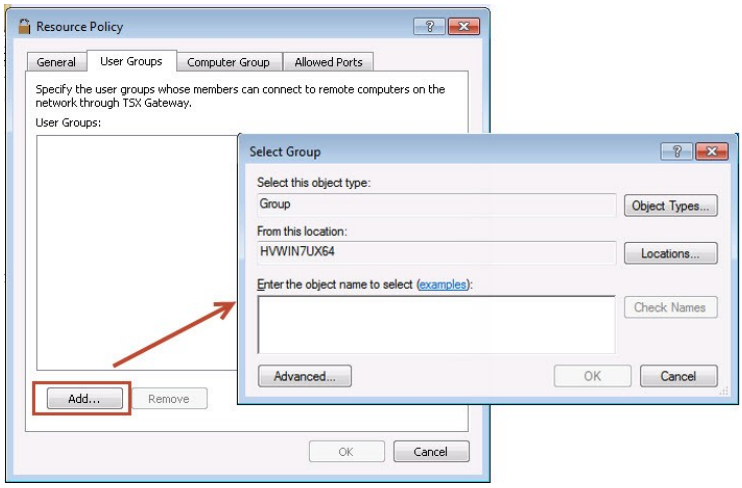
"*Resource Policy*" is divided into 4 sections:

- General
- User Groups
- Computer Groups
- Allowed Ports

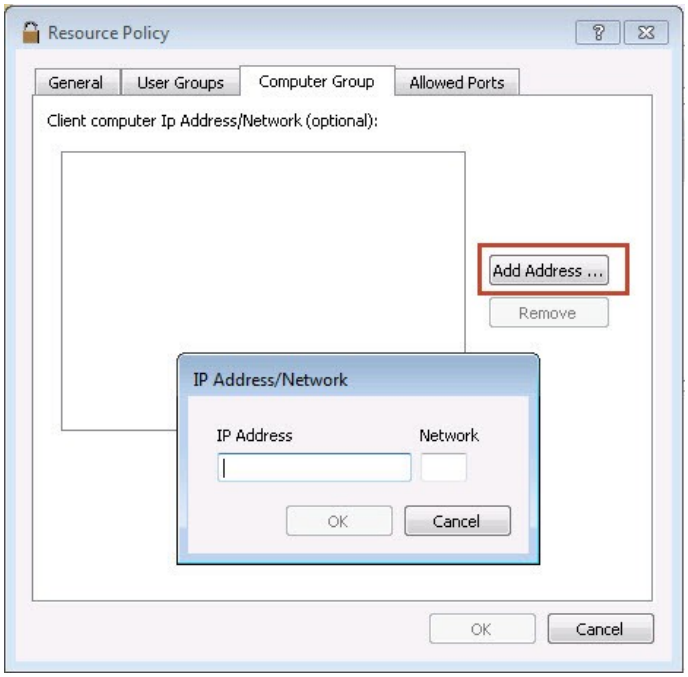
1. Tab "***General***"
   Specify a policy name and a description of your new policy.
   You can also enable/disable the policy.



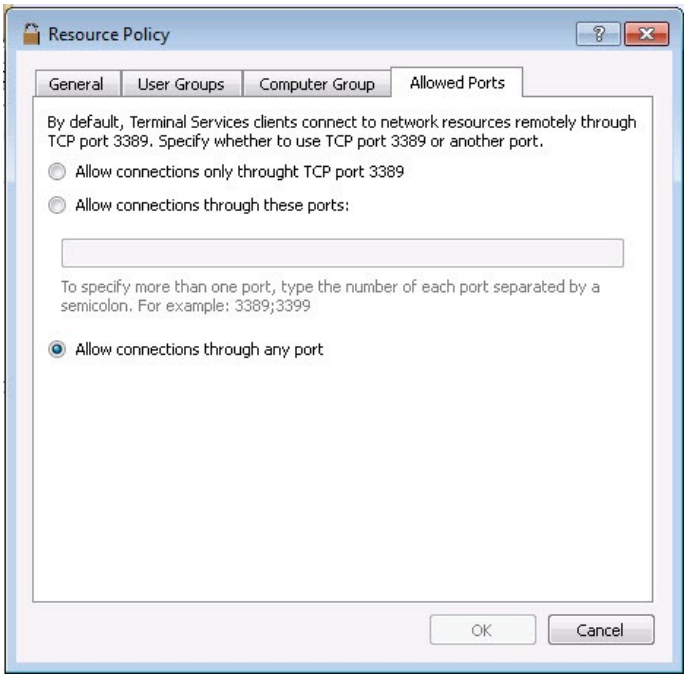
2. Tab „***User Groups***" (required)
   To specify a user group to which you want this RAP to apply please click on "Add Group".



3. Tab „***Computer Groups***“ (optional)
Specify the client computer IP address(es)/range to which this RAP should apply.
Click “Add Address” and enter “*IP-Address*” and “*Network*” of your terminal server (Example: Network “32” specifies one specific host)

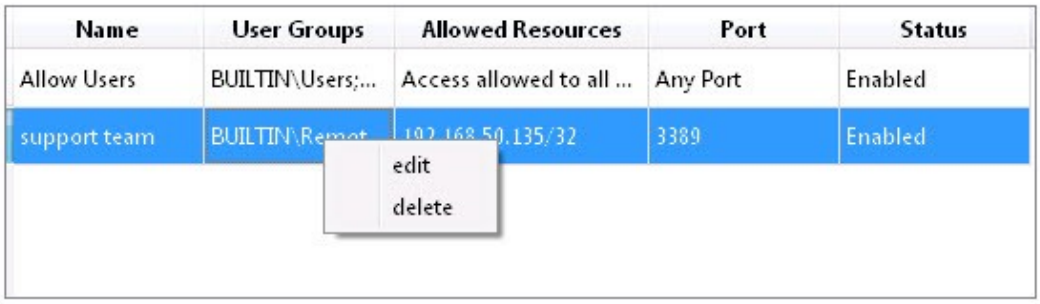


4. Tab „***Allowed Ports***“
By default, Terminal Services clients connect to network resources remotely through TCP port 3389. Specify whether to use TCP port 3389 or another port.



After you have specified the policy move back to tab "General" and click „OK" to enable the new policy.

If you want to delete or edit any of the existing policies (not matter if CAP or RAP) just do a right click and select „*delete*" or „*edit*" in context menu.



5.5 Monitoring

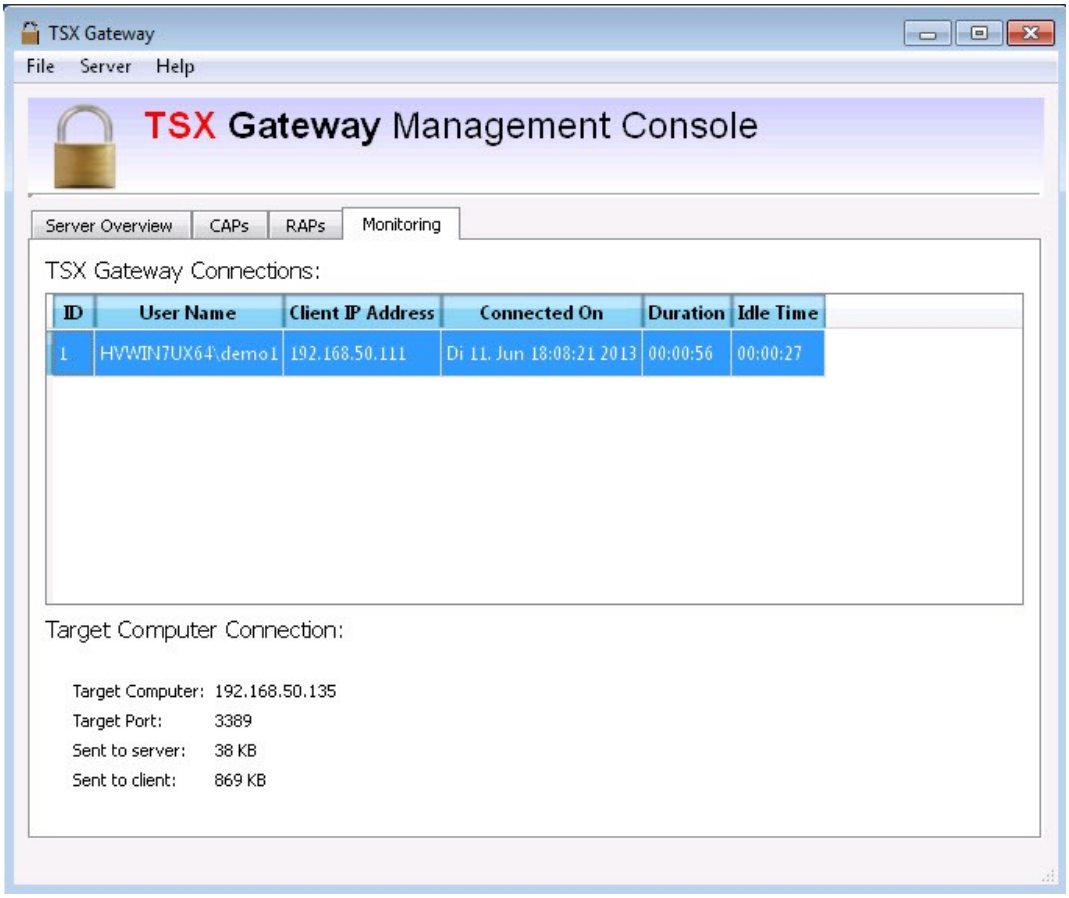
This section describes how to observe all active connections by using the live monitoring of TSX Gateway.

5.5.1 Show Monitoring

To open "*TSX Gateway Manager*" login with a local Windows Administrator account and switch to the tab "*Monitoring*"

You can now observe the following connection details:

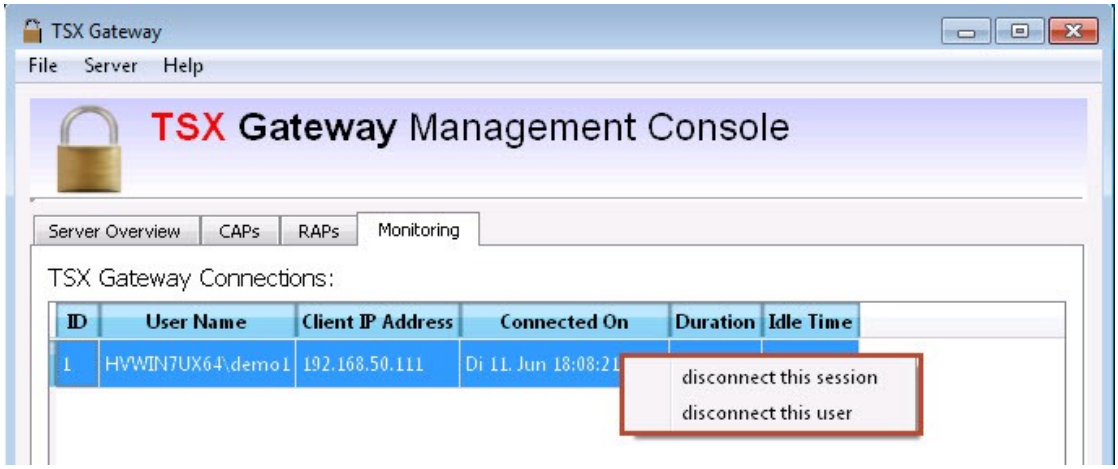
ID, User Name, Client IP Address, Connected On, Duration, Idle Time.



5.5.2 Disconnect a Session / User

To disconnect a session please do the following:

Right click highlighted session and choose from context menu …



1. Select the session/user, which you want do disconnect
2. After that right-click this session and choose "disconnect this session" respectively "disconnect this user"

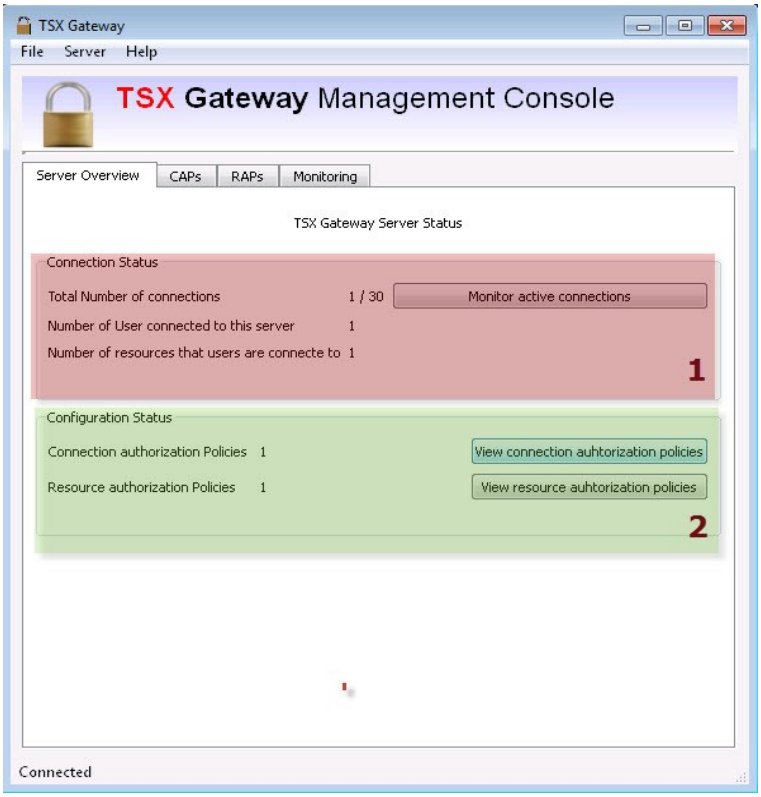
5.6 Server Overview

To open "*TSX Gateway Manager*" login with a local Windows Administrator account and switch to the tab "*Server Overview*"

In this overview you will see

(1) "Connection Status"

(2) "Configuration Status"



(1) Connection Status

In this overview you will get following information

* "*Total Number of connections"*
  (if you click button "*Monitor active connections*" you will switch to tab "Monitoring"
* "*Number of Users connected to this server*"
* "*Number of resources that users are connected to*"

(2) Configuration Status

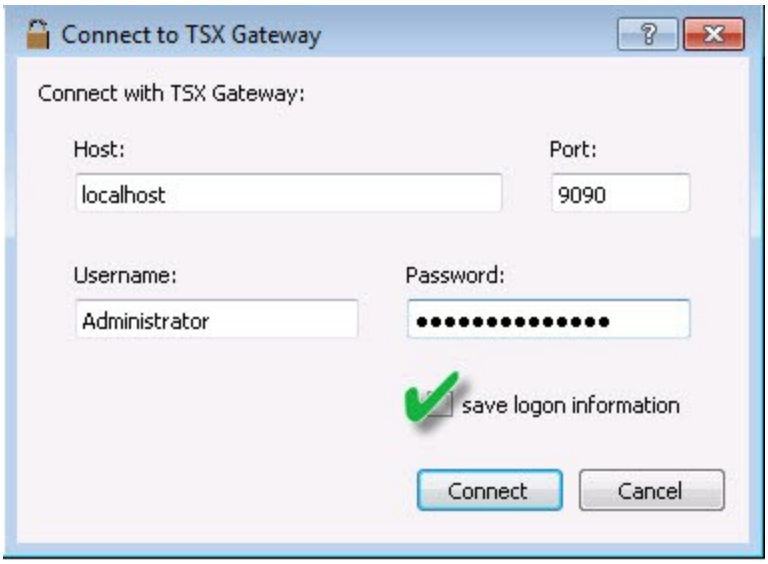
Number of policies

* Connection authorization Policies" (→ if you click "*View connection authorization policies*" you will switch to tab "*CAPs*")
* Resource authorization Policies" (→ if you click "*View connection authorization policies*" you will switch to tab "RA*Ps*")

5.7 Menu Bar

5.7.1 File

1. *Connect to*:



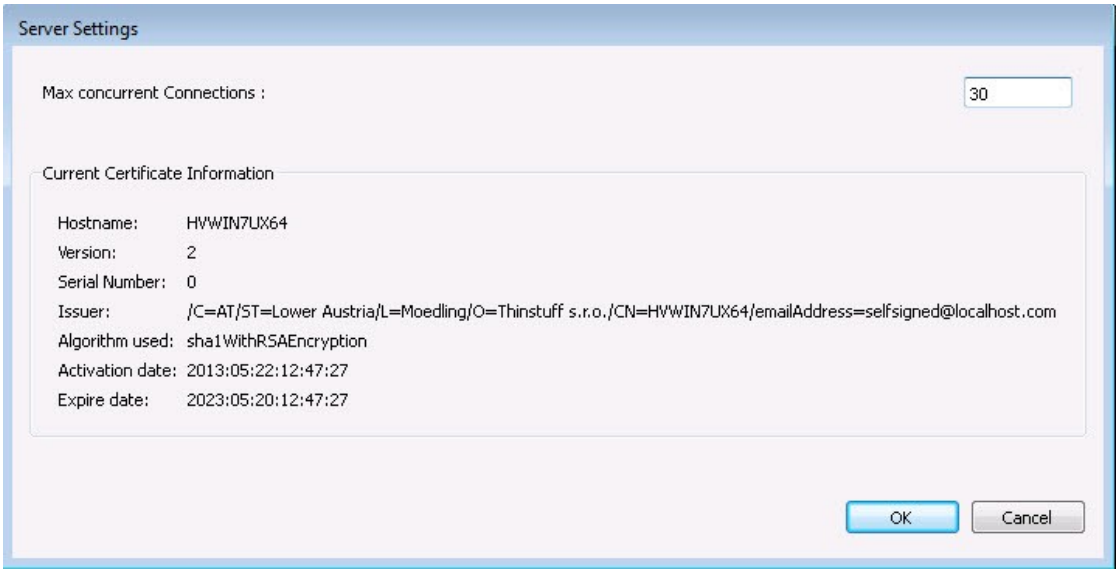
To open *TSX Gateway Manager* login with a local Windows Administrator account

2. *Disconnect*:
   Log-off from *TSX Gateway Manager*
3. *Create self-signed certificate*
   All information you will find in chapter: 5.2.1 Create a self-signed certificate

4. *Import certificate*
   All information you will find in chapter:
   5.2.2 *Upload Certificate (PEM or PFX)*
5. *Download certificate*
   All information you will find in chapter: 5.3.1
6. *Start Server*:
   Part of "TSX Gateway" service – incoming connections will be accepted according configured policies (CAPs and RAPs)
7. *Stop Server*:
   Part of "TSX Gateway" service – all connections will be terminated
8. *Start accepting new connection*:
   Accept new incoming connection – must be started if "*Stop accepting new connection*" was selected before
9. *Stop accepting new connection*:
   Refused only all new incoming connection, existing connections will not be terminated (unlike "*Stop Server*")

5.7.2 Server

1. *Settings*:
   License for TSX Gateway basically accepts a unlimited number of connection. You may limit the maximum number of concurrent connection in the "*Server Settings*":

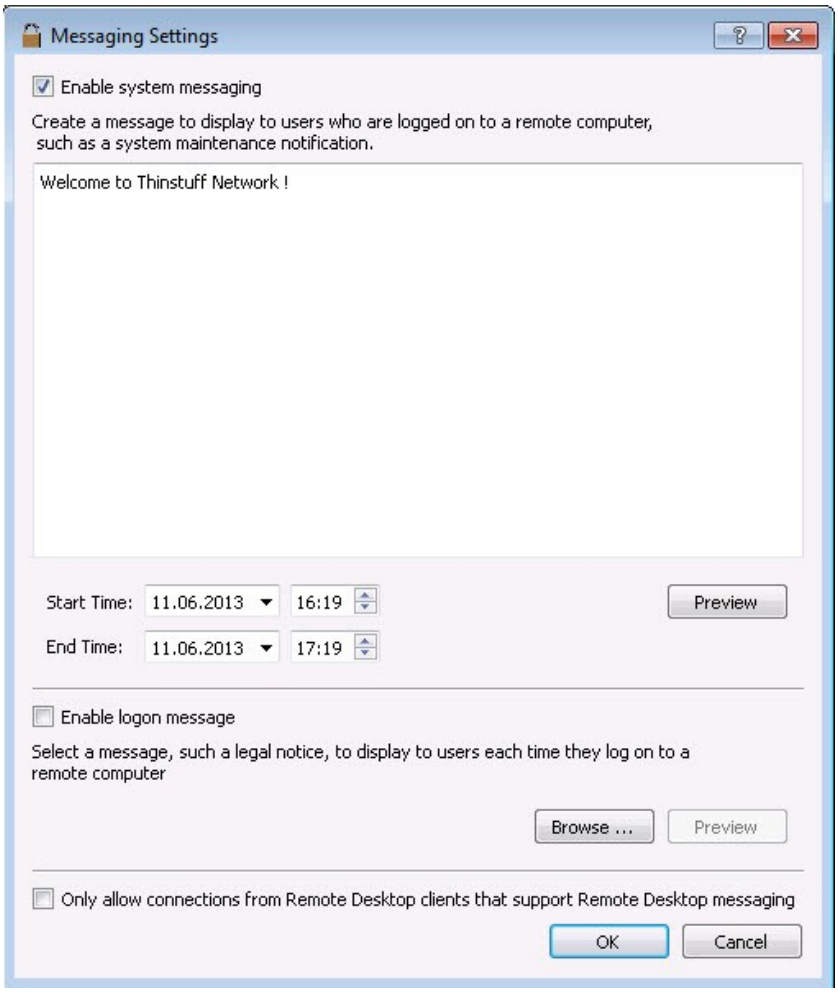


   And here you see the information regarding used certificate.

2. *Messaging*:

Here you may configure
→ "*Enable system messaging*": message will pop-up in configured time period. You may also configure Start Time / End Time for this message
→ "*Enable logon message*": such as legal notice, etc.

→ "*Only allow connections from Remote Desktop clients that support Remote Desktop messaging*"



5.7.3 Help

About Thinstuff TSX Gateway

6 Support

6.1 General Support

Thinstuff Support is available to provide support and will answer your questions about our products, sales, our company and non-technical questions.

All general inquiries should be addressed to: sales@thinstuff.com

6.2 Technical Support

For any technical questions about our products please contact our technical customer support.

Address your support request to support@thinstuff.com and please enter the following information:

- TSX Gateway or XP/VS License-ID
- Thinstuff Customer ID or your email-address
- installed Thinstuff components

6.3 Online Resources

FAQ Page

On this page you will find answers to the most frequently asked questions.

http://www.thinstuff.com/faq

Product Side

http://www.thinstuff.com/products/tsx-gateway/

Download Trial Version

http://www.thinstuff.com/releases/ThinstuffTsxGateway-latest.exe

Changelog

http://www.thinstuff.com/releases/tsx-gateway-changelog.txt