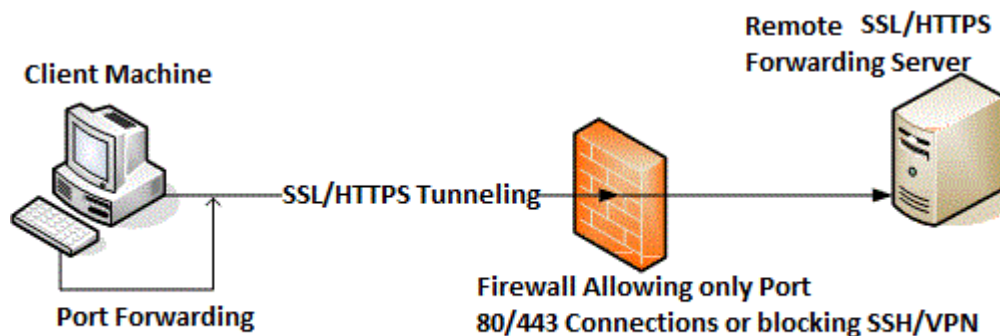


Stealth SSH Tunneling (Windows, Linux, Mac)

In situations where you are behind a strong firewall, Deep Packet Inspection device or proxy that blocks all ports and only allow outgoing connections on ports 80(HTTP) and 443 (HTTPS), we do offer a stealth SSH Tunneling which will enable you to create a secure SSH tunnel (SSH Socks 5 proxy) using only a web browser and Putty/SSH client. Since Putty does not require any Administrative rights to run, you can easily setup a secure SSH tunnel using this technique on any PC in which you cannot install software such as public computer due to lack of admin rights.

How It Works:

Our SSL server runs outside the restricted network and it acts as a normal HTTPS server. A client program (A light weight Java client) from inside the protected network starts up and listen for incoming connection on some local port. The Java client is downloaded and launched by the client browser when the user connects to the server via the browser. The Java client then intercepts TCP/IP requests on the configured port and forward them to the SSL server which in turn routes them to the SSH server. When a new connection is received on this local port, the client program communicates with the SSL server over the restricted network proxy or firewall, and requests the connection to the predefined SSH server.



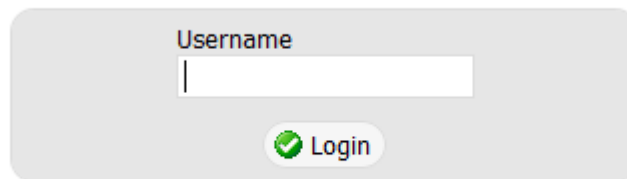
How to Setup

(Instructions for Windows Users):

1. Ensure that Java is installed on your system. If you do not already have Java installed, download and install Java Run Time Environment for your operating system using the link below:
<http://www.java.com/en/download/manual.jsp?locale=en>
2. Using your Java enabled Web Browser (Firefox is Recommended) go to the stealth SSH tunneling web panel URL provided to you

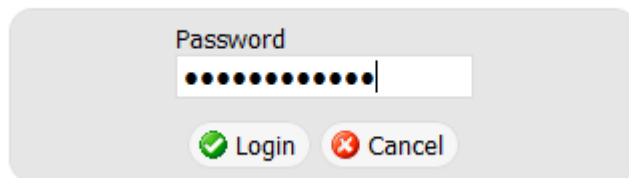
Active subscribers will be provided the URL after signup.

Type your Username and Press Enter or click the Login Icon.



A screenshot of a login form with a light gray background. At the top, the word "Username" is written in a dark gray font. Below it is a white text input field with a vertical cursor on the left. At the bottom of the form is a rounded button with a green checkmark icon and the text "Login".

3. Enter your password and press Enter or click the Login icon:



A screenshot of a password login form with a light gray background. At the top, the word "Password" is written in a dark gray font. Below it is a white text input field where the password is masked with black dots. At the bottom of the form are two rounded buttons: one with a green checkmark icon and the text "Login", and another with a red 'X' icon and the text "Cancel".

4. Accept the self signed certificate when prompted by your browser



This Connection is Untrusted

You have asked Firefox to connect securely to **1** **1** **2**: **4**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- ▶ Technical Details
- ▶ **I Understand the Risks**



This Connection is Untrusted

You have asked Firefox to connect securely to **1**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- ▶ Technical Details
- ▼ **I Understand the Risks**

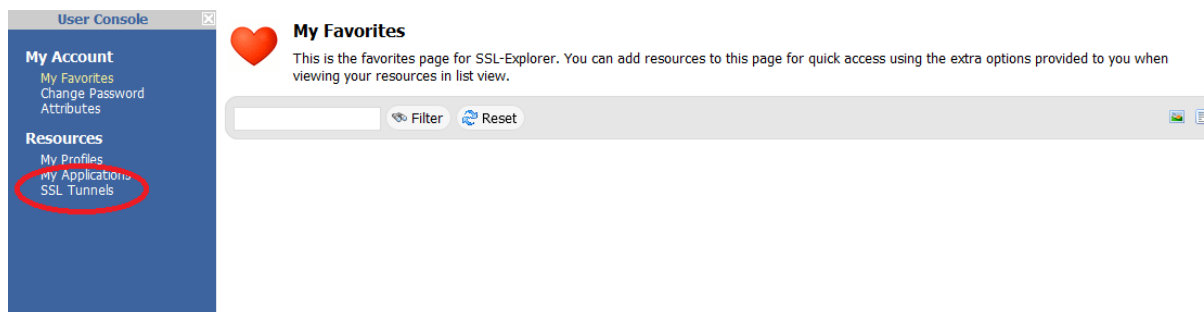
If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

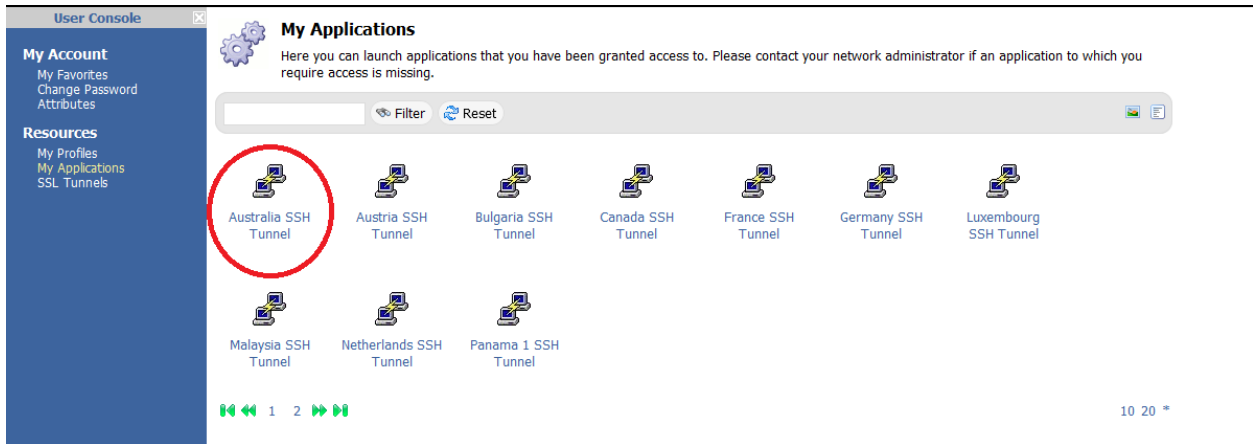
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...



5. After you have login, go to Resources and then **My Applications**. There you will see all our SSH servers with Putty icons. Each server has been configured on a local port 8080. To start your tunnel, first decide on the server you wish to connect to and then click on the server Putty icon. Once clicked, the SSH tunnel will be initialized and a Putty window will automatically open in your computer. You do not have to install or download Putty on your local computer as the SSL Explorer will automatically download and start the Putty.



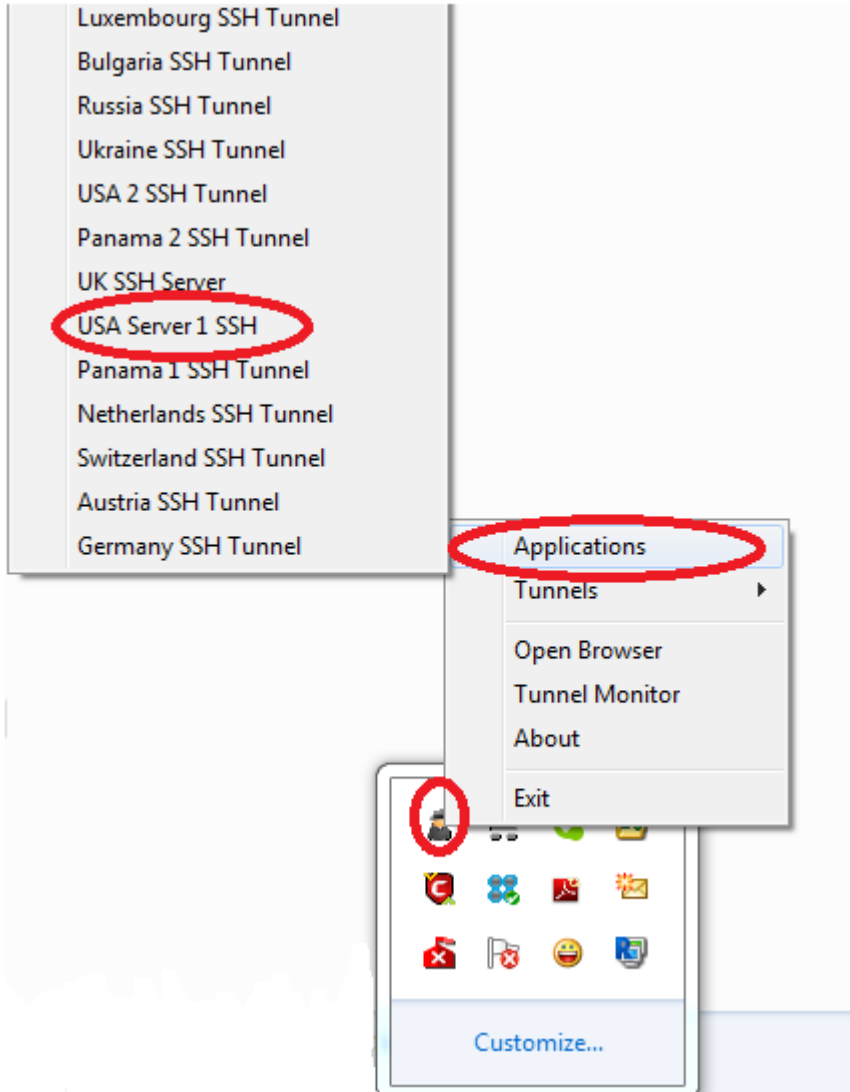


When you login, the SSL Explorer Agent icon will have white nodes/points as shown above. After you start a tunnel, the nodes will be turn to Green which indicates that the Agent is now running. This is shown below:

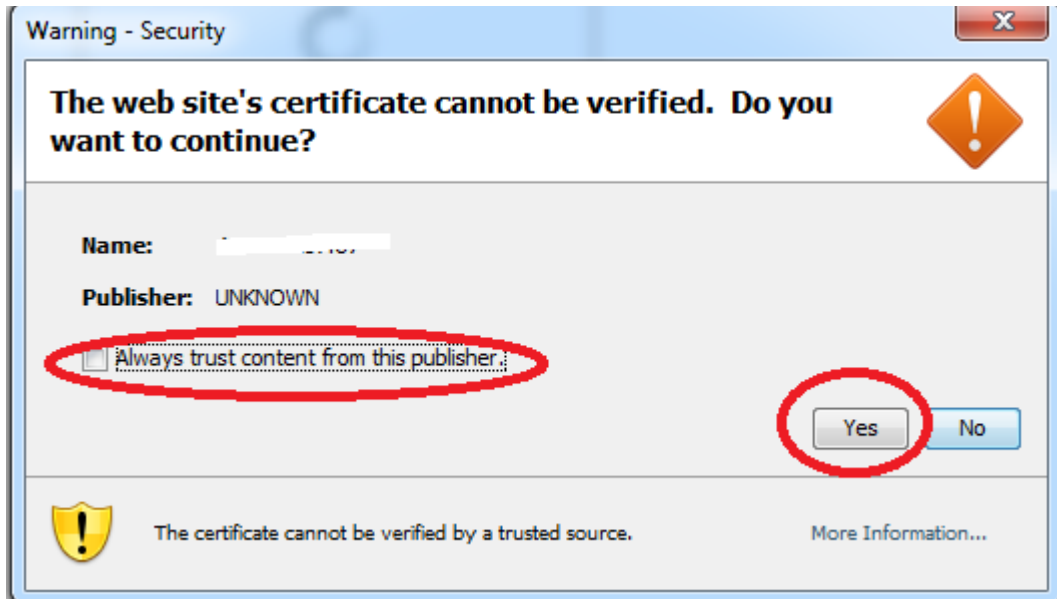


Instead of starting individual resources for each server (SSL Tunnels and Applications), you can also start all the resources for all servers by simply clicking the SSL Explorer Agent icon as shown above.

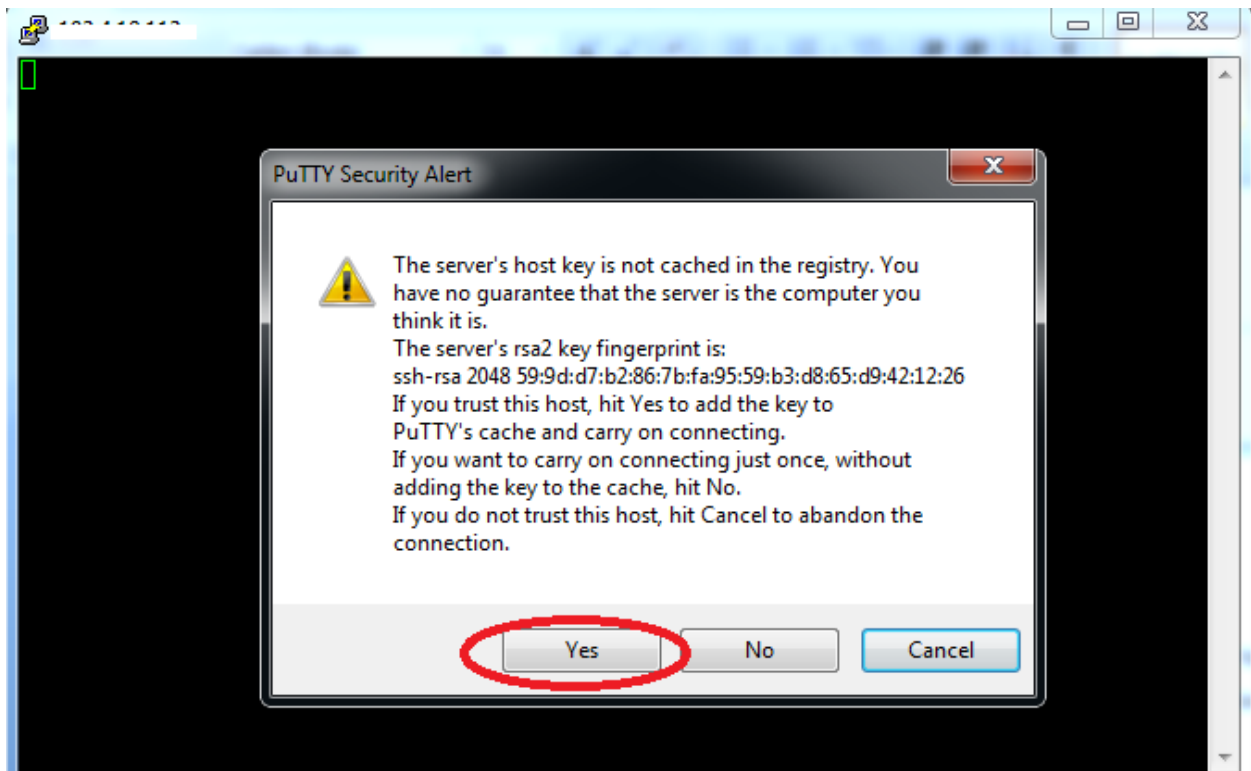
Once the agent is started you can execute any resource assigned to you directly from the SSL Monitor icon in the taskbar. Clicking the right button, the agent icon will present a list of resources that can be executed directly from the agent without having to go through SSL-Explorer. To start the resource, simply select the server and click on it.



As soon as the SSL Explorer Agent is started, you will be prompted to verify the site SSL certificate. Simply tick "Always trust content from this publisher" and click on YES



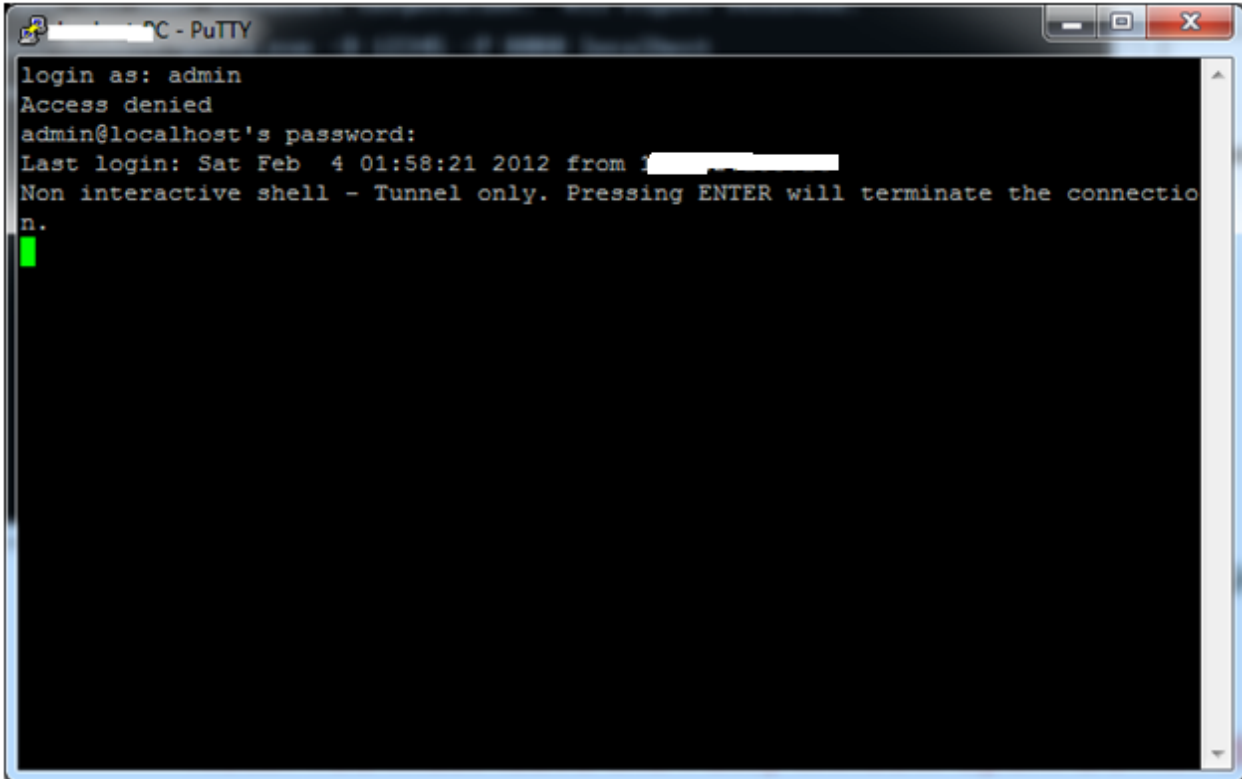
Accept the security warning and click on Yes.



Then finally you will be presented Putty window for Authentication. Simply authenticate using your SSH username and password which corresponds to your member username and password.

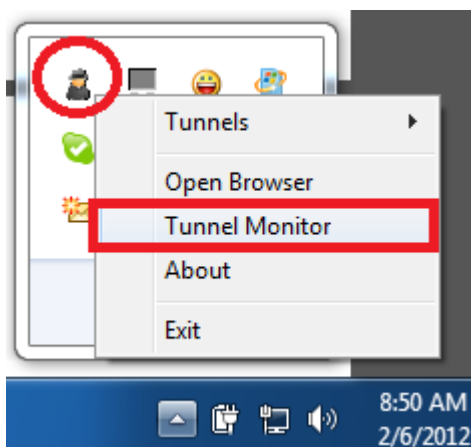
Note: You must leave the Putty window open. Do not close it or attempt to enter any command. You must leave the window open throughout your tunnel session.

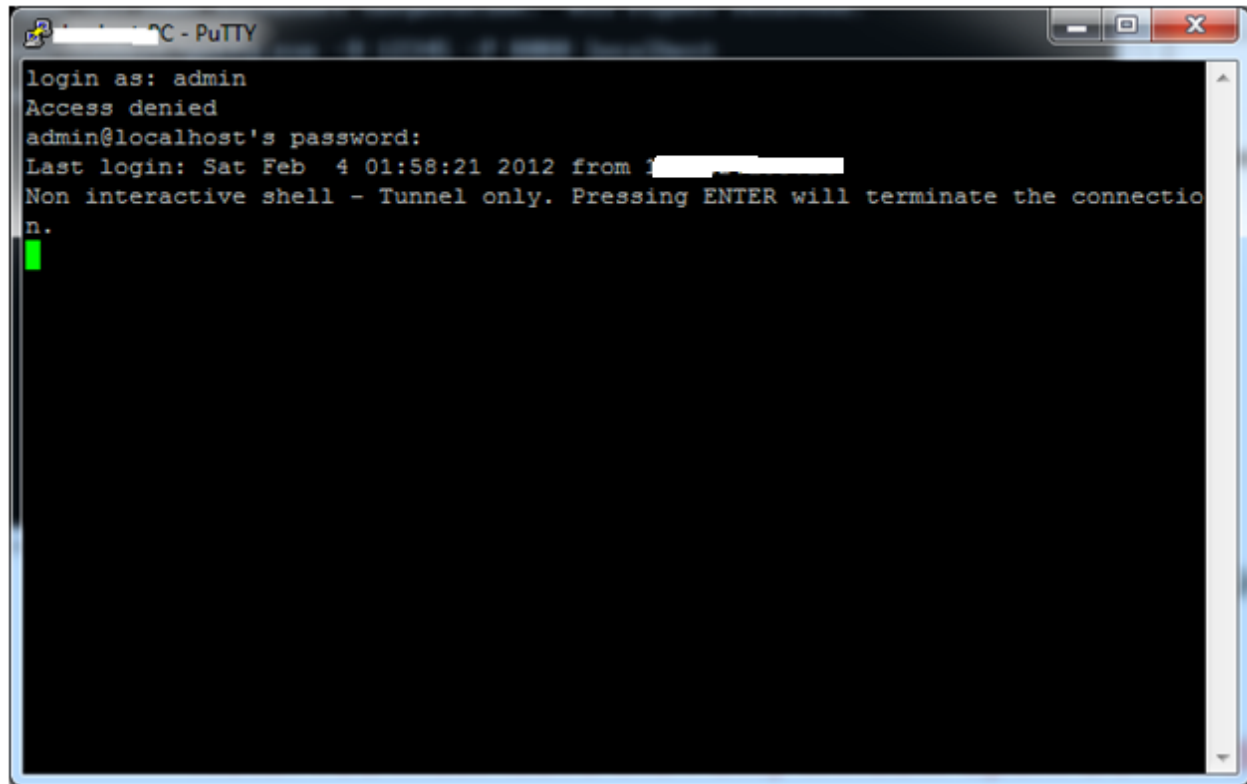
This will connect to your local SSL Explorer Agent first, which negotiates with the remote server, and finally the ssh<=>sshd communication will begin and after authentication you will be dropped to a shell and have a SOCKS proxy running on port 8080.



```
login as: admin
Access denied
admin@localhost's password:
Last login: Sat Feb 4 01:58:21 2012 from [redacted]
Non interactive shell - Tunnel only. Pressing ENTER will terminate the connection.
█
```

To confirm that the SSH tunnel that was successfully initialized, go to the SSL Explorer Agent icon on your taskbar and click on "Tunnel Monitor". There you will see the tunnel server that was successfully initialized and active for tunneling.





```
login as: admin
Access denied
admin@localhost's password:
Last login: Sat Feb  4 01:58:21 2012 from [redacted]
Non interactive shell - Tunnel only. Pressing ENTER will terminate the connection.
█
```

That's all you need to do to open the tunnel. Now you're ready to configure your application such as web browser, VOIP, messengers, OpenVPN etc with the Socks 5 proxy details shown below:

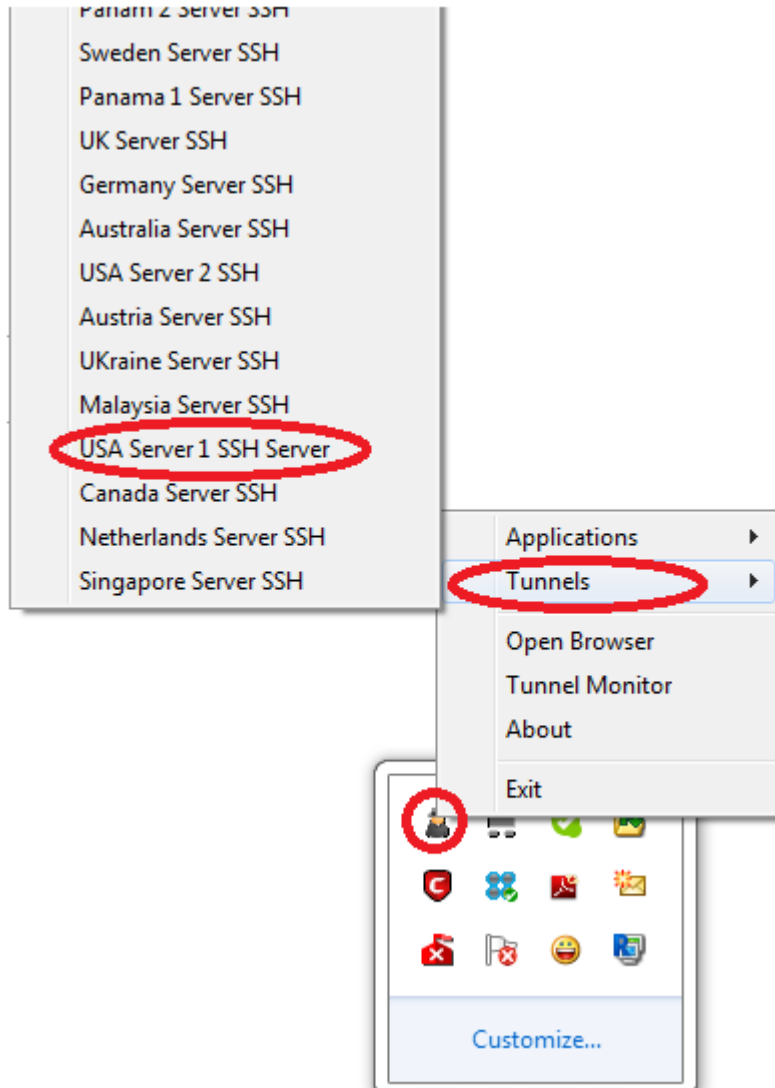
Host: localhost

Port: 8080

Proxy Type: Socks 5 (Requires no authentication)

Instructions for Linux Users

For Linux users, after logging to the SSL Explorer panel, go to **SSL Tunnels** under Resources and then click on the server you wish to setup your tunnel. After clicking on the server icon, SSL Explorer will be initialized and the tunnel will become active. You can also start the tunnel by going to the SSL Explorer Agent taskbar icon and then under “SSL Tunnels” select the server to connect to and click on it as shown below:



However, to setup the tunnel, you must issue the tunnel command via your SSH client. Using **Terminal Console** (instead of using Putty for Windows) type the command below replacing “user” with your member username:

```
ssh -D 12345 user@127.0.0.1 -p 8080
```

Note: In the commands above, replace “user” with your SSH username which by default is your member username.

Enter your member login credentials for the SSH connection

```
[root@~]# ssh -D 12345 test@127.0.0.1 -p 8080
test@127.0.0.1's password:
Last login: Wed Feb  8 06:49:10 2012 from 
Non interactive shell - Tunnel only. Pressing ENTER will terminate the connection.
```

That's all. Now you can configure your application with the Socks 5 proxy:

Host: 127.0.0.1

Port: 12345

Proxy Type: Socks 5 (Requires no authentication)

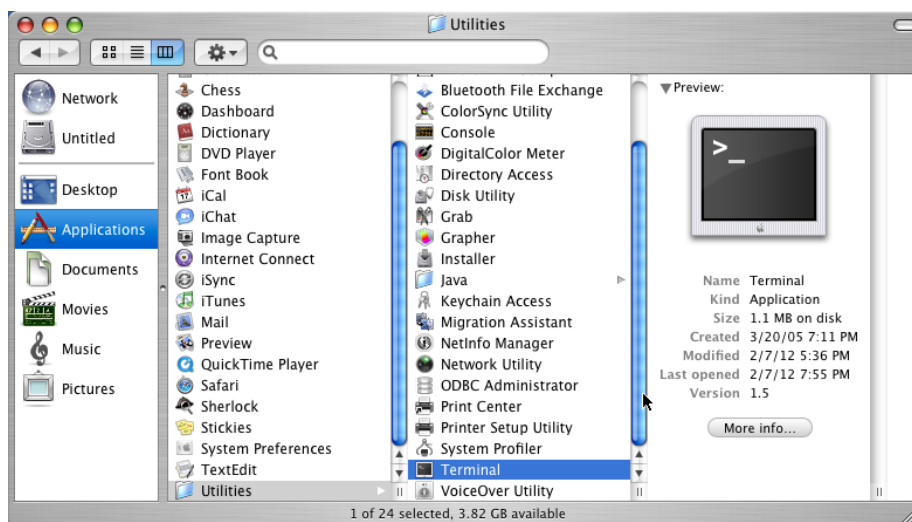
Instructions for MAC Users

Instruction for Mac users is mostly the same as for Linux users, but with this some differences.

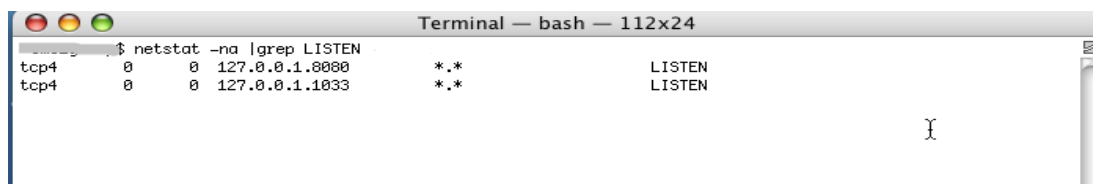
Open and lunch SSL Explorer as described earlier. Start the tunnel either from the SSL explorer panel or from the SSL Explorer Agent taskbar icon as described earlier and click on your desired SSH server.

You can also verify that necessary connection was established in Terminal window.

Open **Terminal** from menu Applications – Utilities - Terminal



and run command `netstat -na |grep LISTEN`. You will see all listened ports on you desktop.



Finally you can connect to noticed local port with the appropriate command:

`ssh -D 12345 user@127.0.0.1 -p 8080`

```
$ ssh -D 12345 test@127.0.0.1 -p 8080
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
RSA key fingerprint is 90:38:85:ba:66:f5:6b:8f:59:31:12:09:30:8c:c3:55.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (RSA) to the list of known hosts.
test@127.0.0.1's password:
Last login: Thu Feb  9 15:51:18 2012 from [redacted]
Non interactive shell - Tunnel only. Pressing ENTER will terminate the connection.
```

Leave this window opened during all time you work through ssh tunnel.

Now you need to configure your application with the Socks proxy.

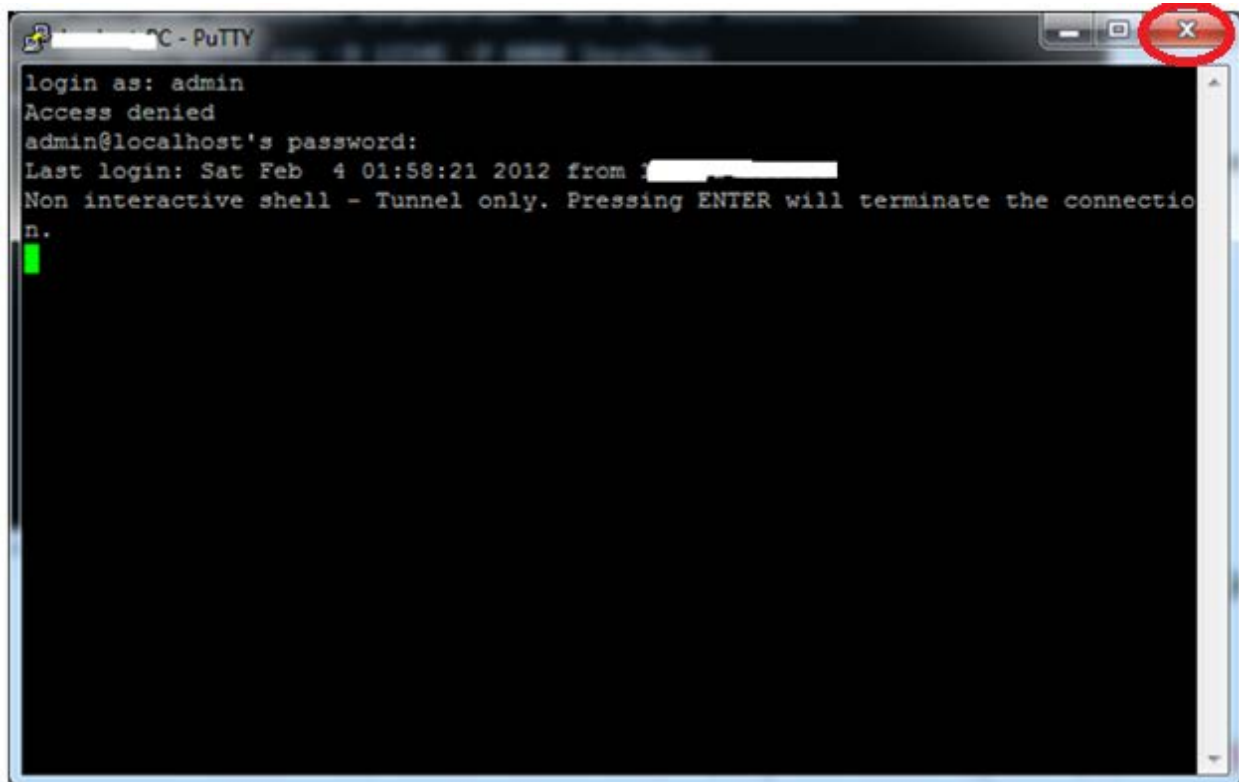
Host: 127.0.0.1

Port: 12345

Proxy Type: Socks 5 (Requires no authentication)

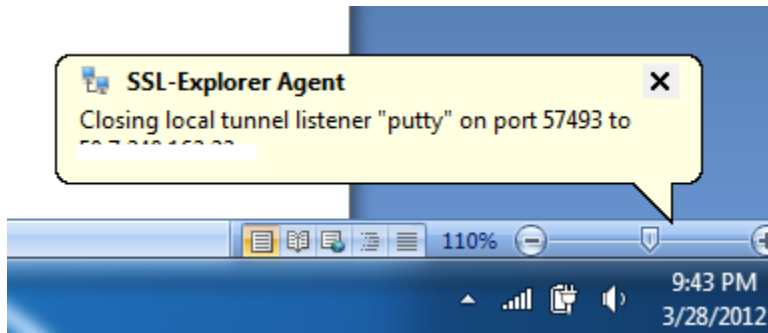
Switching/Terminating Active Tunnel Sessions

To switch from one server to another or terminate your current SSH tunnel session, simply close the active Putty tunnel window. After this, the SSL Explorer agent will notify you that the tunnel has been closed. Thereafter, you can then start a new tunnel for another server using the same procedure as explained above.



```
TC - PuTTY
login as: admin
Access denied
admin@localhost's password:
Last login: Sat Feb 4 01:58:21 2012 from [redacted]
Non interactive shell - Tunnel only. Pressing ENTER will terminate the connection.
█
```

Important: Make sure that only one Putty tunnel window is open in your system at a time. If you attempt to start a new tunnel while another Putty tunnel window is open, the connection will be refused!



Note: After starting a tunnel from the SSL Explorer Agent, you must open your command prompt and enter the SSH command to start the tunneling. If you do not enter the command within few minutes, the tunnel connection will become inactive and will be terminated by the Agent automatically. In addition, if your tunnel session is idle for 120 minutes, the session will be automatically closed.

Logging Out

At the end of your tunnel session, you can logout of the SSL Tunneling web portal. To log out of the SSL Tunneling web portal, you must click on the Logout icon at the top right hand side of the panel as shown below:



Clicking on this icon will terminate the SSL Explorer agent, as well as terminate login session to the SSL Tunneling web panel.

Note: Simply closing your browser window will not log you out of SSL Tunneling web portal. The agent will continue to run until it is closed or it times out.