SMART-SOFT
MANAGING THE NET

HOW TO CONFIGURE TRAFFIC INSPECTOR

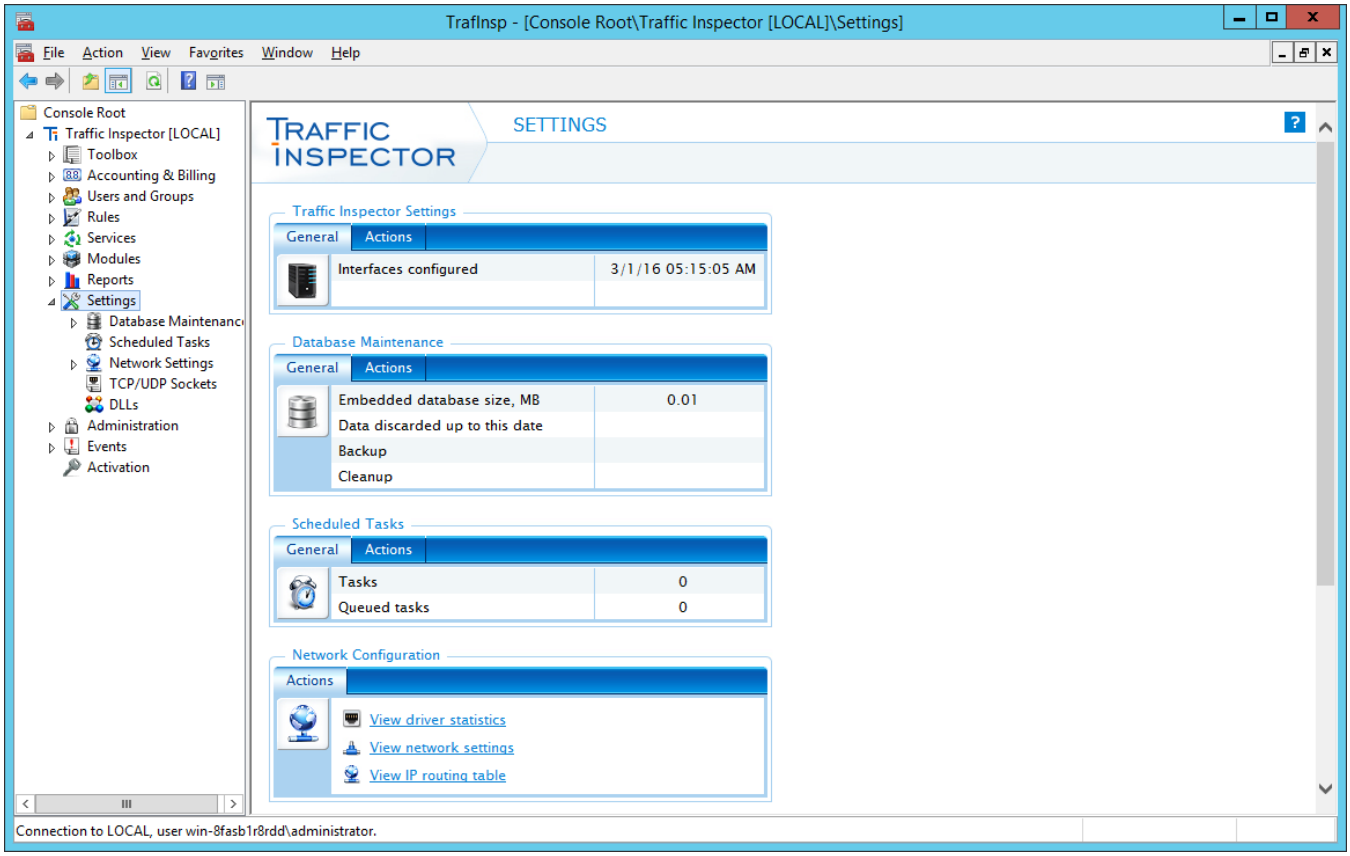
This document describes how to perform the initial Traffic Inspector configuration. The following aspects are described in this tutorial:

- Defining operation mode and networking settings
- Populating the program with user accounts
- Verifying configuration settings and testing user access to the Internet

Defining operation mode and networking settings

Navigate to ***Console Root|Traffic Inspector[]|Settings|***

Locate the **Traffic Inspector settings** group box, select the **Actions** tab and click the **Launch the Advanced Configuration Wizard** link.



The first setting we have to define is the operation mode.

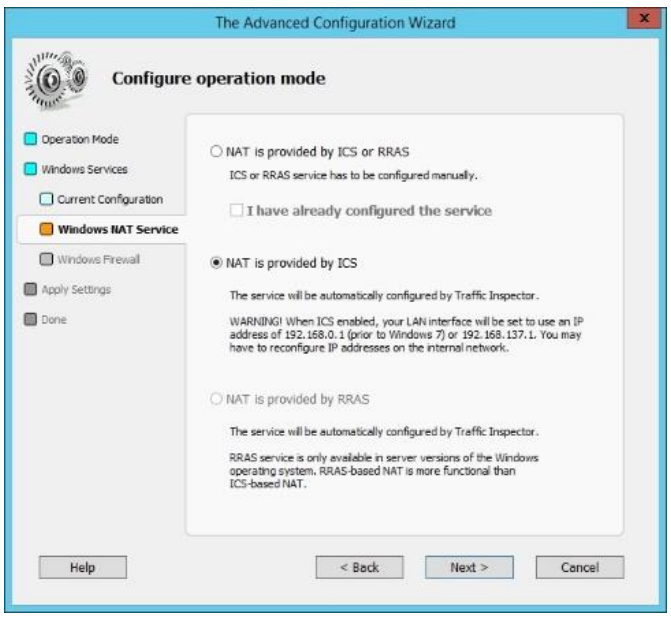
Traffic Inspector supports two operation modes:

- Gateway mode
- Single interface mode

Under gateway mode, Traffic Inspector is deployed at the edge of your home or office network and processes all the traffic that flows into and out of it. This is the most feature-rich operation mode.

The Single interface mode requires Traffic Inspector to only have one network interface that is connected to the internal network. The Single interface implies that an Ethernet switch with the port mirroring capability is used to send a copy of network packets to Traffic Inspector. Under Single interface mode Traffic Inspector can only perform traffic accounting. If you plan to implement Web Access Control, gateway-level anti-virus protection, spam filtering, etc., use Gateway mode instead.

The **Windows NAT service** tab is used to select the service that provides the Network Address Translation (NAT) functionality.

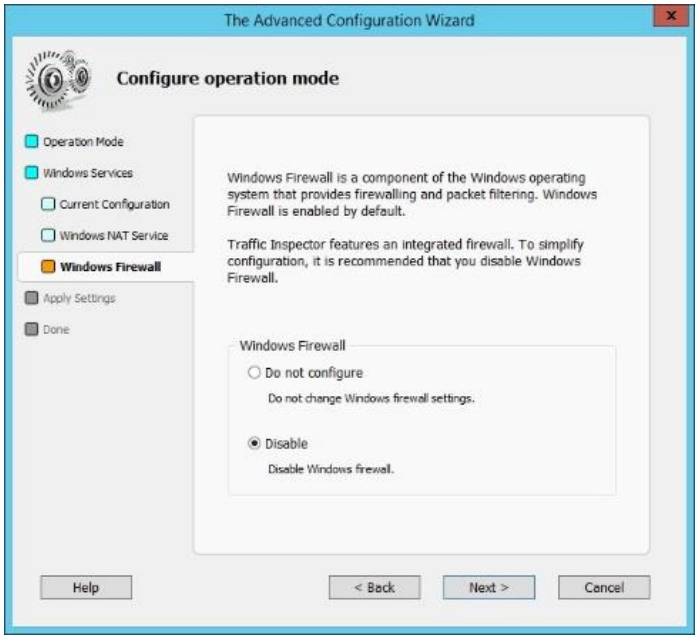


On Windows two services can provide NAT functionality:

- Internet Connection Sharing service (ICS)
- Routing and Remote Access Service (RRAS)

RRAS NAT is more capable than ICS NAT. On Windows Server 2012 R2, you have to install the Remote Access role to be able to use RRAS NAT. Instructions on how to do this can found on the Web. For now we will use ICS-based NAT.

Traffic Inspector features a custom firewall which effectively prevents unauthorized access to your network and services from the Internet. We recommend that you disable Windows Firewall on the Traffic Inspector gateway. Using two firewalls concurrently will lead to greater ambiguity.



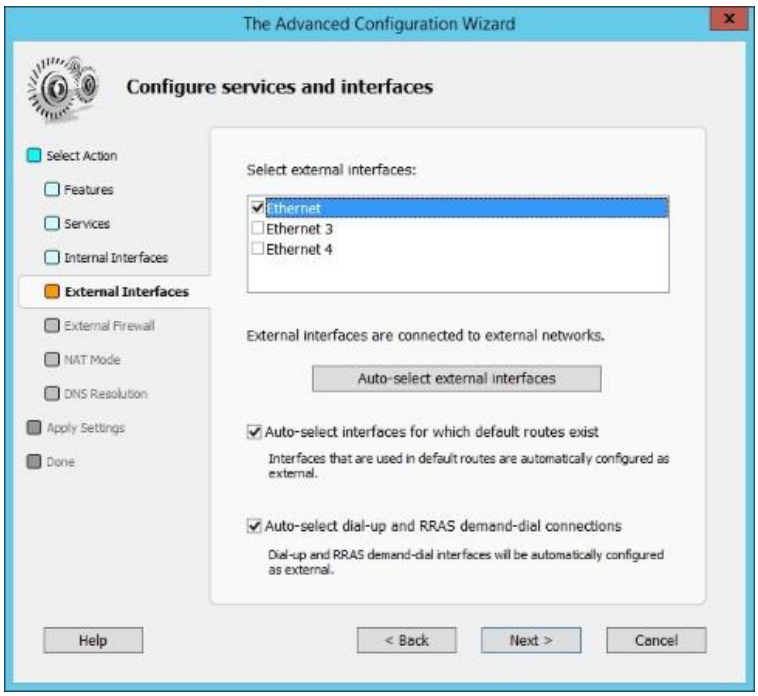
Click **Next** a couple of times to finalize the first part of the configuration process.

The second part of the Configuration Wizard allows you to configure Traffic Inspector services and interfaces. Since, we are only interested in the initial Traffic Inspector configuration, we can ignore the majority of advanced settings. Configure Traffic Inspector as described below.

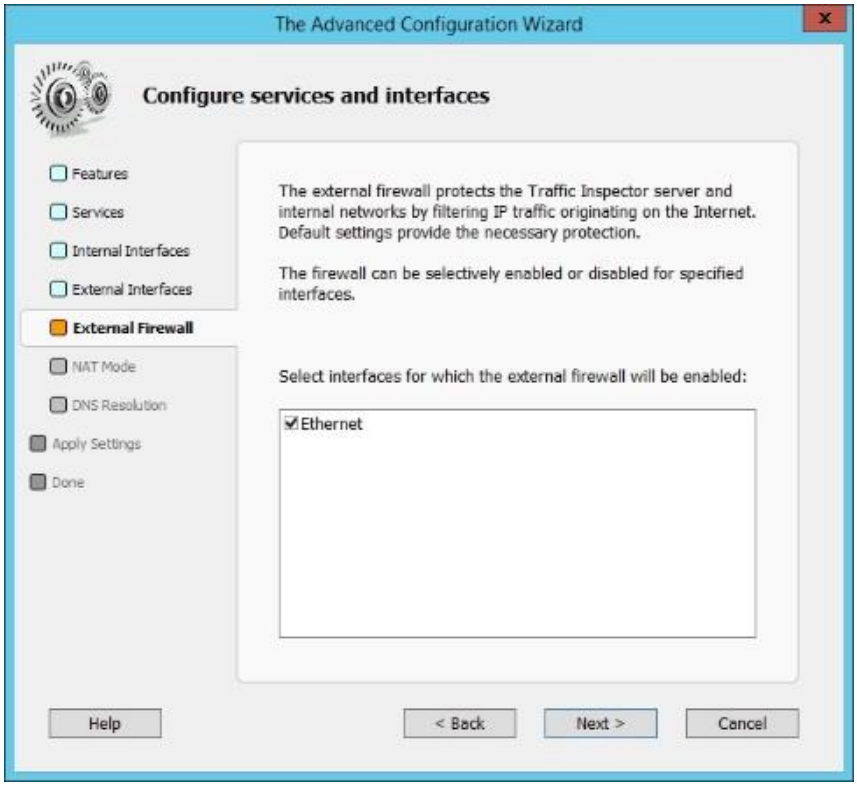
On the **Features** tab select the **Enable Traffic Inspector firewall** option and the **Enable RAS server support** option (required for remote VPN users).

On the **Internal Interfaces** tab select network interfaces that are used by Traffic Inspector to connect to your home / office network.

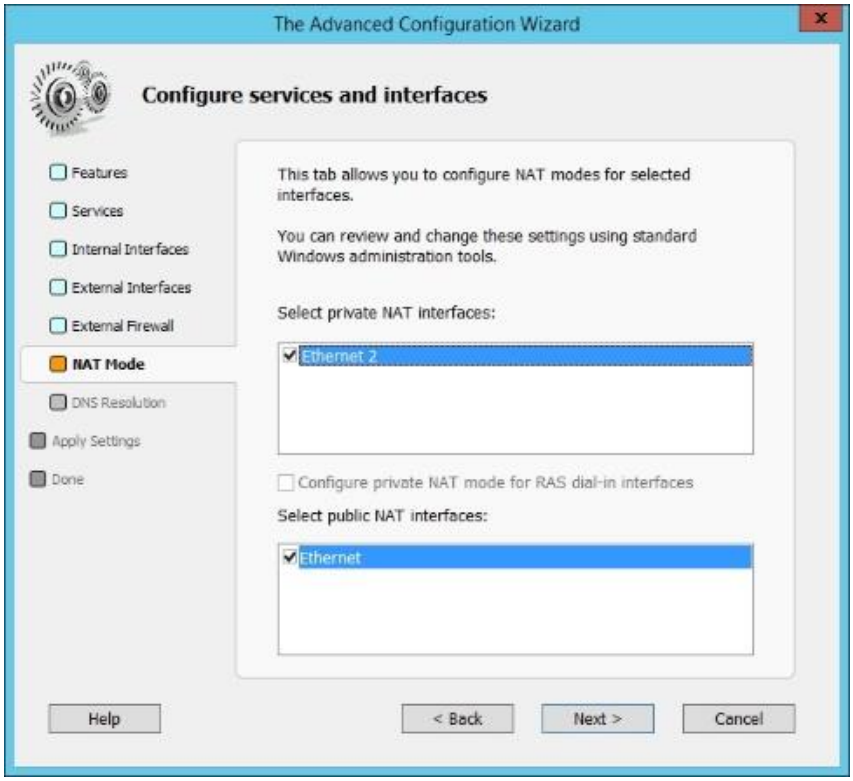
On the **External Interfaces** tab select network interfaces that are used by Traffic Inspector to connect the Internet.



On the **External Firewall** tab select network interfaces for which Traffic Inspector firewall will be enabled.



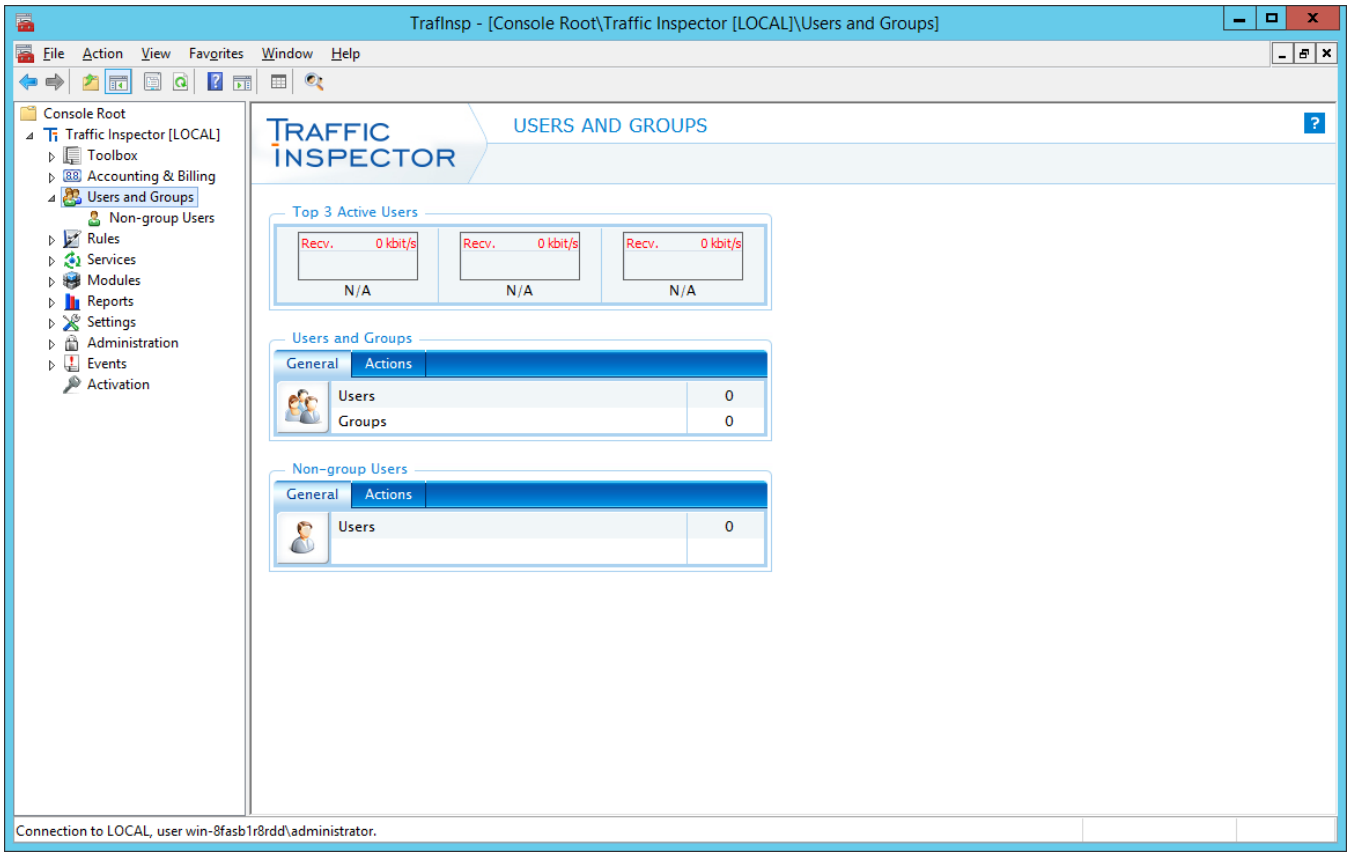
he **Interface NAT Mode** tab allows you to configure public / private mode for previously-selected external and internal interfaces. Make appropriate selections, click the **Next** button twice and wait while the new settings are being applied.



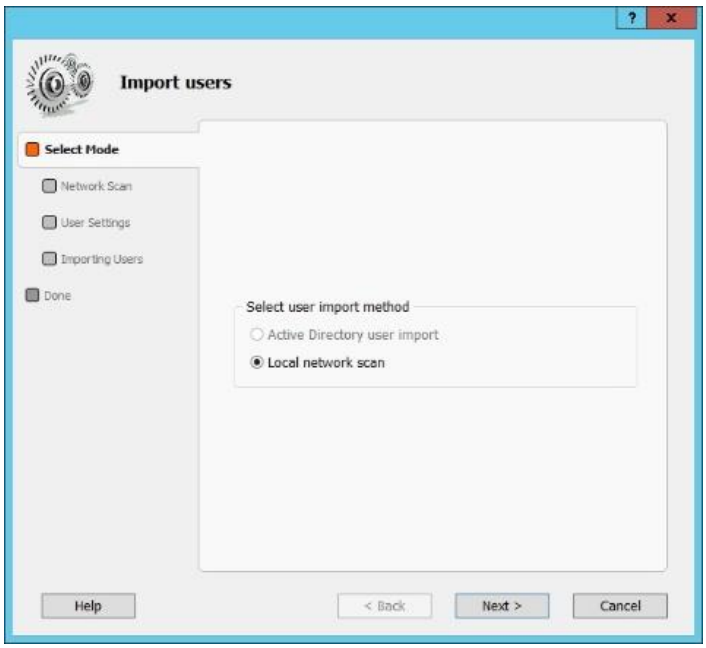
Importing users

Traffic Inspector is designed to control user access to the Internet. Each user that is going to access the Internet via Traffic Inspector must have a user account. You can create each account manually or use a bulk-import method provided by **the User Import Wizard**.

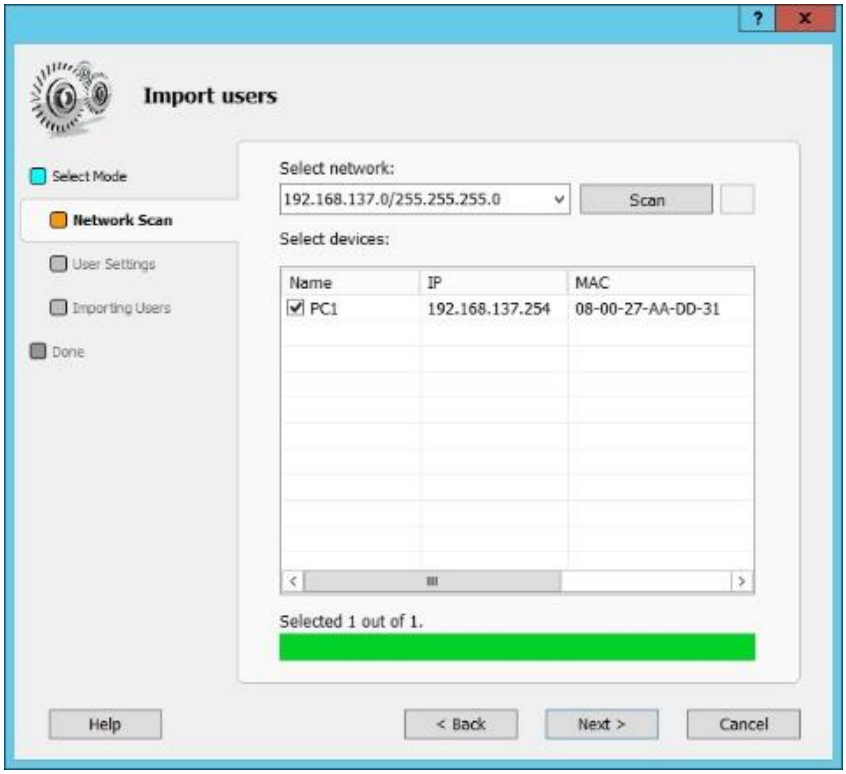
You can launch **the User Import Wizard** in the final step of **the Configuration Wizard**. Alternatively, you can navigate to ***Console Root|Traffic Inspector[]|Users and Groups|***, then locate the **Users and Groups** group box, select the **Actions** tab and click the **Import Users** link.



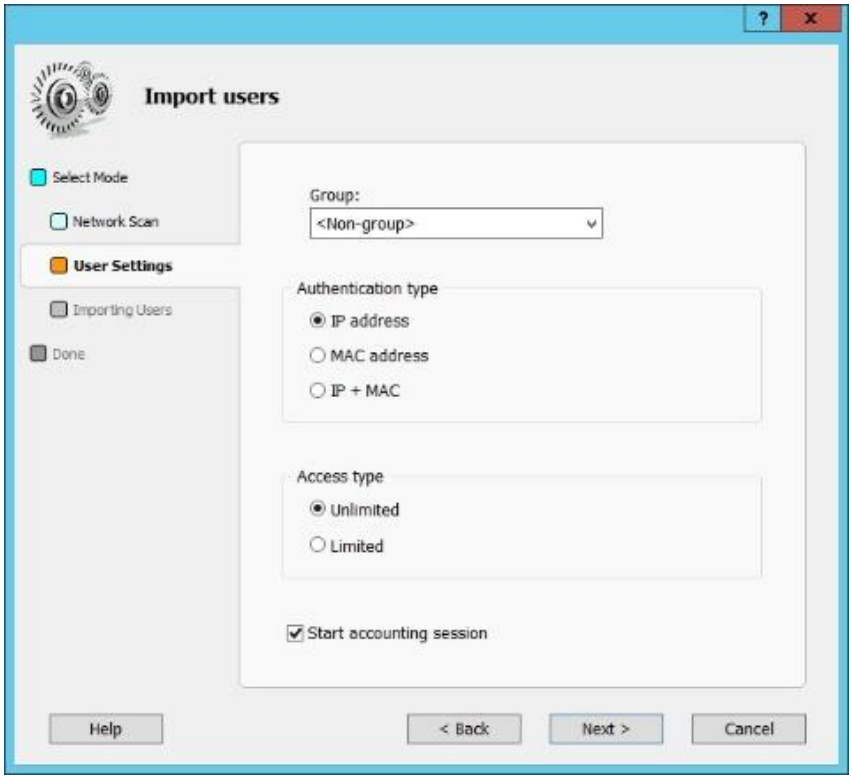
Select the **Local network scan** option and click **Next**. In case your Traffic Inspector gateway is joined to a windows domain, you can also use the **Active Directory user import** option.



Select the users that you want to add to Traffic Inspector and click **Next**.



Define settings for imported users. Set **Authentication type** to **IP address** and **Access type** to **Unlimited**. With IP address authentication, a user is considered to have an authenticated status once he/she turns on their computer. With unlimited access, a user can access the Internet irrespective of their balance.



Finish **the User Import Wizard** by clicking **Next** and **Done**.

Verifying configuration settings and testing user access to the Internet

You can now verify your Traffic Inspector setup.

We have configured Traffic Inspector to use ICS-based NAT. When ICS is enabled, the internal Traffic Inspector interface is automatically set to use IP address 192.168.137.1. Unless you change this address to a different one, ICS will also provide a DHCP and DNS service for the 192.168.137.0/24 network. You can now turn on your LAN PC and it will obtain all the necessary networking settings automatically via DHCP. The IP address assigned to your LAN PC via DHCP may change over time.

If you have changed the IP address of the internal Traffic Inspector to a value other than 192.168.137.1, ICS DHCP server will stop working and you will have to assign an IP address to your LAN PC manually. Be sure to assign an IP address that is in the same range as the Traffic Inspector internal interface's IP address.

On your LAN PC, open a browser and access an Internet website. All should be working.

Congratulations, you have configured Traffic Inspector to provide Internet access for you LAN! From here, you may want to think about configuring advanced Traffic Inspector features including:

- Web Access Control
- Kaspersky Gateway Antivirus
- Spam Filtering
- Advanced Routing
- Logs and Reports
- Administrative access to program
- Automatic backup and cleanup