



What is MultiNetwork Manager?

MultiNetwork Manager is software designed to alleviate many of the technical issues encountered when roaming between different network locations. It allows laptop users to easily connect to the Internet, corporate LANs, client networks, wireless networks, dial-up or mobile networks, etc. and it also alleviates many of the annoying mistakes made when moving about, such as forgetting to change default printer. But most of all, it ensures that your security settings are correct, firewalls are enabled, shares are disabled, Bluetooth adapter disabled or any other security measure needed. With MultiNetwork Manager, laptop roaming is made comfortable and convenient.

This guide will show you MultiNetwork Manager in some areas where security and ease of connection are essential:

1. Troublesome connectivity made easy

Are you often on the move?

Would you like to connect and work from wherever you are?

One of the main features of MultiNetwork Manager is to provide a laptop user with instant Internet connection and access to information independent of where you are.

You can make instant:

- Wireless connections
- Wired connections
- Dial-up connections
- 3G connections
- GPRS/HSDPA connections



2. Wireless access points in range

Need to connect wireless quickly?

When out and about you may need to find out quickly whether there is a network access point, e.g. a hot spot, in range. The MultiNetwork Manager will display a list of all wireless access points in range, and will find one, through which you have access rights, or an open one, and you connect simply by clicking a button.

3. Quickly switch between known locations

Are you often moving between job sites, switching between networks that you return to?

Would you like to get completely set up at your location automatically or by a single mouse click? MultiNetwork Manager provides instant Internet access plus access to resources such as mapped drives, default printers or applications to get started automatically including security settings that you may need. The unique automatic location-sensing feature will in most cases adapt your computer to a new known location completely automatically.

4. Always stay secure

Would you like to get a security overview at a glance?

Would you like to feel comfortable and secure knowing that security measures are in place?

When switching between different networks it is particularly important that you stay in control of your computer's security settings. MultiNetwork Manager will through its status screen at a glance show you whether your current connection is secured by a personal firewall or not, if your anti-virus program is up to date and if you have the latest Windows updates installed. It will tell you which location profile that is currently applied and which adapters and network connections that are active.



But more importantly, you may define default profiles called **policies**, that are automatically invoked at predefined events, your anti-virus data is out of date, your firewall is not enabled, you are connecting to an unknown network or you are changing location.

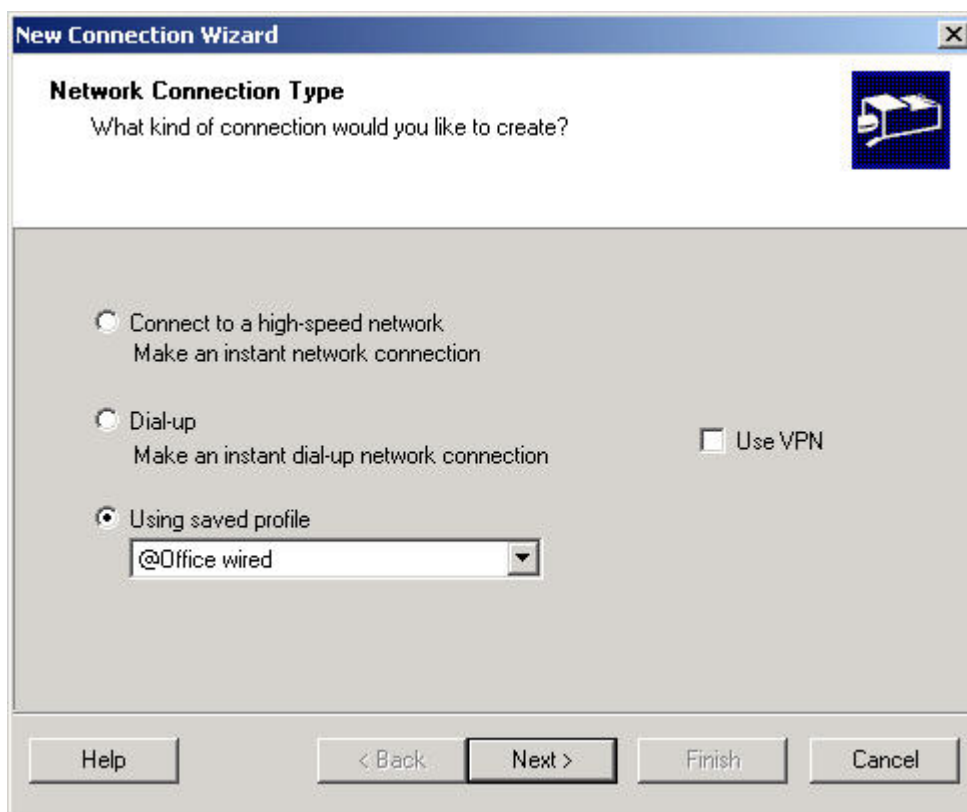
Through these policies you may configure some very advanced security measures. You may run scripts, define environment settings, add registry keys and set security parameters.

With these policies in place you can always feel secure and comfortable when connecting, wherever you are connecting.

1. Troublesome connectivity made easy

One of the main objectives with MultiNetwork Manager is to provide you as a laptop user with instant Internet connection and access to information independent of where you are. You may be in a hotel, an airport or in a café, and you would like to get access to the Internet directly. Or it may be more complicated connection cases if you for instance are visiting a company, with a friend or at another site where you may have to use the local network to access the Internet.

In the top bar of the MultiNetwork Manager screen you will find a Connect button. Simply click the button and select connection type in the window that opens.



When you click *Next*, another couple of windows may open to guide you through the process of getting connected. The auto detect feature of MultiNetwork Manager will find the appropriate settings and automatically apply them, but to get access you may need to enter passwords, WEP codes or similar as appropriate.

To ensure that your security settings are appropriate when you connect to an unknown network, you may have policies defined to apply always when connecting to unknown networks, so you don't need to worry about security when connecting.

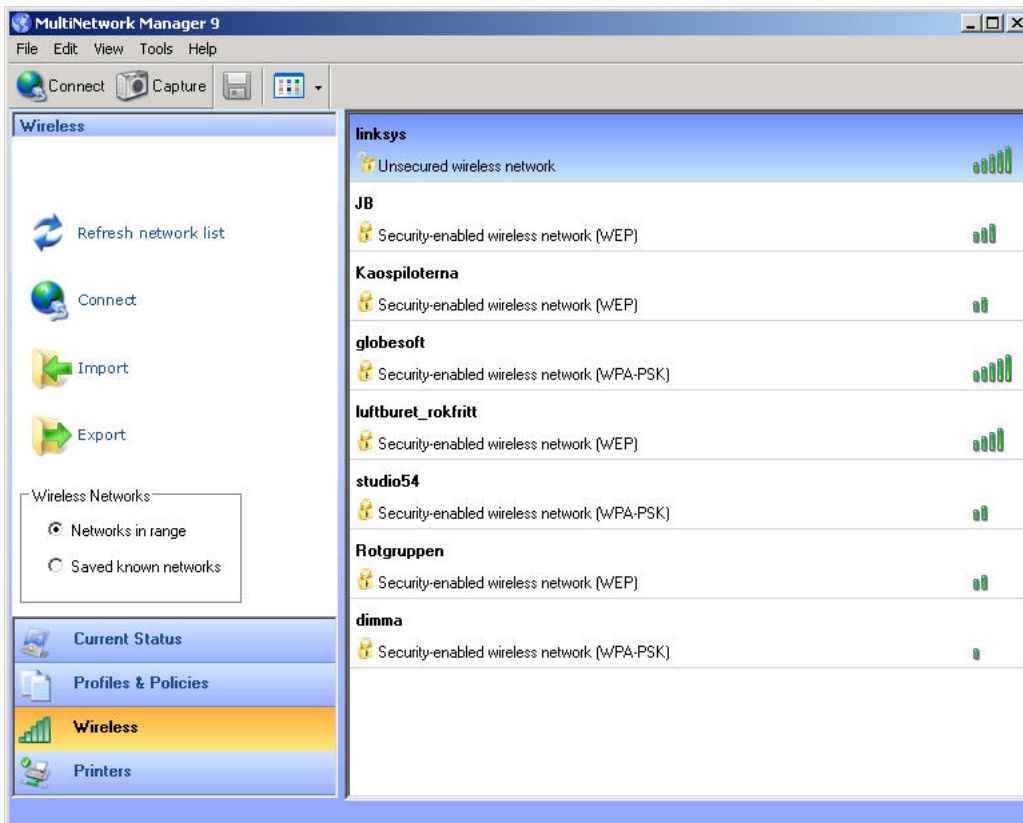
If the location where you connect is a site that you will return to, it may be useful to capture and save the settings, to have them available when you return. You may also modify the profile that you saved to include access to other resources such as printers, network drives, etc.



2. Wireless access points in range

With MultiNetwork Manager you can easily scan for wireless networks no matter where you are. For example when arriving at a hotel, an airport, coffee shop or other hotspot, by clicking the “Refresh network list” button on the “Wireless” screen, you can quickly check whether there are any WLANs available and then choose which one to access. Additionally, while connected to a wired network at the office, you can easily switch to a wireless network by simply going to the “Wireless” screen, pressing the “Refresh network list” button, and selecting the access point you wish to use.

The wireless networks available will appear in a list and you can easily connect to the ones you have access credentials for by double clicking or by using the Connect button.



If you don't have access credentials, a box will open to allow you to enter the data needed.

However, it is very easy to export and import WLAN settings including the access credentials needed. So for a common environment, such as an office, the WLAN settings may be available for import from the Intranet. Or you may simply ask a friend to export the settings to a USB so that you may import them.

Further, if you, or your network administrator, plan to change the WLAN settings, you may prepare a temporary WLAN profile. MultiNetwork Manager will find out when the changes have been made to the Wireless Access Point, and switch to the new one.

3. Quickly switch between known locations

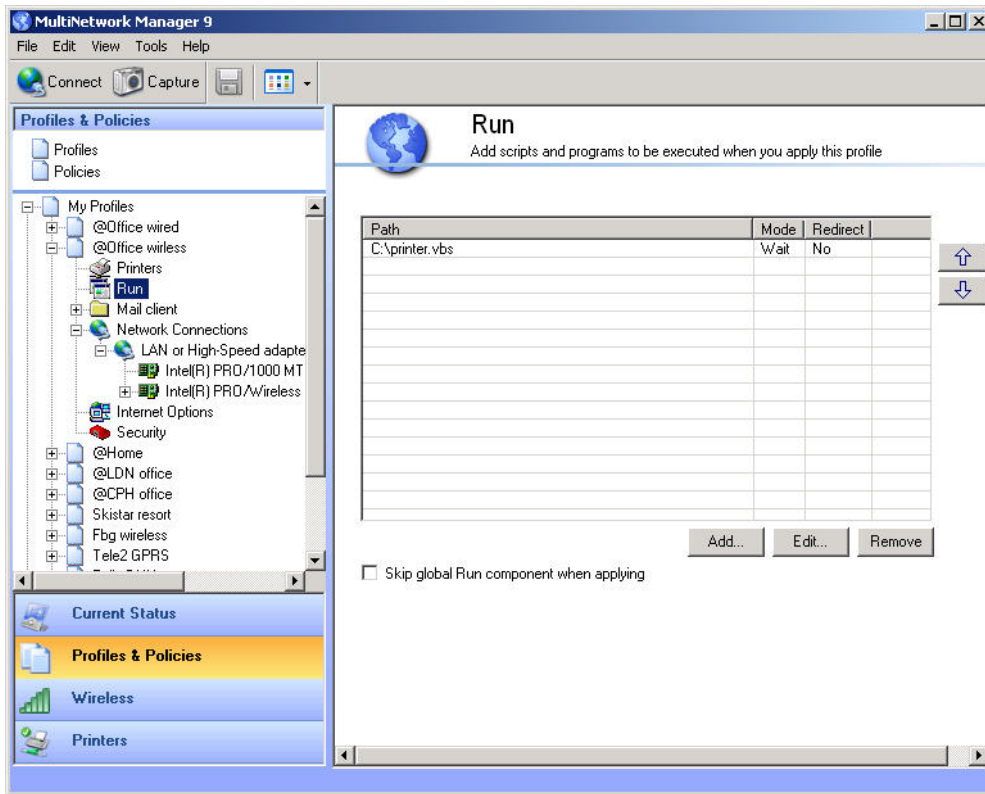
Computers and applications need to be adapted and reconfigured to different networks when roaming between known locations. The MultiNetwork Manager's Profile switching function makes roaming as easy as clicking a button. When you arrive at a location for which you have created a profile, you simply need to select the profile name, for example “@Home” in the Profiles & Policies' menu, right click and choose Apply, and in a couple of seconds your settings will be adapted to that specific location. Going back to your office, you just select the “@Office” profile and your settings will be switched back to your office settings.



You can also apply a profile by right clicking on the MultiNetwork Manager icon in the system tray, select the location profile and click Apply.

In fact, the unique location-sensing feature in MultiNetwork Manager may recognize your location as you start your computer, and suggest the location profile to be applied.

A separate VPN profile has been added to the profile list to make it easier for you to use VPN. The VPN profile can be enabled/disabled in one click.



The tables below show you some typical users and some typical profiles.

Types of users	Examples of locations/situations
General laptop user	Different company sites, office departments, home, home wireless
The consultant/sales representative	Company sites, office departments, customer sites, VPN profile, home
The IT administrator	Profiles for different networks
The student	Profiles for different faculties, student room, coffee shops, friend's home network

Examples of location/situation specific profiles:

1. Office Profile	Domain, proxy, default office printer, personal firewall disabled, VPN disabled, file sharing on	When being at your regular office space you simply need to click "Capture" at the "Profiles & Policies" screen in order to save your current settings into an "office profile".
2. Home Profile	ADSL/dial up etc., personal firewall enabled, workgroup, file sharing disabled, default home printer, company e-mail, wireless adapters disabled (to prevent unintended network connections).	For home use, the IT department can create a specific home profile for you where the firewall gets enabled automatically when applying that profile and where the corporate proxy settings are removed.



3. Home Profile (with VPN):	Same settings as above, but with VPN.	When you need to reach resources at the company intranet it is convenient to have a specific VPN profile where the VPN application is enabled and other settings are changed accordingly, printer, mappings etc.
4. Conference Room	Domain, proxy, default project room printer, personal firewall disabled, VPN disabled, file sharing on	Use MultiNetwork Manager to create a specific profile for the conference room. See below.
5. Customer Site	Domain, TCP/IP, proxy, mapped drivers, personal firewall enabled, default printer	At the customer site you may need to have configuration for the customer's proxy to be able to get network access and other specific settings adapted to the location such as printer and mapped drivers.

User Scenario – Business user on the move

Imagine yourself as a business user who travels extensively between the headquarters' office, different project locations at different client sites and home. In the morning you arrive to the HQ office for a status meeting. While waiting for the meeting to begin, you want to check your e-mail and connect to the network by selecting the profile "HQ Office". This profile was preinstalled on the laptop computer by the IT support department. After the meeting, you drive to the client site to participate in a new project. You create a new profile immediately at startup using MultiNetwork Manager. After having started up with a basic network connection, you modify the new profile by specifying printers and file servers on the local network for the project. The next time you return to the customer site, you only need to select the profile "Customer site A". In the evening, you return to your home and realize you forgot to do your time report. You connect your laptop to your broadband connection. At startup, you select your profile, "Home VPN". MultiNetwork Manager establishes a network connection and enables the VPN client that lets you access resources at the HQ office from home. The network drives will also be mapped, allowing you to complete your tasks.

By clicking the Capture button on the main menu, you may easily create and save your current settings into a profile. Just click the Capture button. Also, if you are familiar with Microsoft networking, you may from the Profiles & Policies screen manage your profiles to exactly meet your needs.

In MultiNetwork Manager 9, VPN connection has been given a special profile status. This allows you to enable a VPN connection irrespective of where and how you are connected to the Internet. You may also add profile components to the VPN profile e.g. to change mappings, mail accounts or default printer when working over a VPN.

4. Always stay secure

One of the most important aspects of laptop roaming is the security aspect. At every location it is important to ensure that the appropriate security settings are in place. However, since this is not always so easily done you may end up with compromises such as having unnecessary safeguards enabled on your company network and still not enough on an unknown network.

MultiNetwork Manager allows you to set security settings in each profile to ensure the proper security level at each known location. Further specific policies may be set to enforce security settings at other instances such as the virus scan is out of date, the firewall is not enabled, you are connecting to an unknown network or you are simply changing location.

You may want to block hostile access to your system by preventing wireless access, e.g. Bluetooth. You may want to ensure that file sharing is off or you may want to run specific scripts or set Registry data to ensure proper security measures.

Also MultiNetwork Manager has put security information into a window to allow you to get a quick overview of your security settings.