

MultiNetwork Manager a powerful tool for IT administrators!

MultiNetwork Manager contains a number of features especially created to facilitate for IT administrators to manage computer network settings in a professional environment. This includes the availability of a number of powerful components that may be used in profiles and policies, and also makes it easy to push out updated or new settings to end users.

MultiNetwork Manager may be used in many ways to manage computer settings, making it easier for IT administrators. A few examples are given here.

1 How to push a profile

A powerful way to ensure that computers in a network environment are up to date with the latest network settings is to use MultiNetwork Manager and provide configuration files with settings for users to import. This may be by just making the files available, inform the users and then leave it to them to import, or it may be done by pushing the files on to the users.

Push technique may also be used when installing MultiNetwork Manager or when distributing an upgrade. The user will be requested to import pushed files when launching MultiNetwork Manager.

Using MultiNetwork Manager new configurations may be distributed in advance so that when changes are made, all connected computers are prepared and the new changes takes effect either automatically via polices or when the user applies a profile.

As an example, to push out a location profile, the IT administrator would create the new profile using MultiNetwork Manager, export the profile to an export folder and include a transform file in the installation package. The transform file would add values to the MSI package e.g.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GlobeSoft\MultiNetManager\  
" PushProfilePath"=" M:\MNM_Support\PushProfiles"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GlobeSoft\MultiNetManager\Options\  
" LIC_ID"=" 130101-00100-0050321"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\GlobeSoft\MultiNetManager\Options\  
" LIC_KEY"=" 313734-6365"
```

This would request the user to open and import the profile in the given folder and also automatically insert the license and key numbers for activation.

2 Remote policies

In organizations IT administrators often define and describe security instructions in documents that are distributed to employees and which are required to be followed. However it is often difficult to ensure that these policies are followed, and often the measures to be taken are forgotten. With MultiNetwork Manager 9 policies may be defined and automatically applied at certain predefined events. These events are

- Anti Virus program not updated
- Fire Wall not enabled
- Connection to unknown (new) network
- Policy run on changed location.

In each of these events, the IT administration can define settings and measures to be taken to ensure safe connection. The measures could be just a textbox to inform the user of the danger, possibly propose actions or inform about company policy. Or it could be to disable adapters, disable file sharing, enable windows firewall, run scripts or set registry keys etc.

Remote policies could be pushed out to the users when installing MultiNetwork Manager or they could be set up as files in a directory for the users to import.

3 Pre created profiles

MultiNetwork Manager includes a number of powerful components that may be used to support the administrative IT work.

To use pre-created profiles is a powerful, complementary tool for the IT administration to provide smooth and hazard free roaming of laptops around the company premises. It could be to set up very advanced IT settings, enable or disable required adapters, run required scripts or set WLAN access parameters, or it could be simply to set the appropriate default printer at a certain company location.

Most laptop users connect their computers also at home. Many also connect at customer or client sites or at hotels etc. With MultiNetwork Manager the IT administration can set up a VPN profile to ensure that VPN is available and set up properly. Having a profile for each of the locations to which an employee returns regularly makes the move between locations easy and secure.

Simply the fact that IT administration has set up a profile for the ordinary office location, including domain settings, proxy, etc. avoids many of the annoying instances when employees have changed their computer settings and are unable to set them back correctly. Applying an office profile ensures that the employee always has the right resources, including printer, mappings etc. available.

Also company networks constantly change. For simple changes the users may be required to change computer settings, but often IT personnel need to make the change, which then often tends to be both lengthy and costly.

With MultiNetwork Manager pre-created profiles may be used to push out such changes. Profiles with the needed changes are either made available or pushed out and imported before the changes are put in service. When the changes take effect, the new profile is applied and the computers are instantly updated.

4 Unified VPN and WLAN client

MultiNetwork Manager makes VPN and WLAN easy to manage by providing a unified interface for different types of VPN and WLAN.

For VPN a separate profile may be set up, preferably by IT administration. The profile may use all connection controlling components available, including security settings and special scripts that may need to be run. This ensures IT administration full control of the VPN connection, and it provides a very easy way for the user to enable and disable the VPN connection that is the same irrespective of which VPN client that is used.

For wireless access points MultiNetwork Manager stores the security settings, including passwords and keys, for all access points that have been used. So on return to such an access point MultiNetwork Manager will automatically connect using the stored access data.

To enter data for a new access point data may be entered via a user dialog, or data may be imported from a file. IT administration may prepare such files with access information, and make them available for users who need to get access at different access points. The user may then import the data and connect via the access point. As a matter of fact, the user may not even know what the security settings are.

Further, to allow for IT administration to easily change security settings new settings may be pushed out to the users in advance. When the changes have been made to the access point, MultiNetwork Manager will discover the change and use the new data automatically. This provides for a smooth and simple update of the wireless network, e.g when changing from WEP keys to WPA key with password.