NETOP™ REMOTE CONTROL

# Mobile│Embedded™

Remote Support for Mobile & Embedded Systems

## User's Guide - Guest

Version 9.10

Netop

# Contents

# 1 Introduction

Welcome to Netop Mobile & Embedded, the Netop remote control software for mobile and embedded computers.

We hope that this product will meet your requirements and fulfill your expectations.

If you encounter problems using this product, first consult with this manual and help systems.

Additional troubleshooting guidance is available from the **Netop KnowledgeBase** that can be searched for detailed technical information.

The local supplier of your Netop product is available for advising you on how to obtain maximum benefit from it.

As a last resort, submit a support request to **Netop Customer & Product Support**. We will endeavor to get back to you as soon as possible with a solution to your problem.

*Netop Customer & Product Support*

## 1.1 Features

Netop Mobile & Embedded comprises Netop's solutions for mobile computers and computers running embedded operating systems.
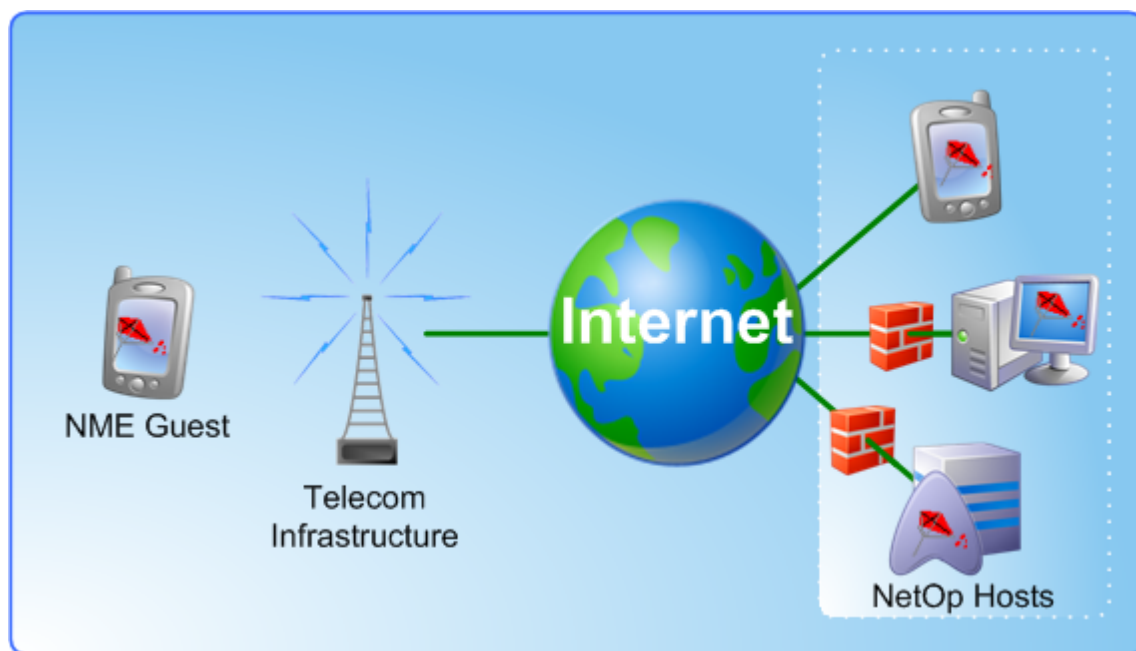


**Figure 1: Netop Remote Control Mobile & Embedded Guest controls, transfers files, chats etc. with PDAs, work stations, unmanned servers, which are all running Netop Remote Control Host.**

In this documentation, we will use the term **Netop Mobile** for Netop Mobile & Embedded and refer to the computer on which Netop Mobile & Embedded is installed as the **mobile device**, even if embedded in stationary equipment.

Netop Mobile & Embedded currently includes these modules:

**Mobile Guest**       Enables remote controlling devices running a Netop Remote Control Host (including Mobile Hosts) from a mobile device connected to your LAN or

|  |  |
|---|---|
| | to the Internet, for example via a cellular telephone network. |
| **Mobile Host** | Enables the mobile device to be remote controlled and interacted with in other ways from a computer that runs Netop Guest. |

**See also**

Mobile Actions
Operating System
Communication Devices
GUI Features

## 1.1.1 Mobile Actions

Netop Remote Control Mobile & Embedded Guest [Mobile Guest] has an extensive list of significant remote control features if allowed by Host Guest Access Security. Only a few are mentioned below:

| | |
|---|---|
| Remote Management | The Guest can start a remote management session with a Host to access Host computer management tools. |
| Inventory | This feature allows the Guest to compile an inventory list from the remote controlled device. |
| File Transfer | This feature allows the Guest to transfer files from the remote controlled Host or to transfer files to the Host. |
| Multi Chat | If Netop Host allows multiple simultaneous Guest connections Netop Guest can start a Chat session to join a Chat session running between another Guest and the Host to form a multi Chat session. |
| Remote Control | This feature allows the Guest user to see and manipulate the Host computer via screen, mouse and keyboard. |

For a full list, see Daily Use.

**See also**

Host Guest Access Security
Remote Management
Inventory
File Transfer
Multi Chat
Remote Control

## 1.1.2 Operating System

NME Guest runs on the following platforms and processors:

**Windows CE Mobile 5 ARM**

**Windows CE Mobile 6 ARM**

**Windows CE Pocket PC 2003 ARM**

## 1.1.3 Communication Protocols

Netop Mobile currently supports these communication protocols:

TCP We label it as LAN (TCP). Good default choice to reach most computers.

HTTP May be used to try to pass through firewalls and proxies.

UDP We label it as TCP/IP (UDP). May be used on local sub-net.

For these three protocols, you may connect to a Netop Host by entering its IP address or DNS name, optionally followed by a colon and a port number. The port number specifies the port number to send to in order to reach the Host. If you omit a port number, the default is 6502 for TCP and UDP, 80 for HTTP.

Examples include:

192.168.105.78

80.48.131.18:1031

mypc.mycompany.com

mypc

yourpc:173

If you do not get a connection, ensure that your mobile device has been assigned an IP address different from 127.0.0.1 by looking on the Info page. Then verify, that you can use the network, for example by using Internet Explorer. Next, make sure that a Netop Host is actually listening on the requested address and port. If you use DNS names like "mypc" or "mypc.mycompany.com", please be informed that the resolving of those names into IP addresses is done by the DNS server for the network, to which your mobile device is connected, not by Netop. If your DNS server does not do the job, you must explicitly enter the IP address yourself.

The data in the protocols is transported via a network. That network can be wireless, wired ethernet, ActiveSync/USB or telephony like GPRS. Most Windows Mobile devices shut down their wireless network when opening ActiveSync or GPRS. Netop is not aware which network is open or closed, that is the responsibility of the operating system. However, you can configure Netop to instruct the operating system to open its Internet or other network connection before trying to connect to a specific Host by setting a connection property in its address information.

**Which protocol shall I choose?**

- You shall always try TCP (LAN (TCP)) first. This protocol has the most reliable delivery and the smallest overhead.

- If your network forces you to pass a HTTP proxy or a firewall which only allows HTTP, you shall go for HTTP, but that will cost you in performance.

- You shall only use TCP/IP (UDP) if you cannot reach the Host using TCP or HTTP. Note that the reliable delivery of UDP packets is by protocol definition not guaranteed. When using GPRS, the UDP packets are sometimes simply dropped by the network.

**Note**

The labels LAN (TCP) and TCP/IP (UDP) are for Netop-historic reasons. TCP works nicely on both LAN and WAN. The UDP protocol uses UDP only by default, but can be reconfigured to use a mixture of UDP and TCP.

**Configuring Protocols**

Instances of the protocols are called profiles by Netop. When the Netop Mobile Guest starts, it will try to open one instance of the UDP protocol. TCP and HTTP profiles are opened automatically when needed. In the Netop Mobile Guest Manager, you can configure the UDP profile. TCP and HTTP profiles can not and need not be configured. The configuration parameters for UDP are:

| | |
|---|---|
| Name | Any string you wish to have. |
| Enabled | If you disable this, you can't connect via UDP at all. |
| Send port | The default remote port which packets are sent to. Useful with Netop Name Servers. |
| Receive port | Reserved for future use. Keep at 0. |
| Use Netop Name Server | A Netop Name Server may be used to resolve Host names into IP addresses. |
| Primary Netop Name Server | A DNS name or an IP address for a Netop Name Server. |
| Secondary Netop Name Server | A DNS name or an IP address for a Netop Name Server. |
| Override port | Enable this to overrule the port information received from the Netop Name Server. |
| Override port number | Use this port number instead of the port number provided by Netop Name Server. |
| Use TCP for session | You can enable this and make the UDP profile actually switch to using TCP instead of UDP whenever possible. |
| MTU | Adjust the maximum transmission unit, that is the maximum UDP packet size generated by Netop. |

**See also**

UDP - TCP/IP

# 1.1.4 GUI Features

The GUI has icons directly related to mobile actions and configuration.

**Home Screen**

The New icon commences the session which was defined in the Tools > Startup Session.

The Session icon opens the session screen.

The Disconnect icon terminates an ongoing connection.

The Favorites icon opens a window listing Host connection information for quick connect. Each Host session establishes a connection and launches a session (e.g. File Management or Remote Management) defined in the session. The session icon is the one used for the selected session. The properties contains possibility for the user to check mark for caching "last session data" related to File Management.

The Addresses icon opens a nested list view, not a single tree view. Entries can be copied to the favorites list.

The History icon fills the list view with information about previous sessions with Host ID, time stamp, address and communication profile. Entries may be copied to Favorites and Addresses.

The Inventory icon opens a screen containing system information (hardware and software) of Hosts.

The Info icon opens the list screen with information about Netop Guest ID, IP addresses and language.

The Tools icon opens the Tools screen.

The Stop icon exits the Mobile Guest.

**Sessions Screen**

The Light bulb icon indicates the connected Host computer.

It is grey when idle and yellow when busy.

The Remote Management button opens a window from which a Netop Host can be managed.

The Remote Control icon opens the Netop Mobile key feature. It enables the user of a mobile device that runs Netop Mobile Guest to display a Netop Host screen image which enables the Mobile Guest user to work with keyboard and mouse on the Host computer.

The File Transfer button opens a *File Manager* window split horizontally (optionally: vertically) with Host pane on top of Guest pane.

The Chat button opens a line based multi chat window. It has a Send button and a Send menu item. The text is also sent by hitting the <enter> button on the keyboard (s). The Send button may not be necessary if hitting <enter> can send the text line.

The Inventory icon opens a window containing information of the connected Host computer.

The Message icon opens the message window where you can compose a new message or use the one created in Properties.

The Run Program icon opens a screen where you can start a program.

The System Command icon opens a screen where you can select: Log off, Restart, Shut down, Wake on LAN or Lock computer.

**Introduction**

**Tools Screen**

The Special keys icon allows you to setup a zoom key and a fullscreen key.

The Properties icon allows you to setup how any new remote connection will be carried out.

**Note**

Individual remote session properties may be added to the Hosts in the Addresses and in the Favorites.

The Credentials icon allows you to setup access passwords to protected workstations, servers etc., it is necessary to send these logon credentials to the device you want to access.

The Startup Session icon allows you to setup  connects to the Netop Host when the Mobile Guest starts.

**List Screen**

The Inventory icon opens a window containing information of the connected Host computer.

The Remote Control icon opens the Netop Mobile key feature. It enables the user of a mobile device that runs Netop Mobile Guest to display a Netop Host screen image which enables the Mobile Guest user to work with keyboard and mouse on the Host computer.

The History icon fills the list view with information about previous connections with Host ID, time stamp, address and communication profile. Entries may be copied to Favorites and Addresses.

**See also**

New
Startup Session
Sessions
Favorites
Properties
Addresses
History
Inventory
Info
Tools
Remote Management
Remote Control
File Transfer
Chat
Message
Run Program
System Commands
Special Keys
Credentials

## 1.2 Common Controls

This section explains the controls of common Netop Remote Mobile & Embedded user interface elements. It includes these sections:

Connect to Host

Menus

### 1.2.1 Connect to Host

This describes the general way of a Mobile Guest connecting with a Netop Host.

Follow these steps:

1. Tap *New* in the main page.

2. Enter the Host's IP address or DNS name.

3. Select session type.

4. Select *Connect*.

**Note**

The Host may be protected by a password or it may be located behind a Gateway. To address these situations, click the links.

**See also**

New
Password
Gateway

### 1.2.2 Menus

The contents of the menu varies with the specific action that is being undertaken.
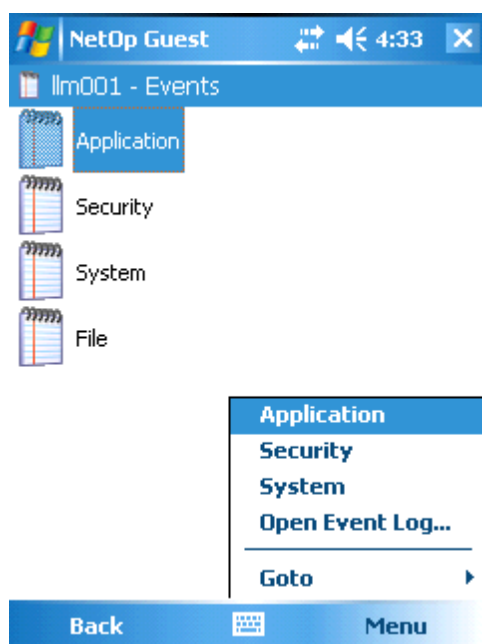
**Introduction**

Select an item and tap *Menu* to access the possible actions.

**See also**

New Menu
Chat Menu
Send Message Menu
Manage Menu
Control Menu
Inventory Menu
Run Program Menu
System Commands Menu
Addresses Menu
History Menu
Favorites Menu
Special Keys Menu
Properties Menu
Credentials Menu
Startup Sessions Menu

# 2 Installation

You can install Netop Mobile Guest directly on your mobile device, or you can install it via your Windows computer. Every installation set contains an **exe** and a **cab** file.

If you install via your desktop, you install from the exe file, and you do not need the cab file. You will install the Netop Mobile Guest Manager on your desktop and the Netop Mobile Guest on your mobile device. If your device is not connected with ActiveSync yet, the installation will be done here the next time you connect it. On your desktop, the manager program can create a configuration file, guest.xml, and put it on your mobile device.

If you want to install directly, you can place the installation cab file on a web- or other file-server, then execute the cab file using your device's Internet Explorer. If you install in this manner, you will get the default configuration. You can at any time copy a configuration file to here from another device. Place it in \Program Files\Netop Guest or whatever other directory you stored the Mobile Guest into.

**See also**

Install on a Desktop Computer
Install from a Desktop Computer
Install from a Web Server
Set Up Netop Mobile Host
Remove

# 2.1 Install on a Desktop Computer

These Netop Mobile installation sets are available:

**PPC2003 - Pocket PC 2003**

**WM50PPC - Windows Mobile 5.0 and 6.0 Pocket PC**

If you want to install by using the setup.exe file, it is not necessary to save the CAB file to your computer.

Use the CAB file to install directly on the device (setup.exe cannot run on the device).

1. Run setup.exe
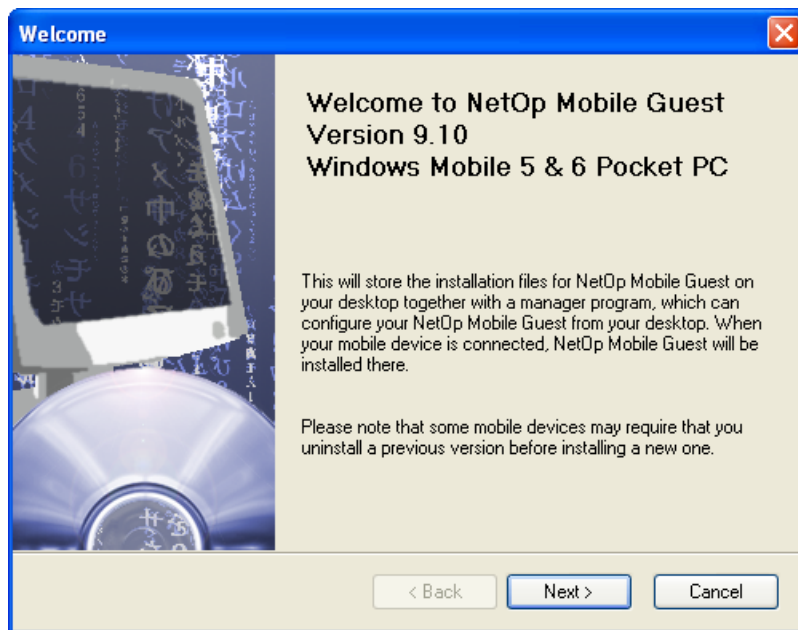
2. Follow the on-screen directions until the installation is finished.
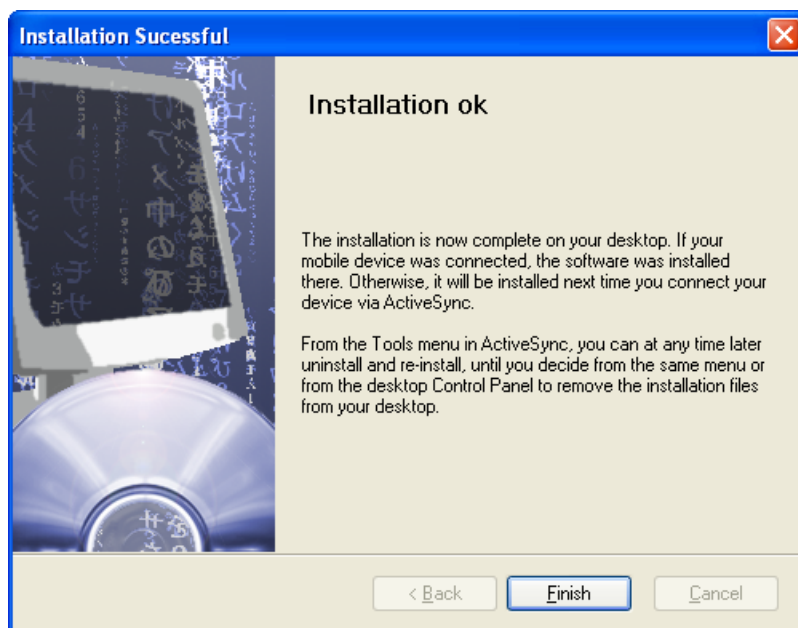


3. Now two programs are visible in the Windows *Start* menu.
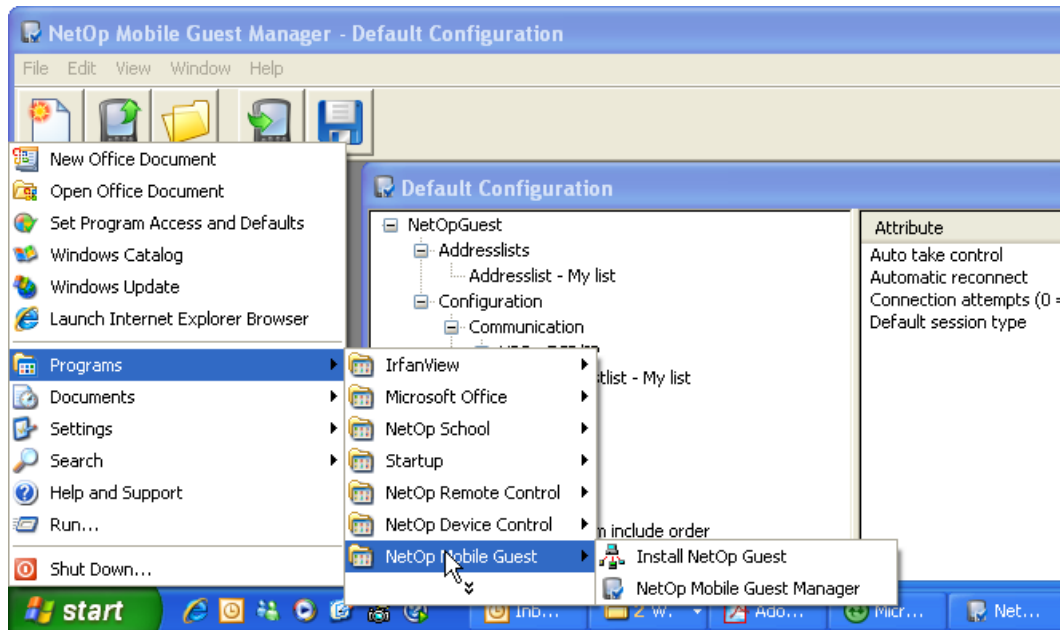
5. Then proceed to install and configure the Netop Mobile on the Mobile Device.

## 2.2 Install from a Desktop Computer

Connect the mobile device physically the desktop computer, which runs ActiveSync, where the Netop Mobile installation files have been installed.

Four scenarios may occur.

1. If the mobile device is connected via ActiveSync during the installation, the Netop ME Guest will be installed simultaneously.

2. If Netop Mobile Guest was not installed on the connected mobile device during Desktop Computer Installation, installation on the mobile device will start automatically when connected by ActiveSync.

3. Otherwise, on the desktop computer select *Start > All Programs > Netop Mobile Guest > Install Netop Mobile Guest* to start installation on the mobile device.

4. Alternatively, in the *Microsoft ActiveSync* window select *Tools > Add/Remove Programs* to display this window:
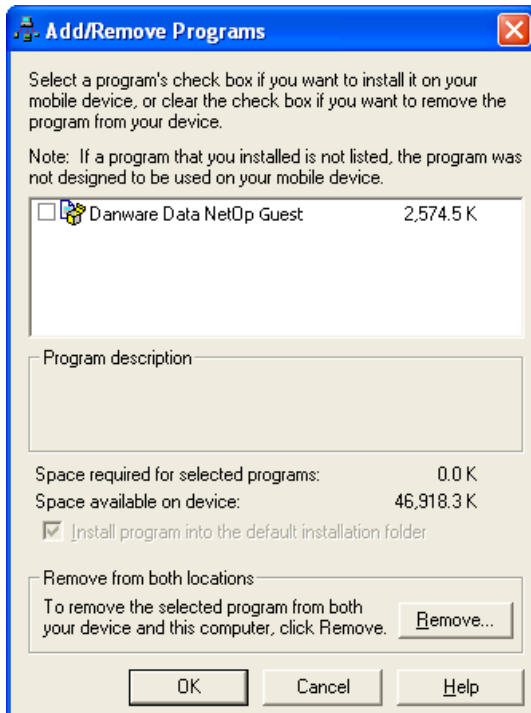


This window can download desktop computer available program installation files to the mobile device.

The pane will display check boxed records of programs for which installation files are available on the desktop computer. If a box is checked, ActiveSync has detected that the program is installed on the mobile device. If the *Danware Data Netop Guest* box is unchecked, check it and click *OK* to start installation on the mobile device.

## 2.3 Install from a Web Server

To enable installation directly on a device from a local web server, upload these files to the web server:

**Guest_PPC_StrongARM.cab**

**Guest_WM50PPC_StrongARM.cab**

To install Netop Mobile Guest on a mobile device, download the CAB file that matches the mobile device operating system to start installation.

## 2.4 Set Up Netop Mobile Guest

To set up Netop Mobile Guest identically on multiple mobile devices:

1. Install from a Desktop Computer on one mobile device.

2. Load Netop Mobile Guest to specify the license number.

3. Customize Netop Mobile Guest setup using Netop Mobile Guest Manager.

4. Copy the mobile device *\Program Files\Netop Host netopguest.lic* (license file) and *NetopGuest.xml* (customized setup file) to a selected desktop computer directory.

5. Install from a Desktop Computer on other mobile devices.

14

6. Copy the selected desktop computer directory *netophost.lic* and *NetopGuest.xml* files to the mobile device *\Program Files\Netop Guest* directory.

**Note**

For a thorough introduction to Guest/Host connectivity, please refer to Netop (Mobile) Host documentation - or take a quick glance here.

# 2.5 Remove

To remove Netop Mobile Guest from a mobile device, tap *Start > Settings > System > Remove Programs >Danware Data Netop Mobile Guest > Remove*.

**Note**

To remove all traces of the installation, manually remove the \Program Files\Netop Guest directory.

To remove a Desktop Computer Installation and Netop Mobile Guest from a mobile device connected to the desktop computer by ActiveSync, in the *Microsoft ActiveSync* window select *Tools > Add/Remove Programs* to display this window:
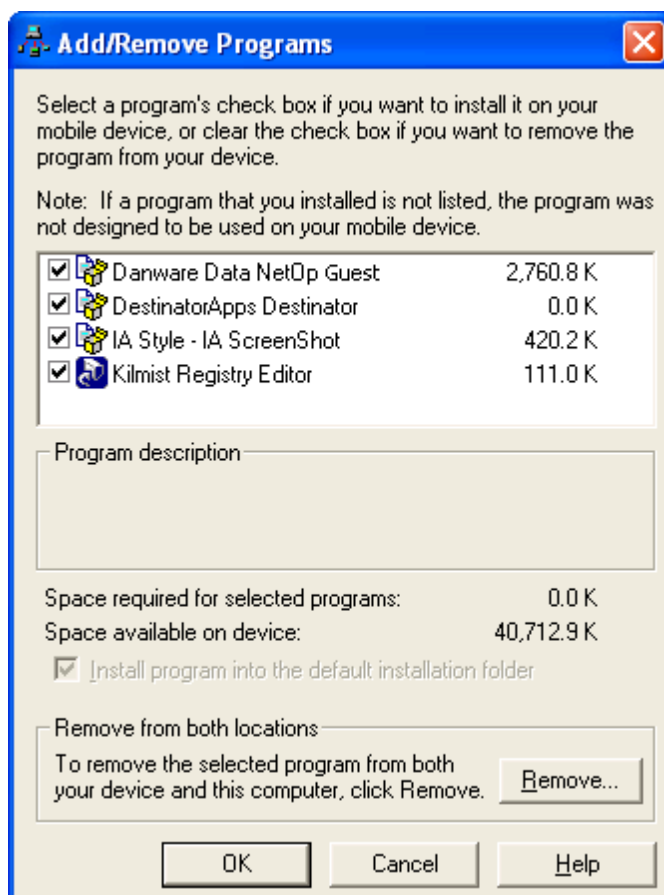


The pane will display check boxed records of programs for which installation files are available on the desktop computer. If a box is checked, ActiveSync has detected that the program is installed on the mobile device. Uncheck the checked *Danware Data Netop Mobile Guest* box and click *Remove* to remove Netop Mobile Guest from the mobile device and remove Netop Mobile Guest Manager and  mobile deviceinstallation files from the

desktop computer.

You can remove Netop Mobile Guest Manager and mobile device installation files from the desktop computer without removing  Netop Mobile Guest from a mobile device connected to the desktop computer by ActiveSync from *Start > Control Panel > Add or Remove Programs > Netop Mobile Guest*.

**Note**

To remove all traces of the desktop computer installation, manually delete the *Start > All Programs > Netop Mobile Guest* program folder.

# 3 Daily Use

This section deals with everyday Netop Mobile Guest issues.
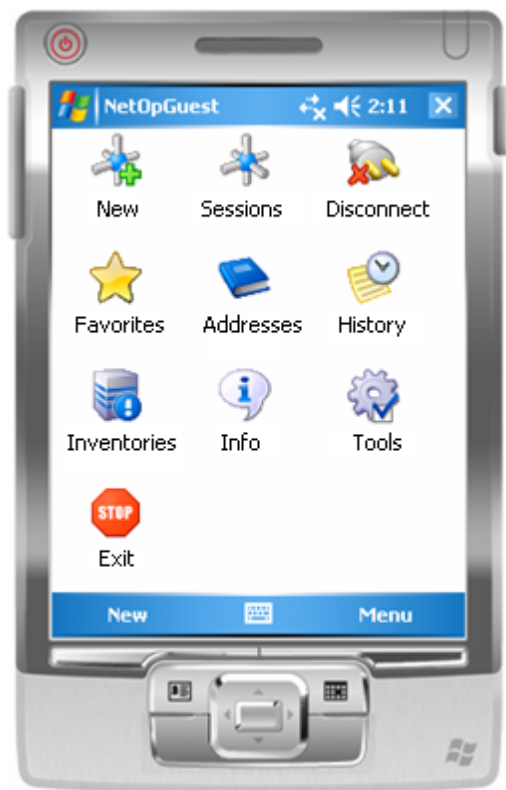


Each of the topics in this section are rooted in the tasks of a technician who has to support different types of equipment.

| | |
|---|---|
| New | Open a new connection. |
| Sessions | Select among session types. |
| Disconnect | Terminate your present session. |
| Favorites | Open saved Netop Hosts. |
| Addresses | Open saved Netop Hosts. |
| History | See and handle previously visited and controlled Netop Hosts. |
| Inventories | Retrieve previously acquired inventories. |
| Info | See Netop Guest specifics. |
| Tools | Access the most used setup tools. |
| Exit | Terminate Netop Mobile Guest |

**See also**

New
Sessions
Disconnect
Favorites
Addresses
History

# 3.1 New

Tap *New* to open a new connection.
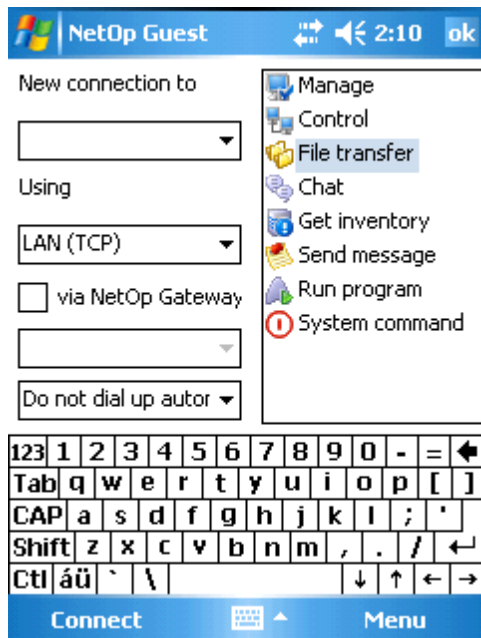


To establish a connection to a new Netop Host follow these steps:

1. Place the cursor in the drop-down list field and enter the IP address or DNS name.

2. Select communication profile. Netop Guest remembers the last type used.

3. Check *via Netop Gateway* if applicable, fill in the Gateway address and select dial up method.

4. Select the session type. The high-lighted session type is your default selection.

5. Tap *connect* and you're connected.

**See also**

Tools

## 3.1.1 Menu

| | |
|---|---|
| Cancel | Return to previous screen. |
| Properties | Configure which session is initiated upon connection. |
| Credentials | To access password protected workstations, servers etc., it is necessary to send these logon credentials to the device you want to access. |

**See also**

New
Properties
Credentials

# 3.2 Sessions

Netop Mobile Guest offers a number of session types (or actions) - especially selected from the ordinary Netop Remote Control - which cover most day-to-day events or incidents.

The following sections exemplifies how the Mobile Guest works in the field and how it is set up via the Mobile Guest Manager.

**Note**

Configuring the Mobile Guest is described in Handling Netop Mobile Guest.

**See also**

Remote actions
Communicating

## 3.2.1 Communicating

A Mobile Guest user can communicate to a Host user in two ways:

Chat

Send Message

### 3.2.1.1 Chat

Chat offers two-way text communication with the connected Host user.

Follow these steps:

1. Select *Chat* from the *Sessions* menu or from the icons.

2. Enter either IP address or DNS name.

3. Tap *Connect* and start chatting.

**Menu**

| | |
|---|---|
| Send | After writing the text, tap *Menu > Send* to transmit text to connected Netop Host. |
| Sessions | Select a session to connect to a Netop Host. |
| Exit | Terminate Netop Guest. |

**See also**

Common Controls
Connect via GPRS
Sessions

### 3.2.1.2 Send Message

Send Message offers one-way communication with the connected Host user.

Follow these steps:

1. Select *Send message* from the *Sessions* menu or from the icons.

2. Enter either IP address or DNS name.

3. Tap *Connect* and write a message.

**Note**

The messages you have sent are automatically saved. Use the drop-down list to choose from.

**Menu**

Send        After writing the text, tap *Menu > Send* to transmit text to connected Netop Host.

Sessions    Select a session to connect to a Netop Host.

Exit         Terminate Netop Guest.

**See also**

Common Controls
Connect via GPRS
Sessions

## 3.2.2 Remote Actions

Controlling, managing, investigating etc. Netop Hosts can all be performed via the mobile device.

The following sections show you how to connect and perform the actions.

**See also**

Manage
Control
File Transfer
Get Inventory
Run Program
System Commands

### 3.2.2.1 Manage

Selecting *Manage* gives you access to the listed items.

To connect - follow the described method.

Tap *Menu* to get access to specific Netop actions and standard Windows OS Explorer actions.

Disks        Details view will display table records with this column content:

Name        Disk drive icon and name.

Type        Disk drive type.

Total Size   Disk drive total size in bytes.

Free Space   Disk drive free space in bytes.

| | | |
|---|---|---|
| | File System | Disk drive file system. |
| | Total Used | Disk drive used space in bytes. |
| | Free % | Disk drive free space in percent of total space. |
| | Used % | Disk drive used space in percent of total space. |
| Events | *Events* contain four icons: Application, Security and System like the Windows Event Viewer. The fourth File icon can display a saved event log. | |
| | Each tab will display Host computer event records in a table with this column content: | |
| | Type | Event type icon and description. |
| | Date | Event date. |
| | Time | Event time. |
| | Source | Event source. |
| | Category | Event category if applicable. |
| | Event | Event ID. |
| | User | Event user name or N/A if not a user event. |
| | Computer | Event computer name. |
| Tasks | *Tasks* contain two icons: Application and Processes. | |
| | *Applications* contains records of applications running on the Host computer like the Windows NT+ (Windows 2003, XP, 2000 and NT) computer *Task Manager* window *Applications* tab in a table with this column content: | |
| | Task | : Windows icon and application description. |
| | Status | Will display Running if the application is running on the Host computer. |

*Processes* has an upper and a lower pane.

> The upper pane will contain records of processes running on the Host computer like the Windows NT+ (Windows 2003, XP, 2000 and NT) computer *Task Manager* window *Processes* tab in a table with this column content:

| | |
|---|---|
| Image Name | Process or executable file name. |
| PID | Process identification number. |
| CPU Usage | Percent of the currently used central processing unit (CPU) resources used by this process. |
| Time | Time that the process has run in the format HH:MM:SS:TTT (H=Hour digits, M=Minute digits, S=Second digits, T=Thousands fraction of a second digits). |
| Kernel Time | Percent of time running in kernel mode. |
| User Time | Percent of time running in user mode. |
| Threads | Number of threads running in the process. |
| Mem Usage | Bytes of memory used by the process. |

> The lower pane will contain records of threads run by the

process selected in the upper pane in a table with this column content:

| | |
|---|---|
| ID | Thread identification number. |
| Time | Time that the thread has run in the format HH:MM:SS:TTT (H=Hour digits, M=Minute digits, S=Second digits, T=Thousands fraction of a second digits). |
| Kernel Time | Percent of time running in kernel mode. |
| User Time | Percent of time running in user mode. |
| Priority | Priority ranking number (a high number means high priority for CPU resources). |

Registry    The Windows registry stores the configuration of the Windows operating system in a structured database. It is created when Windows is installed on the computer and is automatically modified when applications are installed and used and when users create or change personal settings.

---

**Caution**

Typical computer users should never attempt to edit the Windows registry, as even minor mistakes can have disastrous effects on the operation of the computer. Knowledgeable computer users can edit the registry to clean up the computer and modify its Windows configuration. However, always take suitable safety precautions including backing up the registry to avoid ending up in a deadlock.

---

The Windows registry is organized into five predefined subtrees:

HKEY_CLASSES_ROOT

Specifies file and data associations pointing to HKEY_LOCAL_MACHINE\Software\Classes keys. Its keys determine how applications load and associate with data files.

HKEY_CURRENT_USER

Specifies the profile of the user currently logged on to the computer. Its keys that are part of the logged on user's keys in HKEY_USERS take precedence over HKEY_LOCAL_MACHINE keys for duplicated data.

HKEY_LOCAL_MACHINE

Specifies the Windows configuration on the computer and determines how Windows loads.

HKEY_USERS

Contains a DEFAULT subtree that specifies the user profile when no user is logged on to the computer and a subtree that specifies the user profile of the user currently logged on to the computer.

HKEY_CURRENT_CONFIG

Specifies the hardware profile that determines how the installed software uses available hardware. It specifies associations between HKEY_LOCAL_MACHINE\Software keys and HKEY_LOCAL_MACHINE\System keys.

**Extreme Caution**

Importing a registration file will overwrite any matching keys and value records. If imported keys and value records and existing keys and value records mismatch, the registry will become corrupted.

Services    *Services* display all services running on the connected Host in a table.

Name          Service icon and name.

Description   Service description.

Status        Started, Stopped or Paused.

Startup Type  Automatic, Manual or Disabled.

Log On As     LocalSystem, NT AUTHORITY/LocalService, NT AUTHORITY/ NetworkService or <User name>.

Select a service and tap the menu to access:

Actions       start, stop, pause etc.

Properties    tap this to open the *Properties* window.

Refresh       the entire table with new information from the Host.

Add           select this command to enter a new Service.

Remove        select this command to delete the selected Service.

**Caution**

Removing a service may affect dependent services, see Dependencies Tab. If you remove a service of a running application, the service will become Stopped and Disabled. When the application is unloaded, the record will be removed.

Goto          any other Remote Management action type.

Shares      *Shared Folders* gives access to the following three views:

**Shares** displays Host computer shared resources as a table with this contents:

Share Name    Shared resource icon and name.

Folder Path   Directory path or resource description.

Type          Unknown or resource type name.

# Client      Number of current connections from remote computers.
Connections

Description   Shared resource description, if available.

**Note**

For administrative and system use, the operating system automatically creates special shares as hidden resources, typically with $ as the last character in the share name. See: [Special Shares](#).

**Sessions** displays Host computer shared folder sessions as a table with

this contents:

| | |
|---|---|
| User | Session user icon and Windows logon name. |
| Computer | Session computer name or address. |
| Type | Session computer operating system type. |
| Transport | Session communication device specification. |
| # Open Files | Number of session open files. |
| Connected Time | Session time in format HH:MM:SS (H=Hour digits, M=Minute digits, S=Second digits). |
| Idle Time | Time since last session user action in format HH:MM:SS (H=Hour digits, M=Minute digits, S=Second digits). |
| Guest | Displays Yes if the session user is logged on to Windows by a Guest account with typically very limited rights. Displays No if not. |

**Open Files** displays Host computer shared folder open files as a table with this contents:

| | |
|---|---|
| Open File | File icon, path and name. |
| Accessed By | File session user Windows logon name. |
| # Locks | File number of locks. |
| Mode | File permission type. |

| | |
|---|---|
| Inventory | *Inventory* contains a upper Contents Pane and a lower Details Pane. |
| | The Contents Pane displays the inventory directory structure. Each inventory directory folder can contain Host computer inventories that branch out into inventory elements. |
| | The Details Pane displays details of the inventory directory, Host computer inventory or inventory element selected in the Contents Pane. |
| | If allowed by the Host the Guest can get a detailed inventory of the Host computer's hardware and software. The inventory information is organized in four major groups: |

| | |
|---|---|
| Summary | User-defined view on the Host computer's software and hardware configuration. |
| Hardware | In-depth view of the Host computer's hardware configuration organized in three views: Computer, processor and memory. |
| Components | In-depth view of the Host computer's components, e.g. Multimedia, Storage, Base System. |
| Software | In-depth view of the Host computer's software configuration organized in three views: OS Environment, installed software and installed hot fixes. |

| | |
|---|---|
| Console | To access the host computer's *Console* you have to select one of these options: |
| ⊙ Use Host account | Open the Command Console display with the rights of the Host (default selection). |

| | |
|---|---|
| Use this account information | Open the Command Console display with the rights of the account with these computer logon credentials: |

Logon Name: Specify in this field a Host computer domain recognized user name.

Password: Specify in this field the matching password. Characters will display as asterisks.

Domain: Specify in this field the matching domain name.

☑ Load user profile: Leave this box checked to load the user profile of the specified account (default: checked).

Click *OK* to display a Host computer *Command Prompt* window in the Display Panel:

In the console window, you can specify commands that will execute on the Host computer.

| | |
|---|---|
| System | *System* lets you perform a number of actions on the Host computer: Lock, Log off user, Restart computer, Shut down computer. |
| Users | *Users* specifies share permissions. |

From the mobile Guest it is possible to see Groups and Users as a table with this content:

| | |
|---|---|
| User Name | Group or user icon and name. |
| Full Name | User full name, if available. |
| Description | Group or user description, if available. |

The menu allows the following:

| | |
|---|---|
| Add… | Click this button to display the *Select Users* window to add groups and/or users. |
| Delete | Select a record in the pane and click this button to remove it. |
| Permissions | This section specifies the permissions of the group or user selected in the pane above. Check boxes in the Allow column to grant permissions. Click boxes in the Deny column to deny permissions even if granted on the file system level: |
| Full Control | Change permissions plus change file system level permissions. |
| Change | Read permissions plus add files and sub folders, change data in files and delete sub folders and files. |
| Read | View file and sub folder names, view data in files and run program files. |

**Note**

Checking an upper box checks lower boxes. Share permissions

apply only to network users. They do not apply to users that log on locally including terminal server users. Preferably, assign permissions to groups and add users to groups rather than assign identical permissions to multiple users. If you change permissions on special shares, the original permissions may be restored when the server service or the computer is restarted.

Details    *Details* displays these details:

Host computer IP or MAC address

Guest communication profile name

Encryption type icon and name

Host computer operating system name

Session duration in format HH:MM:SS (H=hour digit, M=Minute digit, S=Second digit)

You cannot execute any actions from this section.

**See also**

### 3.2.2.1.1 Special Shares

For administrative and system use, the operating system automatically creates special shares as hidden resources, typically with $ as the last character in the share name.

**Note**

Typically, you should not delete or change special shares. If you delete or change special shares, they may become restored when the server service or the computer is restarted.

These special shares can be displayed on the *Shares* tab:

| | |
|---|---|
| <Drive letter>$ | Enables administrators to connect to the root directory of a drive. |
| ADMIN$ | Enables remote administration of a computer. Its path is always the path of the system root directory. |
| IPC$ | Enables interprogram communication by named pipes during remote administration and when viewing a computer's shared resources. It cannot be deleted. |
| NETLOGON | Required on domain controllers. If you remove it, domain client computers will lose functionality |
| SYSVOL | Required on domain controllers. If you remove it, domain client computers will lose functionality. |
| PRINT$ | Used during remote administration of printers. |
| FAX$ | A server folder that stores temporary telefax files and telefax cover pages. It is used by clients when sending a telefax. |

### 3.2.2.1.2 Menu

View            Change the appearance of the folder.

**GoTo**

Disks   Details view will display table records with this column content:

Name            Disk drive icon and name.

Type            Disk drive type.

Total Size      Disk drive total size in bytes.

Free Space      Disk drive free space in bytes.

File System     Disk drive file system.

Total Used      Disk drive used space in bytes.

Free %          Disk drive free space in percent of total space.

Used %          Disk drive used space in percent of total space.

Events   *Events* contain four icons: Application, Security and System like the Windows Event Viewer. The fourth File icon can display a saved event log.

Each tab will display Host computer event records in a table with this column content:

Type            Event type icon and description.

Date            Event date.

Time            Event time.

Source          Event source.

Category        Event category if applicable.

Event           Event ID.

User            Event user name or N/A if not a user event.

Computer        Event computer name.

Tasks   *Tasks* contain two icons: Application and Processes.

*Applications* contains records of applications running on the Host computer like the Windows NT+ (Windows 2003, XP, 2000 and NT) computer *Task Manager* window *Applications* tab in a table with this column content:

Task            : Windows icon and application description.

Status          Will display Running if the application is running on the Host computer.

*Processes* has an upper and a lower pane.

The upper pane will contain records of processes running on the Host computer like the Windows NT+ (Windows 2003, XP, 2000 and NT) computer *Task Manager* window *Processes* tab in a table with this column content:

Image Name  Process or executable file name.

PID             Process identification number.

CPU Usage   Percent of the currently used central processing unit (CPU)

|  | resources used by this process. |
| --- | --- |
| Time | Time that the process has run in the format HH:MM:SS:TTT (H=Hour digits, M=Minute digits, S=Second digits, T=Thousands fraction of a second digits). |
| Kernel Time | Percent of time running in kernel mode. |
| User Time | Percent of time running in user mode. |
| Threads | Number of threads running in the process. |
| Mem Usage | Bytes of memory used by the process. |
|  | The lower pane will contain records of threads run by the process selected in the upper pane in a table with this column content: |
| ID | Thread identification number. |
| Time | Time that the thread has run in the format HH:MM:SS:TTT (H=Hour digits, M=Minute digits, S=Second digits, T=Thousands fraction of a second digits). |
| Kernel Time | Percent of time running in kernel mode. |
| User Time | Percent of time running in user mode. |
| Priority | Priority ranking number (a high number means high priority for CPU resources). |
| Registry | The Windows registry stores the configuration of the Windows operating system in a structured database. It is created when Windows is installed on the computer and is automatically modified when applications are installed and used and when users create or change personal settings. |

---

**Caution**

Typical computer users should never attempt to edit the Windows registry, as even minor mistakes can have disastrous effects on the operation of the computer. Knowledgeable computer users can edit the registry to clean up the computer and modify its Windows configuration. However, always take suitable safety precautions including backing up the registry to avoid ending up in a deadlock.

---

The Windows registry is organized into five predefined subtrees:

HKEY_CLASSES_ROOT

Specifies file and data associations pointing to HKEY_LOCAL_MACHINE\Software\Classes keys. Its keys determine how applications load and associate with data files.

HKEY_CURRENT_USER

Specifies the profile of the user currently logged on to the computer. Its keys that are part of the logged on user's keys in HKEY_USERS take precedence over HKEY_LOCAL_MACHINE keys for duplicated data.

HKEY_LOCAL_MACHINE

Specifies the Windows configuration on the computer and determines how Windows loads.

HKEY_USERS

Contains a DEFAULT subtree that specifies the user profile when no user is logged on to the computer and a subtree that specifies the user profile of the user currently logged on to the computer.

HKEY_CURRENT_CONFIG

Specifies the hardware profile that determines how the installed software uses available hardware. It specifies associations between HKEY_LOCAL_MACHINE\Software keys and HKEY_LOCAL_MACHINE\System keys.

---

**Extreme Caution**

Importing a registration file will overwrite any matching keys and value records. If imported keys and value records and existing keys and value records mismatch, the registry will become corrupted.

---

Services    *Services* display all services running on the connected Host in a table.

| | |
|---|---|
| Name | Service icon and name. |
| Description | Service description. |
| Status | Started, Stopped or Paused. |
| Startup Type | Automatic, Manual or Disabled. |
| Log On As | LocalSystem, NT AUTHORITY/LocalService, NT AUTHORITY/ NetworkService or <User name>. |

Select a service and tap the menu to access:

| | |
|---|---|
| Actions | start, stop, pause etc. |
| Properties | tap this to open the *Properties* window. |
| Refresh | the entire table with new information from the Host. |
| Add | select this command to enter a new Service. |
| Remove | select this command to delete the selected Service. |

---

**Caution**

Removing a service may affect dependent services, see Dependencies Tab. If you remove a service of a running application, the service will become Stopped and Disabled. When the application is unloaded, the record will be removed.

---

| | |
|---|---|
| Goto | any other Remote Management action type. |

Shares    *Shared Folders* gives access to the following three views:

**Shares** displays Host computer shared resources as a table with this contents:

| | |
|---|---|
| Share Name | Shared resource icon and name. |
| Folder Path | Directory path or resource description. |
| Type | Unknown or resource type name. |
| # Client | Number of current connections from remote computers. |

Connections

Description    Shared resource description, if available.

---

**Note**

For administrative and system use, the operating system automatically creates special shares as hidden resources, typically with $ as the last character in the share name. See: Special Shares.

---

**Sessions** displays Host computer shared folder sessions as a table with this contents:

User    Session user icon and Windows logon name.

Computer    Session computer name or address.

Type    Session computer operating system type.

Transport    Session communication device specification.

# Open Files    Number of session open files.

Connected Time    Session time in format HH:MM:SS (H=Hour digits, M=Minute digits, S=Second digits).

Idle Time    Time since last session user action in format HH:MM:SS (H=Hour digits, M=Minute digits, S=Second digits).

Guest    Displays Yes if the session user is logged on to Windows by a Guest account with typically very limited rights. Displays No if not.

**Open Files** displays Host computer shared folder open files as a table with this contents:

Open File    File icon, path and name.

Accessed By    File session user Windows logon name.

# Locks    File number of locks.

Mode    File permission type.

Inventory    *Inventory* contains a upper Contents Pane and a lower Details Pane.

The Contents Pane displays the inventory directory structure. Each inventory directory folder can contain Host computer inventories that branch out into inventory elements.

The Details Pane displays details of the inventory directory, Host computer inventory or inventory element selected in the Contents Pane.

If allowed by the Host the Guest can get a detailed inventory of the Host computer's hardware and software. The inventory information is organized in four major groups:

Summary    User-defined view on the Host computer's software and hardware configuration.

Hardware    In-depth view of the Host computer's hardware configuration organized in three views: Computer, processor and memory.

Components    In-depth view of the Host computer's components, e.g.

Multimedia, Storage, Base System.

| | |
|---|---|
| Software | In-depth view of the Host computer's software configuration organized in three views: OS Environment, installed software and installed hot fixes. |
| Console | To access the host computer's *Console* you have to select one of these options: |
| Use Host account | Open the Command Console display with the rights of the Host (default selection). |

---

**Note**

If a user is logged on to the Host computer, the Host will typically have the rights of this user, see the Host *Program Options* window *Run As* tab documentation. You can open Netop Host Help in a Remote Control session.

---

| | |
|---|---|
| Use this account information | Open the Command Console display with the rights of the account with these computer logon credentials: |

Logon Name: Specify in this field a Host computer domain recognized user name.

Password: Specify in this field the matching password. Characters will display as asterisks.

Domain: Specify in this field the matching domain name.

Load user profile: Leave this box checked to load the user profile of the specified account (default: checked).

Click *OK* to display a Host computer *Command Prompt* window in the Display Panel:

In the console window, you can specify commands that will execute on the Host computer.

| | |
|---|---|
| System | *System* lets you perform a number of actions on the Host computer: Lock, Log off user, Restart computer, Shut down computer. |
| Users | *Users* specifies share permissions. |

From the mobile Guest it is possible to see Groups and Users as a table with this content:

| | |
|---|---|
| User Name | Group or user icon and name. |
| Full Name | User full name, if available. |
| Description | Group or user description, if available. |

The menu allows the following:

| | |
|---|---|
| Add… | Click this button to display the *Select Users* window to add groups and/or users. |
| Delete | Select a record in the pane and click this button to remove it. |
| Permissions | This section specifies the permissions of the group or user selected in the pane above. Check boxes in the Allow column to grant permissions. Click boxes in the Deny column to deny permissions even if granted on the file system level: |

| | | |
|---|---|---|
| | Full Control | Change permissions plus change file system level permissions. |
| | Change | Read permissions plus add files and sub folders, change data in files and delete sub folders and files. |
| | Read | View file and sub folder names, view data in files and run program files. |

> **Note**
>
> Checking an upper box checks lower boxes. Share permissions apply only to network users. They do not apply to users that log on locally including terminal server users. Preferably, assign permissions to groups and add users to groups rather than assign identical permissions to multiple users. If you change permissions on special shares, the original permissions may be restored when the server service or the computer is restarted.

| | |
|---|---|
| Details | *Details* displays these details: |

Host computer IP address

Guest communication profile name

Encryption type icon and name

Host computer operating system name

Session duration in format HH:MM:SS (H=hour digits, M=Minute digits, S=Second digits).

You cannot execute any actions from this section.

| | |
|---|---|
| Exit | Terminate Netop Guest. |

**See also**

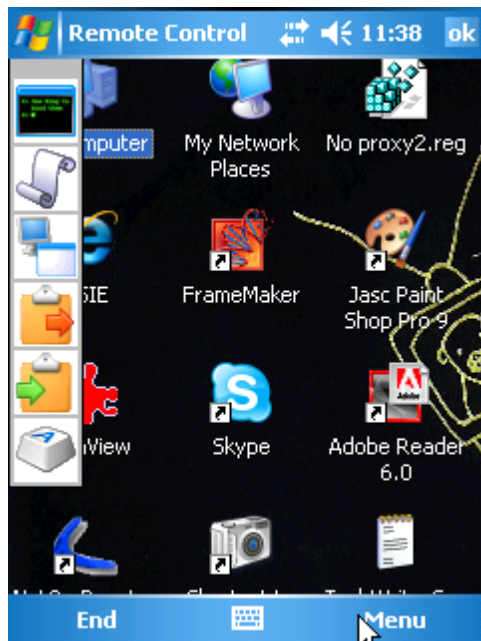## 3.2.2.2 Control

Selecting *Control* gives you access to the listed items.

To connect - follow the described method.

Tap *Menu* to get access to specific Netop actions and standard Windows OS Explorer actions.



**The zoomed-in transferred image from the Netop Host.**

---

**Note**

Tap the small grey area above the six icons to fold them up and maximize the viewing area.

---

 Tap this to zoom out. Tap with the pointer on the view panel to zoom to that particular area.

 Tap this to display/remove scroll bars.

 Tap this to toggle between window display and full screen display.

 Tap this to send local clipboard contents to Host clipboard.

 Tap this to retrieve saved image from the Host clipboard.

 Tap this to access the Remote Control functions.

**See also**

Connect to Host
Menu

### 3.2.2.2.1 Menu

Access the many functions of Remote Control either by tapping the "Special Key" icon or by tapping selecting Menu.

The control functions menu is divided into five parts:

| | | |
|---|---|---|
| Clipboard | Retrieve | Tap this to retrieve saved image from the Host clipboard. |
| | Send | Tap this to send local clipboard contents to Host clipboard. |
| Settings | Tap the setting to activate. | |
| | Activated settings are checkmarked. | |
| | The following settings (they are identical to the icons) are available: Fullscreen, Toolbar, Scrollbars, Zoom and Hotspots. | |
| Control | These control actions offer: | |
| | Grab | Take control of keyboard and mouse. |
| | Guard | Prevent other Netop Guests to connect to the Host. The *Guard* cannot be altered during the connection: it will be reset when the remote control session is terminated. |
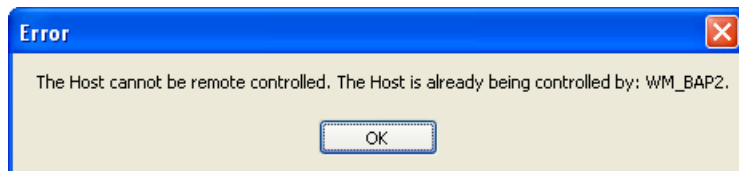


**If another Guest tries to connect to a guarded Host, this message appears on the connecting Guest.**

"Guard" equals the "Suspend further connections"-button on the Netop Remote Control Guest.

Go Solo — Evict other connected Guests. To be able to evict other Guest users it is necessary that the Netop Host recognizes you as the "Multi Guest session Administrator".

**Note**

See Netop Host documentation > Guest Access Privileges tab to learn how to set up one Guest user as Multi Guest session Administrator.

| | |
|---|---|
| Keys | These short cuts replace ordinary keyboard keystrokes. They work accordingly to the "in focus" application's shortcuts. |
| | Below is the list of available keys. |
| | F Keys (from F1 to F12), Esc, Alt, CTRL, AltGr, Windows, Start, Navigation Keys and Key Combos (e.g. CTRL+Alt+Del). |
| Exit | Terminate Netop Guest. |

### 3.2.2.3 File Transfer

When connected, the Guest can start and end a file transfer session from the *Sessions* view or menu.

**Note**

No window will be displayed on the Host computer screen.

The *File Transfer* menu is organized in four sections:
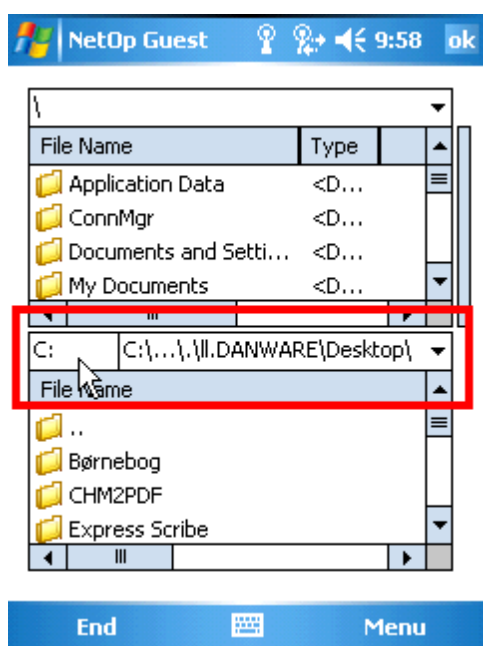
[File](#)

[Edit](#)

[View](#)

[Options](#)

**Note**

If allowed on Guest Access Security, the Guest can start a file transfer session with a Host to transfer files between the Guest and Host computer.

### 3.2.2.3.1 File



***File Transfer* window. The connected Guest's disk drive is highlighted.**

Copy Files   Select Record Panel records and select this command or the matching Record Panel context menu command, press any matching keyboard shortcut, see Layout Tab, or click the matching Toolbar File Transfer Buttons button to display the *Copy* window, see Copy/Move/Synchronize/ Clone.

**Note**

Alternatively, drag records from one Record Panel to the other and drop

them.

| | |
|---|---|
| Move Files | Select Record Panel records and select this command or the matching Record Panel context menu command, press any matching keyboard shortcut, see Layout Tab, or click the matching Toolbar File Transfer Buttons button to display the *Move* window, see Copy/Move/Synchronize/ Clone. |
| Sync Files | Select this command or click the matching Toolbar File Transfer Buttons button to display the *Synchronize* window, see Copy/Move/Synchronize/ Clone. |

**Note**

By default, synchronization will transfer directories and files to include directories and files that exist in either Record Panel in both Record Panels replacing older files by newer files. On the *Options* window *Transfer* tab, you can apply the Synchronize selections Transfer only if file exists and Transfer only one way.

| | |
|---|---|
| Clone Files | Select this command or click the matching Toolbar File Transfer Buttons button to display the *Clone* window, see Copy/Move/Synchronize/Clone. |

**Note**

Cloning will transfer all directories and files in the selected Record Panel to the unselected Record Panel deleting existing directories and files in it.

| | |
|---|---|
| New Folder | It is possible to create a folder on both Guest and Host. Follow these steps: |

1. Select either the Guest or the Host by tapping the disk drive field.

2. Select which drive the folder is to be created on.

3. Specify the new folder name and tap *OK*.

| | |
|---|---|
| Drive Info | Select a drive and see the following disk drive information: |

Source: This pane will display icons and letters of the drives found on the selected Record Panel computer. Select a drive to display information on the drive in the Information section.

Device Type: Drive type.

File System: Drive file system.

Free: Drive free space in bytes.

Total: Drive capacity in bytes.

Tap *OK* to close the view.

| | |
|---|---|
| Delete | Select a file or a folder (or multi-select) for deletion and tap *OK*. |

A new screen opens. Tap the *Menu* to select an action.

Skip: Regret deleting the selected file or folder.

Advanced: Offers five deletion options. Checkmark your choice and tap *OK* to execute:

Deleting non-empty folders

Deleting files

Deleting read-only files

Deleting hidden files

Deleting system files

Delete: Selected file/folder is deleted.

Close the new screen to return to File Transfer.

---

**Caution**

Deleting a directory will delete directories and files in it.

---

Rename      Select a file or a folder to rename.

Tap *Menu > File > Rename* to open a new screen.

Enter the new name and tap *OK* to confirm the new name and return to File Transfer.

Properties      Configure which session is initiated upon connection.

This screen will display the properties of the selected file or folder including attributes that can be changed.

Close      Exit File Transfer and return to Sessions screen

**See also**

File Transfer
Edit
View
Options
Properties

### 3.2.2.3.2 Edit

Select All      Select this command or press any matching keyboard shortcut, see Layout Tab, to select all directories and files in the selected Record Panel.

Select By      A new screen opens.

In the field, replace *.* designating all directories and files by a file mask (a file name with wildcard characters like * designating any characters) to select files and directories with common name characters.

Tap *OK* to select unselected directories and files in the selected Record Panel by the file mask.

Deselect By      A new screen opens.

In this field, replace *.* designating all directories and files by a file mask (a file name with wildcard characters like * designating any characters) to deselect files and directories with common name characters.

Tap *OK* to deselect selected directories and files in the selected Record Panel by the file mask.

Invert Selection      Select this command to make all selected directories and files unselected and all unselected directories and files selected in the selected Record Panel.

Clear      Select this command to deselect all directories and files in the selected

Selection     Record Panel.

### 3.2.2.3.3 View

Large Icons  Select this command to display records as horizontal rows of large icons.

Small Icons  Select this command to display records as horizontal rows of small icons.

List         Select this command to display records as vertical columns of small icons.

Details      Select this command to display records in a table with details in columns (default selection).

Local        Select this command to switch between remote and local file transfer (default: uncheckmarked/released for remote file transfer).

Arrange      This command expands into these commands:
Icons

    By Name      Select this command to sort file records by file name, ascending/descending like the Details view selection.

    By Type      Select this command to sort file records by extension, ascending/descending like the Details view selection.

    By Size      Select this command to sort file records by size, ascending/ descending like the Details view selection.

    By Date      Select this command to sort file records by time, ascending/ descending like the Details view selection.

    Auto Arrange Select this command to uncheckmark/checkmark it to disable/ enable automatically sorting file records by the current selection after changes (default: checkmarked for Auto Arrange enabled).

    **Note**
    Directory records in alphabetically ascending order will always be displayed before files. In Details view, sort records ascending/descending by clicking column headings.

Refresh      Select this command to retrieve new information from the computers to refresh the Record Panel content.

### 3.2.2.3.4 Options

| | |
|---|---|
| Transfer | Select this command to display the Transfer options screen: |

The two top most items are related to *Synchronization* and the remainder are related to *General Transfer*.

**Synchronize**

| | |
|---|---|
| Transfer only if file exists | Check this box to synchronize files only if they exist in the unselected Record Panel (default: unchecked). |
| Transfer only one way | Check this box to synchronize files only from the selected Record Panel to the unselected Record Panel (default: unchecked). |

**General Transfer**:

| | |
|---|---|
| Include subfolders | Leave this box checked to transfer also the contents of subdirectories of selected directories. |
| Use delta file transfer | Leave this box checked to compare source files with matching destination files and transfer only differences between source and destination files to save transmission bandwidth. |
| Enable crash recovery | Leave this box checked to transfer files in a way that they can be recovered after a computer or network crash during file transfer. |
| Close dialog when finished | Check this box to close the *Transfer Status* window when a file transfer is finished. |
| End session when finished | Check this box to end the File Transfer session when a file transfer is finished. |

| | |
|---|---|
| Confirming | Select this command to display the Confirmation settings screen: |

If one or more of these setting are selected a confirm pop-up window will be issued.

| | |
|---|---|
| Deleting non-empty folders | Leave this box checked to display this confirmation window if you are about to delete a directory that contains directories or files. |
| Overwriting existing files | Leave this box checked to display the *Overwrite* window if you are about to overwrite existing files. |
| Overwriting/ deleting read-only files | Leave this box checked to display the relevant confirmation window if you are about to overwrite/delete read-only files. |
| Overwriting/ deleting hidden files | Leave this box checked to display the relevant confirmation window if you are about to overwrite/delete hidden files. |
| Overwriting/ deleting system files | Leave this box checked to display the relevant confirmation window if you are about to overwrite/delete system files. |
| End session when finished | Leave this box checked to end File Transfer when files are transferred. |

> **Note**
>
> If confirmation notification is switched on, tap *OK* on the screen itself.

Other Select this command to display the General options screen:

Checkmark one or more selections (default selection)

Save session pathname at exit.

Generate Log File Leave this box checked to generate a file transfer log file when ending a File Transfer session.

Append if Log File exists Check this box to append new log entries to an existing log file. If unchecked, an existing log file will be overwritten (can only be selected if *Generate Log File* was selected).

Log filename This field will specify the log file (path and) name, by default NFM.LOG that will reside in the Netop Configuration Files directory, typically C:\Documents and Settings\<User name>\Application Data\Danware Data\Netop Remote Control\Guest (can only be selected if *Generate Log File* was selected).

View log file Select this to display the log file.

This will be created only if the *Generate Log File* were checkmarked in General options (Other).

Log files have the file extension *.log.

**See also**

File Transfer
File
Edit
View

### 3.2.2.4 Get Inventory

Once connected to the Host in a *Get Inventory* session, you are offered five different views of the Host.

Generation This view contains session specific data.

Summary The summary contains a customizable and prioritized list of available items (software and hardware).

The list can be configured in the Netop Mobile Guest Manager in Inventory.

Hardware The list contains all hardware related inventory information. It is divided int o three sub-categories:Computer, Processor and Memory.

Components The list contains all component related inventory information.

Software The list contains all software related inventory information. It opens in three sub-categories: OS Environment, Installed Software and Installed Hot-Fixes.
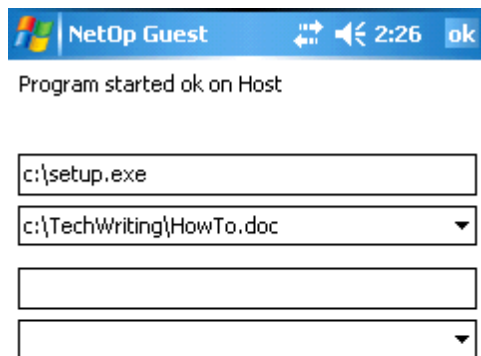
**Menu**

Refresh        Renew the contents of the inventory.

Exit           Terminate Netop Guest.


**See also**

Configuration Panel
Netop Mobile Guest Manager
Inventory


### 3.2.2.5 Run Program

Use this session type to start a program on the Host computer.



**Tap *Menu > Run* to run "Setup.exe" on the connected Host computer.**
**The last *Run Program* session was opening MS Word with a document named "HowTo.doc".**

The screen consists two pairs of fields.

| | |
|---|---|
| Top pair of fields | The field of this box will display the program file path and name (default: empty). |
| | The drop-down box list contains paths and names of files that have been run from this window before. Select a path and name in the list to display it in the field or specify in the field a file path and name. |
| Bottom pair of fields | The field of this box will display switches that will be applied to the command specified in the Program path drop-down box field (default: none). |
| | The drop-down box list will contain switches that have been applied in this window before. Select switches in the list to display them in the field or specify in the field the switches that shall be applied to the file. |

**Menu**

Run            After having entered the command and parameters, tap *Menu > Run*.

Exit           Terminate Netop Guest.


### 3.2.2.6 System Commands

Use this session type to perform one of the following pre-defined commands on the connected Host computer:

Log off        Select this and tap *Menu > Execute* to log off the connected Host computer.

Restart        Select this and tap *Menu > Execute* to restart the connected Host computer.

Shut down      Select this and tap *Menu > Execute* to shut down the connected Host computer.

Wake on LAN    Select this and tap *Menu > Execute* to start a turned off, yet network connected, Host computer.

Lock           Select this and tap *Menu > Execute* to lock the connected Host computer.
computer

**Note**

The Netop Host may have banned certain actions. If a particular action does not work or is greyed out in the menus, look for the reason on the Host side, firstly.


**Menu**

Cancel         Return to previous screen.

Properties     Configure which session is initiated upon connection.

Credentials    To access password protected workstations, servers etc., it is necessary to send these logon credentials to the device you want to access.

**See also**

Properties
Credentials


## 3.3 Disconnect

Tap this to disconnect and end a session.

## 3.4 Favorites

This folder contains entries from the the Addresses or the History folder.

Double-tap an record to start a connection with a predefined session type or use the *Menu > Execute* command.

Favorites records are saved as files in the Favorites directory that resides in the Netop

Configuration Files directory, typically on *My Device\Application Data\Netop Guest\Favorites*.

---

**Note**

Entries in Addresses and Favorites are NOT linked and thus not necessarily identical. It is possible to change the Properties in either view.

---

**See also**

Favorites Menu
Addresses
History
Properties

## 3.4.1 Menu

| | |
|---|---|
| Execute | Start the previously defined session type. |
| Properties | Configure which session is initiated upon connection. |
| Rename | Enter a new name. |
| Delete | Delete the Netop Host record.. |
| Sessions | Select a session to connect to a Netop Host. |
| View | Change the appearance of the folder. |
| Exit | Terminate Netop Guest. |

**See also**

Favorites
Properties
Sessions
View

# 3.5 Addresses

Addresses serves one purpose:

Organizing all important Netop Hosts making it easy to connect to them in your daily work.

Addresses is populated in two ways:

Entering the Netop Host computer via the keyboard of the handheld device, or

Copying the Netop Host computer from the History directory.

The following sections exemplifies how all of the above are carried out.

Address records are saved as files in the Addresses directory that resides in the Netop Configuration Files directory, typically on *My Device\Application Data\Netop Guest\Addresses*.

**See also**

Organize Addresses
Populate Addresses

## 3.5.1 Organize Addresses

To organize the addresses follow these steps:

1. In Addresses, tap *Menu > New* folder.

2. Via the keyboard of the device enter an appropriate folder name.

3. Select an address and tap *Menu > Cut*

4. Open the folder and tap *Menu > Paste*.

This concludes organizing your addresses.

**See also**

Populate Addresses
Addresses Menu
Addresses Menu

### 3.5.1.1 Populate Addresses

There are two methods to populate Addresses, follow these steps:

**Entering address**

1. In Addresses, tap *Menu > New address*.

2. The general connect screen opens.

3. Enter the Host address. You can use DNS name or IP address.

4. Select communication device. You can use LAN (TCP), HTTP or TCP/IP (UDP).

If you have to access the Netop Host through a gateway, proceed with the following steps:

5. Checkmark the "via Netop Gateway" box.

6. Enter the address of the gateway in this format:

    gateway.yourcompany.com:1234

7. Select the connect method. You can use "Do not dial up automatically", "Dial up the Internet if not already dialed" or "Dial up using RAS".

8. Select which session type this address initially will carry out and tap *OK*.

This concludes entering an address.

**Copying address**

1. In the Home screen, tap the History icon.

2. The History screen opens.

3. Select one of the occurrences and tap *Menu > Add to Addresses*.

4. Tap *Home > Addresses* and place the added Netop Host in the correct folder.

This concludes copying an old connection to Addresses.

**See also**

## 3.5.2 Menu

The menu associated to Addrresses contains the following selections:

Properties    Configure how the connection of the Netop Host is to be carried out.

Cut           Remove the Netop Host connection from the list and place it on the clipboard.

Paste         Insert a Netop Host connection from the clipboard.

Duplicate     Place a copy of the Netop Host connection on the clipboard while keeping it in the list.

Rename        Enter a new name.

Delete        Delete the Netop Host record.

Add to        Add the selected Netop Host to the Favorites folder.
favorites

New           Enter a new computer (DNS name or IP address) in the Addresses.
Address

New Folder    Create a new folder.

Sessions      Select a session to connect to a Netop Host.

View          Change the appearance of the folder.

Exit          Terminate Netop Guest.

**See also**

## 3.6 History

A history record is automatically created in the History folder when disconnecting from a Host. All history records in the folder carries within them a timestamp and the performed action.

You can copy and move history records to the Addresses or to  the Favorites.

History records are saved as files in the History directory that resides in the Netop Configuration Files directory, typically on *My Device\Application Data\Netop Guest\History* .

**See also**

Favorites

## 3.6.1 Menu

Properties   View the contents of the selected file.

Delete   Delete the selected file.

Add to   Add the selected file to the Addresses folder.
Addresses

Add to   Add the selected file to the Favorites folder.
favorites

Clear   Delete all files in History.
history

Sessions   Select or start a session.

View   Change the appearance of the folder.

Exit   Terminate Netop Guest.

**See also**

History
Properties
Addresses
Favorites
Sessions
View

## 3.7 Inventory

This folder contains the inventory files - one per Host.

A new inventory file from a Host will overwrite the old inventory file.

Double-tap or tap *Menu > View* to see the contents of a selected inventory record.

**See also**

Get Inventory
Configuration Panel > Inventory

# 3.8 Tools

The tools section on the Mobile Guest consists of the most-used setup options. The other options may be accessed via the Netop Guest Manager.
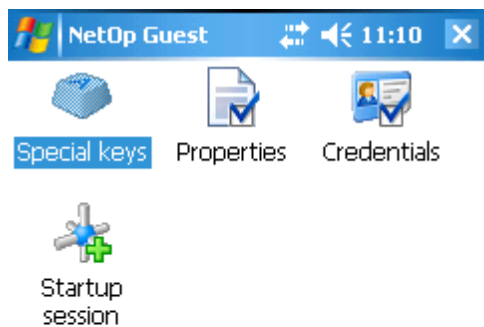




**See also**

Special keys
Properties
Credentials
Startup Session

## 3.8.1 Special Keys

Select which buttons on the mobile device should have special functions.
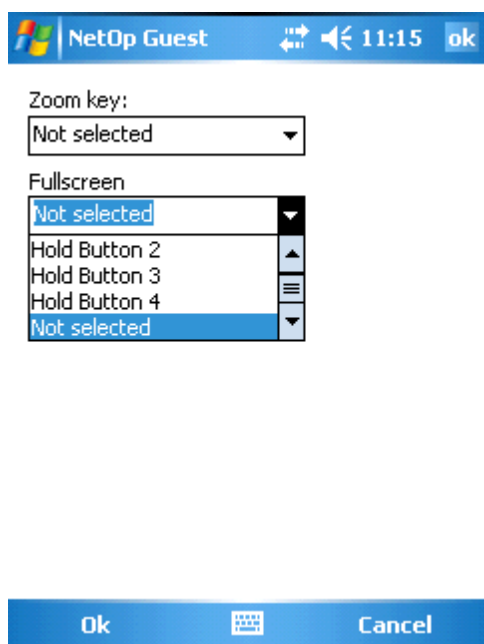
**Daily Use**

Select which of the device's keys should be the zoom key and which should be the fullscreen key.

Follow these steps:

1. On the Mobile Guest, select the zoom key from the drop-down list.

2. On the device, select and hold any key to select it to be the zoom key.

3. The next time you want to zoom a remote controlled Host, press and hold the zoom key for a short while.

4. Proceed with the fullscreen key.

**Note**

It is also possible to +/- zoom by touching the handheld's display.

**See also**

Special Key Menu

### 3.8.1.1 Menu

Sessions      Select a session to connect to a Netop Host.

View          Change the appearance of the folder.

Exit          Terminate Netop Guest.

**See also**

Special Keys
Sessions
View

## 3.8.2 Properties

Set the most-used actions in this screen.



**Note**

Properties must be setup before the session begins.

| | |
|---|---|
| Lock keyboard | Check this to lock the keyboard of the remote controlled Netop Host. |
| Blank screen | Check this to blank the screen of the remote controlled Netop Host. |
| Guard Host | Check this to suspend other Guests from connecting to Host: |
| | The "guarded Host" is indicated in the GUI of the standard Guest. |
| Color transfer | Transmission speed between Guest and Host can be improved by decreasing the number of transferred colors. Select one: |

| | |
|---|---|
| Slowest | Transfer actual colors. |
| Slow | Transfer max 256 colors. |
| Fast | Transfer max 16 colors. |

| | |
|---|---|
| Graphic modes | Transmission speed between Guest and Host can be improved by decreasing the graphic standard. Select one: |

| | |
|---|---|
| Slowest | Command mode graphics. |
| Medium | Bitmap mode graphics. Displays screen correctly. |
| Fastest | Simple bitmap mode. |

| | |
|---|---|
| Encryption | Netop Mobile Guest can communicate with any of the allowed encryption settings in the list. The different encryption types are listed according to their level of security. |

It specifies enabled encryption types. Per default all is enabled. To change settings and learn of the encryption types, see Netop Guest Manager > Security.

| | |
|---|---|
| Compression | Compression speeds up the transfer rate, but the process also consumes time. There are four settings, select one. |

| | |
|---|---|
| Compression automatic | Selects compression based on communication profile properties. In most cases, this will provide the fastest transmission (default selection). |
| No compression | Typical selection for fast communication links. |
| Low compression | Typical selection for medium fast communication links. |
| High compression | Typical selection for slow communication links. |

| | |
|---|---|
| Cache | Command mode Host screen transfer stores the screen image in cache memory and transfers only image changes to save transmission bandwidth and optimize update speed. |

The field of this drop-down box displays the selected cache memory size option (default: Automatic). The drop-down box list contains the options Automatic and values from None to 10240 kb.

Automatic selects the cache memory size based on communication profile properties. In most cases, this will provide the optimum.

| | | |
|---|---|---|
| Window Size | Full screen | This mode eliminates all scroll bars and menu bars on the device's screen. Due to the limited size of the device, hotspots allow you to move the view. The hotspots are located in each corner and in the middle of the screen. |
| | Normal window | This mode has scroll bars and menu bar. |

| | |
|---|---|
| (Parameters) | Tapping this allows you to enter a message to controlled Host. |
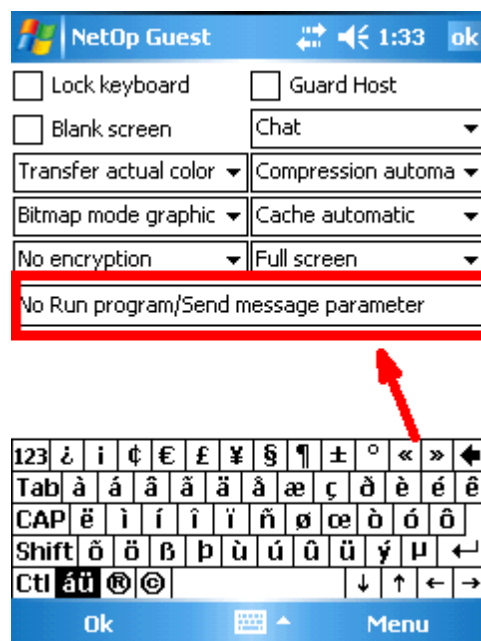
This message is stored with the properties until the next time you are going to use it.

Example: *Your PC is being restarted. Close all programs.*

This only works with Send Message*.*

**See also**

Properties Menu
Security
Send Message

### 3.8.2.1 Menu

Cancel          Return to previous screen.

Credentials  To access password protected workstations, servers etc., it is necessary to send these logon credentials to the device you want to access.

Connect to  Enter a Netop Host (DNS name, IP address or MAC address) as described in New.

**See also**

Properties
Credentials
New

## 3.8.3 Credentials

To access password protected workstations, servers etc., it is necessary to send these logon credentials to the device you want to access.



A Host and a connecting Gateway can authenticate a connecting Guest or Guest user by logon credentials and other checks. See: Setting the Host or Gateway password and Connecting.

**Note**

You can enter username and password in one of two formats: either 'username@domain' or 'domain\username'.

**See also**

Credentials Menu

### 3.8.3.1 Menu

Cancel       Return to previous screen.

Properties   Configure which session is initiated upon connection.

Connect to   Enter a Netop Host (DNS name, IP address or MAC address) as described in New.

**See also**

Credentials
Properties
New

## 3.8.4 Startup Sessions

The startup session automatically connects to the Netop Host when the Mobile Guest starts.
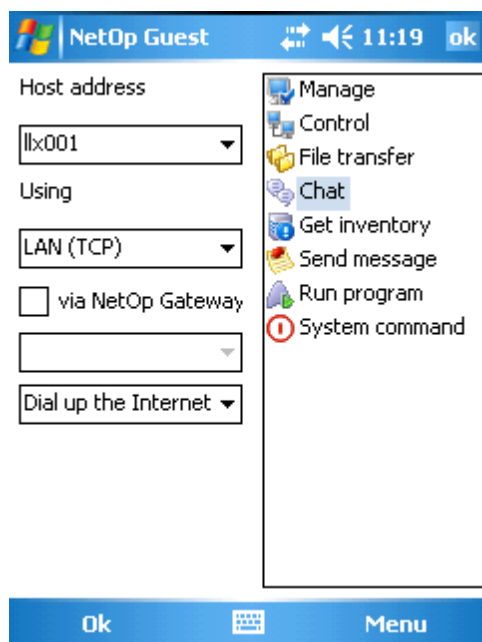


The Host address may be entered as either IP address or DNS name.

Depending on the type of network and/or device, select either LAN (TCP), HTTP or TCP/IP (UDP) communication profile. LAN (TCP) is default.

**See also**

Connect via GPRS
Startup Sessions Menu

### 3.8.4.1 Menu

Cancel       Return to previous screen.

Properties   Configure which session is initiated upon connection.

Credentials  To access password protected workstations, servers etc., it is necessary to send these logon credentials to the device you want to access.

**See also**

Startup Sessions
Properties
Credentials

# 3.9 Connecting

There are several ways to connect the Mobile Guest to different Netop Host types.

In the following you will learn to connect via Wireless and via GPRS.

**See also**

Connect via GPRS
Connect via Wireless

## 3.9.1 Connect via Wireless

Wireless connection to Netop Hosts is particular practical in environments where the supporter or the administrator do not always sit at their desks.
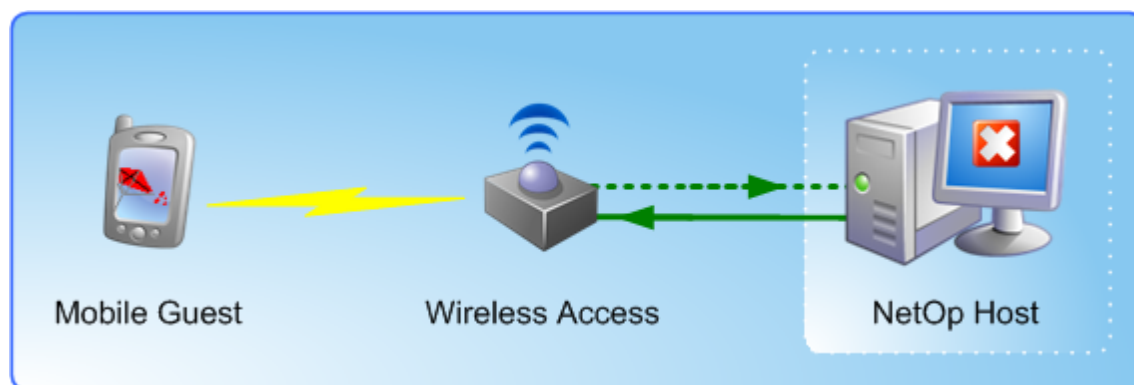


**The Mobile Guest initiates the connection between the handheld device and the Netop Host.**

The user who runs Netop Host has to contact the administrator with the problem and inform him about the IP address, MAC address or DNS name.

Follow these steps to connect:

1. On the Mobile Guest select Sessions - either from the menu or via GUI.

2. Select the session type (ex. *File transfer*) and enter the IP address, MAC address or DNS name.
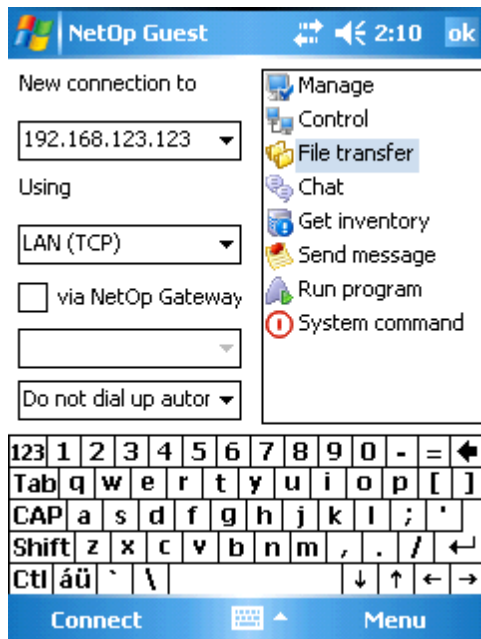


**Enter IP address or DNS, select session type and click Connect.**

3. Enter the Password (set in Netop Host > Tools > Guest Access Security > Default User (see Netop Host documentation)).



**Enter the password and click *OK* to connect.**

4. Ready to remote control the Netop Host.
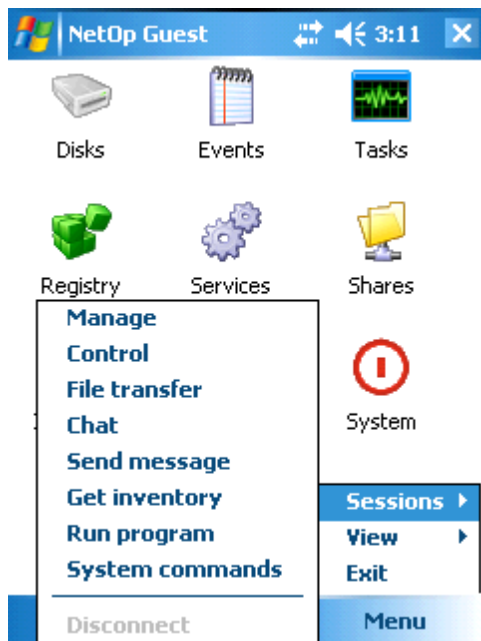
5. Select session type.

This concludes connecting to a Netop Host from within the LAN.

**See also**

GPRS connection

## 3.9.2 Connect via GPRS

If you are outside the wireless LAN you are still able to remote control PC and servers.
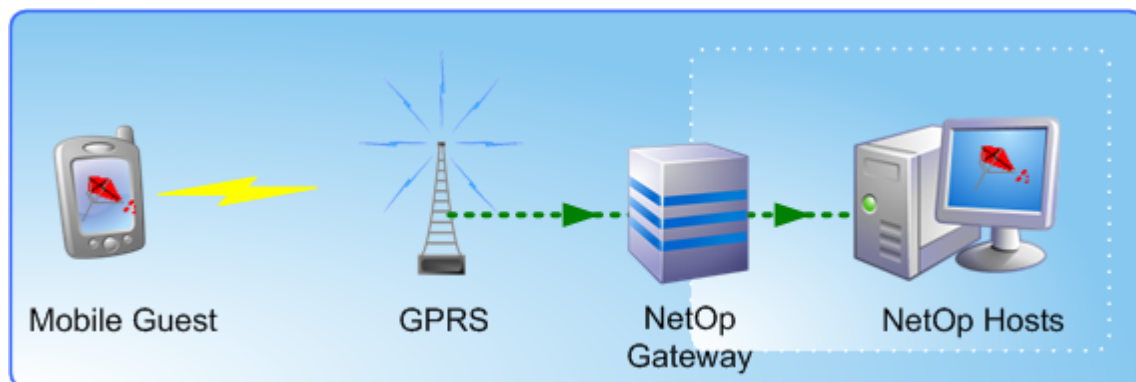


**The Mobile Guest connects via GPRS to the company. The Gateway is optional.**

To access a PC which is located on a LAN via GPRS, follow these steps:

1. On the mobile device, switch off wireless and switch on GPRS.

2. Enter the Netop Gateway address, checkmark *via Netop Gateway* and enter the Netop Host's IP address.
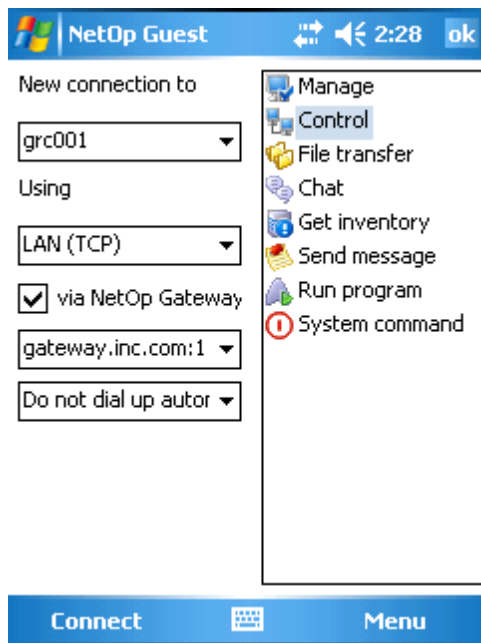
3. Select session type.

4. Tap *Connect*.

This concludes connecting via GPRS.

**Note**

For more information on Netop Gateway, please visit www.netop.com/netop-112.htm.

# 3.10 Info

The Info icon opens the list screen with information about Netop Guest ID, IP addresses and language. Clicking the Home button brings one back to the main view.

# 4 Guest Manager

After the installation of the Netop Mobile Guest Manager use this tool to configure your mobile device.
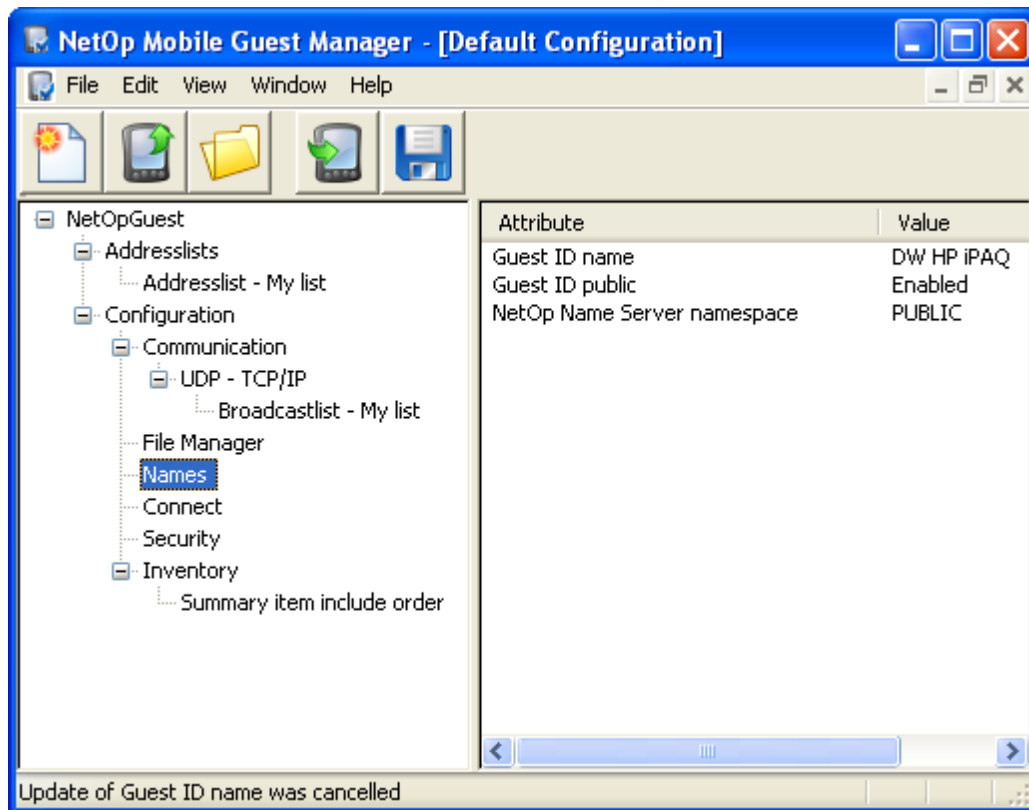


**The Netop Mobile Guest Manager.**

The following sections explain the possibilities for configuring the Mobile Host.

**See also**

## 4.1 Menu



For descriptions of the menu bar and its contents, follow these links:

## 4.1.1 Window Controls

Windows with an icon at the title bar left end share these window controls:

Click the title bar left icon, right-click anywhere in the title bar or press ALT+SPACE to display this standard window control menu:



| | |
|---|---|
| Restore | Select this command or click the matching title bar right end button to restore a maximized or minimized window to its normal size. |
| Move | Select this command to display an arrow-pointed +. Press the keyboard arrow buttons to move the window. Press ENTER to end the operation. |
| | **Note**<br>Typically, move a window by dragging its title bar. |
| Size | Select this command to display an arrow-pointed +. Press the keyboard arrow buttons to display a double arrow at a window border and move the window border to resize the window. Press ENTER to end resizing. |
| | **Note**<br>Typically, resize a window by dragging its borders or corners. |
| Minimize | Select this command or click the matching title bar right end button to minimize the window. The window can minimize into a taskbar button or a notification area button or if inside a window work panel into a minimized window typically in the lower left corner of the work panel. Click a taskbar minimized window button or double-click a notification area minimized window button to restore the window. |
| Maximize | Select this command or click the matching title bar right end button to maximize the window. |
| Close | Select this command, click the matching title bar right end button, press ALT+F4 or double-click the title bar icon to close the window without applying window selections. If the window represents a loaded program, the program will be unloaded.Enter topic text here. |
| Next | Select this command if more windows (configurations) are open to switch from one to another. |

## 4.1.2 File / Toolbar

| | |
|---|---|
| New | Ctrl+N |
| Open Mobile Device's configuartion | Ctrl+P |
| Open... | Ctrl+O |
| Save as Mobile Device's configuration | |
| Save | Ctrl+S |
| Save As... | |
| Close | |
| | |
| 1 C:\Default Configuration2.xml | |
| 2 Default Configuration1.xml | |
| 3 C:\Default Configuration | |
| 4 H:\Default Configuration | |
| | |
| Exit | |

| | | |
|---|---|---|
| New | | Select this command, click the Toolbar New Default Configuration button or press CTRL+N to open in the Configuration Panel the *Default Configuration* window or make it the active window if already open. |
| Open MD configuration | | Select this command or click the Toolbar Open from Mobile Device button to open in the Configuration Panel a Mobile Device window if a mobile device that uses a customized Netop Mobile Guest configuration is connected to the desktop computer by ActiveSync. |
| Open | | Select this command, click the Toolbar Open File button or press CTRL+O to display a Windows *Open* window that specifies Files of type: Netop Mobile Guest Configuration Files (*.xml) to open in the Configuration Panel a window named by the file selected in the *Open* window. |
| Save as MD configuration | | Select this command or click the Toolbar Save to Mobile Device button to save the Configuration Panel active window configuration as a NetopGuest.xml configuration file in the Netop Guest directory of a mobile device that is connected to the desktop computer by ActiveSync. |
| Save | | Select this command, click the Toolbar Save as File button or press CTRL+S to save the Configuration Panel active window configuration if saved in a desktop computer configuration file before, otherwise display the Windows *Save As* window that specifies Save as type: Netop Mobile Guest Configuration Files (*. xml) to save with a specified file name in a selected desktop computer directory. |
| Save As ... | | Select this command to display the Windows *Save As* window that specifies Save as type: Netop Mobile Guest Configuration Files (*. xml) to save the Configuration Panel active window configuration in a file with a specified file name in a selected desktop computer directory. |
| Close | | Select this command to close the Configuration Panel active window. If there are unsaved changes in the window, a confirmation window will be displayed. |
| (Recent | | The next section will contain the paths of recently opened |

| | |
|---|---|
| configs) | configuration files. Select one to open in the Configuration Panel a window named by the configuration file. |
| Exit | Select this command or a Window Control Close control to close the Netop Mobile Guest Manager window to unload Netop Mobile Guest Manager. If there are unsaved changes in a Configuration Panel window, a confirmation window will be displayed. |

## 4.1.3 Edit

| | |
|---|---|
| New ▸ | |
| Delete | |

Select a tree element in the Configuration Panel to show the configuration dialog.

Menu functionalities are explained with the individual parameter tree elements in the Configuration Panel section.

**Note**

Some tree element cannot be renewed or duplicated.

**See also**

Configuration Elements
Configuration Panel

## 4.1.4 View

| |
|---|
| ✔ Toolbar |
| ✔ Status Bar |
| ✔ Intro |
| Split |

| | |
|---|---|
| Toolbar | Select this command to hide/display its check mark to hide/display the Toolbar (default: check marked to display) |
| Status Bar | Select this command to hide/display its check mark to hide/display the Status Bar (default: check marked to display). |
| Intro | Select this command to hide/display its check mark to hide/display the *Netop Mobile Guest Manager Introduction* window when Netop Mobile Guest Manager is loaded (default: check marked to display). |
| Split | Select this command to display a border move mouse pointer on the Configuration Panel active window parameters pane/attributes pane border. Move the pointer and border with the keyboard left/right arrow buttons or by moving the mouse horizontally. Press ENTER or click to remove the pointer. |

**See also**

Netop Mobile Guest Manager

60

## 4.1.5 Window
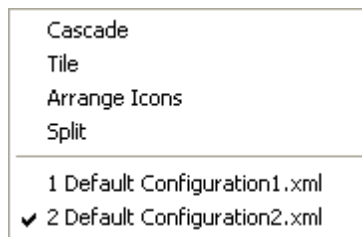


Cascade        Select this command to arrange multiple Configuration Panel windows in
               a diagonally cascading stack.

Tile           Select this command to arrange multiple Configuration Panel windows in
               equally sized tiles above each other.

Arrange Icons  Select this command to arrange Configuration Panel minimized windows
               along the lower border.

Split          Select this command to display a border move mouse pointer on the
               Configuration Panel active window parameters pane/attributes pane
               border. Move the pointer and border with the keyboard left/right arrow
               buttons or by moving the mouse horizontally. Press ENTER or click to
               remove the pointer.

The section below will display the names of Configuration Panel windows. The name of the
active window will be check marked. Select another name to make it the active window.

## 4.1.6 Help
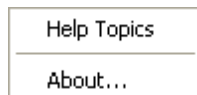


Help Topics    Open the help system.

About...       

               **State the build number if you are contacting Netop Support.**

# 4.2 Configuration Panel

The Configuration Panel consists of two panes: The Configuration Tree and the Configuration Elements.
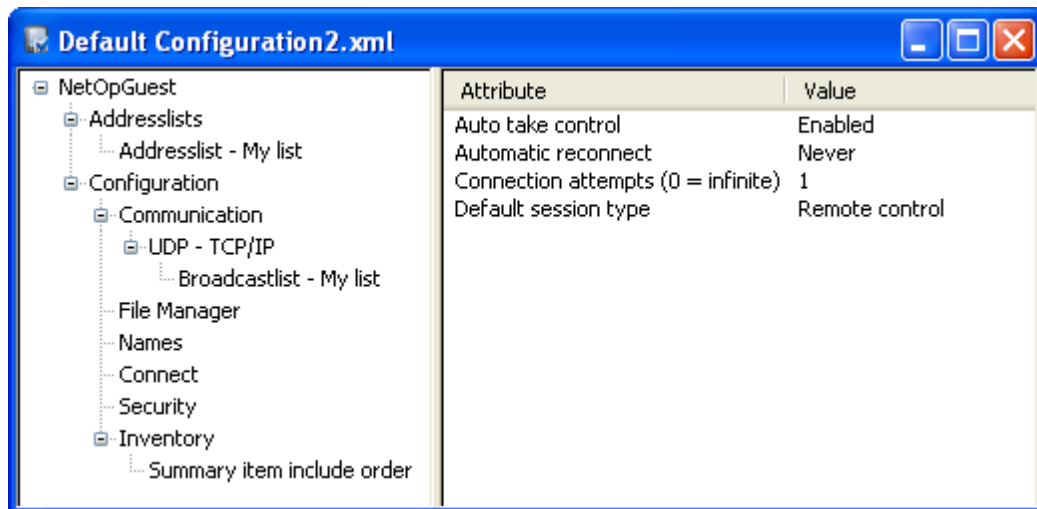


**See also**

Configuration Tree
Configuration Elements

## 4.2.1 Configuration Tree

Access all Mobile Guest configuration elements from this tree.
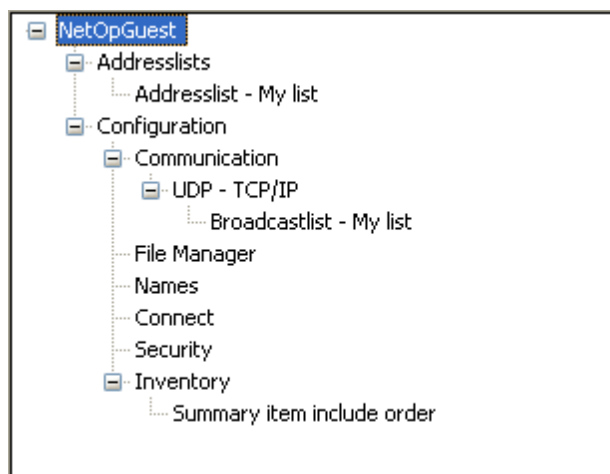


By selecting an entry on the tree an element opens in the adjacent pane.

**See also**

Configuration Elements

## 4.2.2 Configuration Elements

Use the configuration elements of the Mobile Guest to fit IT administrators' or system administrators' needs.
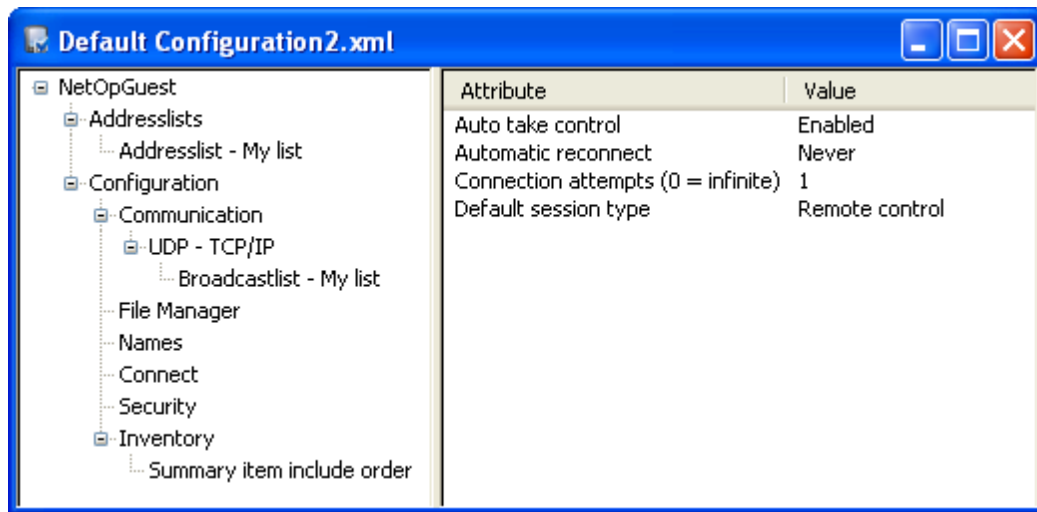


**File Manager configuration elements.**

All configuration elements have a dialog window like this:
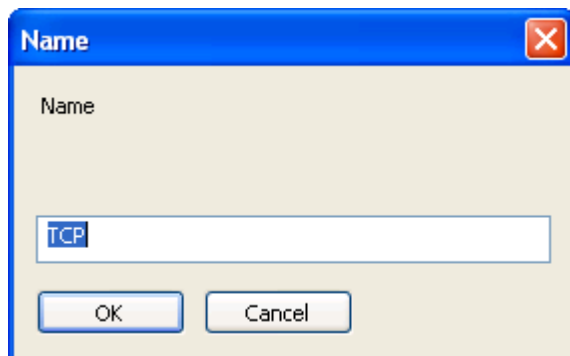


**Configuration element dialog.**

Depending on the element type, some dialogs will only accept either letters or numbers , while others have drop-down lists to choose from.

The tree has two main configuration branches:

Address lists

Configuration

### 4.2.2.1 Addresslists

Populating and organizing the Addresslist can save you valuable time and effort.
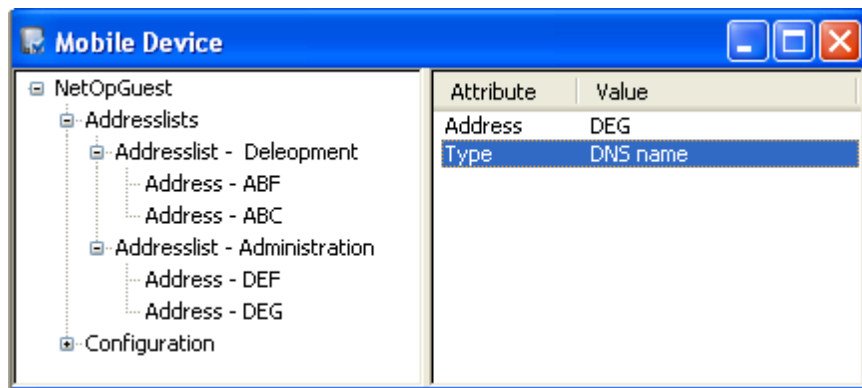


The following topics will guide you through everyday Address Book tasks:

Add and organize entries

Delete entry

---

**Note**

Addresslist only works with TCP/IP (UDP).

---

### 4.2.2.1.1 Add and organize

The address list consists of two levels, each can be made to fit your organization's structure.



---
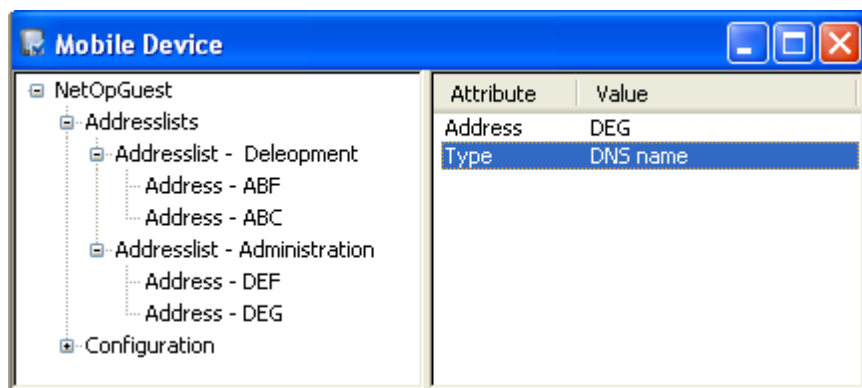
**Note**

The branch called Addresslist cannot be changed or deleted.

---

To add an address list, follow these steps:

1. Select and right-click the branch item *Addresslists*.
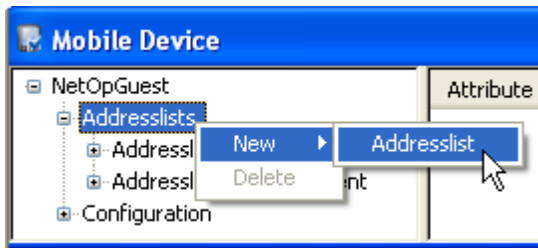
2. A dialog window opens with a randomly generated name.

3. Change the name and click *OK*

4. The new address list appears.
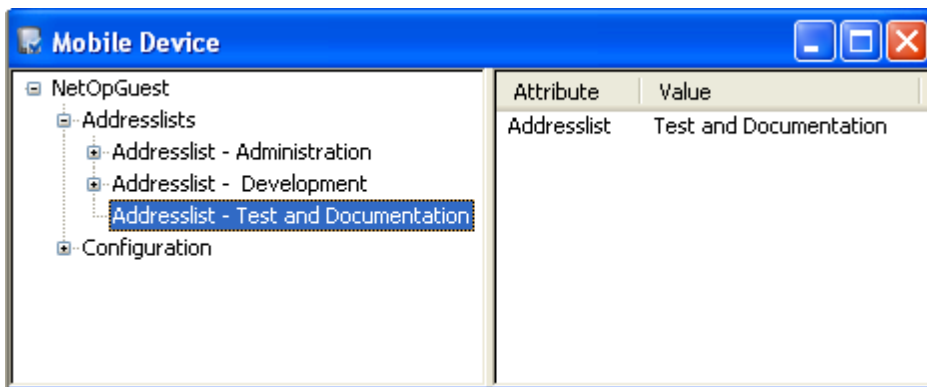


5. Having created the new department branch, add the different users.

6. Select and right-click the new *Addresslist*.

7. Select *New > Address*.

8. A dialog window opens with a randomly generated name. Enter the either an IP address, a MAC address or a DNS name.

9. Click *OK* to save.

10. The right pane contains the Attribute column which lists *Address* and *Type*.

11. Now, select the type which matches the address.

12. Double click the *Type* attributes to select.
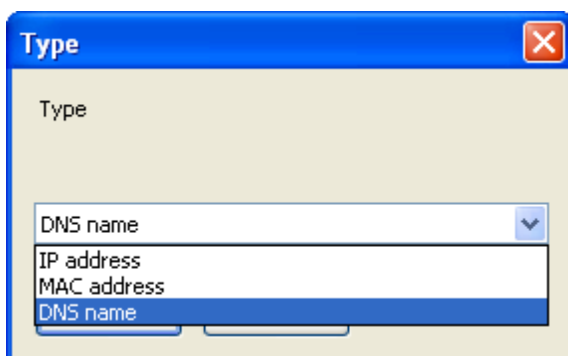


13. Click *OK* to save.

This concludes adding an address entry.

**See also**

### 4.2.2.1.2 Delete

To delete an entry in the configuration tree, follow these steps:

1. Select the entry.

2. Right-click and select Delete.
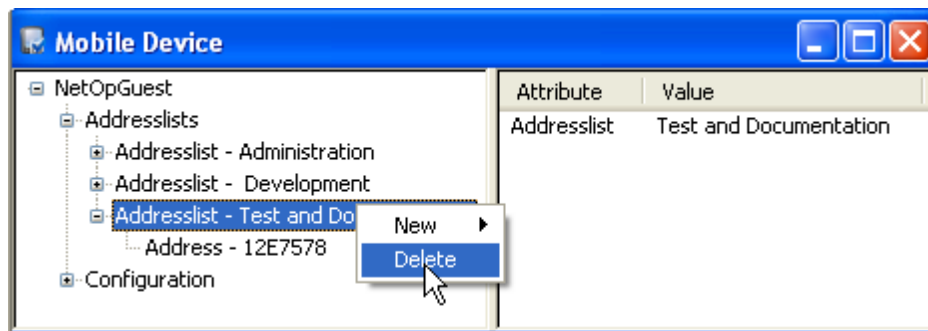


This concludes deleting an entry.

---

**Note**

The given tree elements cannot be deleted or renamed.

---

### 4.2.2.2 Configuration

UDP - TCP/IP > Broadcastlist - My list

File Manager

Names

Connect

Security

Inventory > Summary item include order

### 4.2.2.2.1 UDP – TCP/IP

| | |
|---|---|
| Enabled | Select *Enabled* (default) if you want to Mobile Guest to communicate. Otherwise, the Mobile Guest will not be able to communicate. |
| MTU | Maximum Transmission Unit refers to the size (in bytes) of the largest packet that a given layer of a communications protocol can pass onwards.  A higher MTU brings higher bandwidth efficiency. However large packets can block up a slow interface for some time, increasing the lag on other packets.

Default value is set to 2600. |
| Override port | The Override Port will let you specify a port to use instead of relying on UPnP or the game's port discovery process. This port is useful when you have multiple PCs behind the same NAT and you want to use port forwarding. |

| | |
|---|---|
| Override with port number | Netop Mobile Guest uses port 6502 (default). |
| Primary Netop Name Server | Leave in this field the default name *nns1.netop.com* of the primary public Netop Name Server on the Internet or specify the IP address or DNS name of a primary Netop Name Server on your corporate network. |
| Name | The name of this profile. |
| Receiveport | Netop Mobile Guest uses port 6502 (default). |
| | Edit the number to specify a non-default Receive port number in the range 1025-65535. |
| Secondary Netop Name Server | Leave in this field the default name *nns2.netop.dk* of the secondary public Netop Name Server on the Internet or specify the IP address or DNS name of a secondary Netop Name Server on your corporate network. |
| Sendport | Netop Mobile Guest uses port 6502 (default). |
| | Edit the number to specify a non-default Receive port number in the range 1025-65535. |
| Use Netop Name Server | Check this box to use Netop Name Server to resolve Netop names into IP addresses (default: unchecked). |
| Use TCP for session | Leave this box checked to connect by TCP/IP but if available on Guest and Host switch to TCP/IP (TCP) when connected for high speed session communication (default: checked). |
| Broadcast list | The broadcast list reflects the groups created in the Addresslist section. Select one to make it the default group. |
| | If you want to reach for computers outside the local subnet, add the addresses here. |

**See also**

Communication Protocols
Addresslist

### 4.2.2.2.2 File Manager

| | |
|---|---|
| Close dialog when finished | Default: Disabled. |
| | Check this box to close the *Transfer Status* window when a file transfer is finished. |
| Confirm - Delete non-empty folders | Default: Enabled. |
| | Leave this box checked to display this confirmation window if you are about to delete a directory that contains directories or files. |
| Confirm - Drag and drop | Default: Disabled. |
| Confirm - Overwrite and delete files | Default: Disabled. |
| Confirm - Overwrite and delete hidden | Default: Enabled. |

| | |
|---|---|
| files | Leave this box checked to display the relevant confirmation window if you are about to overwrite/delete hidden files. |
| Confirm - Overwrite and delete read-only files | Default: Enabled.<br><br>Leave this box checked to display the relevant confirmation window if you are about to overwrite/delete read-only files. |
| Confirm - Overwrite and delete system files | Default: Enabled.<br><br>Leave this box checked to display the relevant confirmation window if you are about to overwrite/delete system files. |
| Disconnect when finished | Default: Disabled. |
| Enable crash recovery | Default: Enabled. |
| Include subfolders | Default: Enabled.<br><br>Check this box to include the content of subdirectories of selected directories in the file transfer. |
| Log - Append to existing file | Default: Disabled.<br><br>Check this box to append new log entries to an existing log file (default: unchecked). If unchecked, an existing log file will be overwritten. |
| Log - Enable logging to local file | Default: Enabled. |
| Log - Filename | Default name: nfm.log.<br><br>This field will specify the log file name, that per default resides in the Mobile Device\...\Application Data\Netop Guest\FileManager\nfm. |

**Note**

There are no visible file extensions in File Explorer.

| | |
|---|---|
| Save path per Host | Default: Enabled. |
| Sync - Transfer only if file exists | Default: Enabled. |
| Sync - Transfer only one way | Default: Enabled. |
| Use delta file transfer | Default: Enabled.<br><br>Leave this box checked to compare source files with matching destination files and transfer only differences between source and destination files to save transmission bandwidth. |

### 4.2.2.2.3 Names

| | |
|---|---|
| Guest ID name | Default: Computer name.<br><br>The content of this field specifies the name by which the Guest |

will identify itself when communicating.

| | |
|---|---|
| Guest ID public | Default: Enabled. |
| | If enabled a Mobile Guest can be seen by other Hosts and Guests |
| Netop Name Server namespace | By default, this field will display PUBLIC. |

### 4.2.2.2.4 Connect

| | |
|---|---|
| Auto take control | Default: Enabled. |
| | Uncheck this box to disable acquiring Multi Guest session keyboard and mouse control by a keystroke or mouse click, see Multi Guest Session Buttons. |
| Automatic reconnect | Default: Never. |
| | The field of this drop-down box will display the selected reconnect option if a connection is lost. The drop-down box list contains these options: |
| | Never: Never reconnect. |
| | Only when connection is lost: Reconnect only if the connection was lost by an abnormal event. |
| | Host disconnect only: Reconnect only if the Host disconnected. |
| | Always: Always reconnect. |
| Connection attempts | Default: 1 |
| | Enter a number in the range 1-999 to make this number of connection attempts when you connect to a Host (0 = infinite). |
| Default session type | Default: Remote control. |
| | Remote manage |
| | File transfer |
| | Chat |
| | Select one of these session options to start the selected session when you connect to a Host. |
| | See: Startup Sessions |

### 4.2.2.2.5 Security

| | | |
|---|---|---|
| Allow encryption compatible | Netop Remote Control version 6.5- compatible encryption. | |
| | Description | Compatibility mode for communication with Netop version 6.x, 5.x and 4.x. |
| | Scope | Use for communication in environments where speed and backwards compability are important. |

|  | Encryption | Keyboard and mouse | Proprietary algorithm. |
|---|---|---|---|
|  |  | Screen and other data | None. |
|  |  | Logon and password | Proprietary algorithm. |
|  |  | Integrity check | None. |
|  |  | Key exchange | Proprietary algorithm. |
| Allow encryption data integrity | Verifies data integrity. | | |
|  | Description | Data is protected from being changed in transit. | |
|  | Scope | Use for communication in environments where encryption is prohibited except for authentication. | |
|  | Encryption | None. | |
| Integrity check | Keyboard and mouse | 256 bit SHA HMACs. | |
|  | Screen and other data | 160 bit SHA HMACs. | |
|  | Logon and password | 256 bit SHA HMACs. | |
|  | Key exchange | Combination of 1024 bits Diffie-Hellman and 256 bit SHA hashes. | |
| Allow encryption data integrity and keyboard | Encrypts and verifies keyboard, mouse, logon and password data. | | |
|  | Description | Data is protected from being changed in transit and only keystrokes, login and password details are encrypted. | |
|  | Scope | Use for communication in environments where speed is important, but you require data integrity check and keystrokes / password details must be encrypted. | |
|  | Encryption | Keyboard and mouse | 256 bit AES. |
|  |  | Screen and other data | None. |
|  |  | Logon and password | 256 bit AES. |
|  |  | Integrity control | Keyboard and mouse: 256 bit SHA HMACs. |
|  |  | Screen and | 160 bit SHA HMACs. |

| | | |
|---|---|---|
| | other data | |
| | Logon and password | 256 bit SHA HMACs. |
| | Key exchange | Combination of 1024 bits Diffie-Hellman, 256 bit AES and 256 bit SHA. |
| Allow encryption high | Encrypts and verifies integrity of all data on a high security level. | |
| | Description | All transmitted data is encrypted with 128 bit keys. Keystrokes, mouse clicks and password details are encrypted with 256 bit keys. |
| | Scope | Use for communication in environments where security is important, but speed cannot be ignored. |
| Encryption | Keyboard and mouse | 256 bit AES. |
| | Screen and other data | 128 bit AES. |
| | Logon and password | 256 bit AES. |
| | Integrity control | Keyboard and mouse: 256 bit SHA HMACs. |
| | Screen and other data | 160 bit SHA HMACs. |
| | Logon and password | 256 bit SHA HMACs. |
| | Key exchange | Combination of 1024 bits Diffie-Hellman, 256 bit AES and 256 bit SHA. |
| Allow encryption keyboard | Encrypts and verifies keyboard, mouse, logon and password data. | |
| | Description | Only keystrokes, login and password details are encrypted. |
| | Scope | Use for communication in environments where speed is important, but keystrokes and password details must be encrypted. |
| Encryption | Keyboard and mouse | 256 bit AES. |
| | Screen and other data | None. |
| | Logon and password | 256 bit AES. |
| | Integrity check | Keyboard and mouse: 256 bit SHA HMACs. |
| | Screen and | None. |

| | other data | |
|---|---|---|
| | Logon and password | 256 bit SHA HMACs. |
| | Key exchange | Combination of 1024 bits Diffie-Hellman, 256 bit AES and 256 bit SHA. |
| Allow encryption none | Does not encrypt data and verify data integrity but verifies session uniqueness. | |
| | Description | No encryption at all. |
| | Scope | Use for communication in environments where maximum transfer speed is important and security is no issue. |
| | Encryption | None. |
| | Integrity check | None. |
| | Key exchange | 160 bit SHA for session uniqueness. |
| Allow encryption very high | Encrypts and verifies integrity of all data on a very high security level. | |
| | Description | Everything is encrypted with 256 bit keys. |
| | Scope | Use for communication where security is important and speed is not a major issue. |
| Encryption | Keyboard and mouse | 256 bit AES. |
| | Screen and other data | 256 bit AES. |
| | Logon and password | 256 bit AES. |
| | Integrity control | Keyboard and mouse: 256 bit SHA HMACs. |
| | Screen and other data | 256 bit SHA HMACs |
| | Logon and password | 256 bit SHA HMACs |
| | Key exchange | Combination of 2048 bits Diffie-Hellman, 256 bit AES and 512 bit SHA. |
| Password - Disconnect remote control | Protects a Guest and a Host from being disconnected. | |
| | Description | Kiosk-mode connection is password protected. |
| | Scope | This is a part of the Kiosk-mode. |
| Password - Full screen | Protects the display from being minimized. | |

Description    Kiosk-mode full screen is password protected.

Scope          This is a part of the Kiosk-mode.

### 4.2.2.2.6 Inventory

The Guest user can configure the summary settings to give a quick overview of connected computer or device.

The default value is 0, which means that the item does not appear on the list. Entering a number results in two things: The item becomes visible on the summary list and the number determines the its position on the list, i.e. 1 will place the item at the top of the list and so forth.

---

**Note**

The items are all transferred from the connected Netop Host to the Mobile Guest to their respective sections.

---

Battery level           Default value = 8

BIOS date               Default value = 0

BIOS version            Default value = 0

Boot device             Default value = 0

Computer name           Default value = 1

Cpu count               Default value = 0

Cpu description         Default value = 0

Cpu model               Default value = 0

Cpu name                Default value = 0

Cpu speed               Default value = 0

Cpu position            Default value = 0

Gps position            Default value = 0

HAL                     Default value = 0

Harddisk available      Default value = 0

Harddisk total          Default value = 0

IE version              Default value = 0

Locale                  Default value = 0

IMEI                    Default value = 0

MAC address             Default value = 0

Memory load             Default value = 0

Memory physical         Default value = 7
available

Memory physical totalDefault value = 6

Memory virtual          Default value = 0

available

| | |
|---|---|
| Memory virtual total | Default value = 0 |
| Netop - install directory | Default value = 0 |
| Netop - installed version | Default value = 0 |
| Netop - license key | Default value = 10 |
| Organization | Default value = 0 |
| OS activation needed | Default value = 0 |
| OS build | Default value = 0 |
| OS manufacturer | Default value = 0 |
| OS name | Default value = 2 |
| OS service pack | Default value = 4 |
| OS service pack version | Default value = 0 |
| OS type | Default value = 0 |
| OS uptime | Default value = 0 |
| OS version | Default value = 3 |
| Owner | Default value = 0 |
| Owner address | Default value = 0 |
| Owner phone | Default value = 0 |
| Pagefile name | Default value = 0 |
| Pagefile space | Default value = 0 |
| Pagefile total | Default value = 0 |
| SMBIOS version | Default value = 0 |
| System directory | Default value = 0 |
| System manufacturer | Default value = 0 |
| System model | Default value = 0 |
| System type | Default value = 0 |
| Time zone | Default value = 0 |
| User name | Default value = 5 |
| WIFI signal strength | Default value = 9 |
| Windows directory | Default value = 0 |

## 4.3 Guest XML

The Mobile Guest Manager is in fact an XML tool.

When the configuration is concluded, the file is transferred to the device or saved to the user's computer.

Via an (XML) editor it is possible to change the configuration file.
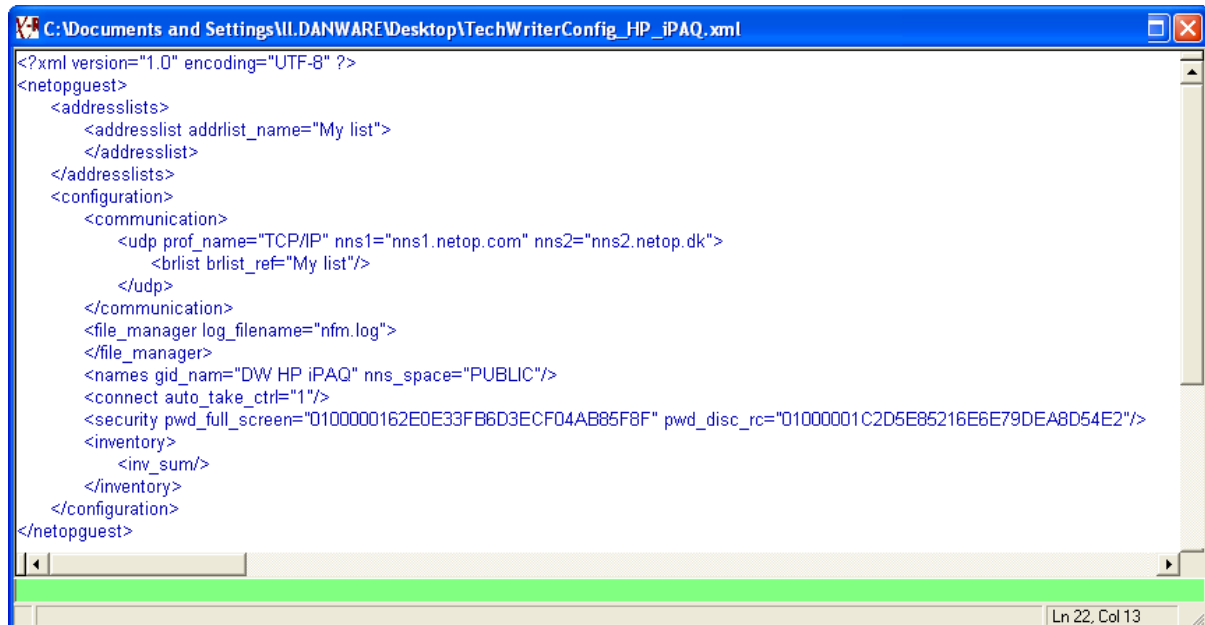


**A representation of the transferred XML file.**

The file is also stored on the device and it is possible to change the settings.

# Index

## A

## B

## C