

# NETOP HOST FOR ANDROID USER'S GUIDE



NETOP®

# RemoteControl

Secure Remote Management and Support

08 March 2017

## Contents

1	Introduction .....	2
1.1	Document Scope.....	2
1.2	Technical Specifications .....	2
2	Using the Netop Host .....	3
2.1	Netop Host Display.....	3
2.2	Netop Host Default Connectivity Configuration.....	4
2.3	Configuring the Netop Host .....	5
2.4	Requesting help from a Guest offering help services.....	5
2.5	Controlling sessions .....	6
2.5.1	Remote Control .....	6
2.5.2	File Transfer .....	6
2.5.3	Chat.....	6
3	Using the Netop Mobile Host Manager .....	7
3.1.1	Netop Mobile Host Manager Display.....	7
3.1.2	Creating Address Lists.....	9
3.1.3	Configuring Netop Host except authentication parameters .....	9
3.1.4	Configuring Netop Host authentication parameters.....	15
3.1.5	Changing the Netop Host configuration using the configuration wizard.....	15
3.1.6	Changing the Netop Host configuration using the configuration panel .....	17
4	FAQ.....	18
4.1	What actions can a Guest perform on the Netop Host? .....	18

## 1 Introduction

Netop Host enables devices running Android to be remote controlled and interacted with in other ways from a computer or device running Netop Guest.

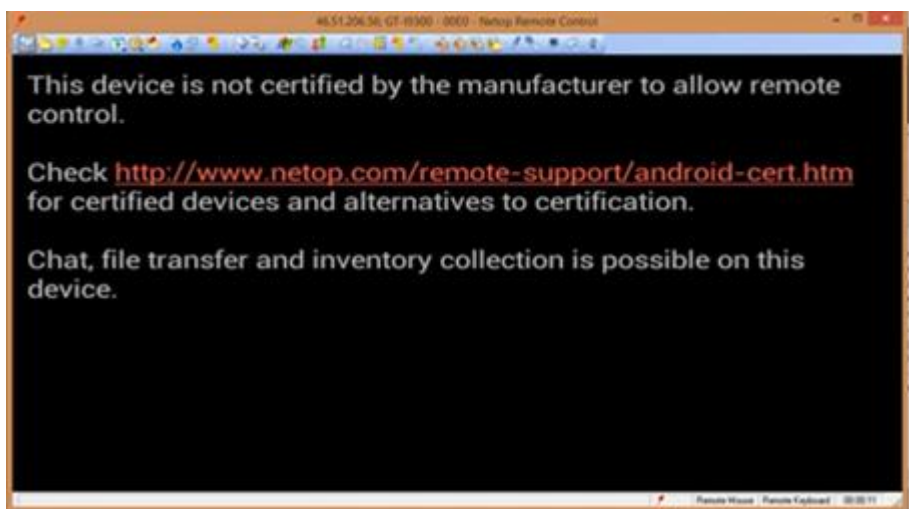
### 1.1 Document Scope

This guide provides information on how to use the Netop Host app for use on Android devices to be remote controlled and interacted with in other ways from a computer or device running Netop Guest.

### 1.2 Technical Specifications

Remote control functionality is only available on Samsung devices running Android v.4.0 or higher.

On devices coming from other manufacturers or on Samsung devices running Android 2.2 or higher, the solution does not support remote control. In case a remote control session is attempted on such a device, the following is displayed:



For information on the supported operating system and technical specification, see the [Netop Knowledgebase](#).

## 2 Using the Netop Host

A newly installed Netop Host will use the default configuration. If Netop Host Mobile Manager is available on a desktop computer, the mobile device user can change the Host configuration.

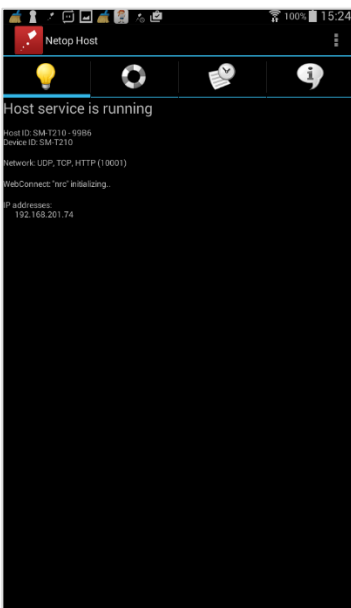
The mobile device user will have access to the options on the Netop Host display.

With regards to security, the Netop Host has two options:

- **Guest Access Security.** You can configure the Netop Host to locally authenticate connecting Netop Guests by a mobile device system password or a configured Netop password and assign a locally stored role specifying which actions will be allowed to all connecting Netop Guests. If Netop Security Management is available on the network, you can configure the Netop Host to use it to centrally authenticate and assign individual roles to connecting Netop Guests.
- **Logging.** You can configure the Netop Host to log selected Netop events locally

### 2.1 Netop Host Display

This is the mobile device Netop Host display:







If the Netop Host is loaded, this display will typically open when you start the mobile device.


In these cases, the Netop Host display will not be open:

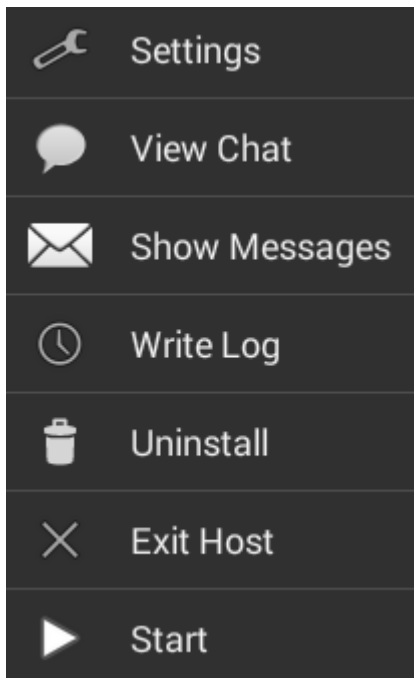
- If it has been hidden.
- If the General branch **Startup** parameter **Load at Boot** attribute has been disabled in the Netop Host Manager. To display the Netop Host in these cases, tap **Start > Netop Host** or **Start > Programs > Netop Host**.

The Host is organized into tabs, shown at the top.

	Displays Netop Host information: Host ID, device ID, the communication profile that is enabled and the Host IP.
	Allows you to request help from a Netop Guest.
	Shows the list of Netop Guest connected / disconnected events since the Netop Host was last started. To return to the Home display, tap the <b>Home</b> icon at the top of the display or the <b>Home</b> button on the menu bar.
	Displays Netop Host information: the name, IP address, regional settings language and possibly other details. To return to the Home display, tap the <b>Home</b> icon at the top of the display or the <b>Home</b> button on the menu bar.

**Note:** The displayed Netop Host name and IP address will be enabled only if the Host communication status is Running or Connected.

This is the Netop Host display menu that can be accessed by tapping  in the upper-left corner of the screen :



Displays the settings that can be configured from the Android Host's interface. More information under [Settings](#).

Displays the chat view. For details on how the chat works see [Sessions > Chat](#).

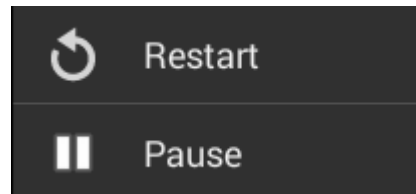
Displays the messages received from the Netop Guest who provided help.

Saves the debug logs into the `/storage/sdcard0/NetopHost` directory.

Uninstalls the Netop Host.

Closes the Netop Host app and service. To allow new connections, the open the Netop Host app and on the menu, tap Restart

Starts the Netop Host service. Starting the app, the following options will be displayed on the menu:



Stops the Netop Host. When the Netop Host is in the Started state, connection can be achieved to the device

**Note:** If a Guest is connected to the device when tapping **Pause**, the Guest will get disconnected.

## 2.2 Netop Host Default Connectivity Configuration

In the default configuration, these communication profiles will be enabled:

- **WebConnect**. A configuration based on a Netop proprietary communication device that enables Netop modules to connect easily over the Internet through a Netop connection service called WebConnect without the need to open firewalls for incoming traffic.
- **TCP/IP (TCP)**. A standard configuration of the TCP/IP communication device.
- **TCP (UDP)**. A standard configuration of the TCP/IP (TCP) communication device.

The following other communication profiles will be available but disabled:

- **HTTP**. An "HTTP encapsulated" configuration of the TCP/IP (TCP) communication device to facilitate communication through firewalls.

**Note:** You may want to modify these standard communication profiles and/or add communication profiles customized to your network environment in Netop Mobile Host Manager.

---

If the mobile device is connected to an IP network, the Netop Guest can connect to the Netop Host directly or alternatively, the end user can request help to initiate a session with the Netop Guest.

## 2.3 Configuring the Netop Host

A newly installed Netop Host will use the default configuration.

Most of the settings can be configured directly from the Netop Host. [Settings](#) and make the desired configuration changes:

For full configuration options, the Netop Mobile Host Manager is required. This needs to be installed on a desktop computer running Windows.

You can install a customized configuration by connecting the mobile device to the desktop computer. Alternatively, you can copy the host.xml file created by Netop Mobile Host Manager to the NetopHost directory of the mobile device..

For detailed information on how to configure the Netop Host using the Netop Mobile Host Manager, see [Using the Netop Mobile Host Manager](#).

---

**Note:** To apply configuration changes, you must restart the Netop Host.

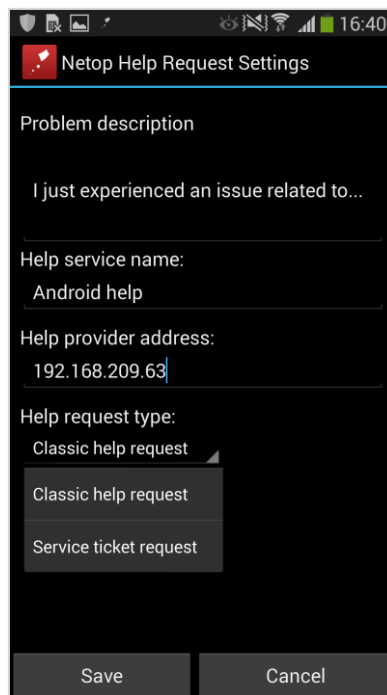
---

## 2.4 Requesting help from a Guest offering help services

If configured in a the Help request parameters in Netop Mobile Host Manager, the Netop Host user can request help from a Netop Guest that offers help services.

To request help from a Netop Guest:

1. Tap [Help Request](#). The Netop Help Request Settings displays.



2. Give a brief description of the problem you have.

3. Enter the **Help service name** and the **Help provider address** (that is, the Netop Guest IP address).
4. Select the **Help request type** from the drop-down list.
5. Tap **Save** and to initialize the help request tap on the Request Help session which is in idle mode.

## 2.5 Controlling sessions

A Netop Guest can connect to the Netop Host to run the following types of sessions:

### 2.5.1 Remote Control

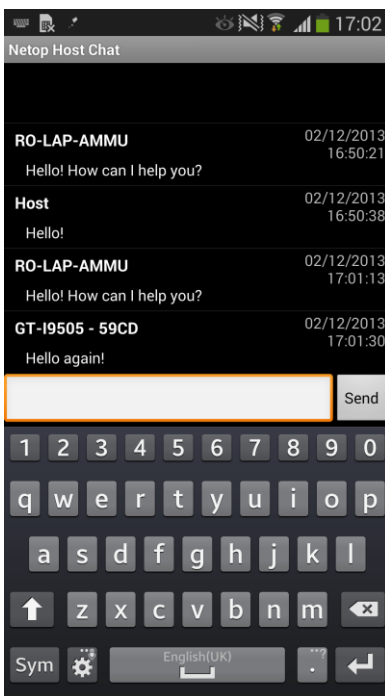
Netop Guest will display a skin, i.e. an image of the mobile device display, to typically enable the Netop Guest user to work in it with keyboard and mouse. See also the *Netop Remote Control User's Guide* for further information on skins. The Netop Host user can control a remote control session only by configuring selected actions to be denied. See [Configure security roles](#).

### 2.5.2 File Transfer

Netop Guest will display mobile device directories and files to transfer directories and files between the mobile device and the Netop Guest computer. Netop Host can control a file transfer session only by configuring selected actions to be denied. See [Configure security roles](#).

### 2.5.3 Chat

When a Netop Guest initiates a chat session with the Netop Host the Chat display will be shown:



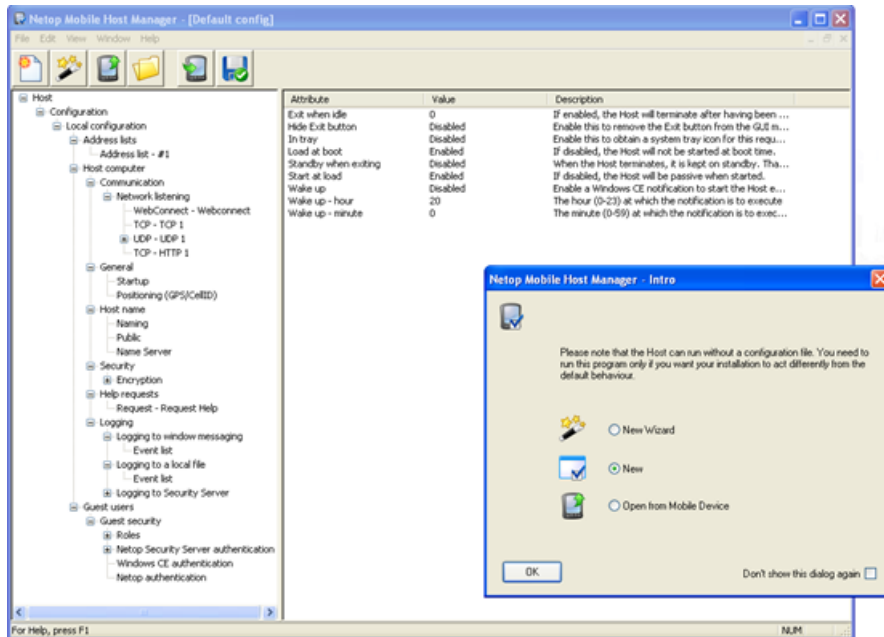
The pane below the field at the top will display the chat dialog with later contributions above earlier contributions.

To send messages, enter your chat message into the text field and tap **Send**.

The Netop Guest user can initialize a chat. Both the Netop Guest user and the Netop Host user can end the chat session.

### 3 Using the Netop Mobile Host Manager

Open the Netop Mobile Host Manager by clicking **Start > All Programs > Netop Mobile Host Manager**. The Intro window will be displayed:



If you do not want to see the Intro window again, you can hide it using the Intro option on the View menu or by selecting **Don't show this dialog again** check box at the bottom of the Intro window.

Select one of these options:

- **New Wizard:** Customize a few essential configuration parameters in the configuration wizard before displaying the configuration in the configuration panel of the Netop Mobile Host Manager window (default selection).
- **New:** Start a new default configuration in the configuration panel of the Netop Mobile Host Manager window.
- **Open from Mobile Device:** Display any customized configuration of Netop Host on a mobile device connected to the desktop computer by ActiveSync in the configuration panel of the Netop Mobile Host Manager window.

---

**Note:** For initial configuration, we recommend selecting the New Wizard option.

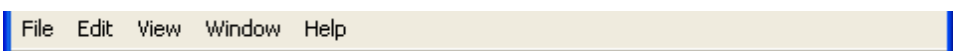
---

#### 3.1.1 Netop Mobile Host Manager Display

The Netop Mobile Host Manger display is organized in a menu bar, toolbar and a configuration panel.

##### 3.1.1.1 Menu bar

The menu bar contains menus that provide access to various commands that you can use to create and customize Host configurations.



When you open a menu and point to a command, an explanation of the command will be displayed in the status bar at the bottom of the window.









From the **File** menu you can open, save and close configurations or start the configuration wizard to be guided through modification of the default configuration. Most of the File menu commands are also available from the toolbar.

From the **Edit** menu you can create new configuration panel elements or delete them. The same commands are available from the context menus of configuration panel elements.

The commands of the rest of the menus are standard menu commands that users will be familiar with.

### 3.1.1.2 Toolbar

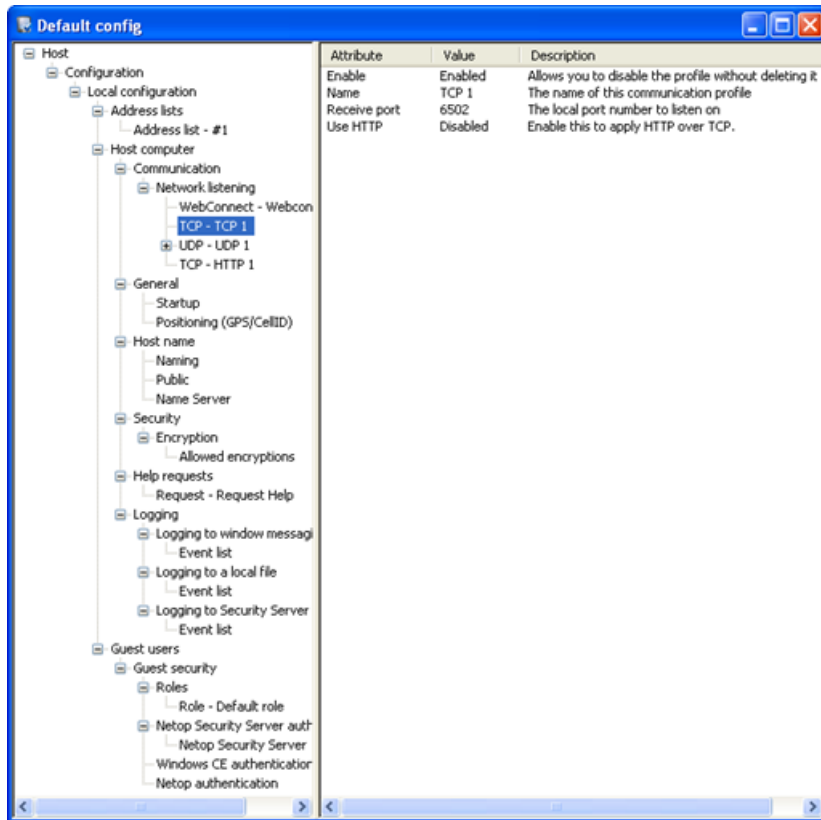
	<p><b>Create a new default configuration:</b> Click this button to open the <b>Default Configuration</b> window the configuration panel or make it the active window if already open.</p> <p>Alternatively, select the <b>New</b> command on the <b>File</b> menu or press <b>CTRL+N</b>.</p>
	<p><b>Create a new configuration using a wizard dialog:</b> Click this button to display the configuration wizard.</p> <p>Alternatively, select the <b>New Wizard</b> command on the <b>File</b> menu or press <b>CTRL+W</b>.</p>
	<p><b>Open the configuration in effect on the mobile device:</b> Click this button to open a <b>Mobile Device</b> window in the configuration panel, if a mobile device using a customized Netop Mobile Host configuration is connected to the desktop computer by ActiveSync.</p> <p>Alternatively, select the <b>Open from Mobile Device</b> command on the <b>File</b> menu.</p>
	<p><b>Open a configuration from an existing local disk file:</b> Click this button to open a customized configuration file (.xml) in the configuration panel.</p> <p>Alternatively, select the <b>Open</b> command on the <b>File</b> menu or press <b>CTRL+O</b>.</p>
	<p><b>Make the configuration effective on the mobile device:</b> Click this button to save the active configuration displayed in the configuration panel as a NetopHost.xml configuration file in the Netop Host directory of a mobile device connected to the desktop computer by ActiveSync.</p> <p>Alternatively, select the <b>Save to Mobile Device</b> command on the <b>File</b> menu.</p>
	<p><b>Save the active configuration to a file with a new name:</b> Click this button to save the active configuration in the configuration panel if the configuration has previously been saved in a desktop computer configuration file.</p> <p>Alternatively, select the <b>Save</b> command on the <b>File</b> menu or press <b>CTRL+S</b>.</p> <p>Otherwise select the <b>Save As</b> command on the <b>File</b> menu to save with a specified file name in a selected desktop computer directory.</p>

The toolbar will be displayed unless hidden from the **Toolbar** command on the **View** menu.

### 3.1.1.3 Configuration panel

The configuration panel of the Netop Mobile Host Manager window displays configurations that you have opened from the Netop Mobile Host Manager Intro window, the **File** menu, or the toolbar.

Each window specifies a Host configuration in a parameter tree structure in the left pane. Parameters are organized in branches. This image shows the configuration panel with a fully expanded parameter tree structure:



### 3.1.2 Creating Address Lists

To create address lists use the **Address lists** branch parameters and specify computer addresses.

---

**Note:** Address list parameters can specify computer addresses, while Broadcast list parameters can specify Address list parameters.

---

### 3.1.3 Configuring Netop Host except authentication parameters

The **Host computer** branch specifies Host configuration used when the Guest logs on to the Host, except authentication parameters.

This includes Communication, General, Host name, Security, Help request, and Logging attributes.

#### 3.1.3.1 Configure Communication

Netop modules and apps communicate by communication profiles.

Communication profiles are named configurations of communication devices that are Netop adaptations of generally available communication protocols or Netop proprietary communication protocols.

The following communication devices are available to the Netop Host:

#### WebConnect

WebConnect is a Netop proprietary communication device that enables networked Netop modules to connect easily over the Internet through a Netop connection service called WebConnect without the need to open firewalls for incoming traffic. All traffic will be outgoing.

#### TCP/IP (UDP)

TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of network communication protocols. TCP/IP includes among many others UDP (User Datagram Protocol) which is a widely used

networking protocol and TCP (Transmission Control Protocol) which is a widely used network point-to-point protocol.

The Netop communication device TCP/IP will connect by TCP/IP (UDP) and optionally switch to TCP/IP (TCP) when a session has been established to increase data transfer speed.

TCP/IP offers three connect options:

- IP Address
- Name response
- Name resolution

**IP address.** You can connect by IP address across segmented IP networks including the Internet. The source module send port number must match the destination module receive port number.

If you connect from outside a network protected by a network address translation (NAT) firewall or proxy server to a network computer Netop module, specify the firewall or proxy server public IP address with the port number assigned to the network computer, e.g. 192.168.1.1:1234. Ask the firewall or proxy server administrator which port number is assigned to a specific network computer.

**Name response.** Name response broadcasts a name, the first characters of a name or without a name requesting Netop modules with a corresponding enabled name to respond. These name response options are available:

- If a Guest connects or browses using the Host name qualifier H::, the Host will respond only if its Public host name attribute is **Enabled**.
- If a Guest connects or browses using the Host name qualifier U::, the Host will respond only if its Public user name attribute is **Enabled**
- If a Host sends a help request, the Guest will respond only if it offers the specified Help Service or issued the specified Service Ticket.

---

**Note:** TCP/IP broadcast will reach only computers on the local network segment and computers whose IP address or DNS name is specified in the communication profile Broadcast list.

---

## Name resolution

Name resolution resolves a specified name into its corresponding IP address to connect by it. These name resolution options are available:

Enable Use Netop Name Server(s), specify the addresses of the Primary Netop Name Server and/or Secondary Netop Name Server and specify the NNS namespace ID used by the Netop modules you want to connect to. Connect by any enabled destination module name, for a Host help request a Guest Help Service name.

If a Guest connects by a name using the Host name qualifier DNS::, a domain name server will attempt to resolve it into a corresponding IP address for the Guest to connect by it.

## Connect problems

In case of connect problems, first verify that an IP connection is available by PING.

---

**Note:** PING utilities for Windows Mobile are available for download from the Internet.

---

If an IP connection is available and connectivity problems persist, consult with your network/system administrator. As a last resort, submit a support request to [Netop Customer & Product Support](#).

## Resources

TCP/IP uses one port for sending and one port for receiving communication.

By default, Netop Mobile and Netop Remote Control use port 6502 for sending and receiving.

You can use other port numbers, but remember that the source module send port number must always match the destination module receive port number.

## MTU size

Range is 512 to 5146 Bytes. A high MTU size will increase communication speed and a low MTU (Maximum Transmission Unit) size may contribute to solving communication problems.

## Use TCP for sessions

Enable to switch to TCP/IP (TCP) communication when a session has been established for maximum data transmission speed.

## TCP/IP (TCP)

TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of network communication protocols.

TCP/IP includes among many others TCP (Transmission Control Protocol) which is a widely used network point-to-point protocol.

TCP/IP (TCP) can connect only by IP address.

If a Host sends a help request, a Guest connected to directly or on a remote Netop Gateway network can respond by its enabled Help Service names.

By default, TCP/IP (TCP) specifies the receive port number 0 to enable the computer system to allocate any available port number to return communication.

Some firewalls allow incoming communication only through a very limited selection of port numbers that typically includes port number 80 that is used for HTTP communication. Using the send port number 80 and adding a HTTP header to each data packet, such firewalls will identify the communication as HTTP traffic to allow incoming communication.

### 3.1.3.2 Configure the Netop Host protection

To specify the Netop Host protection configuration, use the **Security** branch.

Netop Host can communicate with any of the allowed encryption settings listed below. The different encryption types are listed according to their level of security. By default all is enabled.

---

**Note:** The default setting allows all connection types - even the insecure. To ensure, at least, some encryption, disable **No encryption** and **Netop 6.x/5.x Compatible**.

---

<b>Netop 6.x/5.x Compatible</b> 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 compatibility 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.
<b>No encryption</b> 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.
<b>Data integrity</b> 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
<b>Keyboard</b> Encrypts and verifies keyboard, mouse, logon and password data.		
	Description:	Only keystrokes, logon 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 other data: None Logon and password: 256 bit SHA HMACs
	Key exchange:	Combination of 1024 bits Diffie-Hellman, 256 bit AES and 256 bit SHA.
<b>Data integrity and keyboard</b> Encrypts keyboard, mouse, logon and password data and verifies data integrity.		
	Description:	Data is protected from being changed in transit and only keystrokes, logon 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 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.
<b>High</b>	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	Keyboard and mouse: 256 bit SHA HMACs
	control:	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.
<b>Very high</b>	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.

### 3.1.3.3 Configure help requests

To specify the Netop Host help request configurations, use the [Help requests](#) branch.

You can configure Request parameters to:

- Request help from a network connected mobile device by providing the following attributes:
  - Help provider
  - Port number (Send Port)
  - Request mode
  - Description (optional)
- Request help from an ActiveSync connected mobile device by providing the following attributes:
  - Help provider (always uses TCP/IP (TCP))
  - Port number (Send Port)

- Request mode Description (optional)
- ActiveSync - force (Enabled)
- Enable Netop Guests to connect to an ActiveSync connected mobile device by providing the following attributes:
  - Help provider (Netop Gateway)
  - Port number (Send Port)
  - ActiveSync - force (Enabled)
  - Silent (Enabled)
- Request help from a dial-up connected mobile device by providing the following attributes:
  - Dial-up (Enabled)
  - Dial-up mode (Change connection type)
  - Dial-up settings names Help provider
  - Port number Request name

In some cases, you may need additional configurations to:

- Connect incoming through a Netop Gateway that applies Gateway security by providing the following attributes:
  - Netop Gateway - user name
  - Netop Gateway – password
  - Netop Gateway - domain
- Enable help request by a hotkey (keystroke combination) by providing the following attributes:
  - Hotkey - Alt
  - Hotkey - Ctrl
  - Hotkey - Shift
  - Hotkey - number

---

Note: Search for virtual key codes (hexadecimal) on <http://msdn2.microsoft.com>.

---

- Limit the search for help provider Netop Guests by providing the following attributes:
  - Max help providers
  - Timeout (Seconds)
- Encapsulate a help request in HTTP to facilitate firewall passage by providing the following attributes:
  - Use HTTP (Enabled)
  - Port number (80)
- To request help when a mobile device becomes connected by ActiveSync by providing the following attributes:
  - ActiveSync - on connect (Enabled)

#### 3.1.3.4 Configure security roles

To specify the Netop Host roles configurations, use the **Roles** branch.

Netop Host local system authentication or Netop authentication cannot authenticate connecting Netop Guests individually to make use of multiple role configurations. Therefore, only one local Role parameter is available.

Security Server authentication relies on Netop Security Management to enable individual Netop Guest authentication and role assignment. See the [Netop Remote Control Administrator's Guide](#), Netop Security Management section.

### 3.1.3.5 Configure Netop authentication

The Netop authentication parameter has one attribute: **Netop password**.

If a Netop password is specified, Netop Mobile Host will request that each connecting Netop Guest specifies this password to be assigned the locally specified role.

### 3.1.3.6 Configure Netop Security Server authentication

To specify the Host Security Server authentication configuration, use the **Netop Security Server Authentication** branch.

Netop Host requests that each connecting Netop Guest identifies itself by a Netop Guest ID and a corresponding password.

Netop Host sends these credentials to the Netop Security Server group identified by the Netop Security Server group ID. A group Netop Security Server validates the credentials to return the applicable role between the Netop Guest ID and the Netop Mobile Host Netop Host ID.

Netop Host applies this role to the connecting Netop Guest. See the Netop Remote Control Administrator's Guide, Netop Security Management, or the Netop Security Manager Help system.

### 3.1.4 Configuring Netop Host authentication parameters

To specify all authentication parameters used when a Guest logs on to the Host, use the **Guest users** branch.

When you select a parameter in the left pane, a description of the parameter is displayed at the bottom of the configuration panel. You can add or delete parameters using the Edit menu or the context menu.

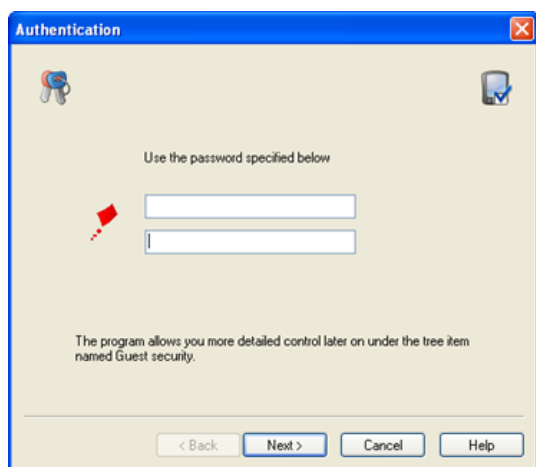
Attributes for the selected parameter are displayed in the right pane along with a description of the individual attribute. You can change attributes by double-clicking them.

### 3.1.5 Changing the Netop Host configuration using the configuration wizard

Use the configuration wizard to customize a few essential configuration parameters before displaying the configuration in the configuration panel of the Netop Mobile Host Manager window.

In the Intro window, select **New Wizard** to display the first configuration wizard page.

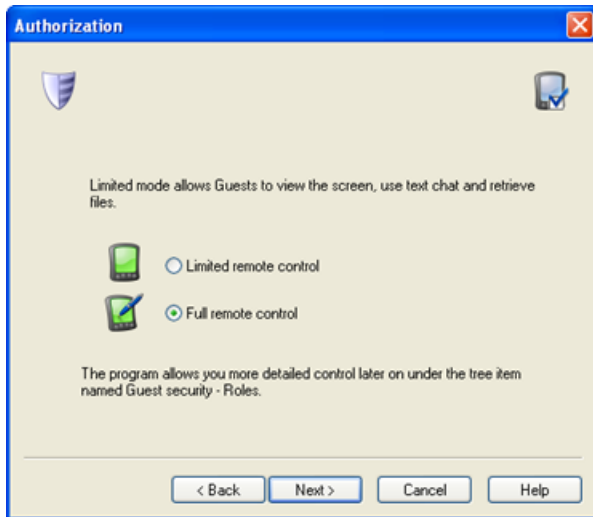
Alternatively, in the Netop Mobile Host Manager window, click **Create a new configuration** using a wizard dialog button on the toolbar, from the File menu select **New Wizard**, or press **CTRL+W**.



The Authentication page allows you to configure a Guest Access Security password. The password will be used by Guests to connect to the Netop Host. Specify the password in the upper field and re-specify it in the lower field for confirmation. Characters will display as dots or asterisks.

Click **Next**. The Authorization page will be displayed:

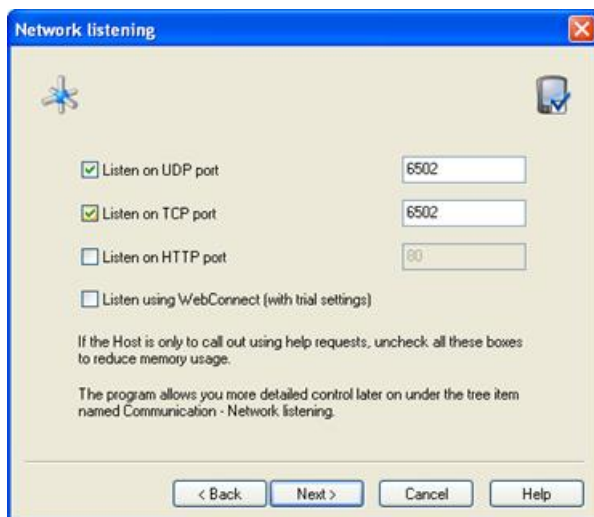




Configure the role that will initially apply to connecting Netop Guests:

- **Limited remote control:** A connecting Guest will be allowed to view the mobile device display, receive files from the mobile device and start a chat session with the mobile device user.
- **Full remote control:** A connecting Guest will be allowed all available actions.

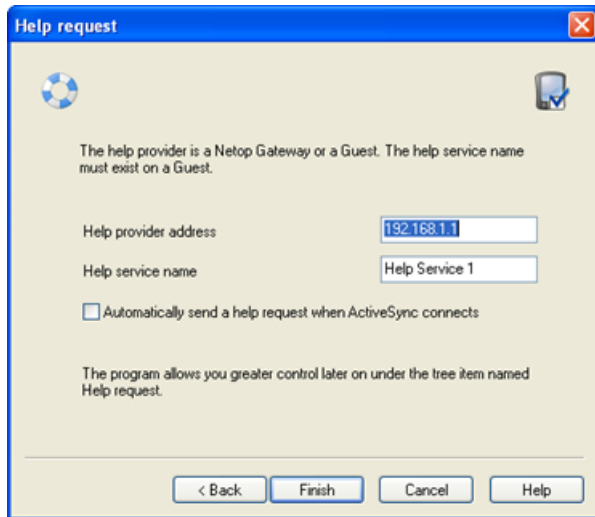
Click **Next**. The Network Listening page will be displayed:



Configure communication profiles by which to communicate with the Netop Guest:

- **Listen on UDP port:** Leave this check box selected to enable a communication profile that uses the TCP/IP communication device with the receive port number specified in the field (default: selected, 6502).
- **Listen on TCP port:** Leave this check box selected to enable a communication profile that uses the TCP/IP (TCP) communication device with the receive port number specified in the field (default: selected, 6502).
- **Listen on HTTP port:** Select this check box to enable a communication profile that uses the TCP/IP (TCP) communication device encapsulated in HTTP with the receive port number specified in the field (default: cleared, 80).
- **Listen using WebConnect (with trial settings):** Select this check box to enable a communication profile that uses the WebConnect communication device.

Click **Next**. The Help Request page will be displayed:



Configure the key attributes of the default Request Help parameter:

- **Help provider address:** Specify in this field an IP address to connect by TCP/IP (TCP) or empty the field to broadcast by TCP/IP to send help requests (default: 192.168.1.1).
- **Help service name:** Specify in this field a help service name to enable a Netop Guest that offers help by this service name to respond (default: Help Service 1).
- **Automatically send a help request when ActiveSync connects:** Select this check box to automatically send a help request on ActiveSync connect to a desktop computer (default: cleared).

To return to previous configuration wizard pages to change your settings, use the **Back** button.

To end the configuration wizard, click the **Finish** button. A NetopHost1 configuration window will be displayed according to your specifications in the configuration panel of the Netop Mobile Host Manager window.

### 3.1.6 Changing the Netop Host configuration using the configuration panel

Netop Mobile Host Manager includes a basic configuration named Default config. To view it, from the **File** menu select **New**, or on the toolbar click **Create a new default configuration**.

You cannot change the basic default configuration, but you can create and save customized configurations from it.

Saving a customized configuration will create an xml file the contents of which specify deviations from the default configuration. You can open a customized configuration xml file in the configuration panel to view and optionally modify its contents.

Click a parameter to display its attributes in the right pane as a table of attribute names, values, and attribute descriptions.

To change a configuration attribute value:

1. Double-click the attribute in the right pane to display its attribute window:

The window may contain an explanation clarifying attribute value implications. The active element of the window will depend on the attribute value type:

- Boolean (check box)
  - String (text field)
  - Numeric (number only field)
  - Enumerate (drop-down box)
2. Change the attribute value. If the specified attribute value is valid, the **OK** button will be enabled.
  3. Click **OK** to confirm the change and close the attribute window.

## 4 FAQ

### 4.1 What actions can a Guest perform on the Netop Host?

If allowed by the assigned role, a connected Netop Guest can execute the following actions:

- **Run Program:** Run an exe program installed on the mobile device.
- **Send Message:** Compose a message and send it to Netop Host to display a message window on top of the Netop Host display. Tap OK to close the message window.
- **Get Inventory:** Get mobile device hardware and software information.
- **Netop Script:** Run a Netop Script with the Netop Host . A Netop Script will execute a specified File Transfer, Run Program, Send Message, Get Inventory and other actions.

---

**Note:** Run Program, Send Message and Get Inventory are in fact based on Netop Script. See the Netop Script section of the Netop Remote Control User's Guide or the corresponding Netop Guest Help system section.

---